NetScaler® Console-Dienst

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Übersicht 65
So funktioniert NetScaler Console 66
Funktionen und Lösungen 67
Versionshinweise 72
Was ist neu 72
September 27, 2026 72
Verwaltung und Überwachung 72
September 15, 2026 76
Behobene Probleme 76
September 01, 2026 77
Neuigkeiten 77
Behobene Probleme 79
August 19, 2026 80
Verwaltung und Überwachung 80
August 04, 2026 81
Neuerungen 81
Behobene Probleme 81
July 14, 2026 82
Neuerungen 82
Behobene Probleme 83
June 30, 2026 84
Verwaltung und Überwachung 84
June 17, 2026 87
Behobene Probleme 87
June 03, 2026 88
Behobene Probleme 88

© 1997–2026 Citrix Systems, Inc. All rights reserved.

May 19, 2026 89
Verwaltung und Überwachung 89
Behobene Probleme 93
March 31, 2026 94
Verwaltung und Überwachung 94
Behobene Probleme 96
March 23, 2026 97
Verwaltung und Überwachung 97
March 09, 2026 98
Was ist neu 98
Behobene Probleme 99
February 20, 2026 100
Was ist neu 100
Behobene Probleme 100
February 04, 2026 101
Sonstiges 103
Behobene Probleme 103
November 11, 2025 105
Verwaltung und Überwachung 105
November 06, 2025 105
Behobene Probleme 105
October 15, 2025 106
Verwaltung und Überwachung 106
Behobene Probleme 107
September 17, 2025 107
Infrastruktur 107
Behobene Probleme 108
September 08, 2025 109

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lizenzierung 109
September 03, 2025 110
Behobene Probleme 110
August 26, 2025 111
Verwaltung und Überwachung 111
August 20, 2025 112
Infrastruktur 112
Behobene Probleme 113
July 17, 2025 114
Infrastruktur 114
Behobene Probleme 114
July 02, 2025 114
Telemetrie 114
Sicherheit 115
Behobene Probleme 116
June 25, 2025 116
Verwaltung und Überwachung 116
June 17, 2025 117
Verwaltung und Überwachung 117
June 03, 2025 118
Behobene Probleme 118
May 26, 2025 118
Analysen 118
Behobene Probleme 120
May 06, 2025 120
Behobene Probleme 120
April 15, 2025 120
Zero-Touch-Zertifikatbereitstellung 120

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Veralten der automatischen Skalierung von NetScaler-Instanzen in öffentlichen Clouds 121
Verbesserungen bei Konfigurationsaufträgen 121
Verbesserungen bei Upgrade-Aufträgen 121
Behobene Probleme 121
February 19, 2025 122
StyleBooks 122
Behobene Probleme 122
Analysen 123
February 06, 2025 123
Analysen 123
Infrastruktur 123
Behobene Probleme 123
January 15, 2025 124
Telemetrie 124
Analysen 124
Infrastruktur 125
StyleBooks 125
Behobene Probleme 126
December 03, 2024 127
Freigabe von Konfigurationsentitäten zwischen migrierten Konfigurationen 127
Analysen von richtlinienbasierter zu profilbasierter Konfiguration migrieren 127
Behobene Probleme 127
November 20, 2024 128
Verbesserte Benutzererfahrung in der NetScaler Console GUI 128
Option zum Löschen von SSL-Zertifikaten aus NetScaler 129
Behobene Probleme 129
November 12, 2024 130
Verwaltung und Überwachung 130

© 1997–2026 Citrix Systems, Inc. All rights reserved.

October 15, 2024 131
Telemetrie 131
Analysen 131
Behobene Probleme 132
Infrastruktur 132
October 03, 2024 132
Lizenzierung 132
StyleBooks 133
Hinweise 133
Behobene Probleme 133
September 19, 2024 134
Infrastruktur 134
Behobene Probleme 134
September 03, 2024 135
Beobachtbarkeit 135
Behobene Probleme 135
August 27, 2024 136
Analysen 136
Anwendungen 136
StyleBooks 136
Behobene Probleme 137
July 25, 2024 137
Behobene Probleme 137
July 15, 2024 138
Infrastruktur 138
Lizenzierung 138
Behobene Probleme 139
July 09, 2024 140

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unterstützung für die Identifizierung und Behebung von CVE-2024-5491 und CVE-2024-5492 140
June 18, 2024 141
Telemetrie 141
June 11, 2024 141
Analysen 141
Infrastruktur 142
Behobene Probleme 143
June 5, 2024 143
Analysen 143
Plattform 144
StyleBooks 144
Behobene Probleme 145
Analysen 145
Infrastruktur 145
StyleBooks 145
May 22, 2024 146
Analysen 146
Lizenzierung 146
StyleBooks 147
Behobene Probleme 147
April 23, 2024 148
Analysen 148
Infrastruktur 148
Behobene Probleme 148
Infrastruktur 148
Lizenzierung 148
Sicherheit 149

© 1997–2026 Citrix Systems, Inc. All rights reserved.

April 10, 2024 149
Analysen 149
Infrastruktur 149
Behobene Probleme 150
Infrastruktur 150
Lizenzierung 150
Sicherheit 150
March 26, 2024 150
Behobene Probleme 150
March 12, 2024 151
Lizenzierung 151
Behobene Probleme 151
February 28, 2024 152
Infrastruktur 152
Analysen 153
StyleBooks 154
Behobene Probleme 154
February 06, 2024 155
Analysen 155
Infrastruktur 155
Behobene Probleme 156
January 24, 2024 157
Analysen 157
Infrastruktur 157
Behobene Probleme 157
January 16, 2024 157
Unterstützung für die Identifizierung und Behebung von CVE-2023-6548 und CVE-2023-6549 157

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- January 09, 2024 158
  - Analysen 158
  - Infrastruktur 159
  - Behobene Probleme 160
  - Lizenzierung 160
- Bekannte Probleme 160
  - Lizenzierung 161
  - Verwaltung und Überwachung 161
  - Infrastruktur 161

Datenkonformität 163

- PCI DSS-Konformität 163
  - NetScaler® Application Delivery Management service PCI DSS-Konformität 163

NetScaler® Telemetrieprogramm 164

- Voraussetzungen 164

Datengovernance 167

- NetScaler®-Telemetrieprogramm 167
- Wie erfassen, speichern und übertragen wir Daten? 167
- Datenkategorien 168
  - Kundeninhalte 168
  - Protokolle 168
  - Detaillierte Kundeninhalte und Protokolle 169
- Sicherheit 171
- Datenaufbewahrungsrichtlinie für den NetScaler Console-Dienst 172
- Drittanbieterdienste 172
  - Referenzen 173

BEDINGUNGEN FÜR DIE NUTZUNG VON IoC-INFORMATIONEN 174

Erste Schritte 175

- Schritt 1: Registrieren Sie sich für Citrix Cloud™ 175

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schritt 2: NetScaler Console mit einem Express-Konto verwalten 175
Schritt 3: Wählen Sie einen NetScaler-Bereitstellungstyp aus 176
Agenten auf einem Hypervisor installieren 177
Externen VM-Agenten in der Public Cloud installieren 178
Agent als Microservice installieren 179
Integrierten Agenten verwenden 179
Instanzen hinzufügen 180
NetScaler-Instanzen über das NetScaler Console GUI-Dashboard integrieren 180
Agent-Aktionen 181
Agent-Diagnose anzeigen und Warnungen zur Endpunktüberprüfung erhalten 181
E-Mail-Benachrichtigung 182
Integrierter Agent zur Verwaltung von Instanzen konfigurieren 182
Voraussetzungen 183
Den integrierten Agenten konfigurieren 184
Lizenzserver über den integrierten NetScaler®-Agenten konfigurieren 187
Fehlerbehebung 188
Installieren Sie einen NetScaler Agent lokal 188
Installation eines NetScaler-Agent in der Microsoft Azure Cloud 190
Voraussetzungen 191
Installieren Sie einen NetScaler Agent auf Amazon Web Services (AWS) 195
Voraussetzungen 195
Starten von einer Website 197
Mit EC2 starten 198
NetScaler-Agent auf GCP installieren 209
Voraussetzungen 209
NetScaler-Agent auf GCP installieren 209
NetScaler Agent in Kubernetes-Cluster mit YAML installieren 210
NetScaler Agent Operator mithilfe der OpenShift-Konsole installieren 211

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Voraussetzungen 211
Agent-Operator installieren 213
Agent-Instanz löschen 214
Agent-Operator deinstallieren 214
Container-basierten Agenten mithilfe eines Helm-Charts installieren 214
So erhalten Sie Hilfe und Support 215
Ein Citrix Cloud-Konto erstellen 215
Bei Ihrem Konto anmelden 215
Kennwort ändern 216
Citrix Cloud Support-Foren 216
Support-Artikel und Dokumentation 217
Citrix Cloud Resource Center 217
Citrix Tech Zone 217
Technischer Support 218
Service Health Dashboard 218
Abonnements für den Dienstzustand 219
Erweiterte grafische Benutzeroberfläche 220
Menü bei Mauszeigerbewegung anzeigen 220
Optimierte Menühierarchie 220
Aktualisierte Untermenübezeichnungen 221
Infrastruktur > Konfiguration 221
NetScaler-Lizenzierung > Pool-Lizenzierung 221
Gateway > HDX Insight 223
Einstellungen 223
Einklappbares Menü 223
Erweitertes Menü 223
Eingeklapptes Menü 223
Seitenleisten-Umschalter 224

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Seitenleiste anzeigen 224

Seitenleiste ausblenden 224

Als Startbildschirm festlegen 224

Favoriten anheften 224

Unkomplizierte Integration von NetScaler-Instanzen mithilfe von Console Advisory Connect 225

Übersicht: Komponenten des NetScaler Console Onboarding-Workflows 225

Ein kurzer Überblick über das Onboarding 227

NetScaler-Instanzen mithilfe von Console Advisory Connect einbinden 228

Schritt 1: Erste Schritte 229

Schritt 2: Einblicke in Ihre NetScaler- und Gateway-Instanzen 230

Schritt 3: NetScaler- und Gateway-Instanzen zum Onboarding auswählen 233

Schritt 4: NetScaler-Instanzen in NetScaler Console integrieren 233

NetScaler-Instanzen mit einem integrierten Agenten integrieren 233

NetScaler-Instanzen mit einem externen Agenten integrieren 235

Agenten in einer öffentlichen Cloud installieren 237

Onboarding-Bereitschaft von NetScaler-Instanzen testen 237

E-Mail-Einstellungen 238

E-Mail-Einstellungen konfigurieren 238

E-Mails für alle Administratoren aktivieren 239

E-Mails für bestimmte Administratoren in der Organisation aktivieren/deaktivieren 240

E-Mails für alle Administratoren deaktivieren 241

Beheben Sie Probleme mit dem Diagnosetool oder der NetScaler Console GUI 241

Diagnosetool manuell verwenden 242

Überprüfen Sie die Bereitschaft der NetScaler-Instanz für das Onboarding mit dem Diagnosetool 243

NetScaler-Diagnoseinformationen in der NetScaler Console GUI anzeigen 243

Fehlerbehebung 244

Ungültiger Benutzername oder ungültiges Kennwort 244

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DNS-Konfigurationsfehler 244
Keine Internetverbindung 245
Keine Verbindung zum NetScaler Console-Endpunkt 245
Timeout des integrierten Agent-Testlaufs 245
Roter Umriss im Dropdown-Menü des Geräteprofils 246
Umstellung von einem integrierten Agenten auf einen externen Agenten 246
Bevor Sie beginnen 246
Umstellung von einem integrierten Agenten auf einen externen Agenten 246
SAML als Identitätsanbieter mit NetScaler Console verbinden 248
Voraussetzungen 248
Cloud Connectors 248
Active Directory 249
SAML-SSO-Konfiguration 250
Systemanforderungen 255
Unterstützte Browser 255
Anforderungen an die Agent-Installation 255
Lightweight Agent für gepoolte oder flexible Lizenzierung 257
Unterstützte Ports 258
Ports für den NetScaler-Agenten 258
Ports für NetScaler-Instanzen 260
Ports für den integrierten NetScaler-Agenten 261
Anforderungen für die NetScaler Console Analytics-Lösung 262
Erforderliche Mindestversionen von Citrix Virtual Apps and Desktops 262
Unterstützte Thin Clients für HDX™ Insight 263
NetScaler-Instanzlizenz für HDX Insight erforderlich 263
Unterstützte Betriebssysteme und Citrix Workspace-Versionen 264
Lizenzen 265
NetScaler-Lizenzierung für NetScaler Console-Funktionen erforderlich 265

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ablaufprüfungen für Abonnements virtueller Server anzeigen 267
Den Typ der auf den virtuellen Servern aktivierten Analysen anzeigen 268
Upgrade-Empfehlung 269
Upgrade-Empfehlung anzeigen 270
Bevorzugte Builds festlegen 270
NetScaler-Instanzen aktualisieren 270
Sicherheitsberatung 273
Landingpage für Sicherheitsberatung 273
Empfehlungen für sichere Konfigurationen 275
CVE-Erkennung 275
Überwachung der Dateintegrität 275
Jetzt scannen 275
Scan-Verlauf 276
Betroffene NetScaler 276
Einstellungen 276
Empfehlungen für eine sichere Konfiguration 277
Priorisierung nach Schweregrad 278
Vorteile einer detaillierten Ansicht auf Instanzebene 278
Konfigurationsempfehlungen beheben 279
CVE-Erkennung 282
Instanzansicht 283
CVE-Ansicht 285
CVE-Repository 286
Wichtige Hinweise 286
Dateiintegritätsüberwachung 288
Von der Konsole erkannt 289
Wichtige Hinweise 290
Vom Gerät gemeldet 290

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Erkennung von Kompromittierungsindikatoren in NetScaler Console 291
Voraussetzungen 291
Vorteile 291
Schwachstellen beheben 293
Schwachstellen für CVE-2026-88771 identifizieren und beheben 294
CVE-2026-88771 beheben 294
Schwachstellen für CVE-2026-88772 identifizieren und beheben 295
CVE-2026-88772 beheben 295
Schwachstellen für CVE-2026-88773 identifizieren und beheben 295
CVE-2026-88773 beheben 296
Schwachstellen für CVE-2026-88774 identifizieren und beheben 296
CVE-2026-88774 beheben 297
Schwachstellen für CVE-2026-88775 identifizieren und beheben 297
CVE-2026-88775 beheben 298
Schwachstellen für CVE-2026-88776 identifizieren und beheben 298
CVE-2026-88776 beheben 298
Schwachstellen für CVE-2026-88777 identifizieren und beheben 299
CVE-2026-88777 beheben 299
Schwachstellen für CVE-2026-88778 beheben 300
CVE-2026-88778 beheben 300
Schritt 1: Aktualisieren der anfälligen NetScaler-Instanzen 300
Schritt 2: Konfigurationsbefehle anwenden 301
Schritt 2: Instanz auswählen 301
Schwachstellen für CVE-2026-19490 identifizieren und beheben 302
CVE-2026-19490 beheben 302
Schwachstellen für CVE-2026-19489 identifizieren und beheben 303
CVE-2026-19489 beheben 303
Schwachstellen für CVE-2026-13474 identifizieren und beheben 304

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CVE-2026-13474 beheben 304
Schritt 1: Betroffene NetScaler-Instanzen aktualisieren 305
Schritt 2: Konfigurationsbefehle anwenden 305
Schwachstellen für CVE-2026-10817 identifizieren und beheben 306
CVE-2026-10817 beheben 307
Schwachstellen für CVE-2026-10816 identifizieren und beheben 307
CVE-2026-10816 beheben 308
Schwachstellen für CVE-2026-8655 identifizieren und beheben 308
CVE-2026-8655 beheben 308
Schwachstellen für CVE-2026-8452 identifizieren und beheben 309
CVE-2026-8452 beheben 309
Schwachstellen für CVE-2026-8451 identifizieren und beheben 310
CVE-2026-8451 beheben 310
Schwachstellen für CVE-2026-4368 identifizieren und beheben 311
CVE-2026-4368 beheben 311
Schwachstellen für CVE-2026-3055 identifizieren und beheben 312
CVE-2026-3055 beheben 312
Schwachstellen für CVE-2025-12101 identifizieren und beheben 313
CVE-2025-12101 beheben 313
Schwachstellen für CVE-2025-8424 identifizieren und beheben 314
CVE-2025-8424 beheben 314
Schwachstellen für CVE-2025-7776 identifizieren und beheben 315
CVE-2025-7776 beheben 315
Schwachstellen für CVE-2025-7775 identifizieren und beheben 316
CVE-2025-7775 beheben 316
Schwachstellen für CVE-2025-6543 identifizieren und beheben 317
CVE-2025-6543 beheben 317
Schwachstellen für CVE-2025-5349 identifizieren und beheben 318

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CVE-2025-5349 beheben 319
Schwachstellen für CVE-2025-5777 beheben 320
CVE-2025-5777 beheben 320
Schritt 1: Aktualisieren Sie die anfälligen NetScaler-Instanzen 321
Schritt 2: Konfigurationsbefehle anwenden 321
Schritt 2: Instanz auswählen 322
Schwachstellen für CVE-2024-8535 beheben 323
CVE-2024-8535 beheben 323
Schritt 1: Die anfälligen NetScaler-Instanzen aktualisieren 324
Schritt 2: Konfigurationsbefehle anwenden 324
Schritt 2: Instanz auswählen 325
Schwachstellen für CVE-2020-8300 beheben 326
CVE-2020-8300 beheben 327
Schritt 1: Anfällige NetScaler-Instanzen aktualisieren 327
Schritt 2: Konfigurationsbefehle anwenden 327
Schritt 2: Instanz auswählen 330
Hinweise zum NetScaler Console Express-Konto 331
Szenario 332
Schwachstellen für CVE-2021-22927 und CVE-2021-22920 beheben 334
CVE-2021-22927 und CVE-2021-22920 beheben 334
Schritt 1: Aktualisieren Sie die anfälligen NetScaler-Instanzen 335
Schritt 2: Konfigurationsbefehle anwenden 335
Schritt 2: Instanz auswählen 338
Szenario 339
Schwachstellen für CVE-2021-22956 identifizieren und beheben 340
Von CVE-2021-22956 betroffene Instanzen identifizieren 341
CVE-2021-22956 beheben 341
Schritt 1: Aktualisieren der anfälligen NetScaler-Instanzen 342

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schritt 2: Konfigurationsbefehle anwenden 342
Schritt 2: Instanz auswählen 343
Schwachstellen für CVE-2022-27509 identifizieren und beheben 345
Von CVE-2022-27509 betroffene Instanzen identifizieren 345
CVE-2022-27509 beheben 346
Nicht unterstützte CVEs im Sicherheits-Advisory 346
Einrichtung 348
Hinzufügen mehrerer Agents 349
Agenten für die Bereitstellung an mehreren Standorten konfigurieren 350
Architektur 350
Agenten-Failover 351
Agent-Upgrade-Einstellungen konfigurieren 352
Agent manuell aktualisieren 353
Dual-NIC-Unterstützung auf NetScaler Console 354
Instanzen hinzufügen 356
So erstellen Sie ein NetScaler®-Profil 357
So fügen Sie eine NetScaler-Instanz zu NetScaler Console hinzu 359
So fügen Sie eine NetScaler CPX-Instanz in NetScaler Console hinzu 360
So fügen Sie eine eigenständige NetScaler BLX-Instanz in NetScaler Console hinzu 361
So fügen Sie hochverfügbare NetScaler BLX-Instanzen in NetScaler Console hinzu 362
So greifen Sie über die NetScaler Console auf eine Instanz-GUI zu 363
Instanzwarnungen beheben 363
Konfigurieren von Syslog auf Instanzen 364
Logstream-Übersicht 366
Logstream als Transportmodus aktivieren 367
So weisen Sie delegierten Administratorbenutzern weitere Berechtigungen zu 368
Zuweisen von Super-Admin-Berechtigungen zu einem delegierten Administrator 369
Zuweisen einer benutzerdefinierten Rolle zu einem delegierten Administrator 369

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Integration mit der ServiceNow-Instanz 370
ServiceNow-Vorfälle für alle NetScaler-Ereignisse generieren 371
ServiceNow-Vorfälle für SSL-Zertifikate generieren, die bald ablaufen 372
ServiceNow-Vorfälle für den Ablauf der NetScaler Console-Lizenz generieren 372
NetScaler Console-Ereignisrichtlinien anpassen 372
Umsetzbare Aufgaben und Empfehlungen 373
Aufgaben 374
Empfehlungen 378
Wie verwende ich den „Guide me“-Workflow und schließe die Empfehlung ab? 381
Benachrichtigungen konfigurieren 381
Häufig gestellte Fragen 381
Ein einheitliches Dashboard zur Anzeige wichtiger Instanz-Metrikdetails 383
Anwendungen 383
NetScaler-Infrastruktur 384
Anwendungssicherheit 384
Gateway 385
API-Analysen 385
Dashboard anpassen 385
Agentendetails anzeigen 386
Filter erstellen und anwenden 386
Filter bearbeiten 387
Benutzerdefinierte Dashboards erstellen, um wichtige Metrikdetails der Instanz anzuzeigen 388
Weitere Optionen im Dashboard 389
Dashboard für andere Benutzer freigeben 390
API-Sicherheit 391
Vorteile der API-Sicherheit 391
Berechtigungen für die API-Sicherheitskonfiguration und -verwaltung erteilen 392
API-Definition erstellen oder hochladen 393

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OAS-Spezifikation hochladen 393
API-Definition erstellen 394
API-Definitionen anzeigen 394
Eine API-Instanz bereitstellen 395
Einen API-Proxy hinzufügen 395
Bereitstellen einer API-Instanz mithilfe des API-Proxys 396
API-Analysen aktivieren 398
Richtlinien zu einer API-Bereitstellung hinzufügen 398
Richtlinientypen 400
Authentifizierung und Autorisierung 400
Ratenbegrenzung 402
WAF 403
Bot 403
Header-Umschreibung 404
URI-Pfad-Umschreibung 404
Verweigern 405
API-Analysen anzeigen 405
API-Endpunktverteilung 406
API-Instanzen 406
API-Endpunkte 406
Authentifizierungsfehler 407
Verschiedene API-Einblicke anzeigen 407
Top-API-Endpunkte in einer Instanz anzeigen 408
Meistgenutzte APIs anzeigen 408
Geostandort eines Endpunkts anzeigen 408
HTTPS-Antwortstatus anzeigen 408
Trend der API-Anfragen anzeigen 409
Bandbreitennutzung eines Endpunkts anzeigen 409

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL-Fehler und -Nutzung anzeigen 409
API-Endpunkte ermitteln 410
API-Endpunkte anzeigen 410
API-Definitionen aus erkannten API-Endpunkten erstellen 411
Vorhandene API-Definition mit erkannten API-Endpunkten aktualisieren 412
Bereitstellung einer API-Instanz aufheben 413
Bereitstellung einer API-Richtlinie aufheben 413
Bereitstellung einer API aufheben 413
Bereitstellung eines API-Proxys aufheben 414
APIs zur Verwaltung der API-Sicherheit verwenden 414
API-Beispiele für Richtlinientypen 416
Ratenbegrenzung 417
OAuth 418
Basisauthentifizierung 419
Keine Authentifizierung 420
Bot 421
WAF 422
Header-Umschreibung 423
URI-Pfad-Umschreibung 424
Autorisierung 426
Verweigern 427
WAF- und BOT-Profile mit StyleBooks erstellen 428
Ein WAF-Profil mit StyleBooks erstellen 429
BOT-Profil mit dem StyleBook erstellen 429
Anwendungen 431
Voraussetzungen 431
Anwendungsübersicht 431
Diskrete Anwendungen 432

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benutzerdefinierte Anwendungen 432
Hinweise 432
Microservices-Anwendungen 432
Anwendungsverwaltung und Anwendungs-Dashboard 432
Anwendungen verwalten 433
Anwendungs-Dashboard 433
Daten in Dashboard-Spalten sortieren 433
Aktualisierungen im neuen Dashboard-Verhalten im Vergleich zum früheren Dashboard 434
Anwendungen verwalten 435
Anwendungsdetails anzeigen 435
Eine Anwendung hinzufügen 436
Erstellen einer Anwendung mit dem StyleBook 438
Eine Anwendung bearbeiten oder löschen 438
Berichte des App-Dashboards und des Sicherheits-Dashboards exportieren 439
Anwendungen anzeigen 439
Microservices-Anwendungen anzeigen 440
Eine Anwendung konfigurieren und mehreren benutzerdefinierten Anwendungen zuordnen 442
Übersicht des Anwendungs-Dashboards 444
Ergebnisse mithilfe der Suchleiste suchen und filtern 447
Filter speichern 447
Tags für Anwendungen erstellen und anwenden 447
Anwendungsdetails 448
Monitorstatus einer Anwendung überprüfen 451
App-Score-Komponenten auswählen und Schwellenwerte festlegen 452
Anwendungsdetails für Microservices-Anwendungen 455
Intelligente App-Analysen 458
Intelligente App-Analysen konfigurieren 458
Leistungsindikatoren für Anwendungsanalysen 460

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Antwortzeit 460
Aktive Dienste 461
Durchschnittliche CPU-Auslastung 461
Durchschnittliche CPU-Auslastung der Anwendung 462
Speicherauslastung 462
NIC-Verwürfe 462
Dienst-Flaps 463
Geringe Sitzungswiederverwendung 464
Falscher Persistenztyp 464
Instabiler Server 465
SSL-Echtzeit-Traffic 466
Ungewöhnlich große HTTP-Pakete 467
Treffer des TCP-Reassembly-Warteschlangenlimits 468
Anstieg der Warteschlangenbildung 468
SSL-Bewertung 469
Fehlerbehebung für App-Dashboard 469
Fehlerbehebungsszenario 470
Anwendung ist lizenziert 470
Metrik-Collector ist aktiviert 470
NetScaler-Instanz älter als Builds 47.x 471
NetScaler-Instanz, Builds neuer als 47.x 472
Anwendungsnutzung und Anomalien 475
Analyse der Spitzen- und Nebennutzung 476
App-Skalierungsgrenzen bewerten 476
Die 5 wichtigsten Wartungsfenster für Apps identifizieren 476
Anwendungsnutzungsanalysen 478
Metrikdetails im grafischen Format anzeigen 485
Automatisieren Sie die Verwaltung von SSL-Zertifikaten 489

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Einen Venafi-Server auf NetScaler Console konfigurieren 489
Verwalten des Lebenszyklus von SSL-Zertifikaten 490
A+ SSL-Bewertungsanalysen 492
Upgrade auf A+ SSL-Bewertung 492
SSL-Bewertung zurücksetzen 493
Auswirkungen der SSL-Bewertung auf den Anwendungsdatenverkehr bestimmen 494
Web Insight-Dashboard 495
Details zu Chiffre-bezogenen Problemen anzeigen 496
Integrierte Cache-Anfragen 497
Anderer Anwendungsfall 498
Grundursache für Anwendungsverlangsamung analysieren 498
Anwendungs-Drilldown 499
Antwortzeit 500
Service-Graph 501
Service-Graph für Anwendungen über alle NetScaler-Instanzen hinweg 501
Service-Graph für Kubernetes-Anwendungen 502
Service-Graph für 3-Tier-Webanwendungen 503
Service-Graph für Kubernetes-Apps 504
Service Graph – Vereinfachtes Onboarding 505
Einen Agenten automatisch als Kubernetes-Job bereitstellen 505
Service Graph manuell konfigurieren 509
Einrichten des Service-Graphen 512
Softwareanforderungen 512
Einzelschicht- oder Unified-Ingress-Topologie 513
Zweischicht- oder Service Mesh Lite-Topologie 514
Service-Mesh-Topologie 514
Details im Service-Graph anzeigen 516
Service-Graph-Dashboard 516

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wichtige Metrik-Trends in der Tabellenansicht anzeigen 518
Pxx-Wert für die Dienstantwortzeit anzeigen 519
Dienstdetails anzeigen 519
Client-Metriken anzeigen 520
TCP- und SSL-Metriken anzeigen 521
Filter anwenden 521
Einstellungsoption 522
Fehler analysieren 523
HTTP-Transaktionsdetails anzeigen 523
Schwellenwerte im Service-Graph konfigurieren 524
Einzelner Schwellenwert 526
Doppelter Schwellenwert 526
Servicedetails anzeigen 527
Metrikdetails 528
Backend-Pod-Details anzeigen 528
Dienste mithilfe der Golden-Signal-Metriken überwachen 529
Ingress-Details zur Fehlerbehebung anzeigen 530
Verteiltes Tracing 534
Voraussetzungen 534
Details zur Dienstverfolgung anzeigen 538
Transaktionsdetails anzeigen 539
Diagnosedetails für teilweise oder keine Daten im Service-Graph anzeigen 541
Diagnose bei fehlenden Daten 541
Diagnose für Teildaten 542
Fehlerbehebung 542
Service-Graph für 3-Schicht-Webanwendungen 543
Anwendungsansicht 543
Ansicht der Netzwerkfunktionen 543

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service-Graph-Ansicht für keine aktiven Transaktionen 544
Metriken analysieren 544
Client-Metriken 544
Metriken der Netzwerkfunktion 544
Dienstmetriken 545
NetScaler-Metriken (nur für GSLB-Anwendungen) 545
Ganzheitliche Ansicht aller Anwendungen im Service-Graph 546
Client-Metriken anzeigen 546
NetScaler-Details anzeigen 546
Diskrete Anwendungen anzeigen 547
Microservice-Anwendungen anzeigen 549
Suchleiste zum Filtern von Ergebnissen 549
StyleBooks 551
StyleBook-Kategorien 553
Standard- und benutzerdefinierte StyleBooks 553
Öffentliche und private StyleBooks 554
Beispiel eines als privat gekennzeichneten StyleBooks 554
StyleBooks anzeigen 554
Benutzerdefinierte StyleBooks herunterladen 555
Benutzerdefiniertes StyleBook aktualisieren 556
Benutzerdefinierte StyleBooks löschen 557
StyleBook-Abhängigkeiten anzeigen 557
So zeigen Sie StyleBook-Abhängigkeiten an 557
Vorwärtsabhängigkeiten 558
Rückwärtsabhängigkeiten 558
NetScaler-Konfiguration anhand von Konfigurationspaketen prüfen 558
Support-Bundle eines Konfigurationspakets herunterladen 559
Ein Tag für das StyleBook erstellen 559

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ein StyleBook klonen 560
StyleBooks aus einem externen Repository importieren und synchronisieren 561
Repository hinzufügen 564
Repository-Optionen 565
Schritte zum Importieren von StyleBooks und Konfigurationspaketen aus GitHub/GitLab 566
Standard-StyleBooks verwenden 566
NetScaler-Funktionen 566
Funktionen der Web Application Firewall 568
Funktionen der Anwendungssicherheit 569
Bot-Verwaltungsfunktionen 570
NetScaler-Netzwerkkonfigurationen 571
Was kommt als Nächstes? 572
StyleBook für Web Application Firewall 572
Bereitstellen von Application Firewall-Konfigurationen 573
StyleBook für SNMP-Konfiguration 575
NetScaler Netzwerkkonfigurationen StyleBook 580
Grundlegende Netzwerkkomponenten bereitstellen 581
Erweiterte Netzwerkkomponenten bereitstellen 583
Prometheus Analytics StyleBook 586
Voraussetzung 586
Migration der NetScaler-Anwendungskonfiguration mit dem StyleBooks Configuration Builder 587
Freigabe von Konfigurationsentitäten zwischen migrierten Konfigurationen 588
Unterstützte NetScaler-Funktionen 589
Erstellen Sie ein StyleBook, um die NetScaler-Anwendungskonfiguration zu migrieren 589
Einschränkungen 592
StyleBooks für Geschäftsanwendungen 592
SSO Google Apps StyleBook 592
So stellen Sie das SSO Google Apps StyleBook bereit 593

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSO Office 365 StyleBook 597

So stellen Sie das SSO Microsoft Office 365 StyleBook bereit 598

StyleBook für Microsoft Skype for Business 603

Konfigurieren von NetScaler-Instanzen in einem Unternehmen 604

Microsoft Exchange StyleBook 611

NetScaler-Funktionen, die mit Microsoft Exchange StyleBook konfiguriert werden 611

Voraussetzungen 612

Konfigurieren des Microsoft Exchange StyleBook 612

So konfigurieren Sie die Microsoft Exchange-Anwendung 612

Microsoft SharePoint StyleBook 614

Voraussetzungen 614

Microsoft ADFS-Proxy-StyleBook 619

Vorteile der Verwendung von NetScaler als ADFS-Proxy 620

Oracle E-Business StyleBook 625

So erstellen Sie eine Konfiguration für Oracle E-Business Suite 12.2 625

Benutzerdefinierte StyleBooks erstellen und verwenden 626

Bevor Sie beginnen 626

Aufbau eines StyleBooks 627

Konfigurationspaket erstellen und bearbeiten 628

Konfigurationspaket erstellen 629

Konfigurationen wiederverwenden, die außerhalb von StyleBooks erstellt wurden, und Konfigurationen zwischen Konfigurationspaketen teilen 630

Ändern des StyleBooks eines Konfigurationspakets 631

Konfigurationspakete exportieren oder importieren 633

Konfigurationspaket als Entwurf speichern 635

Erstellen eines Zeitplans für ein Konfigurationspaket 636

Eine Zielinstanz von einem Konfigurationspaket trennen 638

Erstellen Sie Ihre StyleBooks 638

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBook zum Erstellen eines Lastausgleichs-Virtual-Servers 642
Header 642
Komponenten 648
Erstellen Sie Ihr StyleBook 649
StyleBook zum Erstellen einer grundlegenden Lastausgleichskonfiguration 652
Header 652
Komponenten 655
Ausgaben 660
Erstellen Sie Ihr StyleBook 661
Erstellen Sie ein zusammengesetztes StyleBook 666
Erstellen Sie Ihr StyleBook 666
GUI-Attribute in einem benutzerdefinierten StyleBook verwenden 670
Bezeichnung mit Tooltip für Parameter hinzufügen 670
Einen einklappbaren Bereich für den Parameter festlegen 671
Die Benutzeroptionen als Optionsfelder festlegen 672
Benutzerdefinierte StyleBooks importieren 673
HTML-Formatierungs-Tags in der StyleBook-Beschreibung und im Header verwenden 674
So importieren Sie Ihr StyleBook 675
Erstellen eines StyleBooks zum Hochladen von Dateien 679
StyleBook-Konfiguration 679
Erstellen Sie Ihr StyleBook – 1 679
Erstellen Sie Ihr StyleBook – 2 681
Erstellen von Konfigurationen zum Hochladen von Dateien 683
Erstellen Sie ein StyleBook zum Hochladen von SSL-Zertifikats- und Zertifikatsschlüsseldateien 684
StyleBook-Konfiguration 684
Erstellen von Konfigurationen zum Hochladen von SSL-Dateien 688
Erstellen Sie Ihr StyleBook 689

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL-Zertifikate aus dem Zertifikatsspeicher mit StyleBooks verwalten 693
Parameter 693
Komponenten 695
Erstellen Sie Ihr StyleBook 695
Analysen aktivieren und Alarme auf einem in einem StyleBook definierten virtuellen Server konfigurieren 700
Instanzrollen 702
Abschnitt „target-roles“ 703
Rolle „default“ 703
Komponenten mit Rollen 704
Erstellen Sie Ihr StyleBook 707
Verwenden von APIs 711
Erstellen eines StyleBooks zum Ausführen von Nicht-CRUD-Operationen 713
Unterstützung der Nicht-CRUD-Operationen 713
Bereitstellen von GSLB-Konfigurationen mithilfe von DNS-Domainnamen 715
Workflow für Administratoren 716
NetScaler Console REST API für den Administrator-Workflow 719
Workflow für die Anwendungsbesitzer 753
NetScaler Console REST API für den Workflow des App-Besitzers 755
Erstellen Sie Ihr StyleBook 758
Sonderzeichen in ihrer wörtlichen Form in StyleBook zulassen 768
Mehrere wörtliche Zeichenfolgen verketten 771
Datenquellen verwalten 771
Eine NetScaler-Instanz als Datenquelle verwenden 773
Verwenden der integrierten Datenquelle ohne Sammlung 773
Verwenden der integrierten Datenquelle mit Sammlung 776
Ziel-NetScaler-Instanzen als Datenquellen verwenden 783
Beispiel-StyleBook zur Verwendung der Ziel-NetScaler-Instanz als Datenquelle 784

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benutzerdefinierte Datenquellen verwenden 785

Einen Datenquellentyp hinzufügen 786

Sammlungsschema unter Datentyp der Datenquelle hinzufügen 786

Datenquelle hinzufügen 787

Sammlungsdaten hinzufügen 787

Benutzerdefinierte Datenquelle ohne Sammlung verwenden 787

Benutzerdefinierte Datenquellen mit Sammlung verwenden 789

APIs verwenden, um Konfigurationen aus StyleBooks zu erstellen 793

Beispiel 1 793

Beispiel 2 797

Beispiel 3 799

Beispiel 4 801

Aktualisieren einer Konfiguration 803

Löschen einer Konfiguration 805

Konfigurationen mit APIs erstellen 806

APIs verwenden, um Konfigurationen zum Hochladen beliebiger Dateitypen zu erstellen 810

Benutzerdefinierte StyleBooks mithilfe von APIs importieren 812

Benutzerdefiniertes StyleBook mithilfe der API aktualisieren 816

APIs zum Herunterladen benutzerdefinierter StyleBooks verwenden 816

APIs zum Herunterladen abhängiger StyleBooks und zum Angeben des Komprimierungstyps verwenden 817

API zum Löschen benutzerdefinierter StyleBooks verwenden 817

APIs zum Aktualisieren eines vorhandenen Konfigurationspakets verwenden 818

APIs zum Aktualisieren von Zielinstanzen verwenden 824

API zur Konfigurationsprüfung verwenden 828

API zum Exportieren eines Konfigurationspakets verwenden 828

APIs verwenden, um das Konfigurationspaket auf ein neues StyleBook zu aktualisieren 829

API verwenden, um eine Zielinstanz von einem Konfigurationspaket zu trennen 830

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler-Instanz mit der API zwangsweise aus dem Konfigurationspaket löschen 831
APIs zum Löschen von Konfigurationspaketen verwenden 832
StyleBooks-Grammatik 836
Header 838
StyleBooks importieren 840
Parameter 842
'Name' 842
'Bezeichnung' 842
'Beschreibung' 842
'Typ' 843
'Netzwerk' 844
'dynamic-allocation' 845
'Schlüssel' 846
'erforderlich' 847
'allowed-values' 847
'allow-new-values' 849
'Standard' 850
'Muster' 851
'min-value' 852
'max-value' 852
'min-length' 853
'max-length' 853
'min-items' 854
'max-items' 854
'Benutzeroberfläche' 855
'Spalten' 855
'Aktualisierbar' 855
'collapse_pane' 855

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'Layout' 861

'dependent-parameters' 862

`is_policy_expression` 864

Konstrukt „parameters-default-sources“ 864

Parameters-source-Konstrukt 873

Parameterbedingungen 874

'anzeigen' oder 'ausblenden' 875

'Standardwert festlegen' 875

'set-required' 876

'set-allowed-values' 877

'set-label' 880

'set-description' 881

'collapse-pane' oder 'erweitern-pane' 881

'set-pattern' 882

Verschachtelte Parameterbedingungen 882

Substitutionen 883

Substitutionszuordnung 896

Durch Substitutionslisten iterieren 897

Komponenten 900

Hilfskomponenten 903

Optionale Eigenschaften 907

Properties-default-sources-Konstrukt 910

Berechnung der Eigenschaften der Komponente 913

Verschachtelte Komponenten 914

Bedingungskonstrukt 918

Repeat-Konstrukt 920

Wiederholungsbedingungs-Konstrukt 925

Verschachtelte Wiederholungen 927

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ausgaben 931
Parameterreferenz 932
Elternreferenz 936
Komponentenreferenz 939
Substitutionen-Referenz 942
Variablenreferenz 943
Operationen 945
Analysen 952
Ziel-Virtual-Server und Insight-Typen 956
Alarme 957
Ausdrücke 961
Arithmetische Ausdrücke 962
Zeichenfolgenausdrücke 962
Listenausdrücke 962
Relationale Ausdrücke 963
Logische Ausdrücke – boolesch 964
Splat-Ausdrücke 964
Wörtliche Zeichenfolgenausdrücke 965
Zielausdrücke 966
Validierung des Ausdruckstyps 967
In-Place-Interpolationen 972
Zulässige Typen innerhalb von Interpolationen 973
Einfache Interpolationen 974
Automatische Typumwandlungen 974
Sequenzielle Interpolationen 974
Verschachtelte Interpolationen 974
Interpolationen mit `quotewrap` 974
Integrierte Funktionen 975

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zeichenkette() 976

Ganzzahl() 976

BoolescherWert() 976

Länge() 977

Minimum() 977

Maximum() 978

bin()-Funktion 978

oct()-Funktion 978

hex()-Funktion 979

klein() 979

Großschreibung() 979

Summe() 979

pow()-Funktion 980

ip() 980

ip_network() 980

network_ip() 981

Subnetze() 981

netmask_ip() 981

is_netmask_ip() 982

broadcast_ip() 982

cidr()-Funktion 982

is_cidr() 982

is_in_network() 983

base64.encode() 983

base64.decode() 983

exists()-Funktion 983

Filterfunktion() 984

if-then-else() 984

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verbinden() 985
Teilen() 986
abbilden() 986
Zitieren() 987
ersetzen() 987
trimmen() 989
kürzen() 989
eindeutig() 989
url.encode() 989
url.decode() 989
is-ipv4() 990
is-ipv6() 990
beginntMit() 990
endetMit() 990
enthält() 991
Teilstring() 992
Abgleichen() 993
sha256() 993
verknüpfen() 994
mehrere() 997
umkehren() 998
Abhängigkeitserkennung 999
Zirkuläre Abhängigkeiten 1001
Sicherheit 1005
Anwendungssicherheits-Dashboard 1005
Details zum Bedrohungsindex 1006
Details zum Sicherheitsindex 1007
Einheitliches Sicherheits-Dashboard 1008

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gesicherte Anwendungen 1008
Schutzmaßnahmen für ungesicherte Anwendungen konfigurieren 1009
Details zu Anwendungs-Sicherheitsverletzungen anzeigen 1014
Einrichtung 1015
Webtransaktionseinstellungen aktivieren 1015
Anwendungsübersicht 1016
Verstoßkategorien 1016
WAF-Verletzungsdetails anzeigen 1018
Bot-Verstoßdetails anzeigen 1019
Ereignisverlauf anzeigen 1021
Automatische Signaturaktualisierung 1021
Alle Verstöße 1022
Verstoßkategorien 1022
Dashboard für Sicherheitsverletzungen 1024
Details zur Verletzung 1024
WAF-Lernfunktion 1025
Erste Schritte 1025
WAF-Empfehlungen 1027
Voraussetzungen 1029
WAF-Scan-Einstellungen konfigurieren 1029
WAF-Scan-Empfehlungsprozess 1031
Scanbericht anzeigen 1032
Gateway 1035
Gateway Insight 1035
Gateway Insight aktivieren 1037
AppFlow für einen virtuellen Server in NetScaler Console aktivieren 1037
AppFlow-Benutzernamenprotokollierung auf einer NetScaler Gateway-Appliance über die GUI aktivieren 1038

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway Insight-Berichte anzeigen 1038
EPA-, SSO-, Authentifizierungs-, Autorisierungs- und Anwendungsstartfehler anzeigen 1038
Zusammenfassung der Sitzungsmodi, Clients und der Benutzeranzahl anzeigen 1039
Benutzer 1039
Benutzerdetails anzeigen 1039
Suchleiste und Geo-Kartenansicht 1041
Anwendungen 1041
Anwendungsdetails anzeigen 1041
Gateways 1042
Gateway-Details anzeigen 1042
Berichte exportieren 1043
Einen Bericht exportieren 1043
Gateway Insight-Anwendungsfälle 1044
1. Benutzer kann sich nicht bei der NetScaler Gateway-Appliance oder bei den internen Webservern anmelden 1044
Authentifizierungsfehler 1045
Details zu Authentifizierungsfehlern anzeigen 1045
EPA-Fehler 1045
EPA-Fehlerdetails anzeigen 1046
SSO-Fehler 1046
SSO-Fehlerdetails anzeigen 1046
Details zu Fehlern beim Anwendungsstart anzeigen 1047
Gesamtbytes und Bandbreite, die von einer Anwendung verbraucht werden, anzeigen 1048
Benutzerzugriff auf Ressourcen anzeigen 1048
Zusammenfassung der Sitzungsmodi, Clienttypen und Anzahl der angemeldeten Benutzer anzeigen 1049
Beheben von Gateway Insight-Problemen 1049
Checkliste für die Gateway Insight-Konfiguration 1050

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Checkliste für die Konnektivität zwischen NetScaler und NetScaler Console 1050
Datensatzgenerierung in der NetScaler-Checkliste 1050
Validierungen in NetScaler Console 1051
Gateway Insight-Statistiken 1051
Wenden Sie sich an den technischen Support von Citrix 1051
Bekannte Probleme 1052
HDX™ Insight 1052
Ermitteln der Grundursache für langsame Leistungsprobleme 1053
Szenario 1 1053
Szenario 2 1054
Geokarte für HDX Insight 1055
Einen privaten IP-Block erstellen 1056
Anwendungsfall 1058
Einschränkungen 1058
HDX™ Insight-Datenerfassung aktivieren 1059
Datenerfassung für im Single-Hop-Modus bereitgestellte NetScaler Gateway Appliances aktivieren 1059
Datenerfassung zur Überwachung von NetScalern im transparenten Modus aktivieren 1061
Datenerfassung für im Double-Hop-Modus bereitgestellte NetScaler Gateway Appliances aktivieren 1063
Datenerfassung zur Überwachung von NetScalern im LAN-Benutzermodus aktivieren 1068
Schwellenwerte erstellen und Warnungen für HDX™ Insight konfigurieren 1072
Beispielanwendungsfälle 1073
HDX™ Insight-Berichte und -Metriken anzeigen 1075
Berichte und Metriken der Anwendungsansicht 1076
Berichte und Metriken der Desktop-Ansicht 1083
Berichte und Metriken der Benutzeransicht 1096
Berichte und Metriken der Instanzansicht 1109

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Berichte und Metriken der Lizenzansicht 1113
Fehlerbehebung bei HDX™ Insight-Problemen 1113
HDX Insight-Konfigurations-Checkliste 1114
Checkliste zur Konnektivität zwischen NetScaler und NetScaler Console 1114
Checkliste zur Datensatzgenerierung für HDX/ICA-Verkehr in NetScaler 1115
Fehlerzähler 1124
nstrace-Validierung 1129
Checkliste zur Datensatzpopulation in NetScaler Console 1129
Bevor Sie den technischen Support von Citrix kontaktieren 1129
Bekannte Probleme 1130
Metrikinformationen für Schwellenwerte 1130
Web 1130
Sicherheit 1133
APPANALYTICS 1134
HDX™ 1134
Infrastruktur 1135
Infrastruktur-Analysen 1135
Infrastruktur-Analysen in NetScaler Console 1136
Instanz-Score 1136
Erläuterung der Zustandsindikatoren 1137
NetScaler-Kapazitätsprobleme anzeigen 1139
Wert der Gesundheitsindikatoren 1139
Dashboard für Infrastruktur-Analysen 1140
Kreispack-Ansicht 1140
Instanzkreise 1140
Gruppierte Instanzkreise 1141
Geclusterte Instanzkreise 1141
Circle Pack verwenden 1142

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tabellarische Ansicht 1142
Suchleiste 1143
So verwenden Sie das Übersichtsfenster 1143
Instanzinformationen 1145
Traffic-Profil 1145
Verwenden des Einstellungsbereichs 1145
Ansicht 1146
Metriken auswählen und Gewichtung für die Berechnung des Instanz-Scores anpassen 1146
Benachrichtigungen konfigurieren 1147
So visualisieren Sie Daten auf dem Dashboard 1147
Instanzdetails in Infrastructure Analytics anzeigen 1148
Kapazitätsprobleme in einer NetScaler-Instanz anzeigen 1154
Empfohlene Maßnahmen zur Behebung von Kapazitätsproblemen anzeigen 1155
Erweiterte Infrastruktur-Analysen mit neuen Indikatoren 1156
Tabellarische Ansicht 1158
Details einer Anomalie anzeigen 1158
Instanzverwaltung 1158
Eine Instanz hinzufügen 1159
So verwenden Sie das Instanz-Dashboard 1159
So überwachen Sie global verteilte Standorte 1160
Überwachung global verteilter Standorte in NetScaler Console 1161
Anwendungsfall 1161
Geomaps konfigurieren 1162
So erstellen Sie Tags und weisen sie Instanzen zu 1166
So suchen Sie Instanzen anhand der Werte von Tags und Eigenschaften 1168
So suchen Sie nach NetScaler VPX-Instanzen 1168
Zentrale GeoIP-DB-Updates über NetScaler® Console 1169
Einschränkungen 1170

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfigurieren zentralisierter GeoIP-DB-Updates über NetScaler Console 1170
Verwalten von Administratorpartitionen von NetScaler-Instanzen 1173
Administratorpartitionen anzeigen 1173
Revisionsverlaufsunterschied anzeigen 1174
Unterschied zwischen Vorlage und laufender Konfiguration anzeigen 1175
NetScaler-Instanzen sichern und wiederherstellen 1176
Erstellen einer Sicherung für eine ausgewählte NetScaler-Instanz mithilfe von NetScaler Console 1177
Eine Sicherungsdatei auf ein externes System übertragen 1178
Wiederherstellen einer NetScaler-Instanz mit NetScaler Console 1179
Bericht dieses Dashboards exportieren 1181
Erzwingen eines Failovers auf die sekundäre NetScaler-Instanz 1182
Eine sekundäre NetScaler-Instanz zwingen, sekundär zu bleiben 1183
Instanzgruppen erstellen 1183
So erstellen Sie eine Instanzgruppe mit NetScaler Console 1184
So identifizieren und fügen Sie nicht zugeordnete Instanzen einer Gruppe hinzu 1184
Global Server Load Balancing-Site-Gruppen 1184
Erstellen einer GSLB-Site-Gruppe 1185
SNMP-Manager und -Benutzer für NetScaler-Agent erstellen 1185
Einen SNMP v2-Manager hinzufügen 1186
Einen SNMP v3 Manager hinzufügen 1186
SNMP-Benutzer hinzufügen 1187
Verwalten von SNMP-Ansichten 1188
NetScaler VPX-Instanzen auf SDX bereitstellen 1188
Schritt 1 – Eine VPX-Instanz hinzufügen 1189
Schritt 2 – Lizenzen zuweisen 1189
Schritt 3 - Ressourcen zuweisen 1190
Schritt 4 - Instanzverwaltung hinzufügen 1191

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schritt 5 – Netzwerkeinstellungen angeben 1191
Schritt 6 – Management-VLAN-Einstellungen angeben 1193
Bereitgestellte VPX-Instanz anzeigen 1193
Mehrere NetScaler-Instanzen neu erkennen 1193
Polling-Übersicht 1194
Wie NetScaler Console verwaltete Instanzen und Entitäten abfragt 1195
Verschiedene Arten des Polling von Instanzen 1201
Instanz entwalten 1203
Route zu einer Instanz verfolgen 1203
NetScaler-eigene IP-Adressen anzeigen 1204
NetScaler-eigene IP-Adressen exportieren 1204
Export von NetScaler-eigenen IP-Adressen planen 1205
So ändern Sie das NetScaler MPX- oder VPX-Root-Passwort 1206
Passwort mit der Funktion „Konfigurationsaufträge“ ändern 1207
So ändern Sie ein NetScaler SDX nsroot-Passwort 1209
Passwort ändern 1209
So generieren Sie ein technisches Support-Bundle für eine NetScaler®-Instanz 1210
Ereignisse 1213
Ereignis-Dashboard verwenden 1213
Ereignisregeln erstellen 1215
Ereignisregel konfigurieren 1216
Schritt 1 — Namen und Instanzfamilie angeben 1216
Schritt 2 – Ereignisalter konfigurieren 1216
Schritt 3 – Schweregrad des Ereignisses auswählen 1217
Schritt 4 – Ereigniskategorie angeben 1218
Schritt 5 – NetScaler-Instanzen angeben 1218
Schritt 6 – Fehlerobjekte auswählen 1218
Schritt 7 – Erweiterte Filter angeben 1219

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schritt 8 - Ereignisregelaktionen hinzufügen 1220
Einen Ereignisfilter planen 1228
Berichtete Schweregrade von Ereignissen, die auf NetScaler-Instanzen auftreten, ändern 1228
Ereignisübersicht anzeigen 1229
Ereignismeldungen 1230
Ereignisschweregrade und SNMP-Trap-Details anzeigen 1231
Syslog-Meldungen anzeigen und exportieren 1233
Syslog-Meldungen anzeigen 1233
Syslog-Meldungen suchen 1233
Syslog-Meldungen exportieren 1234
Syslog-Meldungen unterdrücken 1235
Syslog-Meldungen durch Erstellen von Filtern unterdrücken 1236
Deaktivieren des Filters 1237
SSL-Dashboard 1237
Automatisierte Zertifikatserneuerung mit dem ACME-Protokoll 1238
ACME-Unterstützung in NetScaler® Console 1238
Konfigurationsschritte für die ACME-Integration 1240
Ausstellung und Verlängerungen 1248
Zertifikat ausstellen 1250
Drittanbieter-Integration 1251
Einschränkungen 1253
Beheben von Problemen im Zusammenhang mit der automatischen Zertifikatsverlängerung 1253
Zero-Touch-Zertifikatsverwaltung 1255
Zertifikate hochladen 1256
Zero-Touch-Zertifikatsverwaltung aktivieren 1256
Unterstützung des SSL-Filtermodus 1257
Verwenden Sie das SSL-Dashboard 1259

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL-Zertifikate überwachen 1259
Audit-Protokolle für SSL-Zertifikate anzeigen 1261
Standard-NetScaler-Zertifikate im SSL-Dashboard ausschließen 1261
SSL-Zertifikate herunterladen 1261
So löschen Sie das SSL-Zertifikat im SSL-Dashboard 1262
SSL-Zertifikatskette anzeigen 1263
Benachrichtigungen für den Ablauf von SSL-Zertifikaten einrichten 1264
Installiertes Zertifikat aktualisieren 1265
Installieren von SSL-Zertifikaten auf einer NetScaler-Instanz 1266
Eine Zertifikatsignieranforderung (CSR) erstellen 1267
SSL-Zertifikate verknüpfen und Verknüpfung aufheben 1269
Eine Unternehmensrichtlinie konfigurieren 1270
SSL-Zertifikate von NetScaler-Instanzen abrufen 1271
Verwenden Sie den NetScaler Console Zertifikatsspeicher zur Verwaltung von SSL-Zertifikaten 1272
SSL-Zertifikate zum Zertifikatsspeicher hinzufügen 1272
SSL-Zertifikate im Zertifikatsspeicher aktualisieren 1272
SSL-Zertifikate aus dem Zertifikatsspeicher löschen 1273
SSL-Zertifikate auf NetScaler®-Instanzen installieren 1273
Zertifikate von NetScaler-Instanzen importieren 1274
Serverzertifikate ohne Zwischen-Uploads aktualisieren 1274
Konfigurationsjobs 1276
Konfigurationsvorlage 1276
Instanz 1277
Datei 1277
Aufzeichnen und Abspielen 1278
Bericht dieses Dashboards exportieren 1278
Verwandte Artikel 1278

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfigurationsauftrag erstellen 1279

Verwenden Sie „Aufzeichnen und Wiedergeben“, um Konfigurationsaufträge zu erstellen 1283

Konfigurationsaufträge verwenden, um die Konfiguration von einer Instanz auf mehrere Instanzen zu replizieren 1285

Variablen in Konfigurationsaufträgen verwenden 1287

Konfigurationsaufträge aus Korrekturbefehlen erstellen 1291

Laufende und gespeicherte Konfiguration von einer NetScaler-Instanz auf eine andere replizieren 1293

Ausgeführte Konfigurationsaufträge wiederverwenden 1294

SCP (put)-Befehl in Konfigurationsaufträgen verwenden 1295

Konfigurationsvorlagen verwenden 1298

Verwenden der Master-Konfigurationsvorlage 1298

Aufträge planen, die mithilfe integrierter Vorlagen erstellt wurden 1305

Einen Auftrag zum Konfigurieren des Exports von Metriken von NetScaler nach Prometheus planen 1306

Konfigurationsvorlagen zum Erstellen von Audit-Vorlagen verwenden 1309

Aufträge neu planen, die mit integrierten Vorlagen konfiguriert wurden 1310

Konfigurationsüberwachungsvorlagen in Konfigurationsaufträgen wiederverwenden 1311

Konfigurationsvorlagen importieren und exportieren 1314

Konfigurationsaudit 1315

Audit-Vorlagen erstellen 1316

Konfigurationsaudit von NetScaler-Instanzen abfragen 1318

Auditberichte anzeigen 1319

Konfigurationsaudit-Diff für ConfigChange SNMP-Traps generieren 1323

Konfigurationsänderungen über Instanzen hinweg prüfen 1325

Konfigurationsempfehlungen für die Netzwerkkonfiguration erhalten 1328

Upgrade-Aufträge 1329

Vor-Upgrade-Validierung 1331

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade von NetScaler-Instanzen planen 1332
Upgrade von NetScaler SDX-Instanzen planen 1335
Planen der Aktualisierung von NetScaler BLX-Instanzen 1336
Upgrade der Autoscale™-Gruppe planen 1339
Konfiguration eines HA-Paares von NetScaler-Instanzen planen 1340
Planen der Konvertierung eines HA-Instanzpaares in einen Cluster 1341
NetScaler-Instanzen mithilfe von Aufträgen aktualisieren 1341
Voraussetzungen 1342
Upgrade-Überlegungen für angepasste NetScaler-Konfigurationen 1342
NetScaler Hochverfügbarkeitspaar 1343
NetScaler Cluster 1343
NetScaler-Upgrade-Job erstellen 1344
Einen geplanten Upgrade-Job anhalten oder fortsetzen 1348
Fehlgeschlagene Upgrade-Jobs wiederholen 1349
Bereinigen des NetScaler-Speicherplatzes 1350
Benutzerdefinierte Skripte verwenden 1350
NetScaler-Upgrade-Optionen 1352
Upgrade-Jobs für ein NetScaler-Hochverfügbarkeitspaar planen 1352
Konsolidierten Diff-Bericht eines NetScaler-Upgrade-Jobs herunterladen 1353
Netzwerkfunktionen 1354
Berichte für Lastenausgleichsentitäten generieren 1354
Kombinierten Lastausgleichsbericht generieren 1355
Einen individuellen Bericht für Lastausgleichsentitäten generieren 1357
Berichte zu Netzwerkfunktionen exportieren oder den Export planen 1357
Netzwerkberichterstattung 1359
Dashboard für Netzwerkberichterstattung 1360
Netzwerkberichtsdaten durch Anwenden von Aggregationen anzeigen 1362
Netzwerkberichte exportieren 1363

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwellenwerte für Netzwerkberichte in NetScaler Console verwalten 1365
Leistungsabfrageintervall für Netzwerkberichte festlegen 1367
Konfigurieren der Bereinigungseinstellungen für die Netzwerkberichterstattung 1367
Bereitstellung 1367
App-basiertes Provisioning in AWS 1368
Voraussetzungen 1368
Cloud-Zugriffsprofil 1369
App-Umgebung 1369
Anwendungsbereitstellung 1370
Häufig gestellte Fragen 1371
App-basiertes Provisioning in Azure 1373
Voraussetzungen 1374
Cloud-Zugriffsprofil 1374
App-Umgebung 1375
Anwendungsbereitstellung 1375
FAQs 1376
Bereitstellung von NetScaler VPX-Instanzen 1377
Bereitstellung von NetScaler VPX-Instanzen auf AWS 1378
Bereitstellung von NetScaler VPX-Instanzen in Microsoft Azure 1388
Bereitstellen von NetScaler VPX-Instanzen in Google Cloud 1400
NetScaler VPX-Instanzen auf VMware ESX bereitstellen 1409
NetScaler Globaler Lastausgleich für Hybrid- und Multi-Cloud-Bereitstellungen 1414
Architektur der NetScaler Hybrid- und Multi-Cloud-GLB-Lösung 1415
Konfiguration mithilfe der NetScaler Console StyleBooks 1418
Verwenden von StyleBooks zur Konfiguration von GLB 1421
Verwenden von StyleBooks zum Konfigurieren von GLB auf NetScaler LB-Knoten 1426
Orchestrierung 1429
Verwalten des Kubernetes-Clusters für Service Graph 1429

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bevor Sie beginnen 1429

NetScaler-Agent für die Registrierung beim Kubernetes-Cluster konfigurieren 1430

Konfigurieren Sie die NetScaler Console mit einem geheimen Token, um einen Kubernetes-Cluster zu verwalten 1430

Fügen Sie den Kubernetes-Cluster in der NetScaler Console hinzu 1431

NetScaler® Lizenzen 1433

Lizenzaktivierungsdienst 1434

Voraussetzungen 1436

Automatische Aktivierung und Kompatibilität 1436

NetScaler-Versionskompatibilität für LAS 1436

Umstellung auf LAS 1437

Erstmaliger LAS-Benutzer 1438

NetScaler-Instanzen mit LAS lizenzieren 1438

Vorhandene lizenzierte Instanzen zu LAS migrieren 1439

Bestehender LAS-Benutzer 1440

NetScaler-Instanzen mit LAS lizenzieren 1440

Die lizenzierten NetScaler-Instanzen zu LAS migrieren 1440

Informationen, die während des LAS-Lizenzierungs-Workflows an LAS gesendet werden 1441

Bewährte Methoden zur Überwachung Ihrer LAS-migrierten NetScaler Console Service-Umgebung 1442

Voraussetzungen 1443

Überwachung des Ablaufs von LAS-Aktivierungs-Blobs 1443

NetScaler-Instanzen über die GUI anzeigen 1443

NetScaler-Instanzstatus über die CLI anzeigen 1444

Benachrichtigungen 1444

Überwachung des Ablaufs von Lizenzberechtigungen 1445

Benachrichtigungen 1445

Lizenzverwaltung 1446

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LAS-basierte Lizenz 1447

Lizenzserver-Ports 1447

Informationen zum Lizenzablauf 1447

Benachrichtigungseinstellungen 1448

RBAC-Unterstützung für LAS 1451

Manuell verwaltete Berechtigungen (dateibasierte Lizenzen) 1451

Lizenzdateien 1451

Porteinstellungen des Lizenzservers 1455

Informationen zum Lizenzablauf 1455

Benachrichtigungseinstellungen 1456

Mindest- und Höchstkapazität für die Ausleihe 1459

Tabelle 1. Unterstützte Flexed-Kapazität für MPX 1461

Tabelle 2A. Unterstützte Flexed-Kapazität für NetScaler SDX-Versionen vor Build 13.0-47.x 1462

Tabelle 2B. Unterstützte Flexed-Kapazität für NetScaler SDX Version 13 (Build 13.0-47.x und höher), Version 13.1 (Build vor 51.x) und Version 14.1 (Build vor 12.x) 1463

Tabelle 2C. Unterstützte Flexed-Kapazität für NetScaler SDX Version 13.1 (Build 51.x und höher) und Version 14.1 (Build 12.x und höher) 1464

Tabelle 3. Unterstützte minimale/maximale Bandbreite und minimale/maximale Instanzen für NetScaler CPX-Instanzen 1466

Tabelle 4. Unterstützte minimale/maximale Bandbreite und minimale/maximale Instanzen für NetScaler VPX-Instanzen auf Hypervisoren und Cloud-Diensten 1466

Tabelle 5. Unterstützte minimale/maximale Bandbreite und minimale/maximale Instanzen für NetScaler BLX-Instanzen 1467

Tabelle 6. Lizenzanforderung für Nullkapazität für verschiedene Formfaktoren 1467

Verhalten des NetScaler-Agenten 1468

LAS-basierte Lizenzierung 1469

Manuell verwaltete Berechtigung (dateibasierte Lizenzierung) 1469

Manuelles Auswählen eines NetScaler Console-Agenten als LSA 1470

Verhalten mehrerer NetScaler-Agents 1470

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Failover-Verhalten des NetScaler-Agents 1470
Lizenzserver über den integrierten NetScaler-Agenten konfigurieren 1471
Flexed-Lizenz 1472
Nullkapazitäts-Hardware 1474
Z-Cap-Lizenzen verwalten und installieren 1474
Eigenständige NetScaler VPX-Instanzen 1475
Eigenständige NetScaler CPX-Instanzen 1475
Eigenständige NetScaler BLX-Instanzen 1476
Bandbreitenpool 1476
Instanzpool 1476
Lizenz konfigurieren 1477
LAS-basierte Lizenzierung 1478
Voraussetzung 1478
Schritt 1 – Überprüfung der Berechtigungsanzeige 1478
Schritt 2 – NetScaler-Instanz zum Konsolendienst hinzufügen 1478
Schritt 3 – Lizenz mit LAS aktivieren 1479
Schritt 4 – Flexed-Durchsatzkapazität für NetScaler-Instanzen bearbeiten 1479
Spezielle Lizenzierung für nicht lizenzierte MPX-Appliances mit einem externen Agenten 1479
Manuell verwaltete Berechtigungen (dateibasierte Lizenzierung) 1480
Bevor Sie beginnen 1481
Schritt 1 – Lizenzen in NetScaler Console anwenden 1481
Schritt 2 – NetScaler Console als Lizenzserver registrieren und Lizenzen zuweisen 1482
Schritt 3 – Gehen Sie je nach Lizenztyp zum entsprechenden Lizenzverfahren 1484
Flexed- oder Pooled-Kapazität auf NetScaler-Instanzen konfigurieren 1485
Lizenzanforderungen für NetScaler Hochverfügbarkeitspaar (gemeinsam für LAS und dateibasierte Lizenzierung) 1487
NetScaler Flexed-Lizenzierungsstatus (Gemeinsam für LAS- und dateibasierte Lizenzierung) 1487
Lizenz-Dashboard 1488

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zugewiesene Durchsatzkapazität auf einer NetScaler-Instanz bearbeiten 1490
Lizenzen auf einer NetScaler-Instanz freigeben 1491
Fehlerbehebung bei Lizenzierungsproblemen 1491
Lizenzberichterstattung 1492
Umstellung auf Flexed-Lizenzierung 1495
LAS-basierte Lizenzen 1497
Manuell verwaltete Berechtigungen (dateibasierte Lizenzen) 1497
Pooled-Bandbreitenlizenz zu Flexed-Lizenzierung 1497
Von Pooled vCPU zu Flexed Licensing 1498
Von Fixed Subscription oder Perpetual License zu Flexed Licensing 1499
Feste vCPU zu Flexed-Lizenzierung 1499
CICO zu Flexed-Lizenzierung 1500
Selbstverwaltete Bandbreitenlizenz zur Flex-Lizenzierung 1500
Self Managed vCPU zu Flexed-Lizenzierung 1501
Szenarien für den Ablauf von Flexed- oder Pooled-Lizenzen und das Verhalten bei Konnektivitätsproblemen 1501
LAS-basierte Lizenzen 1502
Vor Ablauf der Laufzeit 1502
Nach Ablauf der Laufzeit 1503
Szenarien für das Verhalten bei Konnektivitätsproblemen 1503
Manuell verwaltete Lizenz (dateibasierte Lizenz) 1503
Komponenten von Flexed-Lizenzen 1503
Szenario: MPX-Formfaktor 1503
Szenario: SDX-Formfaktor 1504
Szenario: VPX/BLX/CPX-Formfaktor 1505
Szenarien für das Verhalten bei Konnektivitätsproblemen 1506
NetScaler Console-Server nur als Flexed- oder Pooled-Lizenzserver konfigurieren 1507
Voraussetzungen 1508

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So konfigurieren Sie die NetScaler Console nur als Flexed- oder Pooled-Lizenzserver 1509
Legacy-Lizenzen 1510
Gepoolte Kapazität 1511
Dauerlizenz in NetScaler MPX auf NetScaler Pooled Capacity aktualisieren 1513
Upgrade der unbefristeten Lizenz in einem NetScaler MPX Hochverfügbarkeitspaar auf NetScaler Pooled Capacity 1516
Aktualisieren einer unbefristeten Lizenz in einem NetScaler SDX auf NetScaler Pooled Capacity 1519
NetScaler VPX Check-in- und Check-out-Lizenzierung 1522
Lizenzen in NetScaler Console installieren 1523
Zuweisen einer NetScaler VPX-Lizenz zu einer NetScaler VPX-Instanz mithilfe der NetScaler-GUI 1523
Zuweisen einer NetScaler VPX-Lizenz zu einer NetScaler VPX-Instanz mithilfe der NetScaler CLI 1524
Ablaufprüfungen für NetScaler VPX Check-in/Check-out-Lizenzen konfigurieren 1525
NetScaler Virtual-CPU-Lizenzierung 1525
Virtuelle CPU-Lizenzierung für NetScaler VPX 1527
Häufig gestellte Fragen und weitere Ressourcen 1528
Konfiguration 1529
Lizenzserver-Agent 1530
Häufige Probleme 1531
Migration 1531
Beheben von Problemen mit der Pooled-Kapazitätslizenz 1532
Lizenzstatus überprüfen 1533
Serverstatus prüfen 1535
Lizenznutzungsbericht prüfen 1536
Zähler und Statistiken für Pooled Capacity Licensing 1536
Einstellungen 1539
Mit dem Console-Dienst über Cloud Connect verbundene Console On-Prem-Instanzen 1540

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Console On-Prem-Upload 1540
Analysen auf virtuellen Servern konfigurieren 1542
Analysen auf den erkannten virtuellen Servern konfigurieren 1543
Analysen bearbeiten 1545
Analysen deaktivieren 1545
Globale Analysen konfigurieren 1546
Benutzerdefinierte Richtlinie 1547
Globale Richtlinie 1548
Hinweise 1549
Analyse migrieren 1549
Rollenbasierte Zugriffssteuerung konfigurieren 1550
Benutzer in NetScaler Console konfigurieren 1552
Zugriffsrichtlinien in NetScaler Console konfigurieren 1554
StyleBook-Berechtigungen für Benutzer erteilen 1557
Rollen in NetScaler Console konfigurieren 1558
Gruppen in NetScaler Console konfigurieren 1559
Wie sich der Benutzerzugriff basierend auf dem Autorisierungsbereich ändert 1566
Einschränkungen 1566
Netzwerkprofil für die verwaltete NetScaler-Instanz zuweisen 1567
Voraussetzungen 1567
Verwaltung des Datenspeichers 1568
Ihren Datenspeicher verstehen 1569
Status Ihrer Datenerfassungsaktivität 1570
Gesamtspeicherverbrauch 1570
Status der Datenbereinigung 1571
Speicherverbrauch nach Funktionen 1574
Speicherplatz verwalten 1574
Datenbereinigung durchführen 1575

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Datenaufbewahrungsrichtlinie überprüfen 1576
Benachrichtigung bei Überschreitung des Speicherlimits 1576
Datenaufbewahrungsrichtlinie 1577
Systemalarme konfigurieren und anzeigen 1578
Einen Alarm konfigurieren 1578
Schwellenwerte für Festplattenauslastungsalarme hinzufügen 1579
Observability-Integration 1580
Integration mit Splunk 1580
Splunk für den Empfang von Daten von NetScaler Console konfigurieren 1581
NetScaler Console zum Exportieren von Daten nach Splunk konfigurieren 1584
Dashboards in Splunk anzeigen 1586
Integration mit New Relic 1587
Voraussetzungen 1587
New Relic-Dashboard 1589
Integration mit Microsoft Sentinel 1590
Konfigurieren des Log Analytics Workspace 1590
Erstellen einer Microsoft Entra-Anwendung 1591
Datenerfassungsendpunkt konfigurieren 1592
Tabellen zum Exportieren von Daten erstellen 1593
Ein Abonnement in NetScaler Console erstellen 1604
Protokolle in Microsoft Azure anzeigen 1605
Konfigurieren von NetScaler®-Instanzen für den Export von Einblicken nach Prometheus mithilfe des Standardschemas 1605
Protokolle für fehlgeschlagene Konfigurationen anzeigen 1606
Konfigurieren Sie den Export von NetScaler®-Metriken und Audit-Protokollen nach Splunk 1607
Protokolle für fehlgeschlagene Konfigurationen anzeigen 1608
Analytik-Einstellungen konfigurieren 1608
Schwellenwerte und Warnmeldungen für Analysen erstellen 1608

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benachrichtigungen konfigurieren 1609
E-Mail-Verteilerliste erstellen 1610
Erstellen einer SMS-Verteilerliste 1611
Slack-Profil erstellen 1611
Ein PagerDuty-Profil erstellen 1612
ServiceNow-Profil anzeigen 1612
Berichte exportieren oder den Export planen 1613
Einen Bericht exportieren 1613
Exportbericht planen 1614
Geplante Exportberichte anzeigen und bearbeiten 1615
Globale Einstellungen 1615
Instanzeinstellungen 1615
Instanzkonfiguration verwalten 1615
Instanz-Sicherungseinstellungen konfigurieren 1616
Benachrichtigungen für verwaltete Geräte deaktivieren 1617
Systemkonfigurationen 1618
Keep-Alive-Intervall des Agenten festlegen 1618
NetScaler Console-Zeitzone festlegen 1619
E-Mail-Abonnements 1619
E-Mail-Benachrichtigungen abbestellen 1619
Funktionen aktivieren oder deaktivieren 1620
Eine Aktionsrichtlinie zum Empfangen von Anwendungsereignisbenachrichtigungen konfigurieren 1621
Eine Aktionsrichtlinie konfigurieren 1623
Suchleiste verwenden 1636
Option „Audit-Protokolle“ verwenden 1636
Audit-Protokolle zur Verwaltung und Überwachung Ihrer Infrastruktur verwenden 1636
NetScaler-Instanzbezogene Audit-Protokolle 1637

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console als Syslog-Server konfigurieren 1637
NetScaler Console-bezogene Audit-Protokolle 1638
Anwendungsbezogene Audit-Protokolle 1638
IP-Adressverwaltung (IPAM) konfigurieren 1639
Einen externen IP-Adressanbieter hinzufügen 1639
Infoblox DDI als externer Anbieter 1641
Netzwerk hinzufügen 1642
Zugewiesene IP-Adressen anzeigen 1643
How-to-Artikel 1644
Instanzverwaltung 1644
Konfigurationsverwaltung 1645
Zertifikatsverwaltung 1645
StyleBooks 1646
Ereignisverwaltung 1646
FAQs 1648
Wie viele Agents muss ich installieren? 1648
Wie kann ich mehrere Agents installieren? 1648
Unterstützt der NetScaler Agent AMD-Prozessoren? 1648
Kann ich von einem integrierten Agent zu einem externen Agent wechseln? 1648
Wie erhalte ich einen neuen Aktivierungscode, wenn ich ihn verloren habe? 1648
Wie melde ich mich bei der Agent-VM an? Was sind die Standardanmeldeinformationen? 1649
Welche Ressourcenanforderungen gelten für die Installation eines Agents auf einem lokalen Hypervisor? 1649
Muss ich dem Agenten bei der Bereitstellung eine zusätzliche Festplatte zuweisen? 1649
Kann ich meinen Aktivierungscode mit mehreren Agenten wiederverwenden? 1649
Wie führe ich die Netzwerkeinstellungen erneut aus, wenn ich einen falschen Wert eingegeben habe? 1649
Was mache ich, wenn die Agentenregistrierung fehlschlägt? 1650

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Registrierung war erfolgreich, aber woher weiß ich, ob der Agent ordnungsgemäß funktioniert? 1650

Wie kann ich Agenten über einen Proxy-Server mit NetScaler Console verbinden? 1650

Ich sehe meine Analysereports nicht 1651

Welche Versionen von NetScaler-Instanzen werden in NetScaler Console unterstützt? 1651

Wie exportiere ich Dashboard-Berichte in NetScaler Console? 1651

Was bewirkt die Aktivierung clientseitiger Messungen? 1652

Wird der SSL-Datenverkehr vom Agent zum NetScaler Console-Dienst einer SSL-Inspektion unterzogen? 1652

index 1653

Analysen 1653

Dashboards 1654

Dashboard für ausgehenden Datenverkehr 1654

Benutzer-Dashboard 1656

WAF Insight 1659

So funktioniert WAF Insight 1659

WAF Insight konfigurieren 1660

Geostandorte für Sicherheits-Insight-Berichte konfigurieren 1661

Schwellenwerte 1663

WAF Insight-Anwendungsfälle 1663

Lernprofil konfigurieren 1665

Details zu Netzwerkverstößen 1667

HTTP Slow Loris 1667

DNS Slow Loris 1668

HTTP Slow Post 1668

NXDOMAIN-Flood-Angriff 1669

HTTP-Desync-Angriff 1670

Bleichenbacher-Angriff 1671

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Segment-Smack-Angriff 1671
SYN-Flood-Angriff 1672
Small Window Attack 1673
Zusammenfassung der WAF-Lernaktionen anzeigen 1673
Fehlgeschlagene Regeln anzeigen 1674
Erweiterte Suche 1674
Ergebnisse filtern 1674
Entspannungsregeln, Leerlauf- und Ablehnungsregeln anzeigen 1675
Ablehnungsregeln verwalten 1676
SSL Insight 1677
Voraussetzungen 1678
SSL Insight konfigurieren 1678
Das Insight aktivieren 1678
ULFD-Modus aktivieren 1679
SSL Insight-Parameter aktivieren 1679
Anwendungsfall: Überblick über die SSL-Transaktionen erhalten 1680
Anwendungsfall: SSL-Metriken für Clients 1681
Analysen für Web-Transaktionen anzeigen 1681
Voraussetzungen 1682
Detaillierte Webtransaktionen 1682
Ereignisse anzeigen 1683
Spalten in der Ereignisliste hinzufügen 1685
Erweiterte Suche 1685
Suche speichern 1687
Daten exportieren 1688
Detaillierte Verfahren zur Einrichtung einer Dual-Tier- oder Service-Mesh-Lite-Topologie 1688
Einen NetScaler-Agent konfigurieren 1688
Statische Routen im Agenten konfigurieren 1689

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Beispiel-Bereitstellungsdateien von GitHub herunterladen 1690
Parameter in der CPX-YAML-Datei hinzufügen 1690
VPX- oder SDX- oder MPX- oder BLX-Instanz in NetScaler Console hinzufügen 1691
Kubernetes-Cluster in NetScaler Console hinzufügen 1692
Bereitstellen einer Beispiel-Microservice-Anwendung 1693
CPX bereitstellen und in NetScaler Console registrieren 1694
Automatische Auswahl virtueller Server für die Lizenzierung aktivieren 1694
Web-Transaktions- und TCP-Transaktionseinstellungen aktivieren 1694
Datenverkehr an Microservices senden 1695
Detaillierte Verfahren zum Einrichten der Service-Mesh-Topologie 1695
NetScaler-Agent konfigurieren 1695
Statische Routen im Agenten konfigurieren 1696
Erforderliche Parameter konfigurieren 1697
Beispielanwendung bereitstellen 1699
Kubernetes-Cluster in NetScaler Console hinzufügen 1701
Automatische Auswahl virtueller Server für die Lizenzierung aktivieren 1702
Web-Transaktions- und TCP-Transaktionseinstellungen aktivieren 1703
Datenverkehr an Microservices senden 1703
Detaillierte Verfahren zur Einrichtung einer einstufigen oder vereinheitlichten Ingress-Topologie 1704
VPX-, SDX-, MPX- oder BLX-Instanz in NetScaler Console hinzufügen 1704
Kubernetes-Cluster in NetScaler Console hinzufügen 1705
Datengovernance für das NetScaler®-Telemetrieprogramm 1706
Erforderliche Telemetriedaten 1707
So ändern Sie das Root-Passwort von NetScaler MPX und VPX 1708
Passwort ändern mit der Funktion **Konfigurationsaufträge** 1708
Schritt 1. Erstellen Sie eine **Konfigurationsvorlage** 1709
Konfigurationsauftrag erstellen 1709
Administratorprofil ändern 1710

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Vorherige Releases 1710
December 13, 2023 1711
Infrastruktur 1711
Lizenzierung 1711
Analysen 1712
Infrastruktur 1712
Behobene Probleme 1713
November 29, 2023 1714
Infrastruktur 1714
Behobene Probleme 1714
November 09, 2023 1715
Analysen 1715
Behobene Probleme 1715
October 25, 2023 1716
Analysen 1716
Infrastruktur 1717
Behobene Probleme 1717
October 10, 2023 1717
Verwaltung und Überwachung 1717
September 26, 2023 1718
Analysen 1718
Infrastruktur 1718
Behobene Probleme 1718
Analysen 1719
September 13, 2023 1719
Infrastruktur 1719
Behobene Probleme 1719
August 31, 2023 1720

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Infrastruktur 1720
- Sicherheit 1721
- Behobene Probleme 1721
- Verwaltung und Überwachung 1721

August 11, 2023 1721

- Verwaltung und Überwachung 1721

August 09, 2023 1722

- Infrastruktur 1722
- Sicherheit 1722
- Behobene Probleme 1722

July 26, 2023 1723

- Analysen 1723
- Infrastruktur 1724
- StyleBooks 1725

July 18, 2023 1725

- Verwaltung und Überwachung 1725

July 12, 2023 1726

- Behobene Probleme 1726

July 03, 2023 1726

- Analysen 1726
- Infrastruktur 1727
- Behobene Probleme 1727

June 14, 2023 1728

- Sicherheit 1728
- StyleBooks 1728
- Behobene Probleme 1728

May 31, 2023 1729

- Analysen 1729

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Behobene Probleme 1729
May 18, 2023 1730
Analysen 1730
Infrastruktur 1731
Behobene Probleme 1731
May 09, 2023 1732
Verwaltung und Überwachung 1732
April 25, 2023 1733
Analysen 1733
StyleBooks 1733
Behobene Probleme 1733
Analysen 1733
April 13, 2023 1734
Analysen 1734
Infrastruktur 1735
Behobene Probleme 1735
April 05, 2023 1736
Sicherheit 1736
Behobene Probleme 1736
March 14, 2023 1737
Behobene Probleme 1737
March 02, 2023 1737
Analysen 1737
Infrastruktur 1738
Verwaltung und Überwachung 1738
Sicherheit 1739
Analyse der Anwendungsleistung 1740
Sonstiges 1740

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Behobene Probleme 1740
February 07, 2023 1741
Analysen 1741
Verwaltung und Überwachung 1741
Behobene Probleme 1742
January 24, 2023 1742
Behobene Probleme 1742
January 10, 2023 1743
Verwaltung und Überwachung 1743
StyleBooks 1743
fix 1744

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Übersicht

Der NetScaler Console-Dienst (früher bekannt als NetScaler ADM-Dienst) ist eine webbasierte Lösung zur Verwaltung aller NetScaler-Bereitstellungen, die NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler CPX, NetScaler BLX und NetScaler Gateway umfassen, die lokal oder in der Cloud bereitgestellt werden.

Sie können diese Cloud-Lösung verwenden, um die gesamte globale Anwendungsbereitstellungsinfrastruktur von einer einzigen, einheitlichen und zentralisierten Cloud-basierten Konsole aus zu verwalten, zu überwachen und Fehler zu beheben. NetScaler Console bietet alle Funktionen, die erforderlich sind, um die Anwendungsbereitstellung in NetScaler-Bereitstellungen schnell einzurichten, bereitzustellen und zu verwalten, und bietet umfassende Analysen zur Anwendungszustand, -leistung und -sicherheit.

NetScaler Console bietet die folgenden Vorteile:

- **Agil** – Einfach zu bedienen, zu aktualisieren und zu nutzen. Das Dienstmodell von NetScaler Console ist über die Cloud verfügbar, wodurch die Bedienung, Aktualisierung und Nutzung der von NetScaler Console bereitgestellten Funktionen einfach ist. Die Häufigkeit der Updates, kombiniert mit der automatischen Update-Funktion, verbessert Ihre NetScaler-Bereitstellung schnell.
- **Schnellere Wertschöpfung** – Schnellere Erreichung von Geschäftszielen. Im Gegensatz zur traditionellen lokalen Bereitstellung können Sie Ihre NetScaler Console mit wenigen Klicks nutzen. Sie sparen nicht nur Installations- und Konfigurationszeit, sondern vermeiden auch Zeit- und Ressourcenverschwendung durch potenzielle Fehler.
- **Multi-Site-Management** – Eine einzige zentrale Ansicht für Instanzen über Multi-Site-Rechenzentren hinweg. Mit der NetScaler Console können Sie NetScaler in verschiedenen Bereitstellungstypen verwalten und überwachen. Sie haben eine zentrale Verwaltung für NetScaler, die lokal und in der Cloud bereitgestellt werden.
- **Betriebliche Effizienz** – Optimierte und automatisierte Methode zur Erzielung höherer betrieblicher Produktivität. Mit der NetScaler Console werden Ihre Betriebskosten gesenkt, indem Sie Zeit, Geld und Ressourcen für die Wartung und Aktualisierung traditioneller Hardware-Bereitstellungen sparen.
- **Transparenz des Echtzeit-Internetverkehrs** – Verbesserte Benutzererfahrung durch Echtzeit-Internetverkehrsanalyse. Mit der NetScaler Console können Sie Echtzeit-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benutzerüberwachungsdaten von Clients sammeln, während diese auf Anwendungen in Clouds, Rechenzentren und CDNs zugreifen, und ein ganzheitliches Bild der Internetgesundheit erstellen. Der Datenverkehr wird an Standorte mit der geringsten Latenz und besten Verfügbarkeit geleitet, um eine optimale Benutzererfahrung zu gewährleisten.

- **Multi-Site-Anwendungen** – Erstellen, konfigurieren und bereitstellen einer Anwendung an mehreren Standorten. Mit der NetScaler Console können Sie Anwendungen über mehrere Cloud-Umgebungen hinweg konfigurieren, bereitstellen und verwalten, um hohe Verfügbarkeit und Zuverlässigkeit zu gewährleisten.

So funktioniert NetScaler Console

NetScaler Console ist als Dienst in der Citrix Cloud verfügbar. Nachdem Sie sich für Citrix Cloud angemeldet und den Dienst genutzt haben, installieren Sie Agenten in Ihrer Netzwerkumgebung oder initiieren den integrierten Agenten in den Instanzen. Fügen Sie dann die Instanzen, die Sie verwalten möchten, dem Dienst hinzu.

Ein Agent ermöglicht die Kommunikation zwischen der NetScaler Console und den verwalteten Instanzen in Ihrem Rechenzentrum. Der Agent sammelt Daten von den verwalteten Instanzen in Ihrem Netzwerk und sendet sie an die NetScaler Console.

Wenn Sie eine Instanz zur NetScaler Console hinzufügen, fügt sie sich implizit als Trap-Ziel hinzu und erfasst ein Inventar der Instanz.

Der Dienst sammelt Instanzdetails wie:

- Hostname
- Softwareversion
- Aktive und gespeicherte Konfiguration
- Zertifikate
- Auf der Instanz konfigurierte Entitäten usw.

NetScaler Console fragt verwaltete Instanzen regelmäßig ab, um Informationen zu sammeln. Weitere Informationen finden Sie unter Daten-Governance.

Die folgende Abbildung veranschaulicht die Kommunikation zwischen dem Dienst, den Agents und den Instanzen (MPX, VPX, CPX, BLX):

Um NetScaler Console zu nutzen und zu sehen, wie es funktioniert, lesen Sie Erste Schritte und die zugehörigen Unterthemen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Funktionen und Lösungen

Dieses Dokument beschreibt die Funktionen, die auf der NetScaler Console unterstützt werden.

Anwendungsanalyse und -verwaltung

Die Funktion Anwendungsanalyse und -verwaltung der NetScaler Console stärkt den anwendungszentrierten Ansatz, um Ihnen bei der Bewältigung verschiedener Herausforderungen bei der Anwendungsbereitstellung zu helfen. Dieser Ansatz bietet Ihnen Einblick in die Integritätsbewertungen von Anwendungen, hilft Ihnen, Sicherheitsrisiken zu bestimmen, und hilft Ihnen, Anomalien in den Anwendungsdatenflüssen zu erkennen und Korrekturmaßnahmen zu ergreifen.

- Anwendungsleistungsanalyse: Der App Score ist das Ergebnis eines Bewertungssystems, das definiert, wie gut eine Anwendung funktioniert. Er zeigt, ob die Anwendung in Bezug auf die Reaktionsfähigkeit gut funktioniert, nicht anfällig für Bedrohungen ist und alle Systeme betriebsbereit sind.
- Anwendungssicherheitsanalyse: Das App Security Dashboard bietet einen ganzheitlichen Überblick über den Sicherheitsstatus Ihrer Anwendungen. Es zeigt beispielsweise wichtige Sicherheitsmetriken wie Sicherheitsverletzungen, Signaturverletzungen und Bedrohungsindizes an. Das App Security Dashboard zeigt auch angriffsbezogene Informationen wie SYN-Angriffe, Small-Window-Angriffe und DNS-Flood-Angriffe für die erkannten NetScaler-Instanzen an.
- Intelligente App-Analyse: Die Funktion Intelligente App-Analyse bietet eine einfache und skalierbare Lösung zur Überwachung und Fehlerbehebung von Anwendungen, die über NetScaler-Appliances bereitgestellt werden. Die Intelligente App-Analyse überwacht nicht nur alle Ebenen von Anwendungstransaktionen, sondern verwendet auch maschinelle Lerntechniken, um normale Datenverkehrsmuster in Ihrem Netzwerk zu definieren und Anomalien zu erkennen. Diese Funktion reduziert die Gesamtbearbeitungszeit und verbessert die gesamte Anwendungsverfügbarkeit.

StyleBooks

StyleBooks vereinfachen die Verwaltung komplexer NetScaler-Konfigurationen für Ihre Anwendungen. Ein StyleBook ist eine Vorlage, mit der Sie NetScaler-Konfigurationen erstellen und verwalten können. Sie können ein StyleBook zur Konfiguration einer bestimmten NetScaler-Funktion erstellen oder ein StyleBook entwerfen, um Konfigurationen für eine Unternehmensanwendungsbereitstellung wie Microsoft Exchange oder Skype for Business zu erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instanzverwaltung

Ermöglicht Ihnen die Verwaltung der NetScaler-, NetScaler Gateway- und Citrix Secure Web Gateway-Instanzen.

Ereignisverwaltung

Ereignisse stellen das Auftreten von Ereignissen oder Fehlern auf einer verwalteten NetScaler-Instanz dar. Wenn beispielsweise ein Systemausfall oder eine Konfigurationsänderung auftritt, wird ein Ereignis generiert und in der NetScaler Console aufgezeichnet. Im Folgenden sind die zugehörigen Funktionen aufgeführt, die Sie mit der NetScaler Console konfigurieren oder anzeigen können:

- Erstellen von Ereignisregeln
- Verwenden der NetScaler Console zum Exportieren von Syslog-Nachrichten

Zertifikatsverwaltung

NetScaler Console optimiert für Sie jeden Aspekt der Zertifikatsverwaltung. Über eine einzige Konsole können Sie automatisierte Richtlinien einrichten, um den richtigen Aussteller, die Schlüsselstärke und die korrekten Algorithmen sicherzustellen, während Sie gleichzeitig ungenutzte oder bald ablaufende Zertifikate genau im Auge behalten.

Konfigurationsverwaltung

Mit NetScaler Console können Sie Konfigurationsaufträge erstellen, die Ihnen helfen, Konfigurationsaufgaben wie das Erstellen von Entitäten, das Konfigurieren von Funktionen, die Replikation von Konfigurationsänderungen, System-Upgrades und andere Wartungsaktivitäten auf mehreren Instanzen problemlos durchzuführen. Konfigurationsaufträge und -vorlagen vereinfachen die repetitivsten Verwaltungsaufgaben zu einer einzigen Aufgabe in NetScaler Console.

Konfigurationsprüfung

Ermöglicht Ihnen, Anomalien in den Konfigurationen Ihrer Instanzen zu überwachen und zu identifizieren.

- Konfigurationsberatung: Ermöglicht Ihnen, Konfigurationsanomalien zu identifizieren.
- Prüfvorlage: Ermöglicht Ihnen, die Änderungen über eine bestimmte Konfiguration hinweg zu überwachen.

Lizenzverwaltung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ermöglicht Ihnen die Verwaltung von NetScaler-Lizenzen, indem Sie NetScaler Console als Lizenzmanager konfigurieren.

- NetScaler-Poolkapazität: Ein gemeinsamer Lizenzpool, aus dem Ihre NetScaler-Instanz eine Instanzlizenz und nur so viel Bandbreite entnehmen kann, wie sie benötigt. Wenn die Instanz diese Ressourcen nicht mehr benötigt, gibt sie diese an den gemeinsamen Pool zurück, wodurch die Ressourcen anderen Instanzen zur Verfügung stehen, die sie benötigen.
- NetScaler VPX Check-in- und Check-out-Lizenzierung: NetScaler Console weist NetScaler VPX-Instanzen bei Bedarf Lizenzen zu. Eine NetScaler VPX-Instanz kann die Lizenz von der NetScaler Console entnehmen, wenn eine NetScaler VPX-Instanz bereitgestellt wird, oder ihre Lizenz an die NetScaler Console zurückgeben, wenn eine Instanz entfernt oder zerstört wird.

Netzwerkberichterstattung

Sie können die Ressourcennutzung optimieren, indem Sie Ihre Netzwerkberichterstattung in NetScaler Console überwachen.

Analysen

Bietet eine einfache und skalierbare Möglichkeit, die verschiedenen Einblicke in die Daten der NetScaler-Instanzen zu untersuchen, um die Anwendungsleistung zu beschreiben, vorherzusagen und zu verbessern. Sie können eine oder mehrere Analysefunktionen gleichzeitig verwenden.

- HDX Insight: Bietet End-to-End-Transparenz für den ICA-Datenverkehr, der NetScaler durchläuft. HDX Insight ermöglicht Administratoren die Anzeige von Echtzeit-Client- und Netzwerklatenzmetriken, historischen Berichten, End-to-End-Leistungsdaten und die Behebung von Leistungsproblemen.
- Web Insight: Bietet Transparenz für Unternehmens-Webanwendungen. Es ermöglicht IT-Administratoren, alle von NetScaler bereitgestellten Webanwendungen durch integrierte Echtzeitüberwachung von Anwendungen zu überwachen. Web Insight verarbeitet Daten von NetScaler mithilfe eines Approximationsalgorithmus. Es liefert die Top 1.000 Datensätze der Metriken, die sich auf die Webanwendungen in Ihrem Unternehmen beziehen.
- Gateway Insight: Bietet Einblick in die Fehler, die Benutzer beim Anmelden erfahren, unabhängig vom Zugriffsmodus. Sie können eine Liste der zu einem bestimmten Zeitpunkt angemeldeten Benutzer zusammen mit der Anzahl der aktiven Benutzer, der Anzahl der aktiven Sitzungen und der von allen Benutzern zu einem beliebigen Zeitpunkt verwendeten Bytes und Lizenzen anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Security Insight: Bietet eine Single-Pane-Lösung, die Ihnen hilft, den Sicherheitsstatus Ihrer Anwendungen zu bewerten und Korrekturmaßnahmen zur Sicherung Ihrer Anwendungen zu ergreifen.
- SSL Insight: Bietet Transparenz für sichere Transaktionen im Web (HTTPS). Es ermöglicht IT-Administratoren, alle von NetScaler bereitgestellten Webanwendungen durch integrierte Echtzeit- und historische Überwachung von Webtransaktionen zu überwachen. SSL Insight verarbeitet Daten von NetScaler mithilfe eines Approximationsalgorithmus. Es liefert die Top 1.000 Datensätze der Metriken, die sich auf die Webtransaktionen in Ihrem Unternehmen beziehen.

Rollenbasierte Zugriffssteuerung

Die rollenbasierte Zugriffssteuerung (RBAC) ermöglicht es Ihnen, Zugriffsberechtigungen basierend auf den Rollen einzelner Benutzer in Ihrem Unternehmen zu erteilen. Der erste Benutzer einer Organisation, der sich mit Citrix Cloud™-Anmeldeinformationen anmeldet, hat die Super-Admin-Rolle, die standardmäßig alle Zugriffsberechtigungen besitzt. Den anderen Benutzern dieser Organisation, die später vom Administrator erstellt werden, werden Nicht-Admin-Rollen zugewiesen.

Abonnements

Bietet eine Dashboard-Ansicht der von Ihnen erworbenen Abonnements.

Sie werden standardmäßig einem Express-Konto zugewiesen. Mit diesem Konto können Sie begrenzte NetScaler Console-Ressourcen verwalten. Weitere Informationen finden Sie unter NetScaler Console-Ressourcen mit Express-Konto verwalten.

Die folgenden NetScaler Console-Funktionen sind derzeit nicht verfügbar:

- Bereitstellung
  - Migration von Citrix Insight Center zu NetScaler Console
  - Integration von NetScaler Console mit Citrix Virtual Desktop Director
- Analysen: TCP Insight und Video Insight
- Eingeschränkte Systemeinstellungen
- Orchestrierung
  - Integration mit OpenStack und VMware NSX Manager
  - NetScaler-Automatisierung im Hybridmodus von Cisco ACI

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Container-Orchestrierung: Integration mit Mesos/Marathon und Kubernetes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Versionshinweise

Die Versionshinweise zur NetScaler Console (früher bekannt als NetScaler ADM Service) beschreiben die neuen Funktionen, Verbesserungen an bestehenden Funktionen, behobene Probleme und bekannte Probleme, die in einem Service-Release verfügbar sind.

Weitere Informationen finden Sie unter:

- Neuerungen
- Frühere Versionen

Die NetScaler-Agenten werden standardmäßig automatisch auf die neueste Version der NetScaler Console aktualisiert. Sie können die Agentendetails auf der Seite **Infrastruktur > Instanzen > Agenten** anzeigen. Sie können auch den Zeitpunkt festlegen, zu dem die Agenten-Upgrades erfolgen sollen. Weitere Informationen finden Sie unter Konfigurieren der Agenten-Upgrade-Einstellungen.

Was ist neu

September 27, 2026

Verwaltung und Überwachung

Unterstützung bei der Identifizierung und Behebung von CVE-2026-88771

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2026-88771.

- Die Identifizierung für CVE-2026-88771 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-88771 beheben.

  HINWEIS:

  Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Jobs zum Upgrade von NetScaler-Instanzen verwenden.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

Unterstützung bei der Identifizierung und Behebung von CVE-2026-88772

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2026-88772.

- Die Identifizierung für CVE-2026-88772 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-88772 beheben.

  HINWEIS:

  Der Sicherheitshinweis unterstützt keine NetScaler-Builds, die das Ende der Lebensdauer (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

Unterstützung für die Identifizierung und Behebung von CVE-2026-88773

Der Sicherheitshinweis des NetScaler Console-Dienstes unterstützt jetzt die Identifizierung und Behebung von CVE-2026-88773.

- Die Identifizierung für CVE-2026-88773 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der die Korrektur enthält. Weitere Informationen finden Sie unter CVE-2026-88773 beheben.

  HINWEIS:

  Der Sicherheitshinweis unterstützt keine NetScaler-Builds, die das Ende der Lebensdauer (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

Unterstützung für die Identifizierung und Behebung von CVE-2026-88774

Der Sicherheitshinweis des NetScaler Console-Dienstes unterstützt jetzt die Identifizierung und Behebung von CVE-2026-88774.

- Die Identifizierung für CVE-2026-88774 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der die Korrektur enthält. Weitere Informationen finden Sie unter CVE-2026-88774 beheben.

  HINWEIS:

  Das Sicherheitsbulletin unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, ein Upgrade auf die von NetScaler unterstützten Builds oder Versionen durchzuführen.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

Unterstützung für die Identifizierung und Behebung von CVE-2026-88775

Das Sicherheitsbulletin des NetScaler Console-Dienstes unterstützt jetzt die Identifizierung und Behebung von CVE-2026-88775.

- Die Identifizierung für CVE-2026-88775 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-88775 beheben.

  HINWEIS:

  Das Sicherheitsbulletin unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, ein Upgrade auf die von NetScaler unterstützten Builds oder Versionen durchzuführen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

Unterstützung für die Identifizierung und Behebung von CVE-2026-88776

Das Sicherheitsbulletin des NetScaler Console-Dienstes unterstützt jetzt die Identifizierung und Behebung von CVE-2026-88776.

- Die Identifizierung für CVE-2026-88776 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-88776 beheben.

  HINWEIS:

  Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Jobs zum Upgrade von NetScaler-Instanzen verwenden.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

Unterstützung für die Identifizierung und Behebung von CVE-2026-88777

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2026-88777.

- Die Identifizierung für CVE-2026-88777 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-88777 beheben.

  HINWEIS:

  Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Jobs zum Upgrade von NetScaler-Instanzen verwenden.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

Unterstützung für die Identifizierung und Behebung von CVE-2026-88778

Der NetScaler Console Service-Sicherheitshinweis unterstützt jetzt die Identifizierung und Behebung von CVE-2026-88778.

- Die Identifizierung für CVE-2026-88778 erfordert einen Versionsscan, und die Behebung erfordert einen zweistufigen Prozess:

  a. Aktualisieren Sie die anfällige NetScaler-Instanz auf eine Version und einen Build, der den Fix enthält.

  b. Konfigurationsaufträge anwenden.

  Weitere Informationen finden Sie unter CVE-2026-88778 beheben.

  HINWEIS:

  Der Sicherheitshinweis unterstützt keine NetScaler-Builds, die das Ende der Lebensdauer (EOL) erreicht haben. Wir empfehlen Ihnen, ein Upgrade auf die von NetScaler unterstützten Builds oder Versionen durchzuführen.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

September 15, 2026

Behobene Probleme

Analysen

In einigen Fällen können die für eine Anwendung in NetScaler Console angezeigten Bandbreiten- und Volumen-Gesamtwerte zu niedrig ausgewiesen werden, wenn ein Metrik-Update von NetScaler erneut gesendet wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastruktur

Mit Cloud Connect schlägt das Abrufen der Lizenzberechtigungen fehl, wenn die auf NetScaler Console On-Premises konfigurierte Kunden-ID nicht mit der Groß-/Kleinschreibung der Kunden-ID im NetScaler Console Service übereinstimmt.

In einem NetScaler HA-Setup, das vom integrierten Console-Agent verwaltet wird, kann der integrierte Agent auf dem sekundären Knoten nicht starten, wenn dieser NetScaler eine ältere Build-Version ausführt. Wenn ein Failover auftritt, kann das HA-Paar in NetScaler Console als „Down“ angezeigt werden.

September 01, 2026

Neuigkeiten

Verwaltung und Überwachung

- **Sichtbarkeit der Zertifikatsquelle und Schutz gebundener Zertifikate**

  Zertifikatsdateien zeigen jetzt ihre Quelle an, wodurch Administratoren unterscheiden können zwischen:

  - **Lokal**: Zertifikate, die lokal auf NetScaler installiert sind (einschließlich direkt oder über den Zertifikatsspeicher installierter Zertifikate).
  - **Remote**: Zertifikate, die über Zero Touch Certificate Management (ZTCM) verwaltet und abgerufen werden.

  Diese Verbesserung bietet eine bessere Sichtbarkeit des Zertifikatsursprungs und der Verwaltungsworkflows.

  Gebundener Statusindikator ist ein neuer Statusindikator im Zertifikatsbestand, der Zertifikate identifiziert, die derzeit an SSL-Konfigurationen gebunden und aktiv verwendet werden. Diese Verbesserung gibt Administratoren einen klaren Überblick über die Zertifikatsabhängigkeiten, bevor sie Lebenszyklusoperationen durchführen.

  Sicheres Löschen ermöglicht Administratoren das direkte Löschen von Zertifikatsdateien aus dem Zertifikatsbestand. Um Dienstunterbrechungen zu vermeiden, ist das Löschen nur auf ungebundene Zertifikate beschränkt. Sie können keine Zertifikate löschen, die aktiv an SSL-Entitäten gebunden oder von Zertifikat-Workflows verwaltet werden, bis Sie die Bindung aufheben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Vereinheitlichte Zertifikatsquellenerfahrung und Vorabprüfungen für den Zertifikatsimport für SSL-Zertifikate**

  Die NetScaler Console bietet jetzt eine vereinheitlichte Zertifikatsauswahl, indem Zertifikatsdateien aus verschiedenen Quellen in einer einzigen Ansicht zusammengeführt werden. Zuvor mussten Administratoren zwischen separaten Optionen wie **Dateien auf NetScaler** und **Dateien auf Console** wählen. Mit dieser Verbesserung werden Zertifikatsdateien über einen einzigen, konsolidierten Workflow präsentiert, was die Zertifikatsverwaltung und -auswahl vereinfacht. Zusätzlich wurde die Option zum Hochladen von Zertifikaten aus diesem Workflow entfernt, um die Benutzerfreundlichkeit zu optimieren und die Komplexität der Quellenauswahl zu reduzieren.

  Die NetScaler Console führt außerdem Vorabprüfungen durch, bevor SSL-Zertifikate und -Schlüssel über NetScaler-Instanzen hinweg importiert werden, um unbeabsichtigte Dateikonflikte und Zertifikatsüberschreibungen zu verhindern.

  Die folgenden sind die wichtigsten Verbesserungen, die mit dieser Funktion verbunden sind:

  - **Erkennung doppelter Dateien**: Vor der Installation prüft das System, ob der Zertifikats- oder Schlüsseldateiname bereits auf der Ziel-NetScaler-Instanz vorhanden ist. Ziele mit widersprüchlichen Dateinamen werden vor der Bereitstellung identifiziert und gekennzeichnet.
  - **Überschreibungsschutz**: Zertifikatsimporte überschreiben keine vorhandenen Zertifikats- oder Schlüsseldateien mehr. Wird ein Konflikt erkannt, wird der Import blockiert, und der Administrator muss den Konflikt durch Verwendung eines anderen Dateinamens oder Entfernen des Duplikats beheben.
  - **Validierung pro Ziel**: Bei Massenimporten von Zertifikaten wird jede Zielinstanz unabhängig voneinander bewertet. Administratoren können sehen, welche Ziele für die Installation geeignet oder ungeeignet sind, und nur mit den gültigen Zielen fortfahren.
  - **Backend-Sicherheitsvalidierung**: Während der Installation wird eine zusätzliche Validierung durchgeführt, um sicherzustellen, dass sich die Eignung des Ziels nicht geändert hat. Zertifikate werden nur auf Instanzen installiert, die die abschließenden Validierungsprüfungen erfolgreich bestehen.

  Die folgenden sind die Vorteile dieser Verbesserung:

  - Verhindert das versehentliche Überschreiben vorhandener Zertifikate und privater Schlüssel.
  - Reduziert das Risiko von Unterbrechungen der Zertifikatskette durch Dateiersetzung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Verbessert die Transparenz der Bereitstellungsbereitschaft über mehrere NetScaler-Instanzen hinweg.
- Bietet eine sicherere und vorhersehbarere Erfahrung bei der Zertifikatsbereitstellung.

Behobene Probleme

Analysen

E-Mail-Benachrichtigungen bei Web App Firewall- und BOT-Schwellenwertüberschreitungen werden nicht gesendet, weil der Job die falsche IP-Adressspalte liest, die immer leer ist.

Der NetScaler Console Analytics-Scheduler überträgt die Konfigurationseinstellungen wiederholt an NetScaler-Instanzen, selbst wenn die Konfiguration beim ersten Push erfolgreich angewendet wurde. Dieses Problem löst falsche Fehlermeldungen aus, obwohl alles ordnungsgemäß funktioniert.

NetScaler Console-Überwachungsprotokolle erreichen Microsoft Sentinel möglicherweise nicht, wenn sie an einen nicht deklarierten Stream anstelle des dokumentierten `console_syslog_messages_CL` gesendet werden, was dazu führt, dass Azure jede Charge ablehnt.

Infrastruktur

Benutzer können WAF-Empfehlungen auf NetScaler nicht anwenden, wenn die Option **Anmeldeinformationen für Stylebook-Vorgänge anfordern** aktiviert ist.

In Azure-Umgebungen können SNMPv3-Traps, die von NetScaler an den NetScaler Console Cloud-Agent gesendet werden, mit einem Authentifizierungsfehler "Unbekannter Benutzername" fehlschlagen.

NetScaler Console sendet falsche Schwachstellenbenachrichtigungen, wenn keine verwaltete NetScaler-Instanz für den Dateiintegritätsüberwachungs-Scan qualifiziert ist, und die Slack-Benachrichtigungen für diese Scans sind leer, ohne Scan-Details.

Der NetScaler Console-Agent leitet den Datenverkehr möglicherweise nicht über einen konfigurierten Proxy weiter, was zu Konnektivitätsproblemen zwischen dem Agenten und NetScaler Console führt.

GSLB-Virtual-Server-Einträge werden möglicherweise nicht in der Virtual-Server-Liste in NetScaler Console angezeigt, wenn eine GSLB-Site-Gruppe konfiguriert ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console zeigt aufgrund einer Durchsatzratenbegrenzung fälschlicherweise Paketverluste an.

Während einer Konfigurationsüberprüfung (Config Audit Poll) ausgewählter Instanzen löschte NetScaler Console die zwischengespeicherte Instanzkonfiguration, bevor sie deren Ersatz herunterlud. Infolgedessen blieb die Konfiguration während des gesamten Abfragezeitraums nicht verfügbar. Im Falle eines Abfragefehlers blieb die Konfiguration bis zum nächsten erfolgreichen Durchlauf nicht verfügbar.

Während der `mastools` Registrierung auf Azure-Geräten protokolliert NetScaler Console einen Fehler im `mastools_reg.py` Protokoll. Dieser Fehler blockiert jedoch nicht die mastools-Registrierung für Azure-Geräte.

August 19, 2026

Verwaltung und Überwachung

Unterstützung bei der Identifizierung und Behebung von CVE-2026-19489

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2026-19489.

- Die Identifizierung für CVE-2026-19489 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-19489 beheben.

  HINWEIS:

  Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Aufträge zum Upgrade von NetScaler-Instanzen verwenden.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

Unterstützung für die Identifizierung und Behebung von CVE-2026-19490

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2026-19490.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die Identifizierung für CVE-2026-19490 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-19490 beheben.

  HINWEIS:

  Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Aufträge zum Upgrade von NetScaler-Instanzen verwenden.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

August 04, 2026

Neuerungen

Verwaltung und Überwachung

- **Unterstützung der Dateiintegritätsüberwachung für die Linux-basierte NetScaler VPX-Plattform**

  Die Funktion zur Dateiintegritätsüberwachung wird jetzt für NetScaler VPX-Instanzen auf Linux-Plattformen unterstützt. Mit dieser Funktion können Sie unautorisierte Datei- und Konfigurationsänderungen leicht erkennen.

Behobene Probleme

Analysen

Die auf der NetScaler Console konfigurierten Web Application Firewall- und BOT-Richtlinien verschwinden nach einigen Tagen und erscheinen erst wieder, nachdem die Richtlinie manuell bearbeitet oder umgeschaltet wurde.

Infrastruktur

Wenn der Infoblox DNS-Anbieter für die DNS-01-Domänenvalidierung in NetScaler Console verwendet wird, schlagen die ACME-Zertifikatsausstellung und -erneuerung während der Domänenvalidierung fehl.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Auf der Seite **Zero-Touch-Zertifikatsverwaltung** in NetScaler Console kann die Umstellung von **Benutzerdefinierte Synchronisierung** auf **Globale Synchronisierung** fehlschlagen. Die Instanz bleibt in der benutzerdefinierten Synchronisierung.

Der Versuch, ein SSL-Zertifikat vom SSL-Dashboard herunterzuladen, schlägt mit einem `404 - File not found error` fehl, selbst wenn das Zertifikat auf NetScaler® vorhanden ist und seine Details in NetScaler Console sichtbar sind. Dieses Problem betrifft insbesondere Zertifikate, die in Unterverzeichnissen unter `/nsconfig/ssl/` gespeichert sind.

NetScaler Console meldet den Agenten als „Down“, wenn ein Inventar-Core-Dump auftritt.

July 14, 2026

Neuerungen

Verwaltung und Überwachung

- **GeoIP-Datenbanksynchronisierung für NetScaler Console und Agents**

  Der NetScaler Console-Dienst unterstützt jetzt die zentralisierte GeoIP-Datenbanksynchronisierung für NetScaler Console, bereitgestellte Agents und verwaltete Instanzen über einen einzigen Workflow. Zuvor war die Synchronisierung nur auf NetScaler-Instanzen beschränkt.

  Die GeoIP-Synchronisierungsfunktion umfasst die folgenden Funktionen:

  - **Vereinheitlichte Synchronisierung**: Synchronisieren Sie eine GeoIP-Datenbankdatei in einem einzigen Vorgang mit der NetScaler Console, Agents und Instanzen.
  - **Jetzt synchronisieren**: Die Option „Jetzt synchronisieren“ unterstützt zwei Modi:
    - **Alle synchronisieren**: Die Datei wird automatisch an alle Entitäten übertragen, z. B. verwaltete NetScaler-Instanzen, NetScaler Console und Agents.
    - **Anpassen**: Wählen Sie bestimmte Console-Agents aus.
  - **Geplante Synchronisierung**: Erstellen Sie einmalige oder wiederkehrende Synchronisierungszeitpläne, die auf eine beliebige Kombination von Entitätstypen abzielen.
  - **Historische Jobprotokolle**: Zeigen Sie ein mit Zeitstempel versehenes Protokoll vergangener Synchronisierungsaufträge an, das den Umfang, die verwendete Datei und die Ergebnisse pro Gerät (Status, Startzeit und Endzeit) detailliert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Entitätsbezogener Synchronisierungsstatus**: Greifen Sie auf ein erweiterbares Panel auf der Hauptseite zu, um die Synchronisierungsergebnisse pro Gerät anzuzeigen, filterbar nach Status, IP-Adresse, Entitätstyp oder Version.
- **Letzte Synchronisierungsübersicht**: Bewerten Sie schnell den Synchronisierungszustand mit einer auf einen Blick erfassbaren Zusammenfassung, die die insgesamt ausgewählten Entitäten zusammen mit ausstehenden, laufenden, erfolgreichen, fehlgeschlagenen und gesamten Abschlussquoten anzeigt.

Telemetrie

- **Unterstützung für Telemetrie-Diagnosen**

  Der NetScaler Console-Dienst unterstützt jetzt Telemetrie-Diagnosen, um Administratoren dabei zu helfen, Probleme bei der Telemetrie-Erfassung und dem Upload über verwaltete NetScaler-Instanzen hinweg schnell zu identifizieren und zu beheben. Diese Funktion bietet detaillierte Telemetrie-Einblicke, Statusübersichten auf Geräte- und Agenten-Ebene, Fehlercodes mit Anleitungen zur Fehlerbehebung und Live-Konnektivitätsvalidierungsprüfungen.

  Administratoren können jetzt leicht feststellen, ob Telemetrie-Upload-Fehler durch Geräteerreichbarkeit, SSH-Konnektivität, Agentenkommunikation, Telemetrie-Paketprobleme oder Dienstkonnektivitätsprobleme verursacht werden, wodurch die Fehlerbehebungszeit verkürzt und die Telemetrieabdeckung verbessert wird.

  Einige der Vorteile sind:

  - Telemetrie-Status für verwaltete NetScaler-Instanzen anzeigen.
  - Zugriff auf detaillierte Fehlerdiagnosen mit Fehlercodes und Anleitungen zur Fehlerbehebung.
  - Überwachung des Telemetrie-Zustands des Agenten und Details zur Paketausführung.
  - Durchführen von Live-Konnektivitätsprüfungen für Telemetrie-bezogene Endpunkte und Dienste.

Behobene Probleme

Analysen

Nach der Migration von NetScaler Console On-Premises in die Cloud werden detaillierte Webtransaktionsdatensätze für den betroffenen NetScaler nicht angezeigt, während andere

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analysen, wie Metriken und Bot-Daten, weiterhin normal erscheinen. Dieses Problem trat auf, weil der erforderliche Speicher für diese Transaktionen für migrierte Mandanten nicht vollständig bereitgestellt wurde.

Infrastruktur

NetScaler Console aktiviert regelmäßig LAS auf NetScaler-Instanzen, was Dateien unter /nsconfig/license/ während Token-Aktualisierungen ändert und zu falsch-positiven „Diff Exists“-Warnungen in Config Audit File Diff führt.

NetScaler Console Cloud-Agenten generieren Ereignisprotokolle, die die Quell-IP-Adresse nicht enthalten. Das Quellfeld für diese Ereignisse erscheint leer, anstatt die IP-Adresse des Agenten oder Geräts anzuzeigen, das das Ereignis initiiert hat.

Das Herunterladen von SSL-Zertifikaten, bei denen der Zertifikatsname mit zwei hexadezimalen Zeichen beginnt (zum Beispiel de, ab, ce oder 25), über das NetScaler Console SSL Dashboard schlägt mit dem Fehler „404 – Datei nicht gefunden“ fehl. Dieses Problem tritt auch dann auf, wenn das SSL-Zertifikat auf NetScaler vorhanden ist und seine Details in NetScaler Console sichtbar sind.

Es kann ein „invalid resource“-Fehler auftreten, wenn Sie Benutzergruppen unter Benutzer und Rollen im NetScaler Console-Dienst bearbeiten.

Verschiedenes

In seltenen Szenarien kann NetScaler Console keine Verbindung zu NetScaler über den Agenten herstellen. Infolgedessen kann NetScaler aufgrund falscher Datenbankaktualisierungen in einem Grace-Zustand gemeldet werden.

June 30, 2026

Verwaltung und Überwachung

Unterstützung für die Identifizierung und Behebung von CVE-2026-8451

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2026-8451.

- Die Identifizierung für CVE-2026-8451 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-8451 beheben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Aufträge zum Upgrade von NetScaler-Instanzen verwenden.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

Unterstützung für die Identifizierung und Behebung von CVE-2026-8452

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2026-8452.

- Die Identifizierung für CVE-2026-8452 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-8452 beheben.

HINWEIS:

Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Aufträge zum Upgrade von NetScaler-Instanzen verwenden.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

Unterstützung für die Identifizierung und Behebung von CVE-2026-8655

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2026-8655.

- Die Identifizierung für CVE-2026-8655 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-8655 beheben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

Unterstützung für die Identifizierung und Behebung von CVE-2026-10816

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2026-10816.

- Die Identifizierung für CVE-2026-10816 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-10816 beheben.

HINWEIS:

Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

Unterstützung bei der Identifizierung und Behebung von CVE-2026-10817

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2026-10817.

- Die Identifizierung für CVE-2026-10817 erfordert einen Versionsscan. Zur Behebung ist ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build erforderlich, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-10817 beheben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Der Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

June 17, 2026

Behobene Probleme

Analysen

Wenn Sie BOT Insight auf einem virtuellen Server aktivieren, aber keine Metriken aktivieren, verarbeitet NetScaler Console die BOT-Verletzungen nicht. Dieses Problem tritt auf, weil die Verarbeitung der BOT-Verletzungen von der Aktivierung der Metriken abhängt.

Auf der Seite **Analytics** sehen Benutzer möglicherweise andere Instanzen zusätzlich zu den spezifischen Instanzen, die für den Zugriff basierend auf der für diesen bestimmten Benutzer definierten Benutzer-, Rollen-, Gruppen- und Zugriffsrichtlinie autorisiert wurden.

Infrastruktur

Benutzer können WAF-Empfehlungen auf NetScaler nicht anwenden, wenn die Option **Anmeldeinformationen für Stylebook-Operationen anfordern** aktiviert ist.

In seltenen Fällen tritt ein Fehler auf, wenn Sie versuchen, eine Sicherungsdatei aufzurufen oder herunterzuladen, die ursprünglich mit einer Größe in KB generiert wurde.

Wenn sich ein Microsoft Entra ID (Azure AD)-Benutzer beim NetScaler Console-Dienst unter einem bereits integrierten Citrix Cloud-Mandanten anmeldet, wird dem Benutzer die Standardrolle `adminExceptSystem` zugewiesen, anstelle der Rolle, die seiner Microsoft Entra ID-Gruppe zugeordnet ist. Infolgedessen erhalten betroffene Benutzer umfassendere Berechtigungen als beabsichtigt.

Der NetScaler Console-Agent stürzt ab, wenn ein Cloud-Anbieter ein überdimensioniertes Zertifikat präsentiert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GoDaddy CA wird im NetScaler Console-Dienst nicht unterstützt.

Lizenzierung

Wenn eine NetScaler-Instanz gelöscht und erneut hinzugefügt wird, nimmt NetScaler Console die LAS-Lizenzierung für die NetScaler-Instanz nicht automatisch wieder auf.

NetScaler Console lehnt den Erweiterungs-Blob ab, wenn die Host-ID im Erweiterungs-Blob nicht exakt (Groß-/Kleinschreibung beachten) mit der NetScaler Console GUI-Host-ID übereinstimmt.

Wenn eine gepoolte Lizenz Berechtigungen mit unterschiedlichen Subscription Advantage (SA)-Daten enthält, sendet NetScaler Console wiederholt E-Mails mit Lizenzablaufwarnungen (etwa alle paar Sekunden), anstatt eine einzelne Benachrichtigung pro Ablaufwarnung zu senden.

June 03, 2026

Behobene Probleme

Infrastruktur

Upgrades von NetScaler BLX-Instanzen, die über NetScaler Console initiiert wurden, schlagen fehl, selbst wenn die NetScaler BLX-Instanzen aktiv und betriebsbereit sind. Dieses Problem tritt auf, weil die Vor-Upgrade-Prüfung die Instanzen fälschlicherweise als nicht erreichbar meldet, was das erfolgreiche Upgrade verhindert.

Auf der Seite **NetScaler Console Security Advisory** zeigt die CVE-Erkennung eine CVE-Anzahl für jede Instanz an, aber das Klicken auf die CVE-Anzahl lädt die Details nicht.

Im SSL-Dashboard kann das Ausstellen eines ACME-Wildcard-Zertifikats fehlschlagen.

Lizenzierung

Im gepoolten Lizenzierungsmodus wird für NetScaler SDX-Geräte nur die Platinum Edition zugewiesen. Standard- und Advanced-Editionen werden nicht zugewiesen, selbst wenn Werte angegeben werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

May 19, 2026

Verwaltung und Überwachung

Unterstützung für die Verwaltung von Konflikten bei doppelten Zertifikaten

NetScaler unterstützt jetzt die Vermeidung von Konflikten, die durch doppelte Zertifikatsnamen und -inhalte während der Installations- und Aktualisierungsprozesse verursacht werden. Die Verwaltung doppelter Zertifikatsnamen oder -inhalte ist unerlässlich, wenn Sie Zertifikate installieren oder aktualisieren, da diese Duplikate zu Konfigurationskonflikten führen können. Diese Funktion stellt sicher, dass das System ein sauberes und eindeutiges Zertifikats-Repository verwaltet, was administrative Aufgaben vereinfacht und die Systemzuverlässigkeit erhöht.

Serverzertifikate ohne Zwischen-Uploads aktualisieren

Sie können Zertifikate jetzt erneuern, ohne die sich wiederholende Aufgabe des erneuten Hochladens von Zwischenzertifikaten. Diese Verbesserung reduziert den manuellen Arbeitsaufwand und minimiert das Risiko von Konfigurationsfehlern.

MÜHELOSE VERLÄNGERUNGEN

NetScaler Console bewahrt Ihre vorhandene Zertifikatskette während eines Updates standardmäßig auf. Dies stellt sicher, dass Ihre Kette intakt und gültig bleibt, selbst wenn Sie nur ein neues Serverzertifikat hochladen.

WICHTIGE VERBESSERUNGEN

- Reduzierte Komplexität: Eliminiert obligatorische Zwischen-Uploads bei Standard-Serverzertifikatsaktualisierungen.
- Sicherheit zuerst: Die automatische Kettenkonservierung verhindert „Kettenbrüche“, eine häufige Ursache für SSL-Handshake-Fehler.

NEUE PARAMETER

Die folgenden Parameter bieten eine explizite Kontrolle, wenn Ihre Anforderungen über eine einfache Verlängerung hinausgehen:

PARAMETER	FUNKTION
Vorhandene Zertifikatskette überschreiben	Verwenden Sie dies, um die aktuelle Kette zu ersetzen oder zu entfernen. Mit einem Bundle: Ersetzt die vorhandene Kette durch die neu hochgeladene Kette. Ohne ein Bundle: Entfernt die aktuelle Kette.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	FUNKTION
Zertifikatskette hinzufügen	Wählen Sie diese Option, um Zwischenzertifikate manuell hochzuladen und anzuhängen, falls diese nicht in Ihrer primären Serverzertifikatsdatei enthalten sind.

Informationen zum Aktualisieren von Serverzertifikaten ohne Zwischen-Uploads finden Sie unter Verwenden des NetScaler Console-Zertifikatsspeichers zur Verwaltung von SSL-Zertifikaten.

Unterstützung für benutzerdefinierte SNMP-Traps

Der NetScaler Console-Dienst unterstützt jetzt benutzerdefinierte SNMP-Traps. Sie können die benutzerdefinierten SNMP-Traps unter **Ereignismeldungen** anzeigen, wo sie als benutzerdefiniert gekennzeichnet sind, um sie von den Standard-SNMP-Warnungen zu unterscheiden.

Verwandtes Thema: Ereignisse.

Upgrade-Aufträge: Warnung bei doppeltem Upgrade-Auftragszeitplan

Im Rahmen des Upgrade-Auftragsworkflows zeigt NetScaler Console eine Warnmeldung an, wenn ein Kunde versucht, einen Upgrade-Auftrag für NetScaler-Instanzen zu erstellen, für die bereits ein Upgrade-Auftrag geplant ist. Diese Warnmeldung hilft, das unbeabsichtigte Planen doppelter Upgrade-Aufträge auf derselben NetScaler-Instanz zu verhindern. Diese Verbesserung gewährleistet eine bessere Kontrolle über Upgrade-Aufträge und vermeidet potenzielle Konflikte während Upgrades.

Verwandtes Thema: Upgrade-Aufträge.

Unterstützung für zusätzliche Zertifizierungsstellen und DNS-Anbieter für die ACME-basierte automatisierte Zertifikatserneuerung

Die NetScaler Console ACME-Integration (Automated Certificate Management Environment) für die automatisierte Zertifikatserneuerung unterstützt jetzt weitere Zertifizierungsstellen (CAs) und DNS-Anbieter. Wenn Sie eine der unterstützten CAs oder DNS-Anbieter verwenden, können Sie die ACME-Integration für eine nahtlose Zertifikatsverwaltung nutzen.

Eine vollständige Liste der unterstützten Zertifizierungsstellen (CAs) und DNS-Anbieter finden Sie unter Automatisierte Zertifikatserneuerung mit dem ACME-Protokoll.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dashboard zur Dateiintegritätsüberwachung zeigt Scanfehler an

Das Dashboard zur Dateiintegritätsüberwachung (FIM) zeigt Scanfehlerergebnisse jetzt direkt in der Hauptansicht des Dashboards an. Sie müssen nicht auf die einzelnen Scanergebnisse oder Zeilenelemente klicken, um auf Fehlerdetails zuzugreifen. Jegliche Integritätsprobleme, wie z. B. Hash-Fehlpaarungen oder Scanfehler, werden in einem klaren, zugänglichen Format direkt im Dashboard dargestellt. Diese Verbesserung optimiert den Fehlerbehebungsprozess, sodass Sie Probleme auf einen Blick schnell erkennen und verstehen können. Dadurch können Sie effizienter auf Integritätsprobleme reagieren, Zeit sparen und die Transparenz des gesamten Workflows verbessern.

Verwandtes Thema: Dateiintegritätsüberwachung.

Unterstützung für die Erkennung von Indicators of Compromise (IoC)

Die Funktion zur Erkennung von Indicators of Compromise (IoC) in der NetScaler Console wurde entwickelt, um zu erkennen, ob Ihre NetScaler Appliances potenziell von einer Schwachstelle betroffen sind.

Bei CVE-Ereignissen ist eine der ersten Sorgen, dass böswillige Akteure die Schwachstelle ausnutzen. Ein Exploit verursacht katastrophale Schäden für das Geschäft eines Kunden, und daher ist es entscheidend, solche Vorfälle sofort zu erkennen. IoC wurde in der Vergangenheit für NetScaler über Supportkanäle verteilt, was den Kundenbedürfnissen entspricht, aber mit einem zusätzlichen Aufwand verbunden ist, den Supportprozess des Erstellens eines Tickets und des Gesprächs mit einem Supportmitarbeiter zu durchlaufen, was manchmal nicht ideal ist. Die IoC-Erkennungsfunktion in der NetScaler Console wurde entwickelt, um den aktuellen supportorientierten Prozess abzukürzen und einem Kunden zu helfen, eine schnelle Bewertung seiner NetScaler-Infrastruktur vorzunehmen.

Weitere Informationen finden Sie unter Indicators of Compromise-Erkennung in der NetScaler Console.

Unterstützung des SSL-Filtermodus

Eine NetScaler-Instanz kann jetzt die Metadaten spezifischer SSL-Zertifikate und privater Schlüssel abrufen. Die Implementierung dieses Prinzips der geringsten Rechte stellt sicher, dass Instanzen nur auf die benötigten Assets zugreifen, wodurch verhindert wird, dass eine Kompromittierung einer Instanz Ihre gesamte Zertifikatsinfrastruktur offenlegt. Diese Funktion ist besonders nützlich für Umgebungen mit mehreren Administratoren, die Gruppen von NetScaler-Instanzen für unterschiedliche Zwecke verwalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Einige der Vorteile sind:

- **Sicherheitssegmentierung**: Beschränkt den Metadatenzugriff auf NetScaler-Ebene, um die Angriffsfläche zu minimieren und die Einhaltung der Sicherheitsrichtlinien des Unternehmens zu gewährleisten.
- **Optimierte Administratorerfahrung**: Reduziert die Komplexität in mandantenfähigen oder abteilungsspezifischen Bereitstellungen, indem Administratoren nur die Assets angezeigt werden, die für ihre Gruppe von NetScaler-Instanzen relevant sind.
- **Optimierte Ressourcennutzung**: Verhindert eine Überlastung des Systemspeichers, indem nur die Metadaten der benötigten SSL-Zertifikate und privaten Schlüssel abgerufen werden.

Die Filtermoduskonfiguration definiert, wie NetScaler-Instanzen und SSL-Dateien über spezifische Synchronisierungstypen interagieren. Sie können diese Einstellungen über die NetScaler Console verwalten, um sicherzustellen, dass nur die notwendigen Metadaten von jeder Instanz abgerufen werden.

KOMPONENTE	SYNCHRONISIERUNGSTYP	BESCHREIBUNG
NetScaler-Instanz	Angepasster Sync	NetScaler-Instanzen in diesem Modus rufen nur die Metadaten für Zertifikate und Schlüssel ab, die speziell der Instanz zugeordnet sind.
NetScaler-Instanz	Globale Synchronisierung	NetScaler-Instanzen in diesem Modus rufen die Metadaten für alle hochgeladenen Zertifikate und privaten Schlüssel ab.
SSL-Dateien	Benutzerdefinierte Dateien	Diese Dateien sind speziell NetScaler-Instanzen im Modus „Benutzerdefinierte Synchronisierung“ zugeordnet.
SSL-Dateien	Globale Dateien	Metadaten für diese Dateien werden von allen NetScaler-Instanzen im Modus „Globale Synchronisierung“ abgerufen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FILTERMODUSEINSTELLUNGEN KONFIGURIEREN

Um den Filtermodus zu konfigurieren, definieren Sie Synchronisierungstypen für Ihre Instanzen und Dateien. Dies gewährleistet eine sichere und optimierte Verteilung sensibler Metadaten.

So konfigurieren Sie über die GUI:

1. **Neue Dateien hochladen (Tag Null)**: Navigieren Sie zu **Zertifikatsdateien und NetScaler-Instanzen > Hochladen**, um neue Assets hinzuzufügen. Wählen Sie einen der folgenden Synchronisierungstypen aus:
    - **GLOBAL**: Wählen Sie diese Option, um den globalen Synchronisierungsmodus zu verwenden und den Upload abzuschließen.
    - **BENUTZERDEFINIERT**: Wählen Sie diese Option, um den benutzerdefinierten Synchronisierungsmodus zu verwenden, wählen Sie die spezifischen Instanzen für die Zuordnung aus und laden Sie dann die Dateien hoch.
2. **Vorhandene Dateien verschieben (Tag N)**: Um Zertifikate und Schlüssel vom globalen Synchronisierungsmodus in den benutzerdefinierten Synchronisierungsmodus zu verschieben, wählen Sie die Ziel-NetScaler-Instanzen aus und klicken Sie auf **Vorhandene Dateien hinzufügen**.
3. **Domänen auswählen**: Sobald Instanzen ausgewählt sind, wählen Sie die relevanten Domänen aus, um die Verschiebung auszulösen. NetScaler Console erkennt und verschiebt die entsprechenden Zertifikate und privaten Schlüsseldateien automatisch in den benutzerdefinierten Synchronisierungsmodus.
4. **Assets anzeigen**: Navigieren Sie zur Landingpage, um alle Zertifikate und privaten Schlüsseldateien anzuzeigen, die jeder NetScaler-Instanz im benutzerdefinierten Synchronisierungsmodus zugeordnet sind.
5. **Synchronisierungsmodus wechseln**: Um Instanzen in den globalen Synchronisierungsmodus zurückzusetzen, klicken Sie auf der Landingpage auf **Zu globaler Synchronisierung wechseln**.

Behobene Probleme

Analysen

- Wenn ein Benutzer eine ICA-Sitzung auf einem Server startet, der auf einer IP-Adresse mit '0' gehostet wird (zum Beispiel 10.0.2.3), zeigt NetScaler Console die IP-Adresse als 10.2.3 an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastruktur

- Der Cloud Connect trennen-Vorgang kann in NetScaler Console On-Premises fehlschlagen. Die NetScaler Console On-Premises-Instanz bleibt mit dem NetScaler Console-Dienst verbunden, obwohl die GUI Cloud Connect als getrennt anzeigt. Dies führt dazu, dass On-Premises-Instanzen im NetScaler Console-Dienst als „Up“ angezeigt werden.

- In seltenen Fällen können die Scanergebnisse der Dateintegritätsüberwachung (FIM) Fehler melden.

- In seltenen Fällen kann der Telemetrie-Wiederholungsmechanismus nach einem erfolgreichen Vorgang nicht beendet werden, was zu doppelten Telemetrie-Prozessen auf dem NetScaler-Gerät führt. Dies hat keine funktionalen Auswirkungen auf die Telemetrieerfassung oder -weiterleitung.

- In NetScaler Console können die Protokolldetails zu Anwendungssicherheitsverletzungen nicht geladen werden, obwohl das Diagramm der Verletzungsanzahl die Daten widerspiegelt.

- Ein Verbindungsfehler tritt auf, wenn eine Redis-Instanz vom authentifizierten in den nicht authentifizierten Modus wechselt und der Dienst weiterhin veraltete Authentifizierungsdaten verwendet.

- Der NetScaler Console-Dienst zeigt möglicherweise einen Fehler „Ungültiges Schlüsseldateikennwort“ an, wenn Sie versuchen, passwortverschlüsselte Schlüsseldateien hinzuzufügen.

- Wenn eine Anwendung einer Benutzergruppe zugeordnet ist und der virtuelle NetScaler-Server umbenannt wird, wird die Anwendung automatisch aus der Benutzergruppe entfernt. Dies führt zu einer inkonsistenten Benutzergruppenkonfiguration.

March 31, 2026

Verwaltung und Überwachung

Dateien vom Konfigurationsaudit ausschließen

Sie können jetzt bestimmte Dateien vom Konfigurationsaudit ausschließen, damit sie nicht auf Änderungen überwacht werden. Verwenden Sie Ausschlüsse für systemgenerierte oder häufig

© 1997–2026 Citrix Systems, Inc. All rights reserved.

aktualisierte Dateien (z. B. Dateien, die täglich geändert werden), um Rauschen zu reduzieren und Fehlalarme in den Auditergebnissen zu vermeiden.

Beispiele für Dateinamen (oder relativen Pfad), die vom Konfigurationsaudit-Dateivergleich ausgeschlossen werden sollen:

- Gültiger Dateiname (oder relativer Pfad)
  - `ns.conf`, `ssl/ns.cert`
- Ungültiger Dateiname (oder relativer Pfad)
  - `/ns.txt`, `\nsconfig\ns.conf` (Der ausgeschlossene Dateiname muss ein relativer Pfad sein)
  - `ns.conf` (Der ausgeschlossene Dateiname darf nur ASCII-Zeichen enthalten)
  - `C:/nsconfig/ns.conf` (Der ausgeschlossene Dateiname darf keine Laufwerksbuchstabenpfade verwenden)
  - `ssl/../../ns.conf` (Der ausgeschlossene Dateiname darf keine Traversierung über das übergeordnete Verzeichnis (`..`) enthalten)

HINWEIS:

- Der Dateidifferenzvergleich ist nur für Dateien im Verzeichnis `/nsconfig` anwendbar.
- Beim Ausschließen von Dateien aus dem Konfigurationsaudit müssen Benutzer relative Pfade unter `/nsconfig` angeben. Wenn sich beispielsweise ein `ssl`-Ordner unter `/nsconfig` befindet, können Ausschlüsse wie folgt angegeben werden: `ssl/abc.pem`
- Dateidifferenzen außerhalb von `/nsconfig` werden nicht als Teil der Konfigurationsaudit-Differenz berücksichtigt.

Um Dateien vom Konfigurationsaudit auszuschließen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Infrastructure > Configuration > Configuration Audit**.
2. Wählen Sie **Settings**.
3. Fügen Sie unter **NetScaler Config File Settings** die Dateipfade hinzu, die Sie vom Audit ausschließen möchten.
4. Klicken Sie auf **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RBAC-Unterstützung auf Instanzebene für LAS

NetScaler Console on-prem unterstützt jetzt die rollenbasierte Zugriffssteuerung (RBAC) auf Instanzebene für LAS. Zuvor hatten Administratoren Zugriff auf die Lizenzierung für alle Geräte, was zu Sicherheitsrisiken und operativem Overhead führen konnte. Diese Verbesserung ermöglicht es Administratoren, bestimmten NetScaler-Instanzen eingeschränkten Zugriff zu gewähren. Infolgedessen verwaltet ein Administrator die Lizenzierung nur für die spezifische NetScaler-Instanz, auf die er zugreifen darf. Diese Änderung stellt sicher, dass Lizenzierungsaufgaben denselben Sicherheitsgrenzen folgen wie andere Verwaltungsaktivitäten in NetScaler Console on-prem.

Einige der Vorteile sind:

- **Verbesserte Sicherheit**: Beschränkt Lizenzierungsaktionen nur auf die zugewiesenen Geräte, die einem Administrator zugewiesen sind.
- **Granulare operative Kontrolle**: Stellt sicher, dass Administratoren die Lizenzierung für nicht autorisierte Instanzen nicht versehentlich ändern können.
- **Workflow-Ausrichtung**: Integriert die Lizenzverwaltung nahtlos in etablierte RBAC-Strukturen.

Verwandte Themen:

- Informationen zur Konfiguration von RBAC finden Sie unter Rollenbasierte Zugriffssteuerung.
- Informationen zur Lizenzverwaltung finden Sie unter Lizenzverwaltung.

Behobene Probleme

Analyse

In HA-Setups können gesicherte Anwendungen mit WAF- oder Bot-Richtlinien nach den geplanten EMON-Abfragen zeitweise aus dem ADM Security Dashboard verschwinden. Dieses Problem tritt aufgrund einer internen Datenkorrelationsinkonsistenz auf.

Infrastruktur

NetScaler FIPS-Appliances können möglicherweise keine Verbindung zum NetScaler Console-Dienst in der Government Cloud über den integrierten Agenten herstellen.

Unter **Aufgaben und Empfehlungen** führt das Klicken auf **Anzeigen und Beheben** für die ausgewählte CVE oder eine betroffene Instanz nach Auswahl einer Sicherheitsberatungsaufgabe zu einer leeren Seite.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Während des LAS-Migrationsworkflows kann die Benutzeroberfläche des NetScaler Console-Dienstes Hostnamen für HA-Paare, die von einem internen Agenten verwaltet werden, möglicherweise nicht anzeigen.

In einer HA-Einrichtung von NetScaler-Instanzen, die mit dem Console-Dienst über einen integrierten Agenten registriert sind, kann die Freigabezuweisung für diese Instanzen fehlschlagen, wenn die agent_id fehlt.

March 23, 2026

Verwaltung und Überwachung

Unterstützung für die Identifizierung und Behebung von CVE-2026-4368

Die Sicherheitsberatung des NetScaler Console-Dienstes unterstützt jetzt die Identifizierung und Behebung von CVE-2026-4368.

- Die Identifizierung für CVE-2026-3055 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-4368 beheben.

  HINWEIS:

  Die Sicherheitsberatung unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Jobs zum Upgrade von NetScaler-Instanzen verwenden.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

Unterstützung für die Identifizierung und Behebung von CVE-2026-3055

Das NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2026-3055.

- Die Identifizierung für CVE-2026-3055 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2026-3055 beheben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Das Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, ein Upgrade auf die von NetScaler unterstützten Builds oder Versionen durchzuführen.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

March 09, 2026

Was ist neu

Verwaltung und Überwachung

- **AES-Verschlüsselung für PEM-formatierte private Schlüssel**

  Der NetScaler Console-Dienst unterstützt jetzt den Advanced Encryption Standard (AES) als PEM-Kodierungsalgorithmus, wenn Sie eine Zertifikatsignieranforderung (CSR) erstellen. Beim Generieren einer CSR und Erstellen eines neuen privaten Schlüssels können Sie AES256 auswählen, um den PEM-formatierten privaten Schlüssel zu verschlüsseln und zu schützen, was eine sicherere Alternative zu den bestehenden DES- und 3DES-Optionen darstellt. Diese Verbesserung stellt sicher, dass private Schlüssel mit modernen, branchenüblichen kryptografischen Algorithmen geschützt werden.

  Die Vorteile sind folgende:

  - **Verbesserte Sicherheit**: Bietet eine stärkere Verschlüsselung für den Schutz privater Schlüssel im Vergleich zu älteren DES-basierten Methoden.
  - **Konformität**: Hilft Unternehmen, moderne Best Practices für die Sicherheit und gesetzliche Anforderungen zu erfüllen, die eine AES-basierte Verschlüsselung vorschreiben.
  - **Zukunftssicherheit**: Gleicht die CSR-Generierung an zeitgemäße kryptografische Standards an, die in der gesamten Branche weit verbreitet sind.

  Informationen zur Konfiguration des PEM-Kodierungsalgorithmus während der CSR-Generierung finden Sie unter Zertifikatsignierungsanforderung (CSR) erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sonstiges

- **Flexible Planungsoptionen für Upgrades sekundärer HA-Knoten**

  Unter **Infrastructure > Upgrade Jobs** können Sie beim Erstellen eines Jobs eine Verzögerung (in Stunden) festlegen, die nach Abschluss des ersten Knoten-Upgrades und vor Beginn des zweiten Knoten-Upgrades liegt. Diese Option ist in den folgenden Szenarien nützlich:

  - Zusätzliche Zeit ist erforderlich, um den ersten Knoten zu testen und zu validieren
  - Der Upgrade-Fortschritt hängt von der Betriebsreife und nicht von einer festen Uhrzeit ab
  - Flexibilität ist erforderlich, ohne die Aufgabe manuell neu planen zu müssen

  Zuvor war nur die Option zur Definition eines festen Zeitstempels verfügbar. Mit dieser Option würde, wenn das Upgrade des ersten Knotens verzögert würde, die geplante Zeit des zweiten Knotens verstreichen und das Upgrade würde nie beginnen.

Behobene Probleme

Analysen

- Die Option WAF Recommendation ist möglicherweise in der NetScaler Console Service-GUI beim Konfigurieren von RBAC-Richtlinien nicht sichtbar.

- Auf der Seite **Analysen** sehen Benutzer möglicherweise alle Instanzen, anstatt nur die spezifischen Instanzen zu sehen, für die der Zugriff basierend auf der für diesen bestimmten Benutzer definierten Benutzer-, Rollen-, Gruppen- und Zugriffsrichtlinie autorisiert wurde.

Infrastruktur

- Nach dem Upgrade von NetScaler Console On-Prem auf Version 14.1-60.54 zeigt der Telemetriestatus für alle SDX-Appliances möglicherweise interne Fehler 2500 und 3300 an.

- Der NetScaler Console-Agent stürzt nach einem Upgrade aufgrund eines POCO-Bibliotheks-Upgrades kontinuierlich ab.

- Die Zertifikatssynchronisierung des NetScaler Console-Dienstes kann mit einem HTTP 28-Fehler fehlschlagen. Dieses Problem tritt auf, wenn die Zero-Touch-Funktion aktiviert ist und die Anforderung nach 10 Sekunden abläuft, bevor die Konsole antworten kann, wodurch der Synchronisierungsprozess unterbrochen wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verschiedenes

Der NetScaler Console-Dienst unterstützt die Lizenzierung eines NetScaler VPX mit 20 Mbit/s mittels LAS-basierter Lizenzierung nicht.

```
[ NSHELP-42109 ]
```

February 20, 2026

Was ist neu

Entfernung einiger Validierungsprüfungen vor dem Upgrade

Die folgenden NetScaler Console-Prüfungen vor dem Upgrade wurden aus dem Workflow für Upgrade-Aufträge entfernt:

- **Prüfung der Benutzeranpassungen**: Prüfung bestehender Benutzeranpassungen, einschließlich Startskripten und Cron-Jobs, die das Systemverhalten während oder nach der Installation beeinträchtigen könnten.
- **Prüfung auf HDD-Fehler**: System- und Kernel-Protokollprüfungen auf festplattenbezogene Fehler, E/A-Fehler, Timeouts und Dateisystemprobleme, die die Installationsstabilität beeinträchtigen könnten.
- **Prüfung der Hochverfügbarkeitskonfiguration (HA)**: Prüfung der Konfigurationssynchronisierung zwischen HA-Knoten.

Die vorangegangenen Prüfungen sind veraltet und ressourcenintensiv. Die Entfernung dieser Prüfungen verbessert die Upgrade-Leistung, reduziert den System-Overhead und minimiert falsche Upgrade-Fehler, während alle kritischen Validierungsprüfungen bestehen bleiben.

Weitere Informationen zu den Prüfungen vor dem Upgrade finden Sie unter Upgrade-Aufträge.

Behobene Probleme

Infrastruktur

Der Schweregrad des CVE wird auf der CVE-Ansichtsseite unter **Sicherheitshinweis** nicht angezeigt.

Bei der Bandbreitenzuweisung kann ein Dezimalvalidierungsfehler auftreten, wenn die LAS-Lizenzierung für NetScaler MPX- und SDX-Plattformen konfiguriert wird. Dieses Problem tritt auf, wenn nur eine begrenzte Anzahl von Lizenzeditionen zur Zuweisung verfügbar ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

February 04, 2026

- **Kategorisierung von Pre-Upgrade-Prüfungen im NetScaler Console-Dienst**

  Pre-Upgrade-Prüfungen in NetScaler Console für NetScaler-Upgrades mithilfe von Upgrade-Aufträgen werden jetzt in die folgenden Kategorien gruppiert:

  - Kritisch: Upgrade ist blockiert.
  - Warnung: Upgrade ist mit Administratorgenehmigung zulässig.
  - Hinweis: Upgrade ist mit Administratorgenehmigung zulässig.

  Weitere Informationen finden Sie unter Pre-Upgrade-Validierung.

- **Obligatorischer Zeitparameter für die Generierung von technischen Supportdateien**

  Die Angabe einer Uhrzeit ist jetzt für die Generierung von technischen Supportdateien obligatorisch. Sie müssen explizit einen Zeitbezug auswählen, wenn Sie eine technische Supportdatei generieren. Sie können entweder die benutzerdefinierte Option auswählen und ein benutzerdefiniertes Datum und eine Uhrzeit angeben oder die Option „Jetzt“ verwenden. Die Option „Jetzt“ verwendet die aktuelle Systemzeit. Diese Verbesserung stellt sicher, dass der genaue Zeitkontext explizit definiert wird.

  Weitere Informationen finden Sie unter So generieren Sie ein technisches Support-Bundle für eine NetScaler-Instanz.

- **Upgrade-Aufträge: Eine Warnung wird angezeigt, wenn ausgewählte Instanzen bereits auf dem Ziel-Build sind**

  Um die Auswahl falscher Instanzen während Upgrade-Aufträgen zu verhindern, wird eine Warnung angezeigt, wenn Sie Instanzen auswählen, die bereits den Ziel-Build ausführen. Diese Verbesserung hilft, unnötige Upgrades zu vermeiden. Wenn Sie beabsichtigen, die Instanzen erneut zu aktualisieren, können Sie die Warnung sicher ignorieren und fortfahren.

- **Verbesserungen bei der Sichtbarkeit und Zuordnung von Instanzgruppen**

  Die Registerkarte **Instanzansicht** wird auf der Seite **Instanzgruppe** eingeführt, um die Sichtbarkeit und Verwaltung von Instanzgruppen zu verbessern. Die Registerkarte **Instanzansicht** ist eine zentralisierte Ansicht, die Folgendes bietet:

  - Eine konsolidierte Liste aller verwalteten NetScaler-Instanzen
  - Einblick in die Instanzgruppen, denen jede Instanz zugeordnet ist

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Eindeutige Identifizierung von Instanzen, die keiner Instanzgruppe zugeordnet sind
- Verbesserte Instanzidentifizierung unter Verwendung von Hostname und IP-Adresse

Administratoren können nicht zugeordnete Instanzen schnell zu Instanzgruppen hinzufügen und bereits zugewiesene Instanzen identifizieren, um doppelte Zuordnungen zu verhindern, was zu einer einfacheren und effizienteren Verwaltung von Instanzgruppen führt.

Um die Instanzansicht anzuzeigen, navigieren Sie zu **Infrastruktur> Instanzen-Dashboard> Instanzgruppen> Instanzansicht**.

Weitere Informationen finden Sie unter https://docs.netscaler.com/de-de/netscaler-console-service/networks/instance-management/create-instance-groups.

- **Dateintegritätsüberwachung: Möglichkeit, eine Ausschlussliste für Scans zu erstellen**

  Sie können eine benutzerdefinierte Zulassungsliste erstellen und bestimmte Dateien von Dateintegritätsüberwachungs-Scans ausschließen. Indem Sie definieren, welche Dateien vom Scan ausgeschlossen werden sollen, können Sie die Überwachung optimieren und unnötige Warnungen für vertrauenswürdige Dateien reduzieren. Zuvor wurden bestimmte Dateien bei Dateintegritätsüberwachungs-Scans fälschlicherweise als bösartig identifiziert, obwohl sie nicht bösartig waren.

  Weitere Informationen finden Sie unter https://docs.netscaler.com/de-de/netscaler-console-service/instance-advisory/file-integrity-monitoring%23console-detected.

- **Unterstützung für binäre Signierung und Verifizierung**

  Der NetScaler Console-Dienst unterstützt jetzt die binäre Signierung und Verifizierung. Diese Funktion erhöht die Sicherheit, indem sie einen Mechanismus zur Erkennung und Verhinderung der Ausführung nicht autorisierter oder manipulierter Dateien auf Ihren NetScaler-Instanzen bereitstellt. Bei jedem Versuch, eine nicht autorisierte Datei auf NetScaler auszuführen, wird ein Echtzeit-SNMP-Trap an die NetScaler Console gesendet und markiert.

  Um die Liste der NetScaler-Instanzen anzuzeigen, die Probleme bei der binären Signierung und Verifizierung gemeldet haben, navigieren Sie zu **Infrastructure > Instance Advisory > Security Advisory**, klicken Sie auf **File Integrity Monitoring** und rufen Sie die Registerkarte **Device-Reported** auf.

  Weitere Informationen finden Sie unter Dateisystemintegritätsüberwachung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sonstiges

- **On-Demand-LAS-Berechtigungssynchronisierung**

  Bisher wurden konsolenkompatible Berechtigungen nur einmal alle 24 Stunden mit dem License Activation Service (LAS) synchronisiert. Die neue Option „Lizenzen synchronisieren“ ermöglicht es Ihnen, diese Synchronisierung bei Bedarf manuell auszulösen, um sicherzustellen, dass die Berechtigungen sofort auf dem neuesten Stand sind.

  Informationen zu LAS finden Sie unter License Activation Service.

Behobene Probleme

Infrastruktur

- Wenn Sie einen Massen-Upload von Zertifikaten und Schlüsseln durchführen, bestätigt die GUI den Status „Erfolgreich hochgeladen“. Die Zertifikate werden jedoch nicht in der Zero-Touch-Ansicht angezeigt.

- Das **Security Advisory Dashboard** zeigt möglicherweise ein falsches Datum für den **Nächsten geplanten Scan** an, das nicht mit der definierten **Häufigkeit des geplanten Scans** übereinstimmt.

- Die DNS-Challenge kann während der ACME-Zertifikatsausstellung fehlschlagen, wenn DNS-Anbieter nicht innerhalb des Zehn-Sekunden-Timeouts antworten. Dieses Problem tritt aufgrund von langsamen API-Antworten, hoher Netzwerklatenz oder erheblichen DNS-Propagierungsverzögerungen auf.

- Einige NetScaler-Dateien, die während des Upgrade-Prozesses generiert wurden, könnten durch die Dateintegritätsüberwachungs-Scans fälschlicherweise als anfällig gekennzeichnet werden.

- Der Diagnosestatus für den NetScaler Agent wird im NetScaler Console Service auf Citrix Cloud Japan fälschlicherweise als „Überprüfung erforderlich“ angezeigt, obwohl Japan-Cloud-bezogene URLs zugänglich sind.

- Der NetScaler Console Security Advisory zeigt eine falsche Empfehlung zur sicheren Konfiguration bezüglich unsicherer SSL-Protokollversionen an. Die Empfehlung besagt, dass TLS 1.0 und TLS 1.1 für nicht-primäre Standardprofile verwendet werden, selbst wenn diese Protokolle deaktiviert sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Der StyleBook-Konfigurationspaketvorgang kann mit einem RBAC-Autorisierungsfehler fehlschlagen, wenn die Zielinstanz ein HA-Paar ist, auf dem SNIP für den Verwaltungszugriff konfiguriert ist.
- Die NetScaler Cloud API kann Anfragen an den NITRO-Systemdateiendpunkt möglicherweise nicht weiterleiten. Infolgedessen können API-Aufrufe fehlschlagen.
- E-Mail-Benachrichtigungen für NetScaler Console SSL-Zertifikatsablaufereignisse können fehlschlagen.
- Alle Remote-Zertifikate, die von der Automated Certificate Management Environment (ACME) in NetScaler Console ausgestellt wurden, werden aus NetScaler entfernt, wenn die Anzahl der Zertifikate 20 überschreitet.

Lizenzierung

- In der Tabelle **LAS-lizenziert** unter **Lizenzverwaltung** wird der Hostname für Instanzen möglicherweise nicht angezeigt.
- Für den Lizenztyp „Pooled“ oder „Flexed“ zeigt die lokale GUI der Konsole die Informationen zum Verlängerungsdatum des Berechtigungs-Blobs an. Sie warnt jedoch nicht und sendet keine proaktiven Benachrichtigungen über den Ablauf des Berechtigungs-Blobs. Kunden wird empfohlen, das in der GUI angezeigte Ablaufdatum des Berechtigungs-Blobs zu überwachen und es vor Ablauf zu verlängern, um einen unterbrechungsfreien Betrieb des Produkts zu gewährleisten.

Verschiedenes

- In seltenen Fällen können virtuelle Server auf NetScaler während der Bereitstellung der Zero-Touch-Zertifikatsverwaltung zeitweise ausfallen.
- Die Migration von NetScaler-Instanzen zu LAS-basierter Lizenzierung schlägt fehl, wenn eine Instanz mithilfe eines FQDN anstelle einer IP-Adresse hinzugefügt wird.
- Bei der Verwendung von LAS-Lizenzierung, die nur auf gepoolten Berechtigungen basiert (ausgenommen UHMC/CPL), werden die SDX-Geräte möglicherweise nicht auf der Registerkarte **LAS Managed Entitlements** des Dashboards **Pooled Licensing** angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

- Das Bearbeiten der Ressourcenbindung in einem vorhandenen StyleBook Configpack schlägt fehl.

November 11, 2025

Verwaltung und Überwachung

Unterstützung für die Identifizierung und Behebung von CVE-2025-12101

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2025-12101.

- Die Identifizierung für CVE-2025-12101 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2025-12101 beheben.

  HINWEIS:

  Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

November 06, 2025

Behobene Probleme

Infrastruktur

Nach einem Neustart wird die Scanfrequenz des NetScaler Console On-Prem Security Advisory fälschlicherweise auf 7 Tage anstatt auf 24 Stunden eingestellt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verschiedenes

Der Abschnitt **Lizenzierte NetScaler-Instanzen** unter **Pooled Licensing > Durchsatzkapazität > LAS-verwaltete Berechtigungen** zeigt möglicherweise keine Geräte an, wenn ein Kunde nur gepoolte Lizenzen verwendet und keine flexiblen Lizenzen besitzt.

October 15, 2025

Verwaltung und Überwachung

ISSU-Migrationsabschluss in Upgrade-Aufträgen

Der Workflow für Upgrade-Aufträge unterstützt jetzt die erzwungene In-Service Software Upgrade (ISSU)-Migration. Wenn **ISSU aktivieren, um Netzwerkausfälle auf NetScaler HA-Paaren zu vermeiden** unter **Auftrag erstellen** ausgewählt ist, löst ISSU nach der vom Kunden definierten Verzögerungszeit automatisch die vollständige Migration aus.

Während ISSU wartet NetScaler normalerweise, bis die aktiven Verbindungen auf natürliche Weise geschlossen werden, bevor die Migration abgeschlossen wird. Manchmal können langlebige Verbindungen den Abschluss verzögern oder blockieren. Mit dieser Verbesserung löst NetScaler Console eine erzwungene ISSU-Migration aus, indem langlebige aktive Verbindungen beendet werden. Kritische Verwaltungssitzungen (CLI, GUI, Konsole) sind ausgeschlossen, um einen unterbrechungsfreien administrativen Zugriff zu gewährleisten.

Vorteile:

- Schnellerer, besser vorhersehbarer ISSU-Abschluss.
- Reduzierte Betriebsverzögerungen und -fehler, die durch langlebige Verbindungen verursacht werden.
- Verbesserte Zuverlässigkeit bei Upgrade- und Rollback-Workflows.

Unterstützte Szenarien:

- Die Migration läuft und wartet darauf, dass Verbindungen geschlossen werden.
- Der Rollback wird ausgeführt und wartet darauf, dass Verbindungen geschlossen werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Behobene Probleme

Infrastruktur

Benutzer erhalten möglicherweise keine E-Mail-Benachrichtigungen für SSL-Zertifikate, die sich ihrem Ablaufdatum nähern, obwohl die Einstellungen für die Zertifikatsablaufbenachrichtigung korrekt konfiguriert sind.

Einige NetScaler-Instanzen werden von der Dateiintegritätsüberwachung fälschlicherweise als anfällig gekennzeichnet, da nicht relevante Dateien in den Scan einbezogen werden.

Das auf der Seite **Sicherheitshinweis > Scanverlauf** angezeigte Banner enthält falsche Informationen.

September 17, 2025

Infrastruktur

Automatisierte Zertifikatserneuerung mithilfe des ACME-Protokolls

NetScaler Console unterstützt jetzt das ACME-Protokoll (Automated Certificate Management Environment), um die Verwaltung des SSL/TLS-Zertifikatslebenszyklus zu vereinfachen.

Die Unterstützung des ACME-Protokolls bietet folgende Vorteile:

- Verhindert Ausfallzeiten durch die Erneuerung von Zertifikaten vor Ablauf.
- Reduziert den manuellen Aufwand durch automatische Nachverfolgung und Erneuerungen.
- Gewährleistet höhere Sicherheit mit stets gültigen, CA-konformen Zertifikaten.

NetScaler Console unterstützt den ACME-Client acme.sh und die Integration der Zertifikatserneuerung mit den folgenden CA-Anbietern:

- Let’s Encrypt
- DigiCert

Alle DNS-Anbieter, die vom acme.sh-Client unterstützt werden, werden auch von der Konsole für die DNS-Validierung unterstützt.

Die folgenden Punkte beschreiben den übergeordneten ACME-Kommunikationsfluss:

- NetScaler® Console sendet als ACME-Client eine Anfrage an den ACME-Server (CA) für ein neues Zertifikat oder eine Erneuerung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die CA initiiert eine DNS-01-Challenge.
- NetScaler Console fügt den TXT-Eintrag mit dem von der CA bereitgestellten Token zum konfigurierten DNS-Anbieter hinzu.
- Die CA fragt den DNS-Anbieter ab, um die Domain-Inhaberschaft zu überprüfen.
- Bei erfolgreicher Validierung stellt die CA die Zertifikate aus.

Weitere Informationen finden Sie unter Automatisierte Zertifikatserneuerung mit dem ACME-Protokoll.

Behobene Probleme

Infrastruktur

Historische Daten können für einige Kunden mit einer kostenlosen Lizenz gelöscht werden.

Das Laden von Konfigurationsaufträgen verzögert sich, wenn diese mehreren Gerätegruppen zugeordnet sind und große Befehlssätze enthalten.

Benutzer können auf die folgenden Probleme stoßen:

- Eine Fehlermeldung **Ungültige Ressource**, wenn sie auf **Console on-prem telemetry upload** klicken.
- Eine Fehlermeldung **IP-Adresse existiert bereits**, wenn sie versuchen, ein neues Profil zu erstellen.

Plattform

NetScaler mit mehreren PEs könnte fälschlicherweise als anfällig für CVE-2021-22956 gekennzeichnet werden, wenn er von NetScaler Console gescannt wird.

StyleBooks

Das Update des Konfigurationspakets kann fehlschlagen, wenn das Paket eine NetScaler-Zugriffssteuerungsliste enthält, die einen Quell-IP-Adressdatensatz oder einen Ziel-IP-Adressdatensatz verwendet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

September 08, 2025

Lizenzierung

LAS-Durchsetzung auf NetScaler und NetScaler Console Service

Das dateibasierte Lizenzierungssystem (auch als „manuell verwaltete Berechtigungen“ bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Citrix Produktpalette. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, und unterstützt NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed Term Bandwidth-Lizenzen. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein. Die mindestens erforderlichen NetScaler-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.80, 13.1-60.29, 13.1-37.247 (FIPS)
- NetScaler SVM: 14.1-51.83, 13.1-60.30
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.83

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.83 verfügbar. Die Einstellung/das EOL der dateibasierten Lizenzierung gilt jedoch ab Console on-prem Version 14.1-51.83 und Console on-prem Version 13.1-60.26.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, Perpetual werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden nach dem Upgrade auf die oben genannten Softwareversionen unlizenziert.

LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies gesetzlich oder durch Vorschriften verboten ist.

Bei Fragen oder Bedenken wenden Sie sich bitte an den Kundendienst. Citrix kann Ihre Citrix Maintenance bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder aussetzen, zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften verboten sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LAS-Unterstützung für NetScaler Console Service

Der NetScaler Console Service unterstützt jetzt den Lizenzierungsmechanismus des License Activation Service (LAS). LAS ist eine neue cloudbasierte Lizenzierungslösung, die eine moderne Alternative zur traditionellen dateibasierten Lizenzierung bietet. LAS führt neue Module für die Aktivierung von Citrix- und NetScaler-Produkten ein und gewährleistet einen nahtlosen und modernen Ansatz für die Lizenzverwaltung.

NetScaler Console Service ist jetzt automatisch für den License Activation Service (LAS) aktiviert. Sie können Ihre NetScaler Flexed- und Pooled-Lizenzberechtigungen anzeigen, indem Sie zu Folgendem navigieren: **Lizenzen > Lizenzverwaltung > License Activation Service (LAS)**.

NetScaler-Versionskompatibilität für LAS Um LAS zu verwenden, muss Ihr NetScaler eine der folgenden Mindestversionen oder höher ausführen:

- NetScaler ADC: 14.1 Build 51.x, 13.1 Build 60.x, 13.1 Build 37.x (FIPS)
- NetScaler SVM: 14.1 Build 51.x, 13.1 Build 60.x

HINWEIS:

LAS für NetScaler Console Service unterstützt NetScaler Flexed-Lizenzen (CPL/UHMC) und (ältere) NetScaler Pooled-Lizenzen. Alle anderen Formen älterer NetScaler-Lizenzen, wie z. B. Pooled vCPU, CICO, werden von LAS nicht unterstützt. Weitere Informationen finden Sie unter LAS-Unterstützung für Console Service..

September 03, 2025

Behobene Probleme

Infrastruktur

Das NetScaler-Durchsatzdiagramm wurde vom Dashboard der Admin-Partition entfernt, aufgrund der fehlenden Unterstützung für die erforderliche Zählergruppe „ns“ innerhalb der Admin-Partition.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

August 26, 2025

Verwaltung und Überwachung

Unterstützung für die Identifizierung und Behebung von CVE-2025-7775

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2025-7775.

- Die Identifizierung für CVE-2025-7775 erfordert einen benutzerdefinierten Scan. Bei diesem Scan stellt die NetScaler Console eine Verbindung zur verwalteten NetScaler-Instanz her und überträgt ein Skript. Das Skript wird auf der Instanz ausgeführt, um die Vorbedingung für die CVE zu überprüfen. Wenn die Vorbedingung erfüllt ist, wird eine Versionsprüfung auf dem NetScaler durchgeführt. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2025-7775 beheben.

  HINWEIS:

  Security Advisory unterstützt keine NetScaler®-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung der NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Aufträge zum Upgrade von NetScaler-Instanzen verwenden.
- Weitere Informationen zur CVE finden Sie unter Sicherheitsbulletin.

Unterstützung für die Identifizierung und Behebung von CVE-2025-7776

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2025-7776.

- Die Identifizierung für CVE-2025-7776 erfordert eine Kombination aus Versionsscan und Konfigurationsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2025-7776 beheben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung der NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Aufträge zum Upgrade von NetScaler-Instanzen verwenden.
- Weitere Informationen zur CVE finden Sie unter Sicherheitsbulletin.

Unterstützung für die Identifizierung und Behebung von CVE-2025-8424

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2025-8424.

- Die Identifizierung für CVE-2025-8424 erfordert einen Versionsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2025-8424 beheben.

HINWEIS:

Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Aufträge zum Upgrade von NetScaler-Instanzen verwenden.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

August 20, 2025

Infrastruktur

Unterstützung zum Aktivieren oder Deaktivieren von Sicherheitsscans

Sie können Ihre Präferenzen für Sicherheitsscans jetzt anpassen, indem Sie sich für oder gegen Sicherheitsscans entscheiden. Zusätzlich können Sie bestimmte Scan-Typen auswählen, die in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ihre Sicherheitsbewertung einbezogen werden sollen. Standardmäßig sind nur Scans für Common Vulnerabilities and Exposures (CVE) aktiviert.

So konfigurieren Sie die Einstellungen für Sicherheitsscans:

1. Navigieren Sie zu **Instanzberatung > Sicherheitsberatung**.
2. Klicken Sie auf das Einstellungssymbol in der oberen rechten Ecke.
3. Wählen Sie unter **Systemscan konfigurieren** die Arten von Scans aus, die Sie einschließen möchten.
4. Klicken Sie auf **Speichern**.

Dateisystemintegritätsüberwachung in Systemscans

Sie können Ihre Sicherheitslage jetzt verbessern, indem Sie die Dateisystemintegritätsüberwachung in Ihre Systemscans einbeziehen. Die Dateisystemintegritätsüberwachung ermöglicht es Ihnen, festzustellen, ob Änderungen oder Ergänzungen an Ihrem NetScaler-Dateisystem vorgenommen wurden.

So aktivieren Sie die Dateisystemintegritätsüberwachung:

1. Navigieren Sie zu **Instanzberatung > Sicherheitsberatung**.
2. Klicken Sie auf das Einstellungssymbol in der oberen rechten Ecke.
3. Wählen Sie unter **Systemscan konfigurieren** die Option **Scan zur Dateisystemintegritätsüberwachung** aus.
4. Klicken Sie auf **Speichern**.

Behobene Probleme

Infrastruktur

Die Seite **Instanzberatung > Sicherheitsberatung > CVE-Erkennung > Zur CVE-Ansicht wechseln** zeigt möglicherweise falsche Schweregrade für einige CVEs an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

July 17, 2025

Infrastruktur

Zeitstempel enthält Zeitzoneninformationen

In der NetScaler Console Service-GUI, in der der Zeitstempel angezeigt wird, können Sie jetzt auch die Zeitzoneninformationen sehen. Die Zeitzone wird basierend auf der unter **Systemeinstellungen** ausgewählten Zeitzone angezeigt. Abhängig von Ihrer Konfiguration wird die Zeitzone als GMT, Ihre lokale Zeitzone oder UTC (falls die lokale Abkürzung nicht verfügbar ist) angezeigt.

Zuvor zeigte der Zeitstempel keine Zeitzoneninformationen an. Mit dieser Verbesserung erhalten Sie klarere und genauere Zeitstempeldetails für geplante Aufträge.

Zum Beispiel zeigt die folgende Abbildung eine geplante Zeit an, die die Zeitzone enthält.

Behobene Probleme

Infrastruktur

Die PDF-Berichtserstellung für die Funktion Secure Config Recommendations unter **Infrastruktur > Instanzberatung > Sicherheitsberatung** kann fehlschlagen, wenn eine einzelne Kategorie eine große Anzahl von Empfehlungen enthält.

Das Feld **Letzte Scanzeit** im Dashboard **Sicherheitsberatung** zeigt den Zeitstempel des letzten CVE-Scans nicht an.

July 02, 2025

Telemetrie

Neue Validierung für Telemetriedaten

Im Rahmen des NetScaler-Telemetrieprogramms müssen Sie Ihre Telemetriedaten mindestens alle 90 Tage hochladen. Der NetScaler Console-Dienst überprüft nun, ob die neueste Datei in der hochgeladenen Nutzlast innerhalb von 90 Tagen liegt. Wenn die Datei älter als 90 Tage ist, wird der Upload abgelehnt. Diese neue Validierungsprüfung stellt sicher, dass Ihre hochgeladenen Telemetriedaten aktuell und konform sind.

Wenn Ihr Upload abgelehnt wird:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Laden Sie eine neue Nutzlast von Ihrer lokalen Konsole herunter.
2. Laden Sie sie erneut hoch.

Entfernung des Telemetrie-Analyseprofils von der verwalteten NetScaler-Instanz

Die folgende Telemetrie-Metrikprofilkonfiguration ist für die Telemetrieerfassung nicht mehr erforderlich:

```
add analytics profile telemetry_metrics_profile -type timeseries -outputMode prometheus -metrics ENABLEd -serveMode Pull -schemaFile "./telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300
```

Im Rahmen des NetScaler-Telemetrieprogramms wurde die Telemetrie-Metrikprofilkonfiguration an die verwalteten NetScaler-Instanzen übertragen.

NetScaler Console entfernt diese Konfiguration am July 19, 2025 automatisch von Ihren NetScaler-Instanzen, falls sie noch vorhanden ist. Alternativ können Sie die Konfiguration jederzeit manuell mit dem folgenden Befehl entfernen:

```
rm analytics profile telemetry_metrics_profile
```

Weitere Informationen zur Telemetrie-Metrikprofilkonfiguration finden Sie unter NetScaler-Telemetrieprogramm.

Sicherheit

Verbesserungen des Dashboards für Sicherheitshinweise

Das Dashboard für Sicherheitshinweise wurde verbessert und bietet Administratoren und Sicherheitsexperten sofortige Einblicke in den allgemeinen Zustand und den Schwachstellenstatus ihrer NetScaler-Infrastruktur.

Das Dashboard bietet einen umfassenden Überblick über die Sicherheitslage Ihrer NetScaler-Bereitstellung. Die wichtigsten Funktionen umfassen:

- Ein konsolidiertes Dashboard, das aktive Sicherheitshinweise anzeigt.
- Zusammenfassung der betroffenen Geräte.
- Eine klare Aufschlüsselung potenzieller Risiken.

Sie können kritische Schwachstellen, Empfehlungen für sichere Konfigurationen einschließlich Minderungsmaßnahmen und Links zu relevanter Dokumentation schnell identifizieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen finden Sie unter Sicherheitshinweis

Behobene Probleme

Analysen

Auch nach dem Bearbeiten einer API-Definition und dem Speichern der Änderungen kann der NetScaler Console-Dienst die API-Definition nicht aktualisieren und zeigt fälschlicherweise die Benachrichtigung „Update erfolgreich“ an.

In **HDX™ Insight > Users**, wenn Sie Details unter **Current Sessions** aufrufen, werden die Details mit dem unvollständigen Bericht angezeigt, wenn der mit NetScaler verbundene VDA fehlt.

Infrastruktur

Die Anzahl der Instanzen, die im Abschnitt **Instances on older build summary** von **Upgrade Advisory** angezeigt werden, ist falsch.

Wenn NetScaler von NetScaler Console aktualisiert wird, kann das System den Aktualisierungsstatus nicht als E-Mail-PDF-Anhang senden.

June 25, 2025

Verwaltung und Überwachung

Unterstützung für die Identifizierung und Behebung von CVE-2025-6543

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2025-6543.

- Die Identifizierung für CVE-2025-6543 erfordert eine Kombination aus Versionsscan und Konfigurationsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2025-6543 beheben.

  HINWEIS:

  Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

June 17, 2025

Verwaltung und Überwachung

Unterstützung für die Identifizierung und Behebung von CVE-2025-5349 und CVE-2024-5777

Der NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2025-5349 und CVE-2025-5777.

- Die Identifizierung für CVE-2025-5349 erfordert eine Kombination aus Versionsscan und Konfigurationsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält. Weitere Informationen finden Sie unter CVE-2025-5349 beheben.
- Die Identifizierung für CVE-2025-5777 erfordert einen Versionsscan, und die Behebung erfordert einen zweistufigen Prozess:

  a. Aktualisieren Sie die anfällige NetScaler-Instanz auf eine Version und einen Build, der den Fix enthält.
  b. Konfigurationsaufträge anwenden.

  Weitere Informationen finden Sie unter CVE-2025-5777 beheben.

  HINWEIS:

  Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.
- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Es kann ein paar Stunden dauern, bis der Scan des Sicherheitshinweissystems abgeschlossen ist und die Auswirkungen von CVE-2025-5349 und CVE-2025-5777 im Sicherheitshinweismodul widerspiegelt. Um die Auswirkungen früher zu sehen, können Sie einen On-Demand-Scan starten, indem Sie auf **Jetzt scannen** klicken.

June 03, 2025

Behobene Probleme

Analysen

Wenn Sie Daten für Analysen exportieren, wie z. B. Sicherheitsverletzungen, Gateway Insight und HDX Insight, enthielt der exportierte CSV-Bericht zuvor nur 5000 Einträge. Mit diesem Update wird das Limit auf 10.000 Einträge erhöht.

Infrastruktur

Der NetScaler-Agent verwendet das Proxy-Passwort zeitweise in einem falschen Format, während er über einen Proxy-Server mit dem NetScaler Console-Dienst kommuniziert.

Wenn Sie Benachrichtigungseinstellungen unter **Einstellungen > Systemereignisse > Benachrichtigungen** konfigurieren, indem Sie mehrere Kategorien auswählen und auf **Speichern** klicken, werden die Änderungen nicht gespeichert.

May 26, 2025

Analysen

Verbesserte HDX Insight-Sichtbarkeit auf VPN-Virtual-Server-Ebene

HDX Insight ermöglicht Ihnen jetzt die Überwachung wichtiger Metriken wie aktiver Sitzungen, Desktops und gestarteter Anwendungen auf VPN-Virtual-Server-Ebene. Eine neue Option **Gateway Virtual Servers** ist jetzt unter **Gateway > HDX Insight** verfügbar.

Als Administrator ermöglicht Ihnen diese Verbesserung Folgendes:

- Anzeigen einer Liste aller virtuellen Server unter **Gateway > HDX Insight > Gateway Virtual Servers**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wählen Sie einen virtuellen Server aus, um auf einen umfassenden Bericht zuzugreifen, der eine detaillierte Sichtbarkeit bietet und die Leistungsüberwachung speziell für diesen virtuellen Server vereinfacht.

Zuvor waren detaillierte Berichte zur Endbenutzererfahrung nur auf NetScaler-Instanzebene verfügbar.

Unterstützung zur Anzeige von Web Insight-Analysen für IPv6-Virtual-Server

Sie können jetzt Web Insight-Analysen für virtuelle Server anzeigen, die mit einer IPv6-Adresse konfiguriert sind. Zuvor wurde Web Insight für IPv6-Adressen nicht unterstützt. Als Administrator bietet diese Verbesserung verschiedene Details in Web Insight, die es Ihnen ermöglichen, die Leistung des virtuellen Servers zu analysieren und zu verbessern.

Weitere Informationen finden Sie unter Web Insight.

Zentralisierte GeoIP-DB-Updates über NetScaler Console

NetScaler Console ermöglicht Administratoren das direkte Hochladen der GeoIP-DB-Datei von MaxMind über die NetScaler Console. Sie können die GeoIP-DB-Datei entweder sofort an verwaltete NetScaler-Instanzen übertragen oder das Update für einen späteren Zeitpunkt planen. Diese Dateien sind unerlässlich für eine genaue IP-zu-Standort-Zuordnung, die häufig in GSLB- und Sicherheitsrichtlinien verwendet wird.

Zuvor verfügte NetScaler nicht über einen zentralisierten Mechanismus zur Verwaltung von GeoIP-DB-Updates (Geolocation Database) auf NetScaler. Administratoren mussten die Updates manuell auf jedem Gerät durchführen, was zeitaufwändig, fehleranfällig und in Produktionsumgebungen störend war.

Diese Verbesserung bietet die folgenden Vorteile:

- Automatisierung: Der Aktualisierungsprozess ist automatisiert und wird ohne geplante Ausfallzeiten durchgeführt, wodurch der Betriebsaufwand reduziert wird.
- Effektive Skalierbarkeit: Die Verwaltung von Updates über mehrere NetScaler-Instanzen hinweg ist effizient und einfach zu skalieren.
- Versionsprüfung: Wenn ein Problem auftritt, können Sie die historischen Versionen verfolgen, eine ältere GeoIP-DB-Datei hochladen und synchronisieren.

Weitere Informationen finden Sie unter Zentralisierte GeoIP-DB-Updates über NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Behobene Probleme

Analysen

- Einige Prozesse im NetScaler-Agent stürzen ab und erzeugen Core-Dateien. Infolgedessen ist der Speicherplatz voll.
- Der Export von mehr als 1 MB Daten von NetScaler Console nach Microsoft Sentinel schlägt fehl.
- In Web Insight, wenn Sie auf eine Anwendung klicken, um die Anomalien unter **Anwendungsmetriken** anzuzeigen, zeigt die Client-Netzwerklatenz auf der Registerkarte **Antwortzeit** falsche Details an.

May 06, 2025

Behobene Probleme

Das Klonen eines StyleBooks kann mit dem folgenden Fehler fehlschlagen, wenn eine StyleBook-Definition den Abschnitt „import-stylebooks“ enthält, der leer ist oder keine definierten Importe aufweist:

'NoneType'-Objekt ist nicht iterierbar

Das Importieren einer StyleBook-Definition kann fehlschlagen, wenn die StyleBook-Definition einen Ausdruck enthält, der auf eine Ausgabe einer Komponente verweist.

Das Upgrade eines NetScaler von der NetScaler Console schlägt aufgrund eines beschädigten Build-Images fehl. Aufgrund eines Netzwerkproblems während des Image-Uploads wird das Build-Image beschädigt. Um Diskrepanzen während der Dateiübertragung zu erkennen und zu verhindern, können Sie die Prüfsummenüberprüfung für das hochgeladene Build-Image aktivieren.

In einigen Szenarien werden Benachrichtigungen nicht ausgelöst, wenn sich der Ereignisstatus ändert. Die Protokolle werden generiert, aber die Ereignisaktion wird nicht ausgeführt.

April 15, 2025

Zero-Touch-Zertifikatbereitstellung

Sie können jetzt Zero-Touch-Zertifikate auf den verwalteten NetScaler-Instanzen konfigurieren, die Build 14.1-43.x und höher ausführen. Mit der Zero-Touch-Zertifikatbereitstellung können Sie manuelle Eingriffe eliminieren und den In-Memory-Zero-Touch-Zertifikatspeicher aufbauen, um die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Anwendungsanforderungen zu bedienen. Navigieren Sie zu **SSL Dashboard > Zero-touch certificate management**, um alle Zertifikate und Schlüssel in die NetScaler Console hochzuladen, wählen Sie die NetScaler-Instanzen aus und klicken Sie dann auf **Enable**. Nach dem Hochladen der Zertifikate und der Aktivierung der Zero-Touch-Zertifikatsverwaltung auf den NetScaler-Instanzen fragt NetScaler das Zertifikatsrepository regelmäßig ab und ruft die erforderlichen Zertifikate ab.

Zuvor konnten Sie im SSL-Dashboard nur den manuellen Eingriff bei der Installation des SSL-Zertifikats auf jeder Instanz minimieren.

Weitere Informationen finden Sie unter:

- NetScaler Zero-Touch-Zertifikatsverwaltung
- NetScaler Console Zero-Touch-Zertifikatsverwaltung

Veralten der automatischen Skalierung von NetScaler-Instanzen in öffentlichen Clouds

Die automatische Skalierung der NetScaler-Instanzkonfiguration in öffentlichen Clouds ist in NetScaler Console nicht mehr verfügbar.

Verbesserungen bei Konfigurationsaufträgen

NetScaler Console sendet nun die Ausgabe von Show-Befehlen, die in einem Konfigurationsauftrag hinzugefügt wurden, per E-Mail und Slack.

Verbesserungen bei Upgrade-Aufträgen

Unter **Infrastructure > Upgrade Jobs** können Sie, wenn Sie einen Auftrag zum Upgrade von NetScaler in einer Hochverfügbarkeitsumgebung mithilfe eines zweistufigen Upgrade-Prozesses erstellen, das HA-Failover nun bis zum Beginn des Upgrades des zweiten Knotens verzögern.

Behobene Probleme

Infrastruktur

Wenn Sie in einem Konfigurationsauftrag einen Auftrag über die Option zum Hochladen von Dateien erstellen, wird die folgende Fehlermeldung angezeigt: `File upload not allowed. Max file size 15 MB`

Die maximal zulässige Dateigröße für einen Konfigurationsauftrag beträgt 2 GB.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dienst-zu-Dienst-DeviceAPIProxy-Aufrufe können die Ergebnisse für den NITRO-Aufruf "systemfiles" von NetScaler nicht abrufen.

Unter **Infrastruktur > Konfiguration > Konfigurationsprüfung > Prüfvorlagen** schlägt die Vorschau einer Prüfvorlage fehl, wenn Variablen in den Vorlagenbefehlen definiert sind.

In NetScaler Console kann ein neuer Benachrichtigungskanal für Slack bis März 2025 nicht zum Planen von Exporten verwendet werden. Die vorhandenen Slack-Kanäle können bis dahin zum Planen von Exporten verwendet werden, danach muss ein neuer Kanal erstellt werden.

Die folgenden Bereiche sind in einer App erforderlich:

- channels:read
- groups:read
- im:read
- mpim:read

Weitere Informationen finden Sie in der Slack-Dokumentation.

February 19, 2025

StyleBooks

Unterstützung für den Zugriff auf privat gehostete GitLab/GitHub-Repositorys und Infoblox IPAM

NetScaler Console Service StyleBooks ermöglicht Ihnen jetzt, StyleBooks und Configpacks aus GitLab/GitHub-Repositorys zu importieren und zu synchronisieren, die privat gehostet werden und nur innerhalb des Intranets eines Unternehmens zugänglich sind.

NetScaler Console Service IPAM ermöglicht Ihnen jetzt, einen privat gehosteten Infoblox DDI-Server als externen IPAM-Anbieter zu registrieren.

Zuvor wurden nur öffentlich zugängliche GitLab/GitHub-Repositorys und Infoblox DDI-Server unterstützt.

Weitere Informationen finden Sie unter StyleBooks aus einem externen Repository importieren und synchronisieren und IP-Adressverwaltung (IPAM) konfigurieren.

Behobene Probleme

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analysen

Um unbegrenzte VIPs zu ermöglichen, werden die Abonnementdetails in **Einstellungen > Analytics-Konfiguration** entfernt.

February 06, 2025

Analysen

Web-Transaktionsanalysen auf der Ebene des virtuellen Servers aktivieren

Sie können jetzt Web-Transaktionsanalysen auf der Ebene des virtuellen Servers aktivieren. Dazu müssen Sie, wenn Sie Analysen für einen virtuellen Server aktivieren, die neue Option „Detaillierte Web-Transaktionen“ auswählen, um die Web-Transaktionsanalysen zu aktivieren.

Zuvor wurde, wenn Sie Analysen für einen virtuellen Server aktiviert haben, die Web-Transaktionsanalysen automatisch aktiviert.

Weitere Informationen finden Sie unter Web-Transaktionsanalysen.

Infrastruktur

Benachrichtigungen für verwaltete Geräte während Wartungs- und Fehlerbehebungsfenstern deaktivieren

Administratoren können Benachrichtigungen für bestimmte verwaltete Geräte während Wartungs- und Fehlerbehebungsfenstern vorübergehend deaktivieren. Diese Verbesserung verhindert den Empfang unnötiger Warnungen und Benachrichtigungen bezüglich gerätespezifischer Probleme und Statusaktualisierungen während dieser Zeiträume.

Um Benachrichtigungen zu deaktivieren, navigieren Sie zu **Einstellungen > Verwaltung > Instanzeinstellungen > Benachrichtigungs-Deaktivierungsfenster** und fügen Sie die erforderlichen Details hinzu. Weitere Informationen finden Sie unter Instanzeinstellungen.

Behobene Probleme

Infrastruktur

In der **Auftragsvorlage** wird beim Importieren der Konfigurationsauftragsvorlage über die Schaltfläche **Importieren** der folgende Fehler angezeigt:

`Invalid resource`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 15, 2025

Telemetrie

Änderungen beim Telemetrie-Upload von Console On-Prem

Sie müssen jetzt für jede NetScaler Console On-Prem-Instanz ein Profil erstellen, um die Telemetriedatei in den NetScaler Console-Dienst hochzuladen. Möglicherweise haben Sie mehrere NetScaler Console On-Prem-Instanzen weltweit bereitgestellt. Durch das Erstellen eines Profils für jede On-Prem-Instanz können Sie die Telemetriedatei für diese On-Prem-Instanzen hochladen und die Upload-Frist separat überwachen.

Um ein Profil zu erstellen, navigieren Sie zu **Einstellungen > Console On-Prem Telemetrie-Upload** und klicken Sie auf **Profil erstellen**.

HINWEIS:

Wenn Sie ein bestehender Console On-Prem-Benutzer sind und die Telemetriedatei zuvor in den Console-Dienst hochgeladen haben, müssen Sie ein neues Profil erstellen und dann die Telemetriedatei hochladen. Nach dem Erstellen des neuen Profils kann es zu einer Diskrepanz zwischen der Console On-Prem-Frist und der Console-Dienst-Frist kommen. Stellen Sie sicher, dass Sie die Telemetriedatei am oder vor dem Fälligkeitsdatum, das in Ihrer Console On-Prem angezeigt wird, in den NetScaler Console-Dienst hochladen. Diese Diskrepanz wird behoben, nachdem Sie einen Upload mit dem neuen Profil abgeschlossen haben.

Weitere Informationen finden Sie unter Console On-Prem-Upload.

Analysen

Unterstützung zum Aktivieren eines benutzerdefinierten Headers in den Analyseeinstellungen zum Abrufen der Client-IP-Adresse

Wenn Sie Analysen für eine Anwendung aktivieren, können Sie jetzt einen benutzerdefinierten Header wie X-Real-IP, X-Client-IP oder einen anderen benutzerdefinierten Header definieren, um die tatsächliche Client-IP-Adresse anstelle der Proxy-IP-Adresse abzurufen. Die Option für benutzerdefinierte Header ermöglicht:

- Kompatibilität mit verschiedenen Netzwerk-Proxys, die unterschiedliche Header verwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Genauigkeit, um die tatsächliche Client-IP-Adresse in einer komplexen Netzwerkumgebung mit mehreren Proxy-Ebenen zu erhalten.
- Zusätzliche Sicherheitsmaßnahmen als die von den Standard-Headern bereitgestellten.

Sortier- und Suchunterstützung im benutzerdefinierten Dashboard

Im benutzerdefinierten Dashboard (**Übersicht > Benutzerdefiniertes Dashboard**) können Sie jetzt Folgendes verwenden:

- Sortieroption, um die benutzerdefinierten Dashboards alphabetisch anzuzeigen.
- Suchoption (sowohl Klartext als auch regulärer Ausdruck) zur Eingrenzung der Suchergebnisse.

Infrastruktur

Hostname in E-Mail-Benachrichtigungen zu Systemereignissen

NetScaler Console enthält jetzt den Hostnamen der zugehörigen NetScaler-Instanzen in E-Mail-Benachrichtigungen zu Systemereignissen.

StyleBooks

Importieren und Synchronisieren von StyleBooks aus einem externen GitLab-Repository

StyleBooks unterstützen jetzt den Import und die Synchronisierung von StyleBooks und Konfigurationspaketen aus GitLab-Repositorys. Zuvor war diese Funktion nur für GitHub-Repositorys verfügbar.

Weitere Informationen finden Sie unter: Externes Repository synchronisieren

Auswählen mehrerer Elemente aus einer StyleBook-Datenquelle

Sie können jetzt StyleBooks erstellen, die es Benutzern ermöglichen, mehrere Elemente aus einem Datenquellenparameter auszuwählen. StyleBooks unterstützen jetzt ein Datum-Array als Parametertyp, wodurch Benutzer eine Liste von Datenquellen oder Sammlungselementen als Eingabe auswählen können.

Weitere Informationen finden Sie unter: StyleBook-Datenquellen verwalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unterstützung eines Filters für Datenquellensammlungen

StyleBooks ermöglichen es Ihnen jetzt, einen Sammlungsfilter für einen Datenquellenparameter anzugeben. Bei der Eingabe für einen solchen Parameter in Konfigurationspaketvorgängen sehen Benutzer nur Elemente aus der gefilterten Sammlung und können diese auswählen, anstatt aus allen Elementen.

Weitere Informationen finden Sie unter: Integrierte Datenquelle, Benutzerdefinierte Datenquelle

Behobene Probleme

Analysen

- Unter **Einstellungen > Observability-Integrationen** kann das Bearbeiten oder Löschen eines Abonnements fehlschlagen, wenn ein NetScaler-Befehlsfehler auftritt.
- In **HDX Insight** und **Web Insight** löst der Geolocation-Bericht den Client-IP-Standort für den definierten IP-Block nicht auf.

Infrastruktur

- Wenn ein Benutzer mit allen Standardrollen in der NetScaler Console versucht, den Aktivierungscode für die Registrierung eines Agenten zu generieren, schlägt die Aktion mit dem Fehler **Nicht autorisiert, diesen Vorgang auszuführen** fehl.
- Wenn ein Nicht-nsroot-Benutzer versucht, die Statistiken für einen bestimmten virtuellen Server in Netzwerkfunktionen (**Infrastruktur > Netzwerkfunktionen**) anzuzeigen, wird eine Fehlermeldung angezeigt.

StyleBooks

- Wenn Sie ein Konfigurationspaket auf einem NetScaler HA-Paar bereitstellen und ein Failover auftritt, schlägt der Versuch fehl, das Konfigurationspaket mit der Instanz-ID des neuen Primärservers zu aktualisieren.
- Wenn Sie ein Konfigurationspaket löschen, das einen Richtliniendatensatz enthält, der von der Zugriffssteuerungsliste (ACL) von NetScaler referenziert wird, und die Ressourcenwiederverwendung für das zugehörige StyleBook aktiviert ist, bleibt der Richtliniendatensatz in NetScaler veraltet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wenn Sie Konfigurationspakete unter **Anwendungen > Konfigurationen > Konfigurationspakete** bearbeiten, wird die Reihenfolge der hinzugefügten Elemente nicht beibehalten.

December 03, 2024

Freigabe von Konfigurationsentitäten zwischen migrierten Konfigurationen

Sie können jetzt Konfigurationsentitäten wiederverwenden, wenn Sie Konfigurationen mithilfe des Dienstprogramms **Konfigurationsmigration** migrieren. Nachfolgende Migrationen verwenden erfolgreich vorhandene Konfigurationsentitäten auf dem Ziel-ADC wieder, die durch frühere Migrationen erstellt wurden. Zuvor schlug die Migration von Konfigurationen mit dem Fehler **Ressource existiert bereits** fehl, wenn zwei Konfigurationen migriert wurden, die einige Konfigurationsentitäten gemeinsam nutzten.

Weitere Informationen finden Sie unter: Vereinfachte Migration mit StyleBook

Analysen von richtlinienbasierter zu profilbasierter Konfiguration migrieren

Wenn Sie Analysen auf virtuellen Servern aktivieren, werden die Analysen jetzt über eine profilbasierte Konfiguration angewendet. Zuvor wurden Analysen über eine AppFlow®-Richtlinie konfiguriert. Die profilbasierte Konfiguration bietet die folgenden Vorteile:

- Verbesserte Leistung und Flexibilität
- Einfachere Konfiguration und Verwaltung

Verbesserungen im Zusammenhang mit Analyseeinstellungen werden nur in der profilbasierten Konfiguration unterstützt. Wir empfehlen Ihnen, alle Ihre vorhandenen virtuellen Server, die für Analysen aktiviert sind, zur profilbasierten Konfiguration zu migrieren.

Navigieren Sie zu **Einstellungen > Analyseeinstellungen** und wählen Sie dann **Analysen migrieren**

Weitere Informationen finden Sie unter Analysen migrieren.

Behobene Probleme

Analysen

- In **Web Insight** sind die Daten nicht sichtbar, wenn der benutzerdefinierte Datumsbereich länger als ein Tag ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastruktur

- NetScaler Console kann über das SSL-Dashboard keine Zertifikatsignieranforderung (CSR) generieren.
- Wenn Sie die Berechtigungen in Identity and Access Management (IAM) für eine Azure-Gruppe aktualisieren, werden die Änderungen nicht in NetScaler Console widergespiegelt.
- DeviceAPIProxy-Aufrufe können die Ergebnisse für den NITRO-Aufruf „systemfiles“ von NetScaler nicht abrufen.
- Die **PINNED**-Menüliste ist nur sichtbar, wenn die erste Ebene des Menüs in der erweiterten GUI von NetScaler Console erweitert ist.

StyleBooks

- Der Versuch, einen Link Aggregation Control Protocol (LACP)-Kanal mithilfe eines StyleBook-Konfigurationspakets zu konfigurieren, schlägt fehl.
- Das erzwungene Löschen eines Konfigurationspakets schlägt fehl, wenn obligatorische Parameter fehlen.
- Wenn Sie eine StyleBook-Definition aktualisieren, werden Entwurfs- und geplante Konfigurationspakete unbeabsichtigt bereitgestellt.
- Beim Erstellen einer RBAC-Richtlinie für StyleBook-Konfigurationspaketvorgänge müssen **APIProxy**-Berechtigungen manuell ausgewählt werden. Wenn sie nicht ausgewählt werden, schlägt das Konfigurationspaket fehl.

November 20, 2024

Verbesserte Benutzererfahrung in der NetScaler Console GUI

Der NetScaler Console-Dienst bietet jetzt eine verbesserte grafische Benutzeroberfläche (GUI) für eine bessere Benutzererfahrung. Wichtige Verbesserungen sind:

- **Hover-to-Display-Menü**: Die primäre Menübaumstruktur wird durch eine Hover-to-Display-Funktion für eine einfachere Navigation ersetzt. Sekundäre Menüelemente erscheinen beim Überfahren mit der Maus und zeigen ein Untermenü zur schnelleren Auswahl an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Optimierte Menühierarchie**: Die Menühierarchie ist jetzt auf maximal drei Ebenen begrenzt, was den Zugriff auf wichtige Optionen vereinfacht.
- **Aktualisierte Untermenübeschriftungen**: Die Namen der Untermenüs wurden für Optionen überarbeitet, die zuvor über die dritte Ebene hinaus verschachtelt waren.
- **Einklappbares Menü**: Das gesamte Menü kann jetzt durch Klicken auf ein Symbol im Bereich ein- oder ausgeklappt werden, wodurch mehr Bildschirmfläche zur Verfügung steht.
- **Seitenleisten-Umschalter**: Eine neue Umschalttaste in der Breadcrumb-Navigation ermöglicht es Ihnen, die Seitenleiste aus- oder einzublenden und so den Arbeitsbereich zu optimieren.
- **Startseite festlegen**: Sie können jetzt eine angezeigte Seite als Ihre Startseite festlegen, indem Sie auf das Symbol neben dem Untermenünamen klicken.
- **Favoriten anheften**: Heften Sie Ihre bevorzugten Menüelemente einfach an, um schneller darauf zugreifen zu können.

Weitere Informationen finden Sie unter Enhanced Graphical User Interface.

Option zum Löschen von SSL-Zertifikaten aus NetScaler

Sie können jetzt ein SSL-Zertifikat aus NetScaler löschen. Zuvor, wenn Sie die Datei unter **Infrastructure > SSL Dashboard** gelöscht haben, wurde das Zertifikat nur aus der laufenden Konfiguration entfernt. Die zugehörige Zertifikatsdatei wurde nicht aus NetScaler gelöscht.

Weitere Informationen finden Sie unter SSL Dashboard.

Behobene Probleme

Infrastruktur

- Wenn Sie Zertifikate über den Zertifikatsspeicher (Infrastructure > SSL Dashboard > Certificate Store) aktualisieren, kann NetScaler Console die Zwischenzertifikate auf NetScaler-Instanzen nicht aktualisieren.

- Wenn Sie mehr als 1000 Anwendungen haben, reagiert NetScaler Console nicht mehr und führt zu einer hohen CPU-Auslastung, wenn Sie:

  - Eine Benutzergruppe erstellen (**Settings > Users & Roles > Groups > Add**).
  - Spezifische Anwendungen zuweisen, indem Sie auf der Registerkarte **Authorization Settings** auf **Add** klicken.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wenn sich ein schreibgeschützter Benutzer bei NetScaler Console anmeldet, wird die folgende Fehlermeldung angezeigt:

  Keine oder ungültige Sitzung gefunden.

StyleBooks

Ein Config-Pack-Update schlägt fehl, wenn die Reihenfolge der Richtlinienbindungen, die ursprünglich mit dem StyleBook-Config-Pack konfiguriert wurden, nach Priorität neu angeordnet wird.

November 12, 2024

Verwaltung und Überwachung

Unterstützung bei der Identifizierung und Behebung von CVE-2024-8534 und CVE-2024-8535

Die NetScaler Console Service-Sicherheitswarnung unterstützt jetzt die Identifizierung und Behebung von CVE-2024-8534 und CVE-2024-8535.

- Die Identifizierung für CVE-2024-8534 erfordert eine Kombination aus Versionsscan und Konfigurationsscan. Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der die Korrektur enthält.
- Die Identifizierung für CVE-2024-8535 erfordert einen Versionsscan, und die Behebung erfordert einen zweistufigen Prozess:

  a. Aktualisieren Sie die anfällige NetScaler-Instanz auf eine Version und einen Build, der die Korrektur enthält.
  b. Wenden Sie Konfigurationsaufträge an.

  Weitere Informationen finden Sie unter CVE-2024-8535 beheben.

  HINWEIS:

  Die Sicherheitswarnung unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

- Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Weitere Informationen zum CVE finden Sie unter Sicherheitsbulletin.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitswarnsystems abgeschlossen ist und die Auswirkungen von CVE-2024-8534 und CVE-2024-8535 im Sicherheitswarnmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, können Sie einen On-Demand-Scan starten, indem Sie auf **Jetzt scannen** klicken.

October 15, 2024

Telemetrie

NetScaler Telemetrieseite in der NetScaler Console GUI

Sie können jetzt die NetScaler Telemetrieseite in der GUI anzeigen, die Informationen wie Datenerfassung, Telemetriemodus und Voraussetzungen enthält. Sie müssen lediglich sicherstellen, dass die Voraussetzungen erfüllt sind, und es ist keine Aktion für den Telemetriedaten-Upload erforderlich.

Das NetScaler Telemetrieprogramm für die obligatorische Telemetriedatenerfassung wurde in NetScaler Console Build 14.1-28.x eingeführt.

Analysen

Verbesserungen bei den SSL-Nutzungsanalysen in Web Insight

In **Web Insight** wurden die SSL-Nutzungsanalysen verbessert, mit besserer Sichtbarkeit der wichtigsten Metriken wie Chiffre, Schlüssellänge und Protokolle bei Szenarien mit höherem Datenverkehr. Zuvor wurden bei Szenarien mit höherem Datenverkehr nur begrenzte Details zu diesen wichtigen Metriken angezeigt.

SSL-Widget im benutzerdefinierten Dashboard

Im benutzerdefinierten Dashboard (**Overview > Custom dashboard**) können Sie jetzt Dashboards erstellen, um Metriken zur SSL-Konfiguration anzuzeigen. Weitere Informationen zum Erstellen eines benutzerdefinierten Dashboards finden Sie unter Benutzerdefinierte Dashboards erstellen, um wichtige Instanzmetrikdetails anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Behobene Probleme

Infrastruktur

- Im **Infrastructure > SSL Dashboard** werden die Stamm- und Zwischenzertifikate in der SSL-Zertifikatskette nicht angezeigt.
- Im **Infrastructure > SSL Dashboard** wird der Aussteller der öffentlich verfügbaren Zertifikate fälschlicherweise als **Nicht empfohlen** angezeigt.
- In NetScaler Console werden Ereignismeldungen, die zwischen „**<**“ und „**>**“ liegen, nicht im E-Mail-Text angezeigt.
- Im Sicherheits-Dashboard (**Security > Security Dashboard**) wird beim Konfigurieren von Schutzmaßnahmen für ungesicherte Anwendungen oder beim Ändern von Schutzmaßnahmen und Klicken auf **Deploy** die folgende Fehlermeldung angezeigt:

  ```
  HTTP Error 502 while accessing the data endpoint: "Unified_appsec_profile"
  ```

October 03, 2024

Lizenzierung

Beheben von Problemen im Zusammenhang mit Flexed/Pooled-Lizenzierung

Im Flexed- oder Pooled-Lizenzierungs-Dashboard können Sie unter **Licensed NetScalers** jetzt die Option **Troubleshoot** verwenden, um einige lizenzbezogene Probleme anzuzeigen und zu analysieren. Einige mögliche Lizenzierungsprobleme sind die Kommunikation von der Konsole zu den Instanzen und die Verfügbarkeit der License Server Agents (LSA). Die Option **Troubleshoot** bietet eine Liste der Problemkategorien wie Lizenzserver, LSA, Prozesse, Kommunikation und deren Status. Als Administrator können Sie diese Kategorien analysieren und Fehler beheben, wenn Sie Lizenzierungsprobleme feststellen.

Weitere Informationen finden Sie unter Beheben von Lizenzierungsproblemen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

Verbesserte Integration und Freigabe der Konfiguration in Migrationsdienstprogramm-Konfigurationspaketen

Sie können Konfigurationen jetzt über verschiedene Migrationskonfigurationspakete hinweg integrieren und wiederverwenden. Zuvor konnten außerhalb des Migrationsdienstprogramms erstellte Konfigurationen nicht über mehrere Konfigurationspakete hinweg wiederverwendet werden.

Hinweise

Für den NetScaler Console-Dienst wird eine strengere HTTP-Header-Validierung implementiert. API-Benutzer müssen jetzt den korrekten Content-Type-Header verwenden.

Behobene Probleme

Die Probleme, die in Build Oct 03, 2024 behoben wurden.

Analysen

- Unter **Security > Security Violations**, unter **Application Overview**, werden die Details für WAF-Sicherheitsverletzungen, die in NetScaler 14.1–21.38 gemeldet wurden, leer angezeigt, nachdem Sie:
    a. Eine Anwendung aus den unter WAF gemeldeten **Top Applications** auswählen, um weitere Details anzuzeigen.
    b. Auf **See more** unter **Violation details** klicken.
    c. Unter **Timeline Details** auf **+** klicken und alle Spalten auswählen.

Infrastruktur

- SNMP-Traps werden nach dem MASTools HA-Geräte-Failover nicht empfangen.

StyleBooks

- Die Konfiguration von ADC-Ressourcen mit gemischter Groß-/Kleinschreibung, wie z. B. „Interface“, wird nicht angewendet, selbst wenn der StyleBook-Configpack-Vorgang erfolgreich ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

September 19, 2024

Infrastruktur

Änderungen der Abfrageintervalle für Netzwerkfunktionen

Zusätzlich zum bestehenden Standard-Abfrageintervall für alle NetScaler-Instanzen kann NetScaler Console jetzt auch ausgewählte NetScaler-Instanzen, die Konfigurationsänderungen aufweisen, früher als im Standard-Abfragezyklus abfragen. Mit dieser Verbesserung wurde das Standard-Abfrageintervall auf 720 Minuten geändert. Unter **Infrastruktur > Netzwerkfunktionen** können Sie, wenn Sie auf **Einstellungen** klicken, jetzt eine neue Option **Netzwerkfunktionen-Abfrage bei Empfang des Ereignisses „netScalerConfigChange“ durchführen** unter **Netzwerkfunktionen basierend auf Konfigurationsänderung** anzeigen. Diese Option ist standardmäßig mit einem 15-Minuten-Intervall in der **Verzögerungszeit für Netzwerkfunktionen** aktiviert.

Wenn nun ein Konfigurationsänderungsereignis in NetScaler-Instanzen auftritt, fragt NetScaler Console diese Instanzen erst nach dem 15-minütigen Intervall ab.

HINWEISE:

- Sie können das Standard-Abfrageintervall (zum Abfragen aller NetScaler-Instanzen) auf einen Wert zwischen 30 Minuten und 1440 Minuten ändern.
- Sie können den Standardintervallwert von 15 Minuten (zum Abfragen nur ausgewählter Instanzen) auf einen Wert zwischen 5 Minuten und 60 Minuten ändern.
- Sie können **Netzwerkfunktionen-Abfrage bei Empfang des Ereignisses „netScalerConfigChange“ durchführen** deaktivieren. Wenn diese Option deaktiviert ist, fragt NetScaler Console alle NetScaler-Instanzen gemäß dem Standard-Abfragezyklus ab.

Weitere Informationen finden Sie unter Abfrageübersicht.

Behobene Probleme

Die Probleme, die in Build Sep 19, 2024 behoben wurden.

Infrastruktur

Die Inhalte der Benachrichtigungs-E-Mail für den Exportbericht entsprechen nicht RFC 5322.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

- Das Erstellen eines Konfigurationspakets aus einer StyleBook-Definition, die `snmptrap_snmpuser_binding` enthält, schlägt mit der Fehlermeldung „list index out of range“ fehl.

- Beim Konfigurieren eines StyleBooks wird die GUID der ausgewählten Datenquelle anstelle ihres lesbaren Namens in der Eingabezusammenfassungsansicht angezeigt.

September 03, 2024

Beobachtbarkeit

Anzeigen von NetScaler Console-Audit-Log-Daten in Observability-Tools (Splunk, New Relic und Microsoft Sentinel)

Wenn Sie ein neues Abonnement unter **Einstellungen > Observability-Integration** für die Integration des NetScaler Console-Dienstes mit Splunk, New Relic oder Microsoft Sentinel erstellen, können Sie jetzt die Option **NetScaler Console-Audit-Logs** auswählen. Nachdem Sie ein Abonnement konfiguriert haben, können Sie NetScaler Console-Audit-Logs in diesen Observability-Tools anzeigen.

Weitere Informationen finden Sie unter:

- Integration mit Splunk
- Integration mit New Relic
- Integration mit Microsoft Sentinel

Behobene Probleme

Die Probleme, die in Build Sep 03, 2024 behoben wurden.

Analysen

- In **Web Insight** zeigt der Bericht, wenn Sie den Export (Tabellenformat) für einen Tagesbericht planen, jeden Tag dieselben Daten an.

- In **Web Insight** sind die Daten nicht sichtbar, wenn der benutzerdefinierte Datumsbereich länger als ein Tag ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

August 27, 2024

Analysen

Globale Analysen konfigurieren

Sie können jetzt globale Analysen mithilfe benutzerdefinierter und globaler Richtlinien konfigurieren.

- **Benutzerdefinierte Richtlinie** – Mit der benutzerdefinierten Richtlinie können Sie Instanzen oder virtuelle Server steuern, die nur bestimmte Einblicke erfordern.
- **Globale Richtlinie** – Mit der globalen Richtlinie können Sie Analysen auf den vorhandenen verwalteten virtuellen Servern und allen neuen virtuellen Servern konfigurieren und aktivieren.

Sie können bis zu 10 Richtlinien erstellen: neun benutzerdefinierte Richtlinien und eine globale Richtlinie oder 10 benutzerdefinierte Richtlinien. Navigieren Sie zu **Einstellungen > Analytics-Konfiguration** und klicken Sie unter **Globale Analytics-Zusammenfassung** auf **Globale Analytics-Konfiguration**, um eine benutzerdefinierte oder globale Richtlinie zu konfigurieren.

Weitere Informationen finden Sie unter Globale Analysen konfigurieren.

Anwendungen

Wenn Sie eine Anwendung auf die SSL-Bewertung A+ aktualisieren, können Sie jetzt nur innerhalb von 7 Tagen nach dem Upgrade zur ursprünglichen Bewertung zurückkehren.

App-Dashboard – Tags für Anwendungen (virtuelle Server) erstellen und anwenden

Im **App-Dashboard** können Sie jetzt Tags für Anwendungen erstellen und anwenden. Diese Tags verbessern die Suchfunktion. Nachdem Sie Tags erstellt und auf die Suchleiste geklickt haben, können Sie die Tags verwenden und die Suche verfeinern.

Weitere Informationen finden Sie unter Tags für Anwendungen erstellen und anwenden.

StyleBooks

Konfigurationen, die außerhalb von StyleBooks erstellt wurden, wiederverwenden und Konfigurationen zwischen ConfigPacks teilen

Sie können jetzt Konfigurationen, die zuvor außerhalb von StyleBooks in NetScaler erstellt wurden, als Teil von Stylebook-Konfigurationspaketen integrieren und verwalten. Darüber hinaus können

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie jetzt Konfigurationen über mehrere Konfigurationspakete hinweg teilen, was eine flexiblere und zentralisierte Verwaltung ermöglicht.

Weitere Informationen finden Sie unter Konfigurationspaket erstellen und bearbeiten.

Behobene Probleme

Die Probleme, die in Build Aug 27, 2024 behoben wurden.

Analysen

In **Web Insight** sind die Daten für die virtuellen Server nicht sichtbar, die in allen verwalteten Instanzen denselben Namen haben.

Infrastruktur

- Die Speicherauslastung der NetScaler Console steigt, wenn die verwalteten Instanzen mit mehr als 10000 an die Dienstgruppen gebundenen Health Monitors konfiguriert sind. Infolgedessen ist die NetScaler Console möglicherweise nicht zugänglich.
- Beim Provisioning des NetScaler-Agenten oder NetScaler VPX in Microsoft Azure kann die NetScaler Console Provisioning-Dienst-API die Azure-Subnetzdetails nicht abrufen.

July 25, 2024

Behobene Probleme

Infrastruktur

Unter **Infrastructure > Upgrade Jobs** listet die Vorab-Upgrade-Validierung, wenn Sie eine NetScaler-Instanz aktualisieren, die klassische Richtlinien besitzt, die Instanz als **Instanzen, die vom Upgrade blockiert sind** auf, und das Upgrade wird nicht durchgeführt.

Problemumgehung: Bevor Sie eine Instanz aktualisieren, empfehlen wir Ihnen, die klassischen Richtlinien in erweiterte Richtlinien für die Funktionen umzuwandeln, die vom NSPEPI-Tool unterstützt werden. Weitere Informationen finden Sie unter Upgrade-Überlegungen für Konfigurationen mit klassischen Richtlinien.

Telemetrie

Als Teil des NetScaler-Telemetrieprogramms prüft NetScaler Console die folgende Konfiguration nicht mehr alle 24 Stunden und überträgt sie auch nicht mehr an NetScaler-Instanzen. Zuvor

© 1997–2026 Citrix Systems, Inc. All rights reserved.

wurde die Konfiguration alle 24 Stunden überprüft und bei Fehlen an NetScaler-Instanzen übertragen:

```
enable ns feature AppFlow

add analytics profile telemetry_metrics_profile -type timeseries
-outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "./
telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300
```

July 15, 2024

Infrastruktur

Unterstützung für 3072-Bit-Verschlüsselungsschlüssel im NetScaler Console SSL-Dashboard

Sie können jetzt eine Unternehmensrichtlinie mit einer Schlüssellänge von 3072 Bit für Ihr Zertifikat konfigurieren. Wählen Sie unter **Infrastructure > SSL Dashboard > Settings > Enterprise Policy > Recommended key strengths** einen 3072-Bit-Verschlüsselungsschlüssel aus. Zuvor waren nur Schlüssellängen von 512, 1024, 2048 und 4096 Bit verfügbar.

Weitere Informationen finden Sie unter:Für NetScaler Console Service: Eine Unternehmensrichtlinie konfigurierenFür NetScaler Console On-Prem: Eine Unternehmensrichtlinie konfigurieren

Anzeigen und Exportieren von NetScaler-eigenen IP-Adressen in der NetScaler Console GUI

Sie können jetzt NetScaler-eigene IP-Adressen (**Infrastructure > Instances > NetScaler Owned IPs**) in der NetScaler Console GUI anzeigen und exportieren.

Weitere Informationen finden Sie unter NetScaler-eigene IP-Adressen anzeigen.

Lizenzierung

Details zu VPX-Instanzen anzeigen, die auf einer SDX-Instanz im Flexed Licensing Dashboard bereitgestellt werden

Im Flexed Licensing Dashboard (**NetScaler Licensing > Flexed Licensing > Dashboard**) können Sie unter **Licensed NetScalers** die Anzahl der VPX-Instanzen anzeigen, die für NetScaler SDX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ausgecheckt sind. Sie können jetzt auf die Anzahl klicken, um die Details der bereitgestellten VPX-Instanz für diese SDX anzuzeigen, z. B. Instanzname, IP-Adresse, Durchsatz (MBPS) und Edition.

Zuvor konnten Sie nur die Gesamtzahl der für diese SDX ausgecheckten VPX-Instanzen anzeigen.

MPX/SDX-Host-ID und Seriennummerndetails in Zero-Capacity-Lizenzen anzeigen

Unter **NetScaler Licensing > Zero-capacity licenses** können Sie jetzt die Details zu **Host-ID** und **Seriennummer** für die MPX- und SDX-Instanzen anzeigen.

Behobene Probleme

Die Probleme, die in Build Jul 15, 2024 behoben wurden.

Infrastruktur

- Wenn Sie eine Instanz in **NetScaler Console (Infrastructure > Instances > NetScaler)** ändern, z. B. den Standort oder das Administratorprofil, werden die Schlüssel-Wert-Paare der mit der Instanz verknüpften Tags umgekehrt.
- Wenn Sie in Config Job die Vorlage ShowConfiguration gleichzeitig auf dem primären und sekundären NetScaler in einem HA-Paar ausführen, wird durch Klicken auf „Ergebnisdateien herunterladen“ die Datei nur für die sekundäre Instanz heruntergeladen.
- Wenn ein Dashboard in der Netzwerkberichterstattung (Infrastruktur > Netzwerkberichterstattung) nicht vorhanden ist, erhalten Sie die folgende Fehlermeldung:

  "Sie haben keinen Zugriff auf diese Seite"

  Diese Fehlermeldung kann ignoriert werden und hindert Sie nicht daran, Dashboards zu erstellen.
- Die SNMP-Traps werden im NetScaler Console-Dienst nicht empfangen, wenn dieser mit dem integrierten Agenten konfiguriert ist.

StyleBooks

Wenn Sie in der NetScaler Console-GUI ein Konfigurationspaket bearbeiten, um ein anderes StyleBook zu verwenden, funktioniert das Upgrade nicht wie erwartet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

July 09, 2024

Unterstützung für die Identifizierung und Behebung von CVE-2024-5491 und CVE-2024-5492

Das NetScaler Console-Dienst-Sicherheitshinweis unterstützt jetzt die Identifizierung und Behebung von CVE-2024-5491 und CVE-2024-5492.

- Die Identifizierung für CVE-2024-5491 erfordert eine Kombination aus Versions- und Konfigurationsscan.
- Die Identifizierung für CVE-2024-5492 erfordert einen Versionsscan.

Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält.

HINWEIS:

Der Sicherheitshinweis unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, ein Upgrade auf die von NetScaler unterstützten Builds oder Versionen durchzuführen.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.

Weitere Informationen finden Sie unter Sicherheitsbulletin.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitshinweis-Systems abgeschlossen ist und die Auswirkungen von CVE-2024-5491 und CVE-2024-5492 im Sicherheitshinweis-Modul widerspiegelt. Um die Auswirkungen früher zu sehen, können Sie einen On-Demand-Scan starten, indem Sie auf **Jetzt scannen** klicken.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

June 18, 2024

Telemetrie

NetScaler Telemetrie-Programm

Als bestehender NetScaler Console-Kunde müssen Sie dem NetScaler Telemetrie-Programm entsprechen, das die Erfassung von Telemetriedaten zur Lizenz- und Funktionsnutzung erfordert. Die Telemetriedaten werden alle 24 Stunden automatisch hochgeladen und es ist keine Aktion Ihrerseits erforderlich.

- Weitere Informationen finden Sie unter NetScaler Telemetrie-Programm.
- Weitere Informationen zu den Telemetrieparametern finden Sie unter Datengovernance.

June 11, 2024

Analysen

Metrik-Collector und Analysen zur Nutzung in schwachen Zeiten auf Ebene des virtuellen Servers aktiviert

Der Metrik-Collector und die Analysen zur schlanken Nutzung sind jetzt auf Ebene des virtuellen Servers anstatt auf Instanzebene aktiviert. Mit dieser Verbesserung bleiben der Metrik-Collector und die Analysen zur schlanken Nutzung nur auf Ihren aktiven virtuellen Servern mit hohem Datenverkehr aktiviert.

Sie können Ihre virtuellen Server überprüfen und den **Metrik-Collector** sowie die schlanke Nutzung auf anderen virtuellen Servern aktivieren, indem Sie zu **Einstellungen > Analysekonfiguration** navigieren und unter **Zusammenfassung der Metriken des virtuellen Servers** auf **Metriken konfigurieren** klicken.

Weitere Informationen finden Sie unter Intelligente App-Analysen konfigurieren.

Ein Netzprofil in NetScaler-Instanzen für die Metrikerfassung zuweisen

Wenn Sie den Metrik-Collector für die virtuellen Server in NetScaler Console aktivieren, werden die Metrikdaten vom NetScaler über die NetScaler-Subnetz-IP-Adresse (SNIP) an NetScaler Console exportiert. In einigen Szenarien kann die SNIP aufgrund der Firewall im Netzwerk blockiert sein. In solchen Szenarien müssen Sie möglicherweise eine andere IP-Adresse verwenden. Weitere Informationen zum Netzprofil finden Sie unter Eine angegebene Quell-IP für die Back-End-Kommunikation verwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können jetzt einer NetScaler-Instanz ein Netzprofil für die Metrikerfassung zuweisen. Der Metrik-Collector überträgt die NetScaler-Zählerdaten an NetScaler Console, die zur Erkennung von Anwendungsproblemen verwendet werden. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**, wählen Sie die Instanz aus und klicken Sie in der Liste **Aktion auswählen** auf **Netzprofile für Metrik-Collector konfigurieren**.

Weitere Informationen zum Zuweisen eines Netzprofils finden Sie unter Ein Netzprofil für die verwaltete NetScaler-Instanz zuweisen.

Observability-Integration – Details zu fehlgeschlagenen NetScaler-Abonnements anzeigen

In der **Observability-Integration** können Sie, wenn Sie ein Abonnement für NetScaler zu Splunk oder Prometheus konfigurieren, jetzt detaillierte Protokolle für die fehlgeschlagenen Abonnements anzeigen. Als Administrator können Sie anhand dieser Protokolle den Grund für den Abonnementfehler analysieren.

Weitere Informationen finden Sie unter Protokolle für fehlgeschlagene Konfigurationen anzeigen

Entfernung der Option für den periodischen Export von WAF- und Bot-Einblicken in der Observability-Integration

Die Option für den periodischen Export von WAF- und Bot-Einblicken wurde entfernt, wenn Sie den Export von Einblicken von NetScaler Console an Observability-Tools (wie Splunk, New Relic und Microsoft Sentinel) konfigurieren. Da WAF- und Bot-Verletzungen entscheidend sind, wird empfohlen, die Echtzeit-Exportoption zu verwenden, um Einblicke in Echtzeit zu exportieren, sobald sie auftreten.

Jedes bestehende Abonnement mit periodischer Exportkonfiguration für WAF und Bot wird automatisch auf Echtzeit-Export umgestellt.

Infrastruktur

Unterstützung für „App-basierte“ Bereitstellung

Der NetScaler Console-Dienst führt die „App-basierte“ Bereitstellung für AWS und Azure ein. Diese Funktion optimiert und vereinfacht NetScaler-Bereitstellungen in Cloud-Rechenzentren und ermöglicht eine effiziente Anwendungsbereitstellung aus diesen Umgebungen.

Weitere Informationen finden Sie unter App-basierte Bereitstellung in AWS und App-basierte Bereitstellung in Azure.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Behobene Probleme

Die Probleme, die in Build Jun 11, 2024 behoben wurden.

Analysen

- Ein Prozess in NetScaler Console/Agent kann aufgrund von Speicherbeschädigung abstürzen.
- In **Web Insight** sind die Details für den Lastausgleichs-Virtual-Server, der hinter dem Content-Switching-Virtual-Server konfiguriert ist, in den täglichen, wöchentlichen und monatlichen Berichten nicht sichtbar.

Infrastruktur

- Wenn Nicht-Administrator-Benutzer versuchen, Statistiken für die virtuellen Server in NetScaler Console (**Infrastruktur > Netzwerkfunktionen**) anzuzeigen, wird die folgende Fehlermeldung angezeigt:

  „Nicht autorisiert, auf <vserver_name> zuzugreifen“
- In einem HA-Setup, wenn Sie den integrierten Agenten „mastools“ zusammen mit den Partitionen verwenden, ist der Status der sekundären NetScaler-Instanz im SSL-Dashboard (**Infrastruktur > SSL-Dashboard**) und im Lastausgleich (**Infrastruktur > Netzwerkfunktionen > Lastausgleich**) „unbekannt“.

StyleBooks

- Wenn Sie die Konfigurationspakete bearbeiten, werden Änderungen, die Sie an ACLs oder PBR-Regeln (Policy-Based Routing) vornehmen, wie Hinzufügen, Aktualisieren oder Löschen, nicht angewendet.

June 5, 2024

Analysen

NetScaler Console in Microsoft Sentinel integrieren

Unter **Observability Integration** können Sie jetzt die Integration von NetScaler Console mit Microsoft Sentinel konfigurieren, um Einblicke in Microsoft Sentinel zu exportieren und anzuzeigen. Für eine erfolgreiche Integration stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Azure-Abonnement** – Ein Azure-Abonnement zum Bereitstellen und Verwenden von Microsoft Sentinel.
- **Log Analytics Workspace** – Ein Arbeitsbereich ist erforderlich, um die gesammelten Daten zu speichern und zu analysieren.
- **IAM-Rollen** – Berechtigungsstufen wie Leser, Mitwirkender müssen für den Arbeitsbereich festgelegt werden.
- **Benutzerdefinierte Tabellen** – Zum Speichern und Senden der NetScaler Console-Daten an den Arbeitsbereich.

Weitere Informationen finden Sie unter Integration mit Microsoft Sentinel

Plattform

Unterstützung für OpenSSH Version 9.x

Die OpenSSH-Version auf NetScaler wurde von 8.x auf 9.x aktualisiert.

StyleBooks

Option „Als Entwurf speichern“ in Konfigurationspaketen

Sie können das Konfigurationspaket jetzt als Entwurf speichern. Führen Sie die folgenden Schritte aus, um die Konfiguration als Entwurf zu speichern:

1. Navigieren Sie zu **Applications > Configuration > Config Packs**.
2. Klicken Sie auf der Seite **Configurations** auf **Add**.
3. Wählen Sie ein Stylebook aus und klicken Sie auf **Select**.
4. Klicken Sie auf der Seite **Konfiguration erstellen** auf **Als Entwurf speichern**.

Die gespeicherten Entwürfe werden auf der Registerkarte **Entwurfskonfigurationen** unter **Ausstehende Konfigurationen** angezeigt.

Weitere Informationen finden Sie unter Konfigurationspakete als Entwurf speichern.

Option „Planen“ in Konfigurationspaketen

Sie können jetzt die Bereitstellung neu erstellter Konfigurationspakete planen. Um einen Zeitplan für ein neues Konfigurationspaket zu erstellen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Applications > Configuration > Config Packs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Klicken Sie auf der Seite **Konfigurationen** auf **Hinzufügen**.
3. Wählen Sie das Stylebook aus und klicken Sie auf **Auswählen**.
4. Wählen Sie auf der Seite **Konfiguration erstellen** unter **Ausführung** aus der Liste **Ausführungsmodus** die Option **Später** aus.
5. Wählen Sie die gewünschte Uhrzeit und das Datum für die Planung aus.

Für bereitgestellte Konfigurationspakete können Sie planen, wann die Updates veröffentlicht und wann das Konfigurationspaket gelöscht werden soll. Die Planungsoptionen sind verfügbar, wenn Sie ein bereitgestelltes Konfigurationspaket bearbeiten.

Weitere Informationen finden Sie unter Einen Zeitplan für ein Konfigurationspaket erstellen.

Behobene Probleme

Die in Build Jun 5, 2024 behobenen Probleme.

Analysen

- Die Details zu **Application Heath** im **Übersicht**-Dashboard zeigen nicht die gleichen Details an, die unter **Application Score** im **App Dashboard** verfügbar sind.

- Wenn mehr als 25000 virtuelle Server über NetScaler Console verwaltet werden, kann das App Dashboard länger zum Laden der Details benötigen.

Infrastruktur

- Die Ereignisregeln generieren nicht die erwarteten Aktionen, wenn sich der Status der Dienstgruppe ändert.

StyleBooks

- Wenn Sie Sammlungsdaten mit leeren Werten für Felder vom Typ IP-Adresse, Ganzzahl oder Boolescher Wert zur benutzerdefinierten Datenquelle in StyleBooks hinzufügen, kann der Vorgang fehlschlagen.

- Wenn Sie ein Konfigurationspaket über die NetScaler Console GUI erstellen, kann das System eine leere Liste für die Parameter zurückgeben, die sich auf die integrierte verwaltete-adc-Datenquelle beziehen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wenn Sie versuchen, ein Konfigurationspaket zu erstellen oder einen Probelauf durchzuführen, können die Vorgänge fehlschlagen, wenn beide der folgenden Bedingungen erfüllt sind:
  - Die StyleBook-Definition verweist innerhalb des Komponentenabschnitts auf ein anderes StyleBook.
  - Wenn Sie Parameter vom Typ „Datum“ zu Eigenschaften zwischen dem aktuellen StyleBook und dem referenzierten StyleBook zuweisen.

May 22, 2024

Analysen

Massen-Upgrade von virtuellen SSL-Servern mithilfe der Aufgabe zum Upgrade auf SSL A+-Bewertung

Unter **Aufgaben** können Sie jetzt die Aufgabe **Upgrade auf SSL A+-Bewertung** anzeigen. Der bestehende Prozess zum Upgrade auf die SSL A+-Bewertung im **App-Dashboard** ermöglicht es Ihnen, jeweils nur eine Anwendung zu aktualisieren. Mithilfe der Aufgabe **Upgrade auf SSL A+-Bewertung** können Sie ein Massen-Upgrade durchführen.

NetScaler Console überprüft die SSL-Konfiguration des virtuellen Anwendungsservers mit dem sicheren NetScaler-Frontend-Profil und identifiziert die nicht A+-bewerteten Anwendungen. Die Aufgabe **Upgrade auf SSL A+-Bewertung** zeigt die nicht A+-bewerteten Anwendungen an. Als Administrator können Sie Anwendungen auswählen und ein Massen-Upgrade durchführen, um die SSL-Konformität zu erreichen.

Weitere Informationen finden Sie unter Umsetzbare Aufgaben und Empfehlungen.

Lizenzierung

Tatsächliche Nutzungsdetails in der Flexed-Lizenzberichterstattung

Im Dashboard **Flexed-Lizenzberichterstattung** (**NetScaler-Lizenzierung > Flexed-Lizenzierung > Berichterstattung**) können Sie jetzt die tatsächliche Bandbreiten-/Durchsatznutzung anzeigen, die es Ihnen ermöglicht, die Verbrauchsdetails (Spitzenauslastung und durchschnittliche Auslastung) anzuzeigen. Zuvor zeigte das Dashboard nur die Zuweisungs- und Berechtigungsdetails an.

Darüber hinaus sind die folgenden Verbesserungen auch im Dashboard für die Flexed-Lizenzberichterstattung verfügbar:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Filter zum Anzeigen von Details für ausgewählte NetScaler-Instanzen.
- Option zum Exportieren von Details im PDF-, PNG- und JPEG-Format.
- Bandbreite wird in Durchsatzkapazität umbenannt.

Weitere Informationen finden Sie unter Flexed-Lizenzberichterstellung

StyleBooks

NetScaler-Richtlinienausdrücke in StyleBooks erstellen

Die StyleBooks-GUI ermöglicht es Ihnen jetzt, NetScaler-Richtlinienausdrücke durch Auswahl von Elementen aus Listen zu erstellen, wodurch Sie Ausdrücke schneller und genauer erstellen können. Um den Richtlinienausdruckseditor für einen Parameter verfügbar zu machen, geben Sie das `is_policy_expression` GUI-Attribut in der Parameterdefinition von StyleBooks an.

Weitere Informationen finden Sie unter Richtlinienausdrücke in StyleBooks.

Behobene Probleme

Die Probleme, die in Build May 22, 2024 behoben wurden.

Infrastruktur

Wenn Sie in **Config Job** die Vorlage **ShowConfiguration** gleichzeitig auf dem primären und sekundären NetScaler in einem HA-Paar ausführen, wird durch Klicken auf **Download Result Files** die Datei nur für die sekundäre Instanz heruntergeladen.

StyleBooks

Wenn Sie eine NetScaler-Instanz, die eine Subnetz-IP-Adresse (SNIP) für den Verwaltungszugriff verwendet, aus der NetScaler Console löschen und die Instanz dann erneut hinzufügen, können die Vorgänge für Konfigurationspakete, die vor dem Löschen der Instanz erstellt wurden, fehlschlagen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

April 23, 2024

Analysen

Unterstützung für den Export periodischer Daten für benutzerdefinierte NetScaler-Instanzen

Wenn Sie ein Abonnement für den Datenexport der NetScaler Console nach Splunk oder New Relic erstellen, können Sie jetzt **Periodischer Export** (täglich oder stündlich) auswählen und auf die benutzerdefinierten Instanzen anwenden. Zuvor wurde der Export periodischer Insights-Daten an die benutzerdefinierten Instanzen nicht unterstützt.

Infrastruktur

Zusätzliche Ereigniswarnung für die Festplattenauslastung

Die NetScaler Console ermöglicht es Ihnen jetzt, einen zusätzlichen Schwellenwert für Festplattenauslastungsalarme festzulegen. Mit diesem Schwellenwert können Sie eine Untergrenze festlegen, um Warnungen zu erhalten, bevor ein oberer Schwellenwert überschritten wird. Um den unteren Schwellenwert zu konfigurieren, navigieren Sie zu **Einstellungen > SNMP > Bearbeiten** und aktivieren Sie **Einen unteren Schwellenwert konfigurieren**.

Weitere Informationen finden Sie unter Systemalarme konfigurieren und anzeigen.

Behobene Probleme

Die Probleme, die in Build April 23, 2024 behoben wurden.

Infrastruktur

- Wenn Sie versuchen, den NetScaler Console-Bericht als Snapshot unter **Infrastructure > Instances > NetScaler** zu exportieren, reagiert die Seite nicht mehr.
- Wenn mehr als 10 NetScaler-Instanzen über einen Agent in NetScaler Console verwaltet werden, schlägt das Agent-Inventarsubsystem fehl. Infolgedessen ruft NetScaler Console die neuesten NetScaler-Konfigurationsdaten nicht ab.

Lizenzierung

- Die Anzahl der Instanzen, die auf dem Flexed License-Dashboard angezeigt werden, ist falsch.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sicherheit

- Wenn Sie Verstoßdatensätze in Tabellenform über die Optionen **Export Now** oder **Schedule Export** unter **Security > Security Violations > All Violations > Violation Details** exportieren, werden nur die in der aktuellen Seitenansicht sichtbaren Datensätze in den Bericht aufgenommen, unabhängig von der Anzahl der Datensätze, die unter **Number of Records to Export** ausgewählt wurden.

April 10, 2024

Analysen

Observability-Integration – Unterstützung zur Konfiguration des Exports von NetScaler-Metriken und Audit-Protokollen nach Splunk

Unter **Settings > Observability Integration** können Sie jetzt den Export von NetScaler-Metriken und Audit-Protokollen nach Splunk konfigurieren.

Weitere Informationen finden Sie unter Konfigurieren des Exports von NetScaler-Metriken und Audit-Protokollen nach Splunk.

Infrastruktur

Zugriff auf die NetScaler-GUI über den Hostnamen

Wenn Sie sich über **Infrastruktur > Instanzen > NetScaler** mit NetScaler verbinden, stellt das Klicken auf den Hostnamen nun die Verbindung zur NetScaler-GUI über den Hostnamen her. Zuvor wurde die Verbindung zur NetScaler-GUI über die NSIP hergestellt, wenn Sie entweder auf den Hostnamen oder die IP-Adresse geklickt haben.

Diskrepanzen zwischen Hochverfügbarkeitsknoten während des Upgrades anzeigen

Sie können jetzt Konfigurationsdiskrepanzen zwischen dem primären Knoten und dem sekundären Knoten während des Upgrades der NetScaler-Hochverfügbarkeitsbereitstellung anzeigen. Sie können die Diskrepanzen überprüfen und entscheiden, ob Sie das Upgrade fortsetzen oder anhalten möchten. Um diese Funktion zu nutzen, navigieren Sie zu **Infrastruktur > Upgrade-Aufträge** und zeigen Sie die Diskrepanzen auf der Registerkarte **Pre-upgrade validation** an.

Weitere Informationen finden Sie unter Upgrade-Aufträge .

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Behobene Probleme

Die Probleme, die in Build April 10, 2024 behoben wurden.

Infrastruktur

- Die Seite **Infrastruktur > Ereignisse > Syslog-Meldungen** wird leer angezeigt, wenn die Syslog-Meldungen Sonderzeichen wie hochgestellte Zeichen enthalten.

- Die Anzahl der verwendeten und ungenutzten Zertifikate, die unter **Infrastruktur > SSL-Dashboard > Nutzung** angezeigt wird, ist falsch, wenn die SSL-Zertifikate Zertifikatsketten aufweisen.

Lizenzierung

- Die Ports 27000 und 7279, die auf dem Agenten für Pooled- oder Flexed-Lizenzen benötigt werden, könnten nach dem Neustart der Agentenprozesse nicht mehr verfügbar sein. In solchen Szenarien könnten die NetScaler-Instanzen, die Pooled- oder Flexed-Lizenzen verwenden, in die Kulanzperiode wechseln.

Sicherheit

- Wenn Sie zu **Security > WAF Recommendation** navigieren, wird möglicherweise die folgende Fehlermeldung angezeigt:

  "**HTTP-Fehler 500 () beim Zugriff auf den Datenendpunkt: „apps“**"

March 26, 2024

Behobene Probleme

Die Probleme, die in Build March 26, 2024 behoben wurden.

Infrastruktur

- Beim Erstellen oder Aktualisieren eines Upgrade-Auftrags, wenn Sie versuchen, eine Instanz unter **Infrastructure > Upgrade Jobs > Create Job > Select Instance > Add Instances** auszuwählen, zeigt die Seite **Add Instances** die Registerkarte **Partitions** an, die für den Workflow nicht relevant ist. Wenn Sie eine Partition auswählen, reagiert die Seite nicht mehr und Sie können nicht fortfahren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wenn Sie Slack-Benachrichtigungen unter **Settings > Notifications > Slack > Create Slack Notifications** erstellen und **Notifications with attachment** auswählen, werden die Benachrichtigungen nicht angezeigt und die folgende Fehlermeldung erscheint:

  `Invalid token`

StyleBooks

- Wenn die Option **Nur sicherer Zugriff** unter **Einstellungen > Administration > Systemkonfigurationen > Grundeinstellungen** ausgewählt ist und Sie versuchen, eine Device API Proxy-Operation durchzuführen, schlägt der Vorgang fehl.

March 12, 2024

Lizenzierung

Unterstützung zur manuellen Auswahl eines NetScaler-Agenten als LSA im NetScaler Console-Dienst

Sie können jetzt manuell einen NetScaler-Agenten als Lizenzserver-Agent (LSA) für die NetScaler Pooled-Lizenzierung oder die NetScaler Flexed-Lizenzierung auswählen.

Wenn ein LSA ausgefallen ist, wartet der NetScaler Console-Dienst 24 Stunden, bevor er den nächsten LSA automatisch auswählt. Der Administrator kann den neuen LSA in der Zwischenzeit manuell über diese Funktion auswählen. Der Administrator muss jedoch sicherstellen, dass der Status des neu ausgewählten LSA **UP** und sein Diagnosestatus **OK** ist.

Weitere Informationen finden Sie unter NetScaler-Agent-Verhalten für Flexed- oder Pooled-Lizenzierung.

Behobene Probleme

Die Probleme, die in Build March 12, 2024 behoben wurden.

Analysen

- Wenn Sie **Gateway Insight** für die virtuellen Gateway-Server aktivieren, zeigt die Spalte **Analytics Status** unter **Settings > Analytics Configuration > All Virtual Servers** den Status **Disabled** an.

- Unter **Gateway > Gateway Insight** zeigt die Registerkarte **Authentication** keine Benutzerdetails für fehlgeschlagene Authentifizierungen an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastruktur

- Wenn eine benutzerdefinierte Richtlinie erstellt und ein Benutzer zu dieser Richtlinie hinzugefügt wird, treten bei GET-API-Anfragen für bestimmte Ressourcen Berechtigungsprobleme auf, und die folgende Fehlermeldung wird angezeigt:

  „Nicht autorisiert, da die erforderlichen Berechtigungen nicht erteilt wurden“

February 28, 2024

Infrastruktur

Updates für VIP-Lizenzierung und NetScaler Console Service-Speicher

- **Unbegrenzte VIPs im NetScaler Console Service**: Ab NetScaler Console Service Release 14.1-21.x wird das Konzept der lizenzierten VIPs entfernt. Eine unbegrenzte Anzahl von VIPs ist jetzt im NetScaler Console Service verfügbar. Sie müssen keine NetScaler Console Virtual Server-Lizenzen mehr erwerben, da die VIP-Lizenz-SKU in Kürze End of Sale (EOS) und End of Renewal (EOR) sein wird.
- **NetScaler Console Service-Speicher**:
  - Die NetScaler Console Service-Speicher-SKU wird in Kürze End of Sale (EOS) und End of Renewal (EOR) sein.
  - Der standardmäßige NetScaler Console Service-Speicheranspruch beträgt jetzt 5 GB.
  - Alle in der Vergangenheit erworbenen NetScaler Console Service-Speicherlizenzen werden bis zum Ende der Laufzeit anerkannt.
  - Alle in der Vergangenheit erworbenen NetScaler Console VIP-Lizenzen, die Sie zu einem proportionalen Anspruch auf NetScaler Console Service-Speicher berechtigten, werden bis zum Ende der Laufzeit anerkannt.
  - Wenn Sie ein anderes Lizenzpaket erwerben, das Sie zu einem höheren NetScaler Console-Speicheranspruch berechtigt, werden die standardmäßigen 5 GB entsprechend dem Anspruch geändert.

Updates für Analyse- und Metrik-Collector

- Mit der Unterstützung unbegrenzter VIPs ab Build 14.1 21.x werden alle vorhandenen und neuen virtuellen Server jetzt automatisch lizenziert. Sie können Analysen auf den virtuellen Servern aktivieren, ohne sie explizit zu lizenzieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Der Metrik-Collector ist jetzt standardmäßig für alle NetScaler-Lizenztypen in den neuen NetScaler-Instanzen deaktiviert, die in NetScaler Console ab Build 14.1 21.x hinzugefügt wurden. Die Konfiguration des Metrik-Collectors für die vorhandenen verwalteten Instanzen bleibt unverändert.

Analysen

Aktionsrichtlinien – Benachrichtigungen für die Anwendungsnutzung konfigurieren

In Aktionsrichtlinien (**Einstellungen > Aktionen > Aktionsrichtlinien**) können Sie jetzt eine Aktionsrichtlinie für die Anwendungsnutzung konfigurieren und die Optionen **Anfragen pro Sekunde**, **Durchsatz** und **Datenvolumen** auswählen. Diese Optionen ermöglichen es Ihnen, Benachrichtigungen für den Durchschnitt der Anfragen pro Sekunde, Anomalien bei Anfragen pro Sekunde, den durchschnittlichen Durchsatz, Durchsatzanomalien, das gesamte Datenvolumen und Datenvolumenanomalien zu konfigurieren und zu empfangen. Weitere Informationen finden Sie unter Konfigurieren einer Aktionsrichtlinie zum Empfangen von Anwendungsereignisbenachrichtigungen.

Observability-Integration

Der Konfigurations-Workflow für die Integration mit Splunk und New Relic wurde für eine bessere Benutzererfahrung verbessert und ist jetzt unter **Einstellungen > Observability-Integration** verfügbar. Zuvor war der Konfigurations-Workflow für die Integration mit Splunk und New Relic unter **Einstellungen > Ecosystem-Integration** verfügbar.

Weitere Informationen finden Sie unter Observability-Integration

Observability-Integration – Unterstützung zum Konfigurieren des Exports von NetScaler-Metriken nach Prometheus

Unter **Einstellungen > Observability-Integrationen** können Sie jetzt den Export von NetScaler-Metriken nach Prometheus konfigurieren, indem Sie das Standardschema auswählen.

Weitere Informationen finden Sie unter Prometheus-Integration und Observability-Integration.

Gateway Insight – Verbesserungen beim Export von Berichten

Unter **Gateway > Gateway Insight** können Sie jetzt Berichte nur mit den ausgewählten Optionen exportieren, indem Sie das Einstellungssymbol in allen Tabellen unter jeder Metrik (EPA,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authentifizierung, Autorisierungsfehler, SSO und Anwendungsstart) verwenden. Zuvor zeigte der exportierte Bericht alle Informationen an, unabhängig von den ausgewählten Optionen.

StyleBooks

Updates für Standard-StyleBooks

Standard-StyleBooks, die auf NetScaler Version 10.5 basieren, werden in zukünftigen Releases eingestellt. Ein neuer Satz von Standard-StyleBooks ist jetzt unter **Anwendungen > Konfiguration > StyleBooks > Standard-StyleBooks** verfügbar, basierend auf NetScaler Version 13.0.

Option zum Klonen eines StyleBooks

NetScaler Console ermöglicht Administratoren jetzt, ein Duplikat eines StyleBooks zusammen mit seinen Abhängigkeiten zu erstellen. Administratoren können dieses Paket dann für zusätzliche Anpassungen verwenden, z. B. zum Aktualisieren von `parameters` und `components`.

Um diese Funktion zu nutzen, navigieren Sie zu **Anwendungen > Konfiguration > Stylebooks**, wählen Sie ein Standard- oder benutzerdefiniertes StyleBook aus und klicken Sie auf **Klonen**.

Weitere Informationen finden Sie unter Klonen eines StyleBooks.

Behobene Probleme

Die Probleme, die in Build Feb 28, 2024 behoben wurden.

Infrastruktur

- Die Migration von NetScaler Console zum NetScaler Console-Dienst schlägt fehl, und bestimmte Azure Active Directory-Gruppen sind im NetScaler Console-Dienst nicht verfügbar. Dieses Problem tritt auf, weil die in NetScaler Console erstellten Azure Active Directory-Gruppennamen Leerzeichen enthalten.

- Benutzer können nicht auf NetScaler Console zugreifen, wenn sie mehreren Azure Active Directory-Gruppen angehören.

- In **Web Insight** und **Security Violations** wurde der Workflow „Export planen“ in der GUI für eine bessere Benutzerfreundlichkeit verbessert.

- Unter **Infrastructure > Network Reporting** enthält der tabellarische Exportbericht keine Details wie Dienst, Dienstgruppe, virtueller Server und Schnittstellenname.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Das Dashboard für flexible Lizenzen zeigt NetScaler-Details erst an, nachdem mindestens ein NetScaler aus dem Premium-Bandbreitenlizenzpool ausgecheckt wurde.

February 06, 2024

Analysen

App-Dashboard – Unterstützung zum Anzeigen von Anwendungsmetrikdetails aus der NetScaler-Administratorpartition

Im **App-Dashboard** können Sie jetzt Metrikdetails für Anwendungen anzeigen, die aus den NetScaler-Administratorpartitionen erstellt wurden. Zuvor konnten Sie Anwendungen aus den Administratorpartitionen nur ohne Metriken anzeigen.

Infrastruktur

NetScaler ADM-Rebranding in Citrix Cloud™

Ab Build 14.1 16.x wurde der NetScaler ADM-Dienst in NetScaler Console-Dienst umbenannt. In Fortsetzung dessen wird Application Delivery Management nun an folgenden Stellen in NetScaler Console umbenannt:

- Die Kachel unter **Meine Dienste** auf der Citrix Cloud-Startseite.
- Der Dienstname im **Citrix Cloud-Menü > Meine Dienste**.
- Der Produktname im Workflow „Administrator hinzufügen“ unter **Zugriff festlegen > Benutzerdefinierter Zugriff** aus **Citrix Cloud-Menü > Identitäts- und Zugriffsverwaltung > Administratoren > Administrator/Gruppe hinzufügen**.

Standardvalidierungsskripte in Upgrade-Jobs ausführen

NetScaler Console enthält jetzt eine Option für Standardvalidierungsskripte im Upgrade-Job-Workflow. Diese Standardskripte werden sowohl vor als auch nach einem Upgrade-Job ausgeführt und generieren einen Diff-Bericht. Sie haben weiterhin die Möglichkeit, benutzerdefinierte Standardskripte auszuführen.

Weitere Informationen finden Sie unter NetScaler-Instanzen aktualisieren.

Automatisieren der Bereitstellung von Radarobjekten für NetScaler Console Sites

NetScaler unterstützt die Automatisierung der Bereitstellung von Radarobjekten für NetScaler Console Sites, wodurch die manuelle Bereitstellung auf den NetScaler-Instanzen entfällt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Diese Verbesserung ist nur verfügbar, wenn Sie eine NetScaler-Instanz bearbeiten, und gilt nur für den Standorttyp **Data Center** (mit Typ **Private**) oder **Branch**.

Wenn Sie **Deploy to NetScaler** aus der Liste **Real User Measurements** auswählen, wird die Liste **NetScaler Instance** automatisch ausgefüllt, sodass Sie die spezifische Instanz auswählen können, auf der das Radarobjekt (r20.gif) bereitgestellt werden soll.

Weitere Informationen finden Sie unter Automatisieren der Bereitstellung von Radarobjekten.

Behobene Probleme

Die Probleme, die in Build Feb 06, 2024 behoben wurden.

Analysen

- Der **XML SQL**-Angriff wird weder im Sicherheits-Dashboard (**Security > Security Dashboard**) noch im Dashboard für Sicherheitsverletzungen (**Security > Security Violations**) gemeldet.

Lizenzierung

- Das Flexed-Lizenz-Dashboard zeigt NetScaler-Details erst an, nachdem mindestens ein NetScaler aus dem Premium-Bandbreitenlizenzpool ausgecheckt wurde.

Verwaltung und Überwachung

- Wenn ein Konfigurationsauftrag erstellt wird, zeigt der Status unter **Infrastruktur > Konfiguration > Aufträge** den Status **Abgeschlossen** an, aber **Details > Ausführungsübersicht** zeigt 0 % abgeschlossen an.

- Ein zweistufiger Upgrade-Auftragsstatus für ein NetScaler HA zeigt „Geplant“ an, obwohl das NetScaler HA-Upgrade abgeschlossen ist. Der primäre Knoten zeigt „Abgeschlossen“ an (**Status Stufe 1: Abgeschlossen**), aber der sekundäre Knoten zeigt „Geplant“ an (**Stufe 2: Geplant**).

- Wenn eine Konfigurationsprüfvorlage mit Sonderzeichen im Namen unter **Infrastruktur > Konfiguration > Prüfvorlagen > Hinzufügen** erstellt wird, wird die Vorlage erfolgreich generiert. Ein Differenzbericht kann jedoch für die Vorlage im Dashboard **Konfigurationsprüfung** während der Abfrage nicht generiert werden.

  Dieses Problem tritt auf, wenn andere Sonderzeichen als „-“ (Bindestrich) und „_“ (Unterstrich) verwendet werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 24, 2024

Analysen

Details zur Upgrade-Empfehlung in Aufgaben anzeigen

Unter **Aufgaben** können Sie jetzt die ausführbare Aufgabe **Upgrade-Empfehlung** anzeigen. Basierend auf Ihrer aktuellen Auslastung, wenn Ihre NetScaler-Instanzen das End-of-Life (EOL) oder End-of-Maintenance (EOM) innerhalb von 90 Tagen bereits erreicht haben oder kurz davor stehen, zeigt die Aufgabe **Upgrade-Empfehlung** die Details dieser Instanzen an. Sie können auf **Aktion ausführen** klicken und diese Instanzen auf einen empfohlenen Build aktualisieren.

Infrastruktur

Erweiterte Berechtigungen für schreibgeschützte Benutzer

Benutzer mit schreibgeschützten Berechtigungen für die folgenden Funktionen können jetzt NetScaler-Instanzen abfragen:

- SSL-Zertifikate (**Infrastructure > SSL Dashboard > Poll Now**)
- Netzwerkfunktionen (**Infrastructure > Network Functions > Poll Now**)
- Konfigurationsprüfungen (**Infrastructure > Configuration > Configuration Audit > Poll Now**)

Behobene Probleme

Die Probleme, die in Build Jan 24, 2024 behoben werden.

- Die integrierte Agentenregistrierung in NetScaler SDX zeigt eine Erfolgsmeldung an, aber die SDX-Instanz wird nicht unter **Infrastructure > Instances Dashboard** angezeigt.
- Unter **Infrastructure > Network Functions > Load Balancing** zeigt die Registerkarte **Servers** die Anzahl der Server an, aber keine Tabelleneinträge für Nicht-Standardbenutzer.

January 16, 2024

Unterstützung für die Identifizierung und Behebung von CVE-2023-6548 und CVE-2023-6549

Das NetScaler Console Service Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2023-6548 und CVE-2023-6549.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die Identifizierung für CVE-2023-6548 erfordert einen Versionsscan.
- Die Identifizierung für CVE-2023-6549 erfordert eine Kombination aus Versions- und Konfigurationsscan.

Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält.

HINWEIS:

Das Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

Weitere Informationen zur Verwendung von NetScaler ADM zum Upgrade von NetScaler-Instanzen finden Sie unter Aufträge zum Upgrade von NetScaler-Instanzen verwenden.

Weitere Informationen finden Sie unter Sicherheitsbulletin.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitshinweissystems abgeschlossen ist und die Auswirkungen von CVE-2023-6548 und CVE-2023-6549 im Sicherheitshinweismodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, können Sie einen On-Demand-Scan starten, indem Sie auf **Jetzt scannen** klicken.

January 09, 2024

Analysen

Unterstützung zum Teilen benutzerdefinierter Dashboards mit anderen Benutzern

Als Administrator können Sie das benutzerdefinierte Dashboard jetzt mit anderen Benutzern teilen. Wählen Sie unter **Übersicht > Benutzerdefiniertes Dashboard** ein Dashboard aus und klicken Sie auf **Teilen**. Geben Sie den Benutzernamen ein und klicken Sie auf **Einladen**, um das Dashboard zu teilen. Die zugewiesenen Benutzer können das Dashboard im schreibgeschützten Modus anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastruktur

ITM Radar in NetScaler Console Sites konfigurieren

Das ITM-Radar verbessert die Netzwerküberwachungsfunktionen. Die in Rechenzentren, virtuellen Maschinen oder Cloud-Anbietern bereitgestellten Sites können jetzt das Radarobjekt (r20.gif) hosten, das Einblicke in Leistungskennzahlen bietet. Das ITM-Radarobjekt sammelt aktiv wertvolle Anwendungsstatistiken der Endbenutzer und stellt den Sites robuste ITM-Radar-Telemetriedaten für eine effektivere Netzwerküberwachung und fundierte Entscheidungen zur Verkehrsverwaltung zur Verfügung.

Weitere Informationen finden Sie unter ITM-Radar konfigurieren.

Gateway-Einblicksdaten in Splunk und New Relic anzeigen

Wenn Sie in **Einstellungen > Ökosystemintegration** ein neues Abonnement für die Integration des NetScaler Console-Dienstes mit Splunk und New Relic erstellen, können Sie jetzt die Option **Gateway Insights** auswählen. Nachdem Sie das Abonnement mit der Option **Gateway Insights** konfiguriert haben, können Sie die Gateway-Einblicksdaten in Splunk und New Relic anzeigen.

Weitere Informationen finden Sie unter Integration mit Splunk und Integration mit New Relic.

SSL-Daten sofort nach Splunk und New Relic exportieren

Die SSL-Daten werden jetzt sofort nach der Erstellung eines Abonnements durch einen Administrator durch Auswahl von **SSL Certificate Insight** in Splunk und New Relic exportiert. Zuvor mussten die Administratoren auf **Jetzt abfragen** (**Infrastruktur > SSL-Dashboard**) klicken, um die Daten zum ersten Mal zu exportieren.

Details zur Upgrade-Empfehlung in Aufgaben anzeigen

Unter **Aufgaben** können Sie jetzt die ausführbare Aufgabe **Upgrade-Empfehlung** anzeigen. Basierend auf Ihrer aktuellen Auslastung, wenn Ihre NetScaler-Instanzen bereits das End-of-Life (EOL) oder End-of-Maintenance (EOM) innerhalb von 90 Tagen erreicht haben oder kurz davor stehen, zeigt die Aufgabe „Upgrade-Empfehlung“ die Details dieser Instanzen an. Sie können auf **Aktion ausführen** klicken und diese Instanzen auf einen empfohlenen Build aktualisieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Aktionsrichtlinie – Benachrichtigungen für Anfragen, Bandbreite und Antwortzeit konfigurieren

In **Aktionsrichtlinien** (**Einstellungen > Aktionen > Aktionsrichtlinien**) können Sie beim Konfigurieren einer Aktionsrichtlinie in der Anwendungsleistung jetzt die Optionen **Anfragen**, **Bandbreite** und **Antwortzeit** auswählen. Diese Optionen ermöglichen es Ihnen, Benachrichtigungen für die Gesamtzahl der Anfragen, die Gesamtbandbreite, die durchschnittliche Antwortzeit und Anomalien der Antwortzeit zu konfigurieren und zu empfangen. Weitere Informationen finden Sie unter Eine Aktionsrichtlinie zum Empfangen von Anwendungsereignisbenachrichtigungen konfigurieren.

Zusätzlich können Sie jetzt auch eine Aktionsrichtlinie aus dem Diagrammtrend in **Web Insight** für diese Metriken konfigurieren. Als Administrator, wenn Sie ein ungewöhnliches Datenverkehrsmuster oder einen plötzlichen Anstieg dieser Metriken für eine Anwendung bemerken, ermöglicht Ihnen diese Verbesserung, eine relative Aktionsrichtlinie zu erstellen, indem Sie auf **Aktionsrichtlinie erstellen** klicken, nachdem Sie sie auf einen bestimmten Punkt im Diagramm platziert haben.

Behobene Probleme

Die Probleme, die in Build Jan 09, 2024 behoben wurden.

Lizenzierung

- Nachdem die Flexed- oder Pooled-Lizenz angewendet wurde, wird die Seite **Analytics Configuration** (**Einstellungen > Analytics Configuration**) nicht mit den korrekten Details aktualisiert.
- Das Flexed-Lizenz-Dashboard unter **NetScaler Licensing > Flexed Licensing > Dashboard** wird leer angezeigt.
- Unter **NetScaler Licensing > License Management** funktioniert die Konfiguration für die Schwellenwertüberschreitung per E-Mail-Benachrichtigung nicht wie erwartet.

Bekannte Probleme

NetScaler Application Delivery Management (NetScaler Console) weist die folgenden bekannten Probleme auf:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lizenzierung

- Dieses Problem betrifft Sie, wenn Sie eine SDX migriert haben oder von einer beliebigen Art von NetScaler-Lokallizenz (Abonnement mit fester Kapazität oder unbefristete Lizenz) basierend auf Dateilizenzen zu einer beliebigen Art von Lizenz mit LAS-basierter Lizenzierung migrieren und die alten dateibasierten Lizenzen nicht von der SVM gelöscht wurden.

  Auswirkung: Wenn nach der Umstellung auf LAS noch eine lokale alte dateibasierte Lizenz auf der SVM vorhanden ist, führt der Ablauf der dateibasierten Lizenz am Datum des Ablaufs dieser Lizenzdatei zur Entlizenzierung der SDX (SVM und VPX auf SDX).

  Problemumgehung: Löschen Sie die lokale(n) dateibasierte(n) Lizenz(en) auf der SVM, nachdem die Migration zu LAS erfolgreich abgeschlossen wurde. Die dateibasierten Lizenzen befinden sich im SVM-Ordner /mpsconfig/license und müssen über die Shell-Eingabeaufforderung aus diesem Ordner gelöscht werden.

Verwaltung und Überwachung

- Administratorpartitionen werden sowohl beim Initiieren eines IOC-Scans als auch in den IOC-Scanergebnissen angezeigt. Diese Einträge können ignoriert werden, da der IOC-Scan die gesamte NetScaler-Appliance abdeckt.

- Die NetScaler® Console CVE-Empfehlung kann eine falsche Gesamt-Schweregrad anzeigen, wenn bei Scans zur Dateiintegritätsüberwachung keine Schwachstellen gefunden werden. Der korrekte Schweregrad wird in der detaillierten CVE-Ansicht angezeigt.

- Unter **Infrastruktur > SSL-Dashboard > Zertifikatsspeicher verwalten** kann NetScaler Console NetScaler-Zertifikate im PFX-Format nicht importieren, wenn Sie auf **NetScaler-Zertifikate importieren** klicken.

Infrastruktur

- Wenn in NetScaler Console eine Instanz für eine Systemgruppe autorisiert ist und der Instanz eine neue Partition hinzugefügt wird, wird die Autorisierungseinstellung der Systemgruppe automatisch der neuen Partition zugewiesen.

- Wenn Sie versuchen, ein Zertifikat auf einer NetScaler BLX™-Instanz zu installieren, schlägt die Installation fehl und auf der Seite **Infrastructure > SSL Dashboard > SSL Audit Logs** wird die folgende Fehlermeldung angezeigt:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`SCP: Authentication by password fails on _<ip-address>_.`.

- Wenn eine Ereignisregel mit einigen ausgewählten Entitäten unter **Infrastructure > Events > Rules > Create rule > Select Failure Objects** erstellt wird, werden nicht alle ausgewählten Entitäten angezeigt. Dieses Problem tritt auf, wenn eine große Anzahl von virtuellen Servern, Diensten oder Dienstgruppen vorhanden ist.

  Problemumgehung: Wenden Sie sich an das NetScaler Support-Team, um Unterstützung bei diesem Problem zu erhalten.

- Der SSH- oder SCP-Vorgang, der in den **Konfigurationsaufträgen** verwendet wird, kann mit der folgenden Fehlermeldung fehlschlagen:

  „SSH Failure establishing ssh session: -5“

  Problemumgehung:

  a. Melden Sie sich mit einem SSH-Client bei NetScaler Console an.
  b. Überprüfen Sie die Ausgabe für den folgenden Befehl:

     `ls -l /etc/sshd_config`
  c. Aktualisieren Sie in `/etc/sshd_config` die Datei, um Folgendes hinzuzufügen:

     `HostKey /nsconfig/ssh/ssh_host_ecdsa_key`
  d. Wenden Sie die Änderungen an:

     `ps -aux | grep /usr/sbin/sshd | grep -v grep | tr -s ' ' | cut -d ' ' -f 2 | xargs kill -9`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Datenkonformität

PCI DSS-Konformität

Der Payment Card Industry (PCI) Data Security Standard (DSS) ist ein Sicherheitsstandard der Kreditkartenbranche, der ein erforderliches Sicherheitsniveau für Personen, Prozesse und Technologien definiert, das beim Speichern, Verarbeiten oder Übertragen von Kreditkartendaten vorhanden sein muss. PCI DSS gilt für Händler, Verarbeiter und Dienstleister sowie alle anderen Unternehmen, die Kreditkartendaten speichern, verarbeiten oder übertragen. Die PCI DSS-Konformitätsbescheinigung (AOC) ist letztendlich eine Bestätigung durch ein Unternehmen, dass ein bestimmtes Sicherheitsniveau erforderlich ist und vorhanden ist.

NetScaler® Application Delivery Management service PCI DSS-Konformität

Der NetScaler Application Delivery Management (ADM) Service hat die PCI DSS-Konformität erfolgreich durch eine Bewertung anhand der PCI DSS-Konformitätskontrollbereiche für Kunden erreicht. Der NetScaler Console Service speichert, verarbeitet und/oder überträgt keine PCI-Kundendaten. Der NetScaler Console Service wird außerdem jährlich einer PCI DSS-Bewertung durch einen Qualified Security Assessor (QSA) unterzogen, um unsere Dienste und Kontrollen zu bewerten.

Während Citrix die PCI DSS-Konformität des Kunden unterstützt, erreichen die Verwendung von NetScaler-Produkten und -Diensten allein keine PCI DSS-Konformität. Kunden sind dafür verantwortlich, sicherzustellen, dass sie über ein angemessenes Compliance-Programm, interne Prozesse und Kontrollen verfügen, um ihre PCI DSS-Konformitätsanforderungen zu erfüllen und aufrechtzuerhalten.

Klicken Sie auf NetScaler Console Service PCI-Konformitätsbescheinigung (AOC), um einen Offline-Bericht herunterzuladen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler® Telemetrieprogramm

Das NetScaler-Telemetrieprogramm ist ein obligatorisches Datenerfassungsprogramm, das das Hochladen erforderlicher Lizenz- und Funktionsnutzungsdaten ermöglicht, die für Kunden notwendig sind, um ihren Wartungs- und Support-Lizenzverpflichtungen nachzukommen. Citrix erfasst grundlegende Lizenz-Telemetriedaten sowie NetScaler-Bereitstellungs- und Funktionsnutzungs-Telemetriedaten für seine berechtigten Interessen, einschließlich der Lizenzkonformität. NetScaler Console-Konfigurations- und Funktionsnutzungsdaten werden ebenfalls erfasst, um Citrix-Produkte und -Dienste zu verwalten, zu messen und zu verbessern. Wir empfehlen dringend, NetScaler-Instanzen zu NetScaler Console hinzuzufügen, um Ihre NetScaler-Operationen insgesamt zu verbessern und zu vereinfachen und die Weiterentwicklung unserer Produkte und Dienste durch das Senden von NetScaler-Funktionsnutzungsdaten zu unterstützen. Erfahren Sie mehr. Das NetScaler-Telemetrieprogramm ist ab Build 14.1-28.x automatisch aktiviert.

Voraussetzungen

Stellen Sie sicher, dass:

- Der Agent auf der neuesten Version läuft. Standardmäßig werden die Agenten automatisch aktualisiert. In einigen Szenarien laufen die Agenten möglicherweise noch auf einer älteren Version, und Sie müssen den Agenten manuell aktualisieren. Weitere Informationen zur manuellen Aktualisierung des Agenten finden Sie unter Agenten manuell aktualisieren.
- Der NetScaler-Agent muss über Port 22 mit NetScaler kommunizieren können.
- Port 5140 ist im Netzwerk zugelassen, um die NetScaler Gateway-Telemetriedaten zu empfangen. (Gilt nur für NetScaler-Instanzen mit VPN-Virtual-Server-Konfiguration).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEISE:

- Der Telemetrie-Upload erfolgt alle 24 Stunden automatisch.
- Um die Telemetrie-Metriken in Ihren NetScaler-Instanzen zu erfassen und zu speichern, wurde die folgende Konfiguration im Rahmen des am 18. Juni 2024 veröffentlichten NetScaler-Telemetrieprogramms über NetScaler Console an Ihre NetScaler-Instanzen übertragen.

```
enable ns feature AppFlow

add analytics profile telemetry_metrics_profile -type timeseries
-outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "./
telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300
```

- Sie müssen das Telemetrie-Metrikprofil, das im Rahmen des NetScaler-Telemetrieprogramms übertragen wurde, mit dem folgenden Befehl entfernen:

```
rm analytics profile telemetry_metrics_profile
```

- Wenn Sie die Analysefunktionen von NetScaler oder NetScaler Console nicht verwenden, können Sie den folgenden Befehl verwenden, um die AppFlow-Konfiguration zu entfernen:

```
disable ns feature AppFlow
```

- Die Datei `/nsconfig/.telemetry.conf` wird mit dem folgenden Befehl für die Gateway-Telemetrie aktualisiert. NetScaler Console prüft stündlich auf diesen Befehl und fügt ihn hinzu, falls er fehlt. Dieser Befehl wird nur an NetScaler-Instanzen übertragen, die über eine VPN-Virtual-Server-Konfiguration verfügen:

```
ns_telemetry_server,&lt;Console IP>,5140
```

- Einige Telemetrieparameter werden über Skripte erfasst, die von NetScaler Console an NetScaler-Instanzen übertragen werden. Diese Skripte sind schreibgeschützt und ändern nichts in NetScaler.
- Die durch Telemetrie erfassten Informationen, wie E-Mail-Adressen, Benutzernamen und IP-Adressen, werden durch Hashing der Informationen an der Quelle mittels Einweg-Hashing-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Algorithmen sicher pseudonymisiert. Infolgedessen kann Citrix diese Werte nicht einsehen oder lesen. Diese Telemetriedaten werden ausschließlich für logische Asset-Matching-Zwecke verwendet.

Die folgende Tabelle enthält die Parameterdetails, die im Rahmen des NetScaler-Telemetrieprogramms erfasst werden:

KATEGORIEN	BESCHREIBUNG	WOFÜR WIR ES VERWENDEN
Lizenz- sowie NetScaler-Bereitstellungs- und Nutzungs-Telemetrie	Informationen zu Lizenzberechtigung, -zuweisung, -nutzung und übergeordnete NetScaler-Bereitstellungsdaten sowie NetScaler-Funktionsnutzung.	Lizenzkonformität und zur Verwaltung, Messung und Verbesserung des Dienstes.
NetScaler Console-Bereitstellungs- und Funktionsnutzungs-Telemetrie	Informationen zur Konsolenbereitstellung und Funktionsnutzung.	Zur Verwaltung, Messung und Verbesserung des Dienstes.

Weitere Informationen zur Liste der Telemetrieparameter finden Sie unter Daten-Governance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Datengovernance

Der NetScaler Console Service ist Teil der Citrix Cloud Services und nutzt Citrix Cloud als Plattform für Registrierung, Onboarding, Authentifizierung, Administration und Lizenzierung. Citrix erfasst und speichert Daten in Citrix Cloud als Teil des NetScaler Console Service. Dieses Dokument beschreibt, welche Daten erfasst werden und welche Methoden zur Datenerfassung, -speicherung und -übertragung verwendet werden.

Weitere Informationen zu den Datenschutzpraktiken bei Citrix finden Sie unter Übersicht über den Datenschutz bei Citrix Cloud Services.

Diese Informationen richten sich an Sicherheitsbeauftragte, Compliance-Beauftragte, Informationsprüfer, Administratoren für Netzwerkinfrastruktur und -betrieb sowie an Geschäftsbereichsleiter.

NetScaler®-Telemetrieprogramm

Das NetScaler-Telemetrieprogramm ist im NetScaler Console Service ab Build **14.1-28.x** aktiviert. Mit diesem Programm werden die erforderlichen Daten automatisch hochgeladen. Weitere Informationen zu den erfassten Telemetriedaten finden Sie unter Datengovernance für NetScaler-Telemetrie.

Wie erfassen, speichern und übertragen wir Daten?

Der NetScaler Console Service erfasst Daten von den verwalteten Instanzen und Agents. Diese Instanzen werden in den Räumlichkeiten des Kunden bereitgestellt, und die Daten werden vom Agent (der in den Räumlichkeiten des Kunden bereitgestellt wird) sicher über einen SSL-Kanal, der mit dem TLS 1.2-Protokoll verschlüsselt ist, an die Cloud übertragen.

Daten werden in einer relationalen Datenbank mit mandantenfähiger Datenisolation auf der Datenbankebene und als Dateien im Elastic File System (EFS) gespeichert, das in der AWS-Cloud in den Vereinigten Staaten, EMEA (Frankfurt) und APJ (Sydney) gehostet wird – abhängig vom vom Kunden gewählten Point of Presence (POP). Alle PoPs werden in kommerziellen AWS-Regionen gehostet.

Passwörter, SNMP-Community-Strings, SSL-Zertifikate und NetScaler-Konfigurationsbackups werden mit einem eindeutigen AES-256-Schlüssel pro Mandant verschlüsselt und sicher in der

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Datenbank gespeichert. Weitere Informationen zu den kommerziellen Regionen, die Citrix Cloud verwendet, und zur Präsenz des NetScaler Console Service in jeder Region finden Sie unter Geografische Überlegungen.

Datenkategorien

Für die Datenverarbeitungspraktiken werden die Daten klassifiziert in:

- **Kundeninhalte** – Alle Daten, die zum Speichern auf das Konto des Kunden hochgeladen werden, oder Daten in der Computerumgebung des Kunden, auf die NetScaler Zugriff erhält, um bestimmte Dienste auszuführen.
- **Protokolle** – Umfassen Aufzeichnungen von Diensten, einschließlich, aber nicht beschränkt auf:
  - Daten und Informationen zu Leistung, Stabilität, Nutzung, Sicherheit, Support
  - Technische Informationen über Geräte, Systeme

Kundeninhalte

Der NetScaler Console Service sammelt Informationen aus verschiedenen Quellen:

- NetScaler
- NetScaler Gateway
- NetScaler Web App Firewall (WAF) und Bot-Management

Der NetScaler Console Service sammelt zusätzlich zu den in den Protokollen erwähnten Informationen auch Informationen über die Sitzungs- und Aktivitätsdetails des Administrators.

Protokolle

Protokolle werden verwendet, um die Bereitstellung von Software-Updates, die Lizenzauthentifizierung, den Support, Analysen und andere Zwecke zu erleichtern, die mit den Citrix-Benutzervereinbarungen übereinstimmen.

Gesammelte Metadaten- und Telemetrieprotokolle umfassen:

- NetScaler Service-Agent-Hypervisor oder öffentliche Cloud-Plattform oder sowohl Agent-Hypervisor als auch öffentliche Cloud-Plattform
- Geografischer Standort des Agenten
- NetScaler-Version

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler-Produkttyp
- Lizenzinformationen (Express und Abonnement)
- Nutzung des Cloud-Dienstes durch den NetScaler Console-Administrator (wodurch die Benutzerfreundlichkeit für Administratoren verbessert wird).

Detaillierte Kundeninhalte und Protokolle

- **Ereignisverwaltung (Anmelden > Infrastruktur > Ereignisse)**
  - SNMP-Traps, die Warnungen zum Status und zur Leistung des NetScaler-Netzwerks bereitstellen.
  - Syslog von Webtransaktionen, die NetScaler-Netzwerkstatusinformationen durchlaufen.
  - SMS-Server-, Slack- und PagerDuty-Profildetails zum Auslösen von SMS-/Slack-Benachrichtigungen bei Ereignissen.
  - SMTP-Serverdetails für die E-Mail-Konfiguration.
  - ServiceNow-Profildetails zum Erstellen von Tickets in ServiceNow.
- **SSL-Zertifikatsverwaltung (Anmelden > Infrastruktur > SSL-Dashboard)**
  - SSL-Zertifikate, SSL-Schlüssel, SSL-CSR, CA-Aussteller und Signaturalgorithmen der Web-Apps, die von der NetScaler-Instanz optimiert werden.
- **Konfigurationsprüfung (Anmelden > Infrastruktur > Konfiguration > Konfigurationsprüfung)**
  - Datenverfolgung für NetScaler-Konfigurationsprüfungsänderungen, die sich auf die NetScaler-Instanzen beziehen, einschließlich der IP-Adresse des Web-App-Servers und der IP-Adresse des NetScaler.
- **Konfigurationsaufträge (Anmelden > Infrastruktur > Konfiguration > Konfigurationsaufträge)**
  - NetScaler-Konfigurationsdetails, Instanz-IP-Adresse und IP-Adressdetails des Web-App-Servers.
- **StyleBooks (Anmelden > Anwendungen > Konfiguration > StyleBooks)**
  - NetScaler-Konfigurationen, die als Vorlage gespeichert sind und Details zur IP-Adresse des Web-App-Servers enthalten.
- **Instanzverwaltung (Anmelden > Infrastruktur > Instanzen)**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - IP-Adresse der NetScaler-Instanzen, NetScaler-Instanztyp, NetScaler-Konfigurations-Backup, kritische NetScaler-Ereignisse und Geolokalisierung des Rechenzentrums, in dem die NetScaler-Instanz bereitgestellt wird (falls konfiguriert).

- **Infrastruktur-Analysen (Anmelden > Infrastruktur > Infrastruktur-Analysen)**
    - IP-Adresse der NetScaler-Instanzen, NetScaler-Instanztyp, kritische NetScaler-Ereignisse, Anzahl der zugeordneten Apps und Geolokalisierung des Rechenzentrums, in dem die NetScaler-Instanz bereitgestellt wird (falls konfiguriert).
- **Anwendungen (Anmelden > Anwendungen)**
    - App-Dashboard: Anwendungs-URL, Anforderungsmethode, Antwortcode, Gesamt-Bytes, Details zum Web-App-Server, IP-Adressen des virtuellen Servers, Client-Details, Browser, Client-Betriebssystem, Client-Gerät, SSL-Protokoll, SSL-Chiffrierstärke, SSL-Schlüsselstärke, IP-Adresse der NetScaler-Instanz, Zeitstempel der Server-Flaps und Antwort-Content-Typ.
- **Analysen (AppFlow/ Logstream)**
    - **Web Insights (Anmelden > Anwendungen)**: IP-Adresse des virtuellen Servers, Clients, URLs, Browser, Betriebssysteme, Anforderungsmethoden, Antwortstatus, Domänen, IP-Adresse des Web-App-Servers, SSL-Zertifikate, ausgehandelte SSL-Chiffre, SSL-Schlüsselstärke, SSL-Protokoll und SSL-Fehler-Frontend.
    - **HDX Insight (Anmelden > Gateway)**: ICA-Benutzerdetails, ICA-Anwendungsdetails, VDA-Serverdetails, Desktop-Details in HDX Insight, Geolokalisierungsdetails des App-Clients, HDX-Details zur aktiven Sitzung, VPN-Lizenzen für HDX, Client-NetScaler-IP-Adresse, Client-Typ und Version.
    - **Gateway Insight (Anmelden > Gateway)**: Benutzerdetails, Anwendungsdetails, Browser, Betriebssysteme, Sitzungsmodi, Gateway-Lizenzen, AAA-Serverdetails und auf dem Gateway konfigurierte AAA-Richtlinie.
    - **Sicherheitsverletzungen (Anmelden > Sicherheit)**: Client-IP, URL, Sicherheitsverletzungen (WAF und Bot), Angriffsgeolokalisierung, Angriffszeitstempel, Transaktions-ID, WAF und NetScaler-Sicherheitskonfigurationsstatus.
    - **API-Analysen (Anmelden > Sicherheit > API Gateway)**: Informationen zu API-Instanzen, API-Endpunkten, Gesamtbandbreite, API-Leistungsinformationen, Gesamtanforderungen, Antwortzeit, Fehlern. Möglichkeit, tiefer in jede API-Instanz einzutauchen, um Einblick in einzelne API-Endpunkte und deren Leistung zu erhalten. Sicherheit bezüglich

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authentifizierungserfolg, -fehlern; Ratenbegrenzung, SSL-Chiffre, Protokollinformationen und SSL-Fehlern.

- **Sicherheitshinweis (Anmelden > Infrastruktur > Instanzhinweis > Sicherheitshinweis)**
  - **Versionsscan**: Dieser Scan erfordert, dass NetScaler Console die Version einer NetScaler-Instanz mit den Versionen und Builds vergleicht, für die der Fix verfügbar ist. Dieser Versionsvergleich hilft dem NetScaler Console-Sicherheitshinweis zu identifizieren, ob der NetScaler für die CVE anfällig ist. Die zugrunde liegende Logik für diesen Scan ist, dass, wenn eine CVE in NetScaler-Release und Build xx.yy behoben ist, alle NetScaler-Instanzen auf Builds, die kleiner als Build xx.yy sind, als anfällig gelten. Der Versionsscan wird heute im Sicherheitshinweis unterstützt.
  - **Konfigurationsscan**: Dieser Scan erfordert, dass NetScaler Console ein spezifisches Muster für den CVE-Scan mit der NetScaler-Konfigurationsdatei abgleicht. Wenn das spezifische Konfigurationsmuster in der NetScaler ns.conf-Datei vorhanden ist, gilt die Instanz als anfällig für diese CVE. Dieser Scan wird typischerweise zusammen mit dem Versionsscan verwendet.

    Der Konfigurationsscan wird heute in der Sicherheitsberatung unterstützt.
  - **Benutzerdefinierter Scan**: Dieser Scan erfordert, dass der NetScaler Console-Dienst eine Verbindung zur verwalteten NetScaler-Instanz herstellt, ein Skript darauf überträgt und das Skript ausführt. Die Skriptausgabe hilft NetScaler Console zu identifizieren, ob der NetScaler für die CVE anfällig ist. Beispiele hierfür sind spezifische Shell-Befehlsausgaben, spezifische CLI-Befehlsausgaben, bestimmte Protokolle und das Vorhandensein oder der Inhalt bestimmter Verzeichnisse oder Dateien. Security Advisory verwendet auch benutzerdefinierte Scans für mehrere Konfigurationsmuster, wenn der Konfigurationsscan dabei nicht helfen kann. Für CVEs, die benutzerdefinierte Scans erfordern, wird das Skript jedes Mal ausgeführt, wenn Ihr geplanter oder bedarfsgesteuerter Scan läuft. Erfahren Sie mehr über die gesammelten Daten und Optionen für spezifische benutzerdefinierte Scans in der Security Advisory-Dokumentation für diese CVE.

Sicherheit

Das Citrix Services Security Exhibit beschreibt ausführlich die Sicherheitskontrollen, die auf Citrix Cloud Services angewendet werden, einschließlich Zugriff und Authentifizierung, Systementwicklung und -wartung, Sicherheitsprogrammmanagement, Asset Management, Verschlüsselung, Betriebsmanagement, Personalsicherheit, physische Sicherheit, Geschäftskontinuität und Incident Management.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Sicherheit von Citrix Cloud-Produkten wird durch Verschlüsselungs- und Schlüsselverwaltungspolicen gesteuert. Weitere Informationen dazu, wie Citrix Sicherheit während des gesamten Produktentwicklungszyklus einsetzt, finden Sie im Whitepaper Security Development Processes.

Datenaufbewahrungsrichtlinie für den NetScaler Console-Dienst

Daten wie statistische Messungen, Dashboards, Berichte, Warnungen, Ereignisse und Protokolle innerhalb der NetScaler Console sowie Anmeldedaten werden für den Zeitraum aufbewahrt, in dem der Kunde den Dienst abonniert. Das Benutzerkonto wird dann in ein Express-Konto umgewandelt, in dem der Benutzer nur zwei virtuelle Server verwalten kann.

Das Express-Konto hat eine Kapazität von 500 MB oder 1 Tag Analyse-/Berichtsdaten, je nachdem, welche Grenze das Konto zuerst erreicht. Wenn ein Express-Konto nicht genutzt wird oder der Kunde sich länger als 30 Tage nicht im Konto anmeldet, werden das Konto und alle zugehörigen Kundeninhalte automatisch gelöscht.

Weitere Informationen zur Datenaufbewahrung und -löschung für Citrix Cloud Services-Konten finden Sie in der Citrix Cloud Services Data Protection Overview.

HINWEIS

Alle Analysedaten in NetScaler Console werden maximal 30 Tage lang aufbewahrt.

Drittanbieterdienste

Der NetScaler Console-Dienst wird in Amazon Web Service (AWS)-Rechenzentren in den Regionen Vereinigte Staaten, EMEA (Frankfurt) und APJ (Sydney) gehostet – abhängig vom vom Kunden gewählten Point of Presence (POP).

Der NetScaler Console-Dienst verwendet derzeit Dienste und APIs von verschiedenen Drittanbietertechnologien:

- Für die Produktfunktionalität verwendete Dienste:
    - AWS EFS, AWS RDS, AWS Elastic Cache, AWS ALB, AWS Route 53, AWS EKS, AWS Secret Manager, AWS ECR repository und AWS MSK.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Drittanbieterdienste und -tools, die zur Überwachung und zum Betrieb von NetScaler Console verwendet werden, umfassen:
  - PagerDuty für die Rufbereitschaftsrotation
  - Protokollanalyse mit Splunk
  - Fluentd für die Protokollaggregation
  - Slack für Kommunikation und Benachrichtigungen
  - AWS Cloudwatch, SQS
  - S3 als Speicherbereich in AWS – zum Speichern von Kerndateien und Metriken
  - Prometheus und Grafana für die Überwachung (in Honeycomb-Bereitstellung)

Referenzen

- Weitere Informationen zum Zugriff auf die gesammelten Daten finden Sie unter Citrix Services Security Exhibit.
- Weitere Informationen zur Aufbewahrungsdauer der gesammelten Daten finden Sie unter Citrix Cloud Services Data Protection Overview.
- Citrix Cloud Technical Security Overview.
- Technische und organisatorische Datensicherheitsmaßnahmen von Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BEDINGUNGEN FÜR DIE NUTZUNG VON IoC-INFORMATIONEN

Durch die Nutzung der IoC-Informationen (wie unten definiert) erkennen Sie die folgenden Bedingungen für eine solche Nutzung an und stimmen diesen zu:

Citrix Systems, Inc. und/oder ihre verbundenen Unternehmen („Citrix“) haben Skripte für die Logik von Indicators of Compromise und zugehörige Anleitungen zu Indicators of Compromise (zusammenfassend „IoC-Informationen“) entwickelt, um Unternehmen dabei zu helfen, festzustellen, ob ihre Umgebungen potenziell kompromittiert sind.

Die IoC-Informationen umfassen nicht alle Techniken, Taktiken oder Verfahren („TTPs“), die Bedrohungsakteure bei der Ausrichtung auf relevante Umgebungen verwenden können. Darüber hinaus ändern Bedrohungsakteure TTPs und Infrastruktur häufig. Aus diesen und anderen Gründen können die IoC-Informationen einen begrenzten forensischen Wert haben und tatsächliche Kompromittierungen möglicherweise nicht identifizieren. Es wird dringend empfohlen, die Dienste erfahrener forensischer Ermittler in Anspruch zu nehmen, um Ihre Umgebung zu bewerten.

Die IoC-Informationen werden im Ist-Zustand bereitgestellt. Citrix gibt keine ausdrücklichen oder stillschweigenden Garantien oder Zusicherungen bezüglich der IoC-Informationen ab, einschließlich, aber nicht beschränkt auf die Fehlerfreiheit der IoC-Informationen oder die Erfüllung von Bedingungen der Marktgängigkeit oder Eignung für einen bestimmten Zweck.

Die IoC-Informationen sind vertrauliche und geschützte Informationen von Citrix und unterliegen den Bedingungen der anwendbaren Vertraulichkeitsvereinbarung(en) zwischen dem Empfänger dieser Materialien und Citrix. Kein Teil der IoC-Informationen darf ohne die ausdrückliche vorherige schriftliche Genehmigung von Citrix in irgendeiner Form oder mit irgendwelchen Mitteln reproduziert, weitergegeben oder an Dritte übermittelt werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Erste Schritte

Dieses Dokument führt Sie durch die ersten Schritte beim Onboarding und der erstmaligen Einrichtung von NetScaler Console. Dieses Dokument richtet sich an Netzwerk- und Anwendungsadministratoren, die Citrix-Netzwerkgeräte (NetScaler, NetScaler Gateway, Citrix Secure Web Gateway usw.) verwalten. Befolgen Sie die Schritte in diesem Dokument, unabhängig vom Gerätetyp, den Sie mit NetScaler Console verwalten möchten.

Bevor Sie mit dem Onboarding beginnen, stellen Sie sicher, dass Sie die Browseranforderungen, die Agenteninstallationsanforderungen und die Portanforderungen überprüfen.

Schritt 1: Registrieren Sie sich für Citrix Cloud™

Um NetScaler Console nutzen zu können, müssen Sie zunächst ein Citrix Cloud-Unternehmenskonto erstellen oder einem bestehenden Konto beitreten, das jemand anderes in Ihrem Unternehmen erstellt hat. Detaillierte Prozesse und Anweisungen zum weiteren Vorgehen finden Sie unter Registrieren für Citrix Cloud.

Schritt 2: NetScaler Console mit einem Express-Konto verwalten

Nachdem Sie sich bei Citrix Cloud angemeldet haben, gehen Sie wie folgt vor:

HINWEIS:

- Für Japan müssen Sie sich bei `citrix.citrixcloud.jp` anmelden.
- Für Government Cloud müssen Sie sich bei `citrix.cloud.us` anmelden.

1. Gehen Sie zum Abschnitt **Verfügbare Dienste**.
2. Klicken Sie auf der Kachel **NetScaler® Console** auf **Verwalten**.

   Die Kachel **NetScaler Console** wird in den Abschnitt **Meine Dienste** verschoben.
3. Wählen Sie eine Region aus, die Ihren Geschäftsanforderungen entspricht.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG

- Sie können die Region später nicht mehr ändern.
- Dieser Schritt ist nicht anwendbar, wenn Sie sich über Citrix Cloud Japan (`citrix.citrixcloud.jp`) oder Citrix Cloud Government (`citrix.cloud.us`) anmelden. Sie müssen sicherstellen, dass die entsprechenden Endpunkt-URLs zugelassen sind. Weitere Informationen finden Sie unter Systemanforderungen.

4. Wählen Sie die Rollen und Anwendungsfälle aus, die auf Sie zutreffen.

Sie können sich vom Browser abmelden, während die Initialisierung im Hintergrund abgeschlossen wird, was einige Zeit dauern kann.

HINWEIS:

Citrix weist ein Express-Konto zur Verwaltung von NetScaler Console-Ressourcen zu. Wenn Ihr NetScaler Console Express-Konto 45 Tage lang inaktiv bleibt, wird das Konto gelöscht. Weitere Informationen finden Sie unter NetScaler Console mit einem Express-Konto verwalten.

Wenn Sie sich wieder bei Ihrem Citrix Cloud-Konto anmelden, wird der Bildschirm **NetScaler Console GUI** angezeigt. Klicken Sie auf **Erste Schritte**, um den Dienst zum ersten Mal einzurichten.

Schritt 3: Wählen Sie einen NetScaler-Bereitstellungstyp aus

Führen Sie die folgenden Schritte aus, um NetScaler-Instanzen bereitzustellen oder zu ermitteln:

1. Wählen Sie eine der folgenden Umgebungen aus:

   - **Lokal**
   - **AWS**
   - **Microsoft Azure**
   - **Google Cloud Platform**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Installieren Sie den Agenten, um die Kommunikation zwischen der NetScaler Console und den verwalteten Instanzen in Ihrem Rechenzentrum oder Ihrer Cloud zu ermöglichen.

   Der Schritt **Agent-Typ auswählen** variiert die Installationsoptionen für den Agenten je nach ausgewählter Umgebung.

   - **Externer VM-Agent**
     - **Lokal** – Wenn Sie **Lokal** und dann **Auf einem Hypervisor** auswählen, können Sie einen Agenten auf einem der Hypervisoren installieren, z. B. Citrix Hypervisor™ VMware ESXi, Microsoft Hyper-V oder Linux KVM Server.
     - Wenn Sie eine der öffentlichen Clouds wie AWS, Microsoft Azure oder Google Cloud Platform auswählen, können Sie den **externen Agenten** in der ausgewählten Cloud installieren.
   - **Als Microservice** – Um einen Agenten als Kubernetes-Anwendung bereitzustellen.
   - **Integrierter Agent** – Um einen Agenten innerhalb von NetScaler bereitzustellen.

3. Klicken Sie auf **Weiter**

   Die Schritte zur Installation eines Agenten variieren für jede Option. Die folgenden Links führen Sie zu den spezifischen Schritten zur Installation eines Agenten:

   - Hypervisor
   - Externer Agent
   - Als Microservice
   - Integrierter Agent

Agenten auf einem Hypervisor installieren

Führen Sie die folgenden Schritte aus, um einen Agenten auf einem Hypervisor einzurichten:

1. Wählen Sie den Hypervisor aus und klicken Sie auf **Image herunterladen**, um das Agent-Image auf Ihr lokales System herunterzuladen.

   Eine Dienst-URL und ein Aktivierungscode werden generiert und in der GUI angezeigt.

2. Kopieren Sie die Dienst-URL und einen Aktivierungscode.
3. Geben Sie die kopierte Dienst-URL und den Aktivierungscode bei der Installation des Agenten auf Ihrem Hypervisor an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren. Detaillierte Anweisungen zur Installation eines Agenten auf Ihrem lokalen Hypervisor finden Sie unter Agenten lokal installieren.

4. Kehren Sie nach erfolgreicher Agenteninstallation zur Seite **Agent einrichten** zurück und klicken Sie auf **Agent registrieren**.

Nächster Schritt: Instanzen hinzufügen.

HINWEIS

Wenn Sie während der Ersteinrichtung keine Agenten hinzufügen möchten, klicken Sie auf **Überspringen**, um die von NetScaler Console bereitgestellten Funktionen zu überprüfen. Sie können die Agenten und Instanzen später hinzufügen. Um Agenten später hinzuzufügen, navigieren Sie zu **Einstellungen > Agenten einrichten**. Anweisungen zum späteren Hinzufügen von Instanzen finden Sie unter Instanzen hinzufügen.

Externen VM-Agenten in der Public Cloud installieren

Sie müssen das Agenten-Image nicht von der Seite **Agent einrichten** herunterladen. Das Agenten-Image ist auf dem jeweiligen Cloud-Marktplatz verfügbar.

1. Kopieren und speichern Sie die Dienst-URL und den Aktivierungscode, um sie während der Agenteninstallation zu verwenden.

   Wenn Sie einen neuen Aktivierungscode wünschen, klicken Sie auf **Neuen Aktivierungscode erstellen**, und kopieren und speichern Sie dann den Code zur Verwendung während der Agenteninstallation.

   - Detaillierte Anweisungen zur Installation eines Agenten in der Microsoft Azure Cloud finden Sie unter Agenten in der Microsoft Azure Cloud installieren.
   - Detaillierte Anweisungen zur Installation eines Agenten in AWS finden Sie unter Agenten in AWS installieren.
   - Detaillierte Anweisungen zur Installation eines Agenten in Google Cloud finden Sie unter Agenten in GCP installieren.

2. Nach erfolgreicher Agenteninstallation kehren Sie zur Seite **Agent einrichten** zurück und klicken auf **Agent registrieren**.

Nächster Schritt: Instanzen hinzufügen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Agent als Microservice installieren

Sie können einen Agenten als Microservice im Kubernetes-Cluster bereitstellen, um den **Service-Graph** in NetScaler Console anzuzeigen.

Weitere Informationen zum Einstieg in den Service-Graph finden Sie unter Service-Graph einrichten.

1. Geben Sie die folgenden Parameter an:
    a. **Anwendungs-ID** – Eine Zeichenfolgen-ID zur Definition des Dienstes für den Agenten im Kubernetes-Cluster und zur Unterscheidung dieses Agenten von anderen Agenten im selben Cluster.
    b. **Agentenpasswort** – Geben Sie ein Passwort für CPX an, damit CPX dieses Passwort verwenden kann, um CPX über den Agenten in NetScaler Console zu integrieren.
    c. **Passwort bestätigen** – Geben Sie zur Bestätigung dasselbe Passwort an.
    d. Klicken Sie auf **Senden**.
2. Nachdem Sie auf **Senden** geklickt haben, können Sie die YAML- oder Helm-Chart herunterladen.
3. Klicken Sie auf **Schließen**.

    Weitere Informationen finden Sie unter Agent in einem Kubernetes-Cluster installieren.

Integrierten Agenten verwenden

Die NetScaler-Instanzen in Ihrer Umgebung enthalten einen integrierten Agenten. Sie können den integrierten Agenten initiieren und ihn verwenden, um die Kommunikation zwischen der Instanz und NetScaler Console herzustellen.

1. Kopieren Sie die generierte **Service-URL** und den **Aktivierungscode**. Speichern Sie diese, um sie beim Initiieren des integrierten Agenten auf Ihrer NetScaler-Instanz zu verwenden.

    Detaillierte Anweisungen zum Initiieren des integrierten Agenten auf Ihrer NetScaler-Instanz finden Sie unter Integrierter Agent auf der NetScaler-Instanz initiieren.
2. Nachdem der integrierte Agent initiiert wurde, kehren Sie zur Seite **Agent einrichten** zurück und klicken Sie auf **Instanz registrieren**.

Nächster Schritt: Instanzen hinzufügen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instanzen hinzufügen

Instanzen sind Netzwerk- oder virtuelle Appliances, die Sie über NetScaler Console erkennen, verwalten und überwachen möchten. Um diese Instanzen zu verwalten und zu überwachen, müssen Sie die Instanzen dem Dienst hinzufügen.

Nach erfolgreicher Agenteninstallation und -registrierung werden die Agenten auf der Seite **Agent einrichten** angezeigt. Wenn der Agentenstatus im UP-Zustand ist, erkennbar an einem grünen Punkt daneben, klicken Sie auf **Weiter**, um mit dem Hinzufügen von Instanzen zum Dienst zu beginnen.

1. Auf der Seite **Instanzen hinzufügen** sehen Sie die NetScaler-Instanzen, die mit dem registrierten Agenten verbunden sind. Stellen Sie sicher, dass die Instanz den Status **Up** hat, und klicken Sie auf **Weiter**.
2. Klicken Sie auf **Fertig**, um Ihre Ersteinrichtung abzuschließen und mit der Verwaltung Ihrer Bereitstellung zu beginnen.

HINWEIS

Wenn Sie während der Ersteinrichtung keine Instanzen hinzufügen möchten, können Sie auf **Fertig** klicken, um die Einrichtung abzuschließen und die Instanzen später hinzuzufügen. Anweisungen zum späteren Hinzufügen von Instanzen zu NetScaler Console finden Sie unter Instanzen hinzufügen.

NetScaler-Instanzen über das NetScaler Console GUI-Dashboard integrieren

Wenn Sie das Onboarding der NetScaler-Instanzen im Workflow **Erste Schritte** beim erstmaligen Einrichten von NetScaler Console übersprungen haben, können Sie die Instanzen über das NetScaler Console GUI-Dashboard integrieren. Wenn die NetScaler-Instanzen noch nicht hinzugefügt wurden, fordert Sie die GUI auf, die Instanzen hinzuzufügen.

Wenn Sie auf ein beliebiges Modul in der linken Navigationsleiste klicken, wird auf der rechten Seite eine tabellarische Vorschau der Funktionen und Vorteile dieses Moduls angezeigt. Diese Funktionen und Vorteile helfen Ihnen, NetScaler-Instanzen mithilfe von NetScaler Console besser zu verwalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Klicken Sie auf **NetScaler-Instanzen hinzufügen**, um die Instanzen zu integrieren. Der Workflow **Erste Schritte** wird neu gestartet. Befolgen Sie die Schritte ab Schritt 3: NetScaler-Bereitstellungstyp auswählen in diesem Dokument, um die Instanzen zu integrieren. Wenn die NetScaler-Instanzen bereits integriert sind, sehen Sie nach der Anmeldung bei NetScaler Console nur die NetScaler Console-Landingpage mit der Navigationsleiste auf der linken Seite.

Agent-Aktionen

Nachdem Sie Ihre NetScaler Console eingerichtet haben, können Sie verschiedene Aktionen auf einen Agent anwenden. Navigieren Sie zu **Infrastruktur > Instanzen > Agents**.

Unter **Aktion auswählen** können Sie die folgenden Funktionen verwenden:

- **Neues Zertifikat installieren**: Wenn Sie ein anderes Agent-Zertifikat benötigen, um Ihre Sicherheitsanforderungen zu erfüllen, können Sie eines hinzufügen.
- **Agent-Passwort ändern**: Um die Sicherheit Ihrer Infrastruktur zu gewährleisten, ändern Sie das Standardpasswort eines Agents.
- **Technische Supportdatei generieren**: Generieren Sie eine technische Supportdatei für einen ausgewählten Agent. Sie können diese Datei herunterladen und zur Untersuchung und Fehlerbehebung an den technischen Support von Citrix senden.

Agent-Diagnose anzeigen und Warnungen zur Endpunktüberprüfung erhalten

NetScaler Console führt eine regelmäßige (stündliche) Diagnoseprüfung für den Agent durch und liefert die folgenden Informationen:

- **Endpunkt-Erreichbarkeit** – Überprüft, ob alle Endpunkte erreichbar sind. Der Agent verwendet verschiedene Endpunkte für die Kommunikation zwischen NetScaler Console und NetScaler-Instanzen. Weitere Informationen finden Sie unter Softwareanforderungen.
- **Integritätsprüfung** – Zeigt den Zeitstempel der letzten Integritätsprüfung an.
- **Agent-Proxy** – Überprüft, ob der Agent-Proxy vorhanden ist.

Wenn sich der Status der Agent-Endpunkt-Erreichbarkeit ändert (von **OK** zu **Überprüfung erforderlich**), erhält der Superadministrator eine E-Mail-Benachrichtigung mit den Problemdetails. Navigieren Sie zu **Infrastruktur > Instanzen > Agents**, um die neu hinzugefügte Option **Diagnosestatus** anzuzeigen, die den Status wie **Überprüfung erforderlich** oder **OK** angibt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Klicken Sie hier, um die Diagnoseinformationen eines Agenten anzuzeigen.

- **Kategorie**. Gibt die Problemkategorie an.
- **Status**. Gibt den Problemstatus an, z. B. **Überprüfung erforderlich** oder **OK**.
- **Empfehlung**. Bietet die erforderliche Empfehlung zur Behebung des Problems.

Nachdem Sie das Problem behoben haben und der Erreichbarkeitsstatus des Endpunkts von **Überprüfung erforderlich** zu **OK** wechselt, erhält der Superadministrator eine E-Mail-Benachrichtigung, dass das Problem behoben wurde.

E-Mail-Benachrichtigung

Das folgende Beispiel ist eine E-Mail-Benachrichtigung, nachdem sich der Erreichbarkeitsstatus des Endpunkts von **OK** zu **Überprüfung erforderlich** geändert hat:

Das folgende Beispiel ist eine E-Mail-Benachrichtigung, nachdem sich der Erreichbarkeitsstatus des Endpunkts von **Überprüfung erforderlich** zu **OK** geändert hat:

Integrierter Agent zur Verwaltung von Instanzen konfigurieren

Ein integrierter Agent ist auf NetScaler MPX-, VPX- und Gateway-Instanzen, die die Version `12.1.48.13` oder höher ausführen, sowie auf NetScaler SDX-Instanzen, die Version 13.0 61.x oder höher und 12.1 58.x oder höher ausführen, verfügbar. Sie können diesen Agent auf der NetScaler-Instanz initiieren, anstatt einen dedizierten Agent in Ihrem Rechenzentrum oder Ihrer Public Cloud zu installieren. Der integrierte Agent ermöglicht die Kommunikation zwischen der Instanz und NetScaler Console.

HINWEIS:

Der integrierte Agent ist nur für die folgenden NetScaler-Instanztypen verfügbar:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Gateway

Der integrierte Agent ist ideal für kleinere NetScaler-Standalone- oder HA-Pair-Bereitstellungen. Wenn Sie mehrere NetScaler-Instanzen haben, verwenden Sie einen dedizierten Agent für Bereitstellungen. Dieser Agent gewährleistet bessere Datenaggregationsfunktionen als der integrierte Agent. Weitere Informationen finden Sie unter Agent lokal installieren.

Der integrierte NetScaler Console-Agent unterstützt Instanzverwaltung, Überwachung und Pooled- oder Flexed-Lizenzierung. Die folgenden Funktionen werden jedoch im integrierten Agent nicht unterstützt:

- Anwendungs-Dashboard
- Web Insight
- SSL Insight
- HDX™ Insight
- Gateway Insight
- Sicherheitseinblicke
- Erweiterte Analysen
- Gepoolte oder flexible Lizenzierung (dateibasierte Lizenzierung)

Sie können von einem integrierten Agenten zu einem externen Agenten wechseln. Weitere Informationen finden Sie unter Wechsel von einem integrierten Agenten zu einem externen Agenten.

Voraussetzungen

Bevor Sie einen integrierten Agenten auf der NetScaler-Instanz konfigurieren, stellen Sie Folgendes sicher:

- Die NetScaler-Instanz (MPX, VPX oder Gateway) läuft unter Version `12.1.48.13` oder höher. Die SDX-Instanz läuft unter Version `13.0.61.x` und höher.
- Ein DNS-Nameserver ist auf der NetScaler-Instanz hinzugefügt.

  Weitere Informationen finden Sie unter Nameserver hinzufügen.
- Sie haben ein Citrix Cloud-Konto. Weitere Informationen finden Sie unter Für Citrix Cloud registrieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Alle Informationen zu Ports und anderen Systemanforderungen finden Sie unter Systemanforderungen.

Den integrierten Agenten konfigurieren

Führen Sie die folgenden Aufgaben aus, um den integrierten NetScaler-Agenten zu konfigurieren:

1. Wählen Sie die Option „Integrierter Agent“ wie unter Erste Schritte beschrieben.
2. Kopieren Sie die **Dienst-URL** und den **Aktivierungscode**.

   Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren. Überspringen Sie Schritt 7, wenn Sie ein MPX- oder Gateway-Kunde sind.
3. Initialisieren Sie den integrierten Agenten mithilfe eines SSH-Clients. Gateway-Benutzer müssen diesen Schritt überspringen.

   a. Melden Sie sich bei Ihrer NetScaler-Instanz an. Weitere Informationen finden Sie unter Zugriff auf einen NetScaler.

   b. Navigieren Sie zum `/var/mastools/scripts`-Verzeichnis und geben Sie den folgenden Befehl ein:

   Auf der SDX-Instanz

	REGISTRIERUNG MIT NETSCALER-PROFIL	REGISTRIERUNG OHNE NETSCALER-PROFIL
Voraussetzung	Erstellen Sie vor der Registrierung ein NetScaler-Profil. Weitere Informationen finden Sie unter So erstellen Sie ein NetScaler-Profil.	
Führen Sie diesen Befehl aus	`./mastools_init.sh <device-profile-name> <service-url> <activation-code> -sdx -profile`	`./mastools_init.sh <user_name> <service-url> <activation-code> -sdx`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	REGISTRIERUNG MIT NETSCALER-PROFIL	REGISTRIERUNG OHNE NETSCALER-PROFIL
Benutzeranmeldeinformationen	Geben Sie `nsroot` in `<device_profile_name>` ein. Alternativ können Sie einen Benutzernamen verwenden, der dieselben Zugriffsrechte wie nsroot besitzt.	Geben Sie `nsroot` in `<user_name>` ein. Alternativ können Sie einen Benutzernamen mit denselben Zugriffsrechten wie nsroot verwenden.

HINWEIS:

NetScaler Console erkennt alle VPX-Instanzen, die auf dieser SDX ausgeführt werden, und Sie müssen die VPX-Instanzen nicht einzeln registrieren.

Auf VPX-Instanzen, die nicht auf einer SDX-Appliance ausgeführt werden, sowie auf MPX- und Gateway-Instanzen:

Wenn die NetScaler-Image-Version niedriger als 13.0 61.x oder 12.1 57.x ist, müssen Sie die `mastools`-Version überprüfen, indem Sie den Befehl `cat /var/mastools/version.txt` eingeben. Wenn die Ausgabe `0.0-0.0` ist, ist es das erste Mal.

Geben Sie je nach Softwareversion einen der folgenden Befehle ein.

HINWEIS:

Bevor Sie sich mit einem NetScaler-Profil registrieren, müssen Sie das Profil erstellen. Weitere Informationen finden Sie unter So erstellen Sie ein NetScaler-Profil.

NETSCALER-IMAGE-VERSION	IST MASTOOLS_VERSION `0.0-0.0` ?	BEFEHL ZUR REGISTRIERUNG MIT PROFIL	BEFEHL ZUR REGISTRIERUNG OHNE PROFIL
Niedriger als 13.0 61.xx und 12.1 57.xx	Ja	`./mastools_init.sh <device_profile_name> <service_url>`	`./mastools_init.sh <user_name> <pwd> <service_url>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETSCALER-IMAGE-VERSION	IST MASTOOLS_VERSION `0.0-0.0` ?	BEFEHL ZUR REGISTRIERUNG MIT PROFIL	BEFEHL ZUR REGISTRIERUNG OHNE PROFIL
		`"MAS;<activation_code>" -profile`	`"MAS;<activation_code>"`
Niedriger als 13.0 61.xx und 12.1 57.xx	Nein	`./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile`	`./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>`
Höher als 13.0 61.x und 12.1 57.xx	Nicht zutreffend	`./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile`	`./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>`

HINWEIS:

- Geben Sie in `<device_profile_name>` oder `<user_name>` `nsroot` ein. Alternativ können Sie einen Benutzernamen verwenden, der dieselben Zugriffsrechte wie nsroot besitzt.
- Führen Sie bei einem HA-Paar die Registrierung auf dem primären Knoten durch. Wenn Sie die Registrierungsbefehle auf dem sekundären Knoten ausführen, wird die folgende Meldung angezeigt: **Bitte führen Sie den Registrierungsbefehl auf dem primären Knoten aus**.

4. Kehren Sie zur NetScaler Console-Seite zurück und klicken Sie auf **Instanz registrieren**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Zeigen Sie unter **Instanzen hinzufügen** die Instanz an, in der Sie den integrierten Agenten initialisiert haben. Stellen Sie sicher, dass sich die Instanz im Status **Up** befindet, und klicken Sie auf **Weiter**.
6. Klicken Sie auf **Fertig**.

Nach erfolgreicher Konfiguration des integrierten Agenten können Sie auf die NetScaler Console-Funktionen zugreifen, wie zum Beispiel:

- **Virtueller Server und Analysen** – Wenden Sie Lizenzen auf Ihren virtuellen Server an, um NetScaler-Instanzen zu verwalten. Weitere Informationen finden Sie unter Abonnements verwalten.
- **Anwendungs-Dashboard** – Um alle Anwendungen ganzheitlich anzuzeigen. Weitere Informationen finden Sie unter Anwendungsverwaltung und Dashboard.
- **Infrastruktur-Analysen** – Diese Funktion hilft Ihnen, die Faktoren zu visualisieren, die zu einem Problem bei den Instanzen geführt haben oder führen könnten. Weitere Informationen finden Sie unter Infrastruktur-Analysen.

Lizenzserver über den integrierten NetScaler®-Agenten konfigurieren

HINWEIS:

Dem integrierten NetScaler-Agenten kann die LSA-Rolle nicht zugewiesen werden.

Wenn Sie einen Lizenzserver-Agenten (LSA) an einem Standort konfiguriert haben und denselben LSA von anderen Standorten aus verwenden möchten, können Sie einen integrierten NetScaler-Agenten verwenden. Bei der Verwendung des integrierten Agenten müssen Sie den Lizenzserver mit dem folgenden Befehl auf der NetScaler-Instanz konfigurieren.

```
add licenseserver 127.0.0.1 -port 27000
```

In dieser Konfiguration kann NetScaler den Lizenzserver-Agenten (LSA) über den Konsolendienst erreichen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Sie können den integrierten Agenten auch konfigurieren, indem Sie zur Seite **Infrastructure > Instances > Agents > Generate Activation code** navigieren. Kopieren Sie die URL und den Aktivierungscode und fügen Sie sie in eine NetScaler-Instanz ein, um diese Instanz zu erkennen.

Nachdem der integrierte Agent initialisiert wurde, navigieren Sie zu **Infrastructure > Instances > NetScaler**. Diese Seite zeigt die Details zur verwalteten Instanz an, die mit dem integrierten Agenten erkannt wurde.

Fehlerbehebung

Sie können die Protokolle überprüfen, wenn die Registrierung fehlschlägt oder wenn die Registrierung erfolgreich ist, der integrierte Agent jedoch nicht in der NetScaler Console-GUI angezeigt wird.

- Wenn die Registrierung fehlschlägt, überprüfen Sie die Protokolle in `/var/mastools/logs/mastools_reg.py.log`
- Wenn die Registrierung erfolgreich ist, der integrierte Agent jedoch nicht in der NetScaler Console GUI angezeigt wird, überprüfen Sie Folgendes:
  - **Mastools_upgrade**-Protokolle in `/var/mastools/logs/mastools_upgrade.log`
  - **Binärprotokolle** in `/var/log/mastoolsd.log`.

Installieren Sie einen NetScaler Agent lokal

Der Agent fungiert als Vermittler zwischen der NetScaler Console und den erkannten Instanzen im Rechenzentrum.

Bevor Sie mit der Installation des Agenten beginnen, stellen Sie sicher, dass Sie die erforderlichen virtuellen Computerressourcen haben, die der Hypervisor für jeden Agenten bereitstellen muss. Weitere Informationen finden Sie unter Anforderungen an die Agenteninstallation und Leichtgewichtiger Agent für gepoolte Lizenzierung.

HINWEIS

Alle Informationen zu Ports und anderen Anforderungen finden Sie unter Unterstützte Ports.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So installieren Sie den NetScaler Agent:

1. Laden Sie das Agenten-Image herunter, wie unter Erste Schritte beschrieben.
2. Importieren Sie die Agenten-Image-Datei in Ihren Hypervisor.
3. Konfigurieren Sie auf der Registerkarte **Konsole** die anfänglichen Netzwerkkonfigurationsoptionen, wie im folgenden Beispiel gezeigt:

   HINWEIS

   Stellen Sie sicher, dass Sie Ihr DNS so konfigurieren, dass Ihr NetScaler Agent Internetzugriff erhält.

4. Nach Abschluss der anfänglichen Netzwerkkonfiguration speichern Sie die Konfigurationseinstellungen. Melden Sie sich bei Aufforderung mit den Standardanmeldeinformationen (`nsrecover/nsroot`) an.

   Wenn Sie die konfigurierten Netzwerkeinstellungen auf dem Agenten ändern möchten, geben Sie den Befehl `networkconfig` ein und folgen Sie den Anweisungen in der CLI.

5. Wenn keine Aufforderung zur Eingabe der Service-URL angezeigt wird, navigieren Sie zu /mps im NetScaler-Agent und führen Sie dann eines der folgenden Skripte aus:

   ```
   deployment_type.py
   ```

   ```
   register_agent_cloud.py
   ```

6. Geben Sie die **Service-URL** und den **Aktivierungscode** ein, die Sie beim Herunterladen des Agent-Images gespeichert haben. Der Agent verwendet die Service-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.

7. Nach erfolgreicher Agent-Registrierung wird der Agent neu gestartet, um den Installationsvorgang abzuschließen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nachdem der Agent neu gestartet wurde, greifen Sie auf die NetScaler Console-GUI zu und navigieren Sie zu **Infrastructure > Instances > Agents**, um den Status des Agenten zu überprüfen. Nachdem der Agent konfiguriert wurde, müssen Sie das Kennwort ändern.

1. Navigieren Sie zu **Infrastructure > Instances > Agents**
2. Wählen Sie den Agenten aus und klicken Sie in der Liste **Aktion auswählen** auf **Kennwort ändern**.

3. Geben Sie das aktuelle Kennwort (`nsroot`) ein, geben Sie dann ein neues Kennwort an und klicken Sie auf **OK**, um das Kennwort zu ändern.

   Das Kennwort muss:

   - Mindestens sechs Zeichen lang sein
   - Mindestens ein Sonderzeichen enthalten
   - Mindestens einen Großbuchstaben enthalten
   - Mindestens einen Kleinbuchstaben enthalten
   - Mindestens eine Ziffer enthalten

   HINWEIS:

   Nachdem Sie den NetScaler Agent vor Ort konfiguriert haben, empfehlen wir, bis zu 10 Minuten zu warten, bevor Sie eine Lizenz auf eine NetScaler-Instanz anwenden.

Installation eines NetScaler-Agent in der Microsoft Azure Cloud

Der Agent fungiert als Vermittler zwischen der NetScaler Console und den verwalteten Instanzen im Unternehmensrechenzentrum oder in der Cloud.

Um den NetScaler-Agent in der Microsoft Azure Cloud zu installieren, müssen Sie eine Instanz des Agents im virtuellen Netzwerk erstellen. Beziehen Sie das NetScaler-Agent-Image vom Azure Marketplace und verwenden Sie dann das Azure Resource Manager-Portal, um den Agent zu erstellen.

Bevor Sie mit der Erstellung der NetScaler-Agent-Instanz beginnen, stellen Sie sicher, dass Sie ein virtuelles Netzwerk mit den erforderlichen Subnetzen erstellt haben, in denen sich die Instanz

© 1997–2026 Citrix Systems, Inc. All rights reserved.

befindet. Sie können virtuelle Netzwerke während der VM-Bereitstellung erstellen, jedoch ohne die Flexibilität, verschiedene Subnetze zu erstellen. Weitere Informationen finden Sie in der *Azure-Dokumentation*.

Konfigurieren Sie den DNS-Server und die VPN-Konnektivität, die einer virtuellen Maschine den Zugriff auf Internetressourcen ermöglicht.

Voraussetzungen

Stellen Sie sicher, dass Sie Folgendes haben:

- Ein Microsoft Azure-Benutzerkonto
- Zugriff auf Microsoft Azure Resource Manager

HINWEISE

- Wir empfehlen, dass Sie Ressourcengruppe, Netzwerksicherheitsgruppe, virtuelles Netzwerk und andere Entitäten erstellen, bevor Sie die virtuelle NetScaler-Agent-Maschine bereitstellen, damit die Netzwerkinformationen während der Bereitstellung verfügbar sind.
- Damit der NetScaler-Agent mit der NetScaler Console und den NetScaler-Instanzen kommunizieren kann, stellen Sie sicher, dass die empfohlenen Ports geöffnet sind. Vollständige Details zu den Portanforderungen für den NetScaler-Agent finden Sie unter Ports.

So installieren Sie den NetScaler-Agent in der Microsoft Azure Cloud:

1. Melden Sie sich mit Ihren Microsoft Azure-Anmeldeinformationen beim Azure-Portal (https://portal.azure.com) an.
2. Klicken Sie auf **+Ressource erstellen**.
3. Geben Sie `NetScaler agent` in die Suchleiste ein und wählen Sie **NetScaler-Agent** aus.

4. Klicken Sie auf **Erstellen**.

5. Geben Sie im Bereich **Virtuellen Computer erstellen** die erforderlichen Werte in jedem Abschnitt an, um einen virtuellen Computer zu erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Grundlagen:

Geben Sie auf dieser Registerkarte **Projektdetails**, **Instanzdetails** und **Administratorkonto** an.

- **Ressourcengruppe** – Wählen Sie die Ressourcengruppe, die Sie erstellt haben, aus der Dropdown-Liste aus.

  HINWEIS

  Sie können an dieser Stelle eine Ressourcengruppe erstellen, wir empfehlen jedoch, eine Ressourcengruppe unter **Ressourcengruppen** im Azure Resource Manager zu erstellen und die Gruppe dann aus der Dropdown-Liste auszuwählen.

- **Name des virtuellen Computers** – Geben Sie einen Namen für die NetScaler-Agent-Instanz an.
- **Region** – Wählen Sie die Region aus, in der Sie einen Agent bereitstellen möchten.
- **Verfügbarkeitsoptionen** – Wählen Sie den Verfügbarkeitssatz aus der Liste aus.
- **Image** – Dieses Feld zeigt das bereits ausgewählte Agent-Image an. Wenn Sie zu einem anderen Agent-Image wechseln möchten, wählen Sie das gewünschte Image aus der Liste aus.
- **Größe** – Geben Sie den Typ und die Größe der virtuellen Festplatte für die Bereitstellung Ihres NetScaler-Agenten an.

  Wählen Sie den unterstützten Typ der virtuellen Festplatte (**HDD** oder **SSD**) aus der Liste.

  Weitere Informationen zu unterstützten Größen virtueller Festplatten finden Sie unter Anforderungen an die Agent-Installation und Lightweight-Agent für gepoolte Lizenzierung.
- **Authentifizierungstyp** – Wählen Sie Kennwort.
- **Benutzername und Kennwort** – Geben Sie einen Benutzernamen und ein Kennwort an, um auf die Ressourcen in der von Ihnen erstellten Ressourcengruppe zuzugreifen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG

- Wir empfehlen Ihnen, einen eigenen Benutzernamen und ein eigenes Kennwort für Ihren Agenten anzugeben. Verwenden Sie `nsrecover` oder `nsroot` nicht als Benutzernamen, da diese für Agent-Benutzer reserviert sind.
- Legen Sie während der Bereitstellung einen Benutzernamen fest, der nicht `nsroot` oder `nsrecover` ist. Der erste Login nach der Bereitstellung muss jedoch `nsrecover` als Benutzernamen verwenden.

Datenträger:

Auf dieser Registerkarte geben Sie **Datenträgeroptionen** und **Datenträger** an.

- **Typ des Betriebssystemdatenträgers** – Wählen Sie den Typ der virtuellen Festplatte (HDD oder SSD).

Netzwerk:

Geben Sie die erforderlichen Netzwerkdetails an:

- **Virtuelles Netzwerk** – Wählen Sie das virtuelle Netzwerk aus.
- **Subnetz** – Legen Sie die Subnetzadresse fest.
- **Öffentliche IP-Adresse** – Optional, wählen Sie die IP-Adresse aus.
- **Netzwerksicherheitsgruppe** – Optional, wählen Sie die von Ihnen erstellte Sicherheitsgruppe aus.
- **Eingehende Ports auswählen** – Wenn Sie öffentliche eingehende Ports zulassen, stellen Sie sicher, dass die Regeln für eingehenden und ausgehenden Datenverkehr in der Sicherheitsgruppe konfiguriert sind. Wählen Sie dann die eingehenden Ports aus der Liste aus. Weitere Informationen finden Sie unter Voraussetzungen.

HINWEIS

Stellen Sie sicher, dass der Agent Internetzugang hat.

Verwaltung:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Geben Sie **Azure Security Center**, **Überwachung** und **Identität** an.

Erweitert:

Optional, geben Sie **Erweiterungen**, **Benutzerdefinierte Daten** und **Näherungsplatzierungsgruppe** an.

HINWEIS

Geben Sie unter **Benutzerdefinierte Daten** die **Dienst-URL** und den **Aktivierungscode** an, die Sie von der Seite **Agenten einrichten** in NetScaler Console kopiert haben, wie unter Erste Schritte beschrieben. Geben Sie die Details im folgenden Format ein:

```
registeragent -serviceurl &lt;apigatewayurl> -activationcode
&lt;activationcodevalue>
```

Der Agent verwendet diese Informationen, um sich während des Systemstarts automatisch bei der NetScaler Console zu registrieren.
Wenn Sie dieses automatische Registrierungsskript angeben, überspringen Sie Schritt 7 und 8.

Tags:

Geben Sie das Schlüssel-Wert-Paar für die NetScaler-Agent-Tags ein. Ein Tag besteht aus einem Groß-/Kleinschreibung-sensitiven Schlüssel-Wert-Paar. Diese Tags ermöglichen es Ihnen, den Agenten einfach zu organisieren und zu identifizieren. Die Tags werden sowohl auf Azure als auch auf die NetScaler Console angewendet.

Die Konfigurationseinstellungen werden validiert und die Registerkarte **Überprüfen und erstellen** zeigt das Ergebnis der Validierung an.

- Wenn die Validierung fehlschlägt, zeigt diese Registerkarte den Grund für den Fehler an. Gehen Sie zurück zum entsprechenden Abschnitt und nehmen Sie die erforderlichen Änderungen vor.
- Wenn die Validierung erfolgreich ist, klicken Sie auf **Erstellen**. Der Agent-Bereitstellungsprozess beginnt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Der Bereitstellungsprozess kann etwa 10–15 Minuten dauern. Sobald die Bereitstellung erfolgreich abgeschlossen ist, können Sie Ihre virtuelle NetScaler-Agent-Maschine in Ihrem Microsoft Azure-Konto anzeigen.

6. Sobald der Agent betriebsbereit ist, verwenden Sie einen SSH-Client, um sich bei Ihrem NetScaler-Agenten anzumelden. Verwenden Sie den Benutzernamen und das Kennwort, die während der Erstellung der virtuellen Maschine angegeben wurden.
7. Führen Sie das Bereitstellungsskript aus, indem Sie den Befehl an der Shell-Eingabeaufforderung eingeben: **deployment_type.py**.
8. Geben Sie die **Service-URL** und den **Aktivierungscode** ein, die Sie von der Seite **Agenten einrichten** in der NetScaler Console kopiert und gespeichert haben, wie unter Erste Schritte beschrieben. Der Agent verwendet die Service-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.

Nach erfolgreicher Agentenregistrierung startet der Agent neu, um den Installationsprozess abzuschließen.

Nachdem der Agent neu gestartet wurde, greifen Sie auf NetScaler Console zu und überprüfen Sie auf der Seite **Agent einrichten** unter **Ermittelte Agenten** den Status des Agenten.

Installieren Sie einen NetScaler Agent auf Amazon Web Services (AWS)

Der NetScaler Agent fungiert als Vermittler zwischen der NetScaler Console und den erkannten Instanzen im Rechenzentrum oder in der Cloud.

Voraussetzungen

Um ein NetScaler Agent AMI innerhalb einer Amazon Web Services (AWS) Virtual Private Cloud (VPC) über die Amazon GUI zu starten, benötigen Sie:

- Ein AWS-Konto
- Eine AWS Virtual Private Cloud (VPC)
- Ein IAM-Konto
- Eine Service-URL und einen Aktivierungscode, damit sich der Agent mit dem NetScaler Console-Dienst verbinden kann. Navigieren Sie in der NetScaler Console-Dienst-GUI zu

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastructure > Instances > Agents und klicken Sie auf **Generate Activation Code**, um Ihre Service-URL und Ihren Aktivierungscode zu generieren.

HINWEIS

- Bevor Sie eine virtuelle NetScaler Agent-Maschine bereitstellen, empfiehlt Citrix, eine Sicherheitsgruppe, ein virtuelles privates Netzwerk, ein Schlüsselpaar, ein Subnetz und andere Entitäten zu erstellen. So sind die Netzwerkinformationen während der Bereitstellung verfügbar.
- Damit ein NetScaler Agent mit der NetScaler Console und den NetScaler Instanzen kommunizieren kann, stellen Sie sicher, dass die empfohlenen Ports geöffnet sind. Ausführliche Informationen zu den Portanforderungen für einen NetScaler Agent finden Sie unter Ports.

So installieren Sie den NetScaler Agent auf AWS:

1. Melden Sie sich mit Ihren AWS-Anmeldeinformationen beim AWS Marketplace an.
2. Geben Sie im Suchfeld **NetScaler agent** ein, um nach dem NetScaler Agent AMI zu suchen, und klicken Sie auf **Go**.
3. Klicken Sie auf der Suchergebnisseite in der verfügbaren Liste auf das **NetScaler Console External agent AMI**.
4. Auf der Seite **NetScaler Console External Agent AMI** klicken Sie auf **Continue to Subscribe**.

5. Nachdem das Abonnement erfolgreich war, klicken Sie auf **Continue to Configuration**.

6. Auf der Seite **Diese Software konfigurieren**:

   a. Wählen Sie das AMI aus der Liste **Fulfillment option** aus.

   b. Wählen Sie die neueste NetScaler Agent-Version aus der Liste **Software Version** aus.

   c. Wählen Sie Ihre Region aus der Liste **Region** aus.

   d. Klicken Sie auf **Continue to Launch**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Auf der Seite **Diese Software starten** haben Sie zwei Optionen, den NetScaler Agent zu registrieren:

   a. **Starten von der Website**

   b. **Starten mit EC2**

Starten von einer Website

Um von einer Website zu starten, wählen Sie:

1. Einen EC2-Instanztyp aus der Liste **EC2 Instance Type**
2. Eine VPC aus der Liste **VPC Settings**. Klicken Sie auf **Create a VPC in EC2**, um eine VPC für Ihre Software zu erstellen.
3. Ein Subnetz aus der Liste **Subnet Settings**. Klicken Sie auf **Create a subnet in EC2**, um ein Subnetz zu erstellen, nachdem Sie die VPC ausgewählt haben.
4. Eine Sicherheitsgruppe für die Firewall aus der Liste **Security Group Settings**. Klicken Sie auf **Create New Based On Seller Settings**, um eine Sicherheitsgruppe zu erstellen.
5. Ein Schlüsselpaar zur Gewährleistung der Zugriffssicherheit aus der Liste **Key Pair Settings**. Klicken Sie auf **Create a key pair in EC2**, um ein Schlüsselpaar für Ihre Software zu erstellen.
6. Klicken Sie auf **Launch**

7. Der Start von einer Website war erfolgreich.

   HINWEIS

   Der Bereitstellungsprozess kann etwa 10–15 Minuten dauern. Nachdem die Bereitstellung erfolgreich abgeschlossen wurde, können Sie Ihre virtuelle NetScaler-Agent-Maschine in Ihrem AWS-Konto anzeigen.

8. Sobald der Agent bereitgestellt ist, weisen Sie Ihrem NetScaler-Agent einen Namen zu.
9. Sobald der Agent betriebsbereit ist, weisen Sie Ihrem NetScaler-Agent eine elastische IP-Adresse zu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Eine elastische IP-Adresse ermöglicht dem NetScaler-Agenten die Kommunikation mit NetScaler Console. Eine elastische IP-Adresse ist jedoch möglicherweise nicht erforderlich, wenn Sie ein NAT-Gateway konfiguriert haben, um den Datenverkehr ins Internet zu leiten.

10. Melden Sie sich über einen SSH-Client bei Ihrem NetScaler-Agenten an.

    HINWEIS

    Sie können sich auf eine der folgenden Weisen beim NetScaler-Agenten anmelden:

    - Verwenden Sie `nsrecover` als Benutzernamen und die AWS-Instanz-ID als Kennwort.
    - Verwenden Sie `nsroot` als Benutzernamen und ein gültiges Schlüsselpaar als Kennwort.

11. Geben Sie den folgenden Befehl ein, um den Bereitstellungsbildschirm aufzurufen: **deployment_type.py**
12. Geben Sie die **Service-URL** und den **Aktivierungscode** ein, die Sie von der Seite **Agenten einrichten** in NetScaler Console kopiert und gespeichert haben, wie unter Erste Schritte beschrieben. Der Agent verwendet die Service-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.

Nach erfolgreicher Agentenregistrierung startet der Agent neu, um den Installationsvorgang abzuschließen.

Nachdem der Agent neu gestartet wurde, greifen Sie auf NetScaler Console zu und überprüfen Sie auf der Seite **Agent einrichten** unter **Erkannte Agenten** den Status des Agenten.

Mit EC2 starten

Um mit EC2 zu starten, wählen Sie **Launch through EC2** aus der Liste **Aktion auswählen** und klicken Sie dann auf **Launch**.

1. Wählen Sie auf der Seite **Instanztyp auswählen** die Instanz aus und klicken Sie auf **Weiter: Instanzdetails konfigurieren**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Geben Sie auf der Seite **Instanzdetails konfigurieren** die erforderlichen Parameter an.

   Im Abschnitt **Erweiterte Details** können Sie einen Zero-Touch-Agenten aktivieren, indem Sie Authentifizierungsdetails oder ein Skript im Feld **Benutzerdaten** angeben.

   - **Authentifizierungsdetails** – Geben Sie die **Service-URL** und den **Aktivierungscode** an, die Sie von der Seite **Agenten einrichten** in der NetScaler Console kopiert haben, wie unter Erste Schritte beschrieben. Geben Sie die Details im folgenden Format ein.

     ```
     registeragent -serviceurl <apigatewayurl> -activationcode
     <activationcodevalue>
     ```

     Der Agent verwendet diese Informationen, um sich während des Bootvorgangs automatisch bei der NetScaler Console zu registrieren.

   - **Skript** – Geben Sie ein Skript zur automatischen Agentenregistrierung als Benutzerdaten an. Das Folgende ist ein Beispielskript:

     ```
     #!/var/python/bin/python2.7

     import os

     import requests

     import json

     import time

     import re

     import logging

     import logging.handlers

     import boto3



     '''

     Overview of the Script:
     ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
The script helps to register a NetScaler agent with NetScaler
Console. Pass it in userdata to make NetScaler agent in AWS to
autoregister on bootup. The workflow is as follows

1)  Fetch the NetScaler Console API credentials (ID and secret) from
AWS secret store (NOTE: you have to assign IAM role to the NetScaler
agent that will give permission to fetch secrets from AWS secret
store)

2)  Login to NetScaler Console with credentials fetched in step 1

3)  Call NetScaler Console to fetch credentials (serviceURL and
token) for agent registration

4)  Calls registration by using the credentials fetched in step 3

'''



'''

These are the placeholders which you need to replace according to
your setup configurations

aws_secret_id: Id of the AWS secret where you have stored NetScaler
Console Credentials

The secrets value should be in the following json format

{ "adm_user_id_key": "YOUR_ID", " adm_user_secret_key":
"YOUR_SECRET"}

'''



aws_secret_id = "<AWS_secret_id>"

adm_ip_or_hostname = "<YOUR_ADM_POP>.adm.cloud.com"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
'''

Set up a specific logger with your desired output level and log file
name

'''

log_file_name_local = os.path.basename(__file__)

LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'

LOG_MAX_BYTE = 50*1024*1024

LOG_BACKUP_COUNT = 20



logger = logging.getLogger(__name__)

logger.setLevel(logging.DEBUG)

logger_handler = logging.handlers.RotatingFileHandler(LOG_FILENAME,
maxBytes=LOG_MAX_BYTE, backupCount=LOG_BACKUP_COUNT)

logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%
(funcName)30s:%(lineno)4d: [%(levelname)s] %(message)s',
datefmt="%Y-%m-%d %H:%M:%S")

logger_handler.setFormatter(logger_fortmater)

logger.addHandler(logger_handler)



class APIHandlerException(Exception):

    def __init__(self, error_code, message):

        self.error_code = error_code

        self.message = message

```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    def __str__(self):

        return self.message + ". Error code '" +
str(self.error_code) + "'"



def parse_response(response, url, print_response=True):

    if not response.ok:

        if "reboot" in url:

            logger.debug('No response for url: reboot')

            resp = {"errorcode": "500", "message": "Error while
reading response."}

            return resp



        if print_response:

            logger.debug('Response text for %s is %s' % (url,
response.text))



        response = json.loads(response.text)

        logger.debug("ErrorCode - " + str(response['errorcode']) +
". Message -" + str(response['message']))

        raise APIHandlerException(response['errorcode'],
str(response['message']))

    elif response.text:

        if print_response:

            logger.debug('Response text for %s is %s' % (url,
response.text))
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        result = json.loads(response.text)

        if 'errorcode' in result and result['errorcode'] > 0:

            raise APIHandlerException(result['errorcode'],
str(result['message']))

        return result



def _request(method, url, data=None, headers=None, retry=3,
print_response=True):

    try:

        response = requests.request(method, url, data=data,
headers=headers)

        result = parse_response(response, url,
print_response=print_response)

        return result

    except [requests.exceptions.ConnectionError,
requests.exceptions.ConnectTimeout]:

        if retry > 0:

            return _request(method, url, data, headers, retry-1,
print_response=print_response)

        else:

            raise APIHandlerException(503, 'ConnectionError')

    except requests.exceptions.RequestException as e:

        logger.debug(str(e))

        raise APIHandlerException(500, str(e))
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    except APIHandlerException as e:

        logger.debug("URL: %s, Error: %s, Message: %s" % (url,
e.error_code, e.message))

        raise e

    except Exception as e:

        raise APIHandlerException(500, str(e))



try:

    '''Get the AWS Region'''

    client = boto3.client('s3')

    my_region = client.meta.region_name

    logger.debug("The rgion is %s" % (my_region))



    '''Creating a Boto cleint session'''

    session = boto3.session.Session()

    client = session.client(

        service_name='secretsmanager',

        region_name=my_region

    )



    '''Getting the values stored in the secret with id:
<aws_secret_id>'''

    get_id_value_response = client.get_secret_value(
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        SecretId = aws_secret_id

    )

    adm_user_id = json.loads(get_id_value_response["SecretString"])
["adm_user_id_key"]

    adm_user_secret =
json.loads(get_id_value_response["SecretString"])
["adm_user_secret_key"]



except Exception as e:

    logger.debug("Fetching of NetScaler Console credentials from AWS
secret failed with error: %s" % (str(e)))

    raise e



'''

Initializing common NetScaler Console API handlers

'''

mas_common_headers = {

    'Content-Type': "application/json",

    'Accept-type': "application/json",

    'Connection': "keep-alive",

    'isCloud': "true"

}



'''
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
API to login to the NetScaler Console and fetch the Session ID and
Tenant ID

'''

url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/
login"

payload = 'object={"login":{"ID":"' + adm_user_id + '","Secret":"' +
adm_user_secret + '"}}'

try:

    response = _request("POST", url, data=payload,
headers=mas_common_headers)

    sessionid = response["login"][0]["sessionid"]

    tenant_id = response["login"][0]["tenant_name"]

except Exception as e:

    logger.debug("Login call to the NetScaler Console failed with
error: %s" % (str(e)))

    raise e



'''

API to fetch the service URL and Token to be used for registering
the agent with the NetScaler Console

'''

mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)

url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/
trust_preauthtoken/" + tenant_id +"?customer="+ tenant_id

logger.debug("Fetching Service URL and Token.")
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
try:

    response = _request("GET", url, data=None,
headers=mas_common_headers)

    service_name  = response["trust_preauthtoken"][0]
["service_name"]

    token = response["trust_preauthtoken"][0]["token"]

    api_gateway_url = response["trust_preauthtoken"][0]
["api_gateway_url"]

except Exception as e:

    logger.debug("Fetching of the Service URL Passed with error. %s"
% (str(e)))

    raise e



'''

Running the register agent command using the values we retrieved
earlier

'''

try:

    registeragent_command = "registeragent -serviceurl
"+api_gateway_url+" -activationcode "+service_name+"\;"+token

    file_run_command = "/var/python/bin/python2.7 /mps/
register_agent_cloud.py "+registeragent_command

    logger.debug("Executing registeragent command: %s" %
(file_run_command))

    os.system(file_run_command)

except Exception as e:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    logger.debug("Agent Registeration failed with error: %s" %
(str(e)))

        raise e
```

Dieses Skript ruft die Authentifizierungsdetails vom AWS Secrets Manager ab und führt das Skript `deployment.py` aus, um den Agenten bei der NetScaler Console zu registrieren.

HINWEIS

Sie können zwar automatisch eine öffentliche IP-Adresse zuweisen, aber auch eine elastische IP-Adresse zuweisen. Die Zuweisung einer elastischen IP-Adresse ist erforderlich, wenn das NAT Gateway nicht konfiguriert ist.

Wenn die elastische IP-Adresse in diesem Schritt nicht festgelegt ist, können Sie dies immer noch in der EC2-Konsole tun. Sie können eine neue elastische IP-Adresse erstellen und diese dem NetScaler-Agenten mithilfe der Instanz-ID oder ENI-ID zuordnen.
Klicken Sie auf **Speicher hinzufügen**.

3. Konfigurieren Sie auf der Seite **Speicher hinzufügen** die Einstellungen für das Speichergerät der Instanz und klicken Sie auf **Weiter: Tags hinzufügen**.

4. Definieren Sie auf der Seite **Tags hinzufügen** den Tag für die Instanz und klicken Sie auf **Weiter: Sicherheitsgruppe konfigurieren**.

5. Fügen Sie auf der Seite **Sicherheitsgruppe konfigurieren** Regeln hinzu, um bestimmten Datenverkehr zu Ihrer Instanz zuzulassen, und klicken Sie auf **Überprüfen und starten**.

6. Überprüfen Sie auf der Seite **Instanzstart überprüfen** die Instanzeinstellungen und klicken Sie auf **Starten**.
7. Erstellen Sie im Dialogfeld **Vorhandenes Schlüsselpaar auswählen oder neues Schlüsselpaar erstellen** ein Schlüsselpaar. Sie können auch aus den vorhandenen Schlüsselpaaren auswählen.

   Akzeptieren Sie die Bestätigung und klicken Sie auf **Instanzen starten**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Der Bereitstellungsprozess kann etwa 10–15 Minuten dauern. Nachdem die Bereitstellung erfolgreich abgeschlossen wurde, können Sie Ihre NetScaler Agent-VM in Ihrem AWS-Konto anzeigen.

NetScaler-Agent auf GCP installieren

Der NetScaler-Agent fungiert als Vermittler zwischen der NetScaler Console und den erkannten Instanzen im Rechenzentrum oder in der Cloud. Sie können den Agenten auf der Google Cloud Platform (GCP) bereitstellen, um die sichere Fernverwaltung von NetScaler-Instanzen zu erleichtern, die innerhalb des virtuellen Google Cloud-Netzwerks über die NetScaler Console bereitgestellt werden. Weitere Informationen finden Sie im Google Cloud Platform Marketplace.

Voraussetzungen

Um einen NetScaler-Agenten auf GCP zu installieren, benötigen Sie ein GCP-Konto.

NetScaler-Agent auf GCP installieren

Führen Sie die folgenden Schritte aus, um einen NetScaler-Agenten auf GCP zu installieren.

1. Melden Sie sich mit Ihren Anmeldeinformationen bei der GCP-Konsole (console.cloud.google.com) an und gehen Sie zum Marketplace.
2. Geben Sie im Suchfeld **NetScaler agent** ein.
3. Klicken Sie im Ergebnisfeld auf **NetScaler agent** und dann auf **Launch**.

4. Auf der Seite **New NetScaler agent deployment** sind die meisten Optionen standardmäßig festgelegt. Sie können die Standardkonfigurationen bei Bedarf ändern und auf **Deploy** klicken.

5. Nachdem der Agent bereitgestellt wurde, klicken Sie auf den Instanzlink und überprüfen Sie die Details auf der Seite **VM instance details**.

6. Melden Sie sich über einen SSH-Client unter Verwendung der externen IP-Adresse des Agenten beim Agenten an. Verwenden Sie die folgenden Befehle:

   ```
   ssh nsrecover@<external IP address of the agent>
   ```

   Passwort: Instanz-ID

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie finden die externe IP-Adresse und die Instanz-ID auf der Seite **VM-Instanzdetails**.

7. Geben Sie den folgenden Befehl ein, um den Bereitstellungsbildschirm aufzurufen: **deployment_type.py**
8. Geben Sie die **Dienst-URL** und den **Aktivierungscode** ein, die Sie von der Seite **Agenten einrichten** in NetScaler Console kopiert und gespeichert haben, wie unter Erste Schritte beschrieben. Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.

Nach erfolgreicher Agentenregistrierung startet der Agent neu, um den Installationsvorgang abzuschließen.

Nachdem der Agent neu gestartet wurde, greifen Sie auf NetScaler Console zu und überprüfen Sie auf der Seite **Agent einrichten** unter **Erkannte Agenten** den Status des Agenten.

NetScaler Agent in Kubernetes-Cluster mit YAML installieren

HINWEIS

Die Vorgehensweise zur Installation eines Agenten als Microservice finden Sie im Abschnitt Erste Schritte.

Im Kubernetes-Masterknoten:

1. Speichern Sie die heruntergeladene YAML-Datei
2. Führen Sie den folgenden Befehl aus:

   `kubectl create -f <yaml file>`

   Zum Beispiel, `kubectl create -f testing.yaml`

   Der Agent wurde erfolgreich erstellt.

Navigieren Sie in der NetScaler Console zu **Infrastructure > Instances > Agents**, um den Agent-Status anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Der in einem Kubernetes-Cluster mit YAML konfigurierte NetScaler Agent unterstützt automatische Agent-Upgrades (Evergreen-Upgrade).

NetScaler Agent Operator mithilfe der OpenShift-Konsole installieren

HINWEIS:

Der OpenShift-Agent wird nur im NetScaler Console-Dienst unterstützt.

Ein Operator ist ein Open-Source-Toolkit, mit dem Sie Kubernetes-Anwendungen effektiv, automatisiert und skalierbar bereitstellen und verwalten können. Als Administrator können Sie einen Agenten im OpenShift-Cluster mithilfe des **NetScaler® ADM Agent Operator** bereitstellen.

HINWEIS:

Ein im OpenShift-Cluster konfigurierter Agent wird standardmäßig nicht automatisch aktualisiert.

Voraussetzungen

Stellen Sie vor der Bereitstellung sicher, dass:

- Sie über die privilegierten Sicherheitskontextbeschränkungen verfügen, um Berechtigungen für Pods zu steuern. Führen Sie für den Agenten den folgenden Befehl aus, um die privilegierten Sicherheitskontextbeschränkungen für das Dienstkonto abzurufen:

  ```
  oc adm policy add-scc-to-user privileged -z adm-agent-serviceaccount
  ```

- Führen Sie den folgenden Befehl aus, um ein Agent-Anmeldegeheimnis zu erstellen:

  ```
  kubectl create secret generic admlogin --from-literal=username=nsroot --from-literal=password=<adm-agent-password> -n <namespace>
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- `<adm-agent-password>` ist ein Beispielpasswort. Sie müssen ein Passwort für den Agenten festlegen, und NetScaler CPX verwendet diese Anmeldeinformationen, um sich beim Agenten zu registrieren.
- Geben Sie **admlogin** für `loginSecret` in der Agent-YAML an, während Sie die Instanz erstellen.

Wenn Sie NetScaler CPX™ und den Agent in verschiedenen Namespaces bereitstellen, stellen Sie Folgendes sicher:

- Bezeichnen Sie den Namespace mit `citrix-cpx=enabled`, in dem der NetScaler CPX bereitgestellt wurde.
- Setzen Sie `helper.required` auf „true“ oder „false“ während der Installation des Agent-Operators.

HINWEIS:

Standardmäßig ist `helper.required` auf **false** gesetzt. Wenn dieser Parameter auf „false“ gesetzt ist, müssen Sie sicherstellen, dass Sie in jedem Namespace ein **admlogin**-Secret erstellen, wenn NetScaler CPX und der Agent in verschiedenen Namespaces sind.

- Sie haben `accessSecret`, die in der Agent-YAML erforderlich sind. Diese Anmeldeinformationen sind erforderlich, damit der Agent eine Verbindung mit dem NetScaler Console-Dienst herstellen kann.

```
kubectl create secret generic <secretname> --from-literal=accessid=<ID> --from-literal=accesssecret=<Secret> -n namespace
```

HINWEIS:

Geben Sie beim Erstellen der Instanz einen Secret-Namen für accessSecret in der Agent-YAML an.

Sie können die Zugriffs-ID und das Secret für den Zugriff auf die NetScaler Console über das folgende Verfahren erhalten:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Melden Sie sich bei der Citrix Cloud™ Managementkonsole an.

b. Wählen Sie im Citrix Cloud-Menü **Identitäts- und Zugriffsverwaltung** aus.

c. Geben Sie auf der Registerkarte **API-Zugriff** einen sicheren Clientnamen ein und klicken Sie auf **Client erstellen**.

d. ID und Secret werden generiert. Klicken Sie auf **Herunterladen** und speichern Sie die CSV-Datei.

ID- und Secret-Datei(/en-us/netscaler-console-service/media/id-secret.png)

Agent-Operator installieren

1. Melden Sie sich an der OpenShift-Clusterkonsole an.
2. Navigieren Sie zu **Operators > OperatorHub**.
3. Geben Sie in der Suchleiste den Agent-Namen ein, wählen Sie den **NetScaler ADM Agent Operator** aus und klicken Sie dann auf **Installieren**.

   Agent-Operator(/en-us/netscaler-console-service/media/install-agent-openshift.png)
4. Auf der Seite **Operator installieren** haben Sie zwei Optionen:

   - **Alle Namespaces im Cluster (Standard)** – Ermöglicht dem Agent-Operator, alle im Cluster verfügbaren Namespaces zu abonnieren, und erlaubt Ihnen, die Instanz des Agent-Operators von jedem Namespace im Cluster aus zu initiieren.
   - **Ein spezifischer Namespace im Cluster** – Ermöglicht dem Agent-Operator, einen ausgewählten Namespace im Cluster zu abonnieren, und Sie können die Instanz des Agent-Operators nur von dem ausgewählten Namespace aus initiieren.

     In diesem Beispiel wird der Agent-Operator einem Namespace namens **Default** zugewiesen. Wählen Sie unter **Update approval** die Option **Automatic** aus und klicken Sie auf **Installieren**.

     Installieren(/en-us/netscaler-console-service/media/install-agent-openshift-namespace.png)

     Warten Sie, bis der Agent-Operator erfolgreich abonniert wurde.

     Abonniert(/en-us/netscaler-console-service/media/install-agent-openshift-success.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Navigieren Sie zu **Workloads > Pods** und vergewissern Sie sich, dass der `netscaler-adm-agent-operator-controller` Pod aktiv und ausgeführt wird.
6. Nachdem der Pod läuft, klicken Sie auf **Instanz erstellen**.

7. Wählen Sie die **YAML-Ansicht**, um Parameter zu aktualisieren, und klicken Sie dann auf **Erstellen**.

HINWEIS:

Stellen Sie sicher, dass pro OpenShift-Cluster nur eine Agent-Instanz vorhanden ist.

8. Navigieren Sie zu **Workloads > Pods** und stellen Sie sicher, dass die Agent-Pods ausgeführt werden.

Agent-Instanz löschen

Sie können die Agent-Instanz aus dem Cluster löschen, indem Sie zu **Operators > Installed Operators** navigieren. Wählen Sie auf der Registerkarte **NetScaler ADM Agent Operator** die Instanz aus und wählen Sie **AdmAgent löschen** aus der Liste aus.

Agent-Operator deinstallieren

Wenn Sie den Agent-Operator-Pod aus dem Cluster deinstallieren möchten, navigieren Sie zu **Operators > Installed Operators** und wählen Sie dann **Operator deinstallieren** aus der Liste aus.

Container-basierten Agenten mithilfe eines Helm-Charts installieren

Sie können einen Container-basierten Agenten bereitstellen, um NetScaler CPX mit NetScaler Console zur Verwaltung und Überwachung von NetScaler CPX zu verbinden. Um einen Container-basierten Agenten bereitzustellen, befolgen Sie das Verfahren, das in diesem Dokument verfügbar ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Der Container-basierte Agent wird standardmäßig nicht automatisch aktualisiert (Evergreen-Upgrade).

So erhalten Sie Hilfe und Support

Als Citrix Cloud™-Benutzer benötigen Sie manchmal Hilfe, um einen reibungslosen Betrieb unserer Infrastruktur sicherzustellen. Dieses Thema bietet weitere Informationen zu den verschiedenen Hilfe- und Supportoptionen und wie Sie darauf zugreifen können.

Ein Citrix Cloud-Konto erstellen

Wenn beim Registrieren für ein Citrix Cloud-Konto ein Fehler auftritt, wenden Sie sich an den Citrix Kundendienst.

Bei Ihrem Konto anmelden

Wenn Sie Probleme bei der Anmeldung bei Ihrem Citrix Cloud-Konto haben:

- Stellen Sie sicher, dass Sie sich mit der E-Mail-Adresse und dem Kennwort anmelden, die Sie bei der Registrierung für Ihr Konto angegeben haben.
- Citrix Cloud fordert Sie automatisch auf, Ihr Kennwort zurückzusetzen, bevor Sie sich anmelden können, wenn:
  - Sie sich schon länger nicht bei Citrix Cloud angemeldet haben
  - Ihr Kennwort die Anforderungen von Citrix Cloud nicht erfüllt
- Weitere Informationen finden Sie unter Ändern Ihres Kennworts in diesem Artikel.
- Wenn Ihr Unternehmen Benutzern erlaubt, sich mit ihren Unternehmensanmeldeinformationen anstelle eines Citrix-Kontos bei Citrix Cloud anzumelden, klicken Sie auf **Mit meinen Unternehmensanmeldeinformationen anmelden** und geben Sie die Anmelde-URL Ihres Unternehmens ein. Sie können dann Ihre Unternehmensanmeldeinformationen eingeben, um auf das Citrix Cloud-Konto Ihres Unternehmens zuzugreifen. Wenn Sie die Anmelde-URL Ihres Unternehmens nicht kennen, wenden Sie sich an den Administrator Ihres Unternehmens, um Unterstützung zu erhalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Kennwort ändern

Wenn Sie Ihr Citrix Cloud-Kontokennwort vergessen haben, klicken Sie auf **Benutzernamen oder Kennwort vergessen?** und geben Sie Ihre Konto-E-Mail-Adresse ein. Sie erhalten eine E-Mail zum Zurücksetzen Ihres Kennworts. Wenn Sie die E-Mail zum Zurücksetzen des Kennworts nicht erhalten oder weitere Unterstützung benötigen, wenden Sie sich an den Citrix Kundendienst.

Um Ihr Kontopasswort sicher zu halten, fordert Citrix Cloud Sie möglicherweise zur Zurücksetzung Ihres Passworts auf, wenn Sie versuchen, sich anzumelden. Diese Aufforderung erfolgt, wenn:

- Ihr Passwort die Komplexitätsanforderungen von Citrix Cloud nicht erfüllt. Passwörter müssen mindestens 8 Zeichen lang sein und Folgendes enthalten:
  - Mindestens eine Zahl
  - Mindestens einen Großbuchstaben
  - Mindestens ein Symbol: `! @ # $ % \^ * ? + = -`
- Ihr Passwort Wörter aus dem Wörterbuch enthält.
- Ihr Passwort in einer bekannten Datenbank kompromittierter Passwörter aufgeführt ist.
- Sie sich in den letzten sechs Monaten nicht bei Citrix Cloud angemeldet haben.

Wenn Sie dazu aufgefordert werden, wählen Sie **Passwort zurücksetzen**, um ein neues, sicheres Passwort für Ihr Konto zu erstellen.

Citrix Cloud Support-Foren

In den Citrix Cloud Support-Foren können Sie Hilfe erhalten, Feedback und Verbesserungsvorschläge geben, Unterhaltungen anderer Benutzer ansehen oder eigene Themen starten.

Die Supportmitarbeiter von NetScaler® verfolgen diese Foren und sind bereit, Ihre Fragen zu beantworten. Andere Mitglieder der Citrix Cloud-Community bieten möglicherweise ebenfalls Hilfe an oder beteiligen sich an der Diskussion.

Sie müssen sich nicht anmelden, um Forumsthemen zu lesen. Sie müssen sich jedoch anmelden, um einen Beitrag zu verfassen oder auf ein Thema zu antworten. Um sich anzumelden, verwenden Sie Ihre vorhandenen Citrix-Kontodaten oder die E-Mail-Adresse und das Passwort, die Sie bei der Erstellung Ihres Citrix Cloud-Kontos angegeben haben. Um ein Citrix-Konto zu erstellen, gehen Sie zu Konto erstellen oder anfordern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support-Artikel und Dokumentation

NetScaler bietet eine Fülle von Produkt- und Supportinhalten, um Ihnen dabei zu helfen, das Beste aus Citrix Cloud herauszuholen und viele Probleme zu lösen, die Sie möglicherweise mit NetScaler-Produkten haben.

Citrix Cloud Resource Center

Das Citrix Cloud Resource Center bietet verschiedene Ressourcen, die Ihnen den Einstieg in Citrix Cloud-Dienste erleichtern, mehr über Funktionen erfahren und Probleme beheben. Die angezeigten Ressourcen sind auf die Funktion oder den Dienst in Citrix Cloud zugeschnitten, mit dem Sie gerade arbeiten. Wenn Sie sich beispielsweise in der Verwaltungskonsole des Virtual Apps and Desktops-Dienstes befinden, zeigt Ihnen das Resource Center die folgenden Ressourcen an.

Greifen Sie jederzeit auf das Resource Center zu, indem Sie auf das blaue Kompasssymbol unten rechts in der Citrix Cloud-Konsole klicken.

- **Erste Schritte**: Bietet eine kurze geführte Einführung in wichtige Aufgaben, die für den Dienst spezifisch sind, mit dem Sie gerade arbeiten. Sie finden auch Links zu Schulungs- und Onboarding-Ressourcen, die Ihnen helfen, mehr über die Dienstfunktionen zu erfahren und Ihre Endbenutzer erfolgreich einzurichten.
- **Ankündigungen**: Bietet Benachrichtigungen über neu veröffentlichte Funktionen und Links zu wichtigen Citrix-Mitteilungen. Klicken Sie auf eine Funktionsbenachrichtigung, um eine kurze geführte Einführung in die Funktion zu erhalten.
- **Artikel suchen**: Bietet eine Liste von Produktdokumentationen und Knowledge Center-Artikeln für gängige Aufgaben und hilft Ihnen, weitere Artikel zu finden, ohne Citrix Cloud zu verlassen. Geben Sie eine Suchanfrage in das Feld **Wie mache ich das...** ein, um eine gefilterte Liste von Artikeln basierend auf dem Dienst zu erhalten, mit dem Sie arbeiten. Im Allgemeinen erscheinen Support-Artikel zuerst in der Liste, gefolgt von Artikeln zur Produktdokumentation.

Citrix Tech Zone

Citrix Tech Zone enthält eine Fülle von Informationen, die Ihnen helfen, mehr über Citrix Cloud und andere NetScaler-Produkte zu erfahren. Hier finden Sie Referenzarchitekturen, Diagramme, Videos und technische Dokumente, die Einblicke in den Entwurf, die Erstellung und die Bereitstellung von Citrix-Technologien bieten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Technischer Support

Wenn Sie ein Problem haben, das technische Hilfe erfordert, klicken Sie auf das Symbol **Feedback und Support** oben rechts auf dem Bildschirm und wählen Sie dann **Ticket öffnen**.

Klicken Sie auf **Zu My Support** und dann auf **My Support**, um ein Ticket über das My Support-Portal zu öffnen. Sie können das My Support-Portal auch verwenden, um Ihre bestehenden Tickets zu verfolgen und Ihre aktuellen Produktberechtigungen anzuzeigen.

Service Health Dashboard

Das Citrix Cloud Service Health Dashboard bietet einen Überblick über die Echtzeitverfügbarkeit der Citrix Cloud-Plattform und -Dienste in jeder geografischen Region. Wenn Sie Probleme mit Citrix Cloud haben, überprüfen Sie das Service Health Dashboard, um sicherzustellen, dass Citrix Cloud oder bestimmte Dienste normal funktionieren.

Verwenden Sie das Dashboard, um mehr über die folgenden Bedingungen zu erfahren:

- Der aktuelle Verfügbarkeitsstatus aller Citrix Cloud-Dienste, gruppiert nach geografischer Region
- Der Dienstzustandsverlauf jedes Dienstes für die letzten sieben Tage (Standard) oder für frühere Sieben-Tage-Intervalle
- Wartungsfenster für bestimmte Dienste

Standardmäßig wird der Dienstzustand als Liste angezeigt, Sie können den Status aber auch in einer Kalenderansicht anzeigen. Wählen Sie **Weiter** oder **Zurück**, um den Dienstzustandsverlauf in Sieben-Tage-Intervallen zu durchsuchen. Sie können die Liste auch filtern, um nur betroffene Dienste anzuzeigen.

Um detailliertere Informationen zum Dienstzustandsvorfall für einen betroffenen Dienst anzuzeigen:

- In der Listenansicht klicken Sie auf das Symbol neben der Dienststatusanzeige, um detailliertere Informationen zum Dienstzustandsvorfall anzuzeigen.

- In der Kalenderansicht klicken Sie auf den Diensteintrag, um den Status des Dienstzustandsvorfalls anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Abonnements für den Dienstzustand

Um Benachrichtigungen zum Dienstzustand zu erhalten, klicken Sie oben rechts im Dashboard auf **Abonnieren** und wählen Sie die gewünschte Benachrichtigungsmethode aus.

Sie können Benachrichtigungen für alle Dienste oder nur für die von Ihnen ausgewählten Dienste abonnieren. Standardmäßig erhalten Sie alle Benachrichtigungen für einen Dienstzustandsvorfall. Um die Häufigkeit der Benachrichtigungen während eines Vorfalls zu begrenzen, können Sie wählen, nur die erste und letzte Benachrichtigung zu erhalten.

Je nach Abonnementmethode sind Links zum Abbestellen und zum Ändern Ihrer Präferenzen in der Abonnementbestätigungsnachricht, die Sie erhalten (zum Beispiel beim Abonnieren von Telefonbenachrichtigungen), oder in jeder Benachrichtigungsnachricht (zum Beispiel, wenn Sie E-Mail-Benachrichtigungen abonnieren) enthalten.

Bestätigung des Service Health-Abonnements per Telefon(/en-us/netscaler-console-service/media/service-health-subscribe-confirm-phone.jpg)

Service Health-Benachrichtigungs-E-Mail mit hervorgehobenen Abonnementoptionen(/en-us/netscaler-console-service/media/service-health-subscribe-edit-email.png)

So kündigen Sie Ihr Abonnement oder ändern Ihre Abonnementpräferenzen:

1. Suchen Sie eine vorhandene Benachrichtigung und wählen Sie den Link zum Abbestellen oder Ändern Ihrer Benachrichtigungseinstellungen aus.
2. Wenn Sie sich abmelden möchten, wählen Sie **Abbestellen** und wählen Sie dann die Benachrichtigungsmethode aus, die Sie kündigen möchten. Um alle Benachrichtigungsmethoden abzubestellen, wählen Sie **Alle Abonnements entfernen**.
3. Wenn Sie Präferenzen ändern, wählen Sie die Benachrichtigungsmethode aus, nehmen Sie die entsprechenden Änderungen an den Diensten und den Benachrichtigungen über Mindestvorfälle vor und wählen Sie dann **Speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Erweiterte grafische Benutzeroberfläche

Die grafische Benutzeroberfläche (GUI) der NetScaler Console bietet ein bereicherndes Erlebnis mit mehreren wichtigen Funktionen. Diese Funktionen bieten:

- **Optimierter Bildschirmplatz:** Benutzer können die Seitenleiste nach ihren Wünschen ein- oder ausblenden.
- **Schneller Zugriff auf Favoriten:** Häufig verwendete Menüpunkte für eine schnellere Navigation anheften.
- **Verbesserte Sichtbarkeit von Untermenüs:** Fahren Sie mit der Maus über Menüpunkte, um Untermenüs anzuzeigen und eine klarere Ansicht aller verfügbaren Optionen zu erhalten.
- **Verbesserte Untermenüstruktur:** Ein konsistentes, dreistufiges Untermenüsystem gewährleistet eine nahtlose Navigation in der NetScaler Console und bietet durchgängig ein einheitliches Erlebnis.

Diese Seite führt Sie durch die Funktionen der NetScaler Console GUI und bietet ein bereicherndes Benutzererlebnis.

Menü bei Mauszeigerbewegung anzeigen

Zuvor wurde das Untermenü der zweiten Ebene in einer Baumstruktur angezeigt. Die NetScaler Console GUI bietet eine nahtlose Navigation, bei der das sekundäre Menü beim Überfahren mit der Maus angezeigt wird und das Untermenü enthüllt. Diese Navigation verbessert das Anzeigeerlebnis, indem alle Untermenüoptionen ohne Scrollen angezeigt werden.

Optimierte Menühierarchie

Die Menühierarchie ist auf maximal drei Ebenen optimiert. Untermenüs, die zuvor über die dritte Ebene hinaus angezeigt wurden, sind jetzt auf der dritten Ebene positioniert. Die Navigation wurde für Folgendes aktualisiert:

- **Infrastruktur > Konfiguration**
- **NetScaler® Lizenzierung > Pooled Licensing**
- **Gateway > HDX™ Insight**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Aktualisierte Untermenübezeichnungen

Die Namen einiger Untermenüs wurden geändert, um sie an diesen Navigationsansatz anzupassen. Die Änderungen an der Bildschirmnavigation und die Aktualisierungen der Untermenübezeichnungen sind:

Infrastruktur > Konfiguration

VORHERIGE BILDSCHIRMNAVIGATION	GEÄNDERTE BILDSCHIRMNAVIGATION	GIBT ES EINE ÄNDERUNG IN DER UNTERMENÜBEZEICHNUNG ?
Konfiguration > Konfigurationsaufträge > Aufträge	**Konfiguration > Konfigurationsaufträge**	Ja
Konfiguration > Konfigurationsaufträge > Konfigurationsvorlagen	**Konfiguration > Konfigurationsvorlagen**	Nein
Konfiguration > Konfigurationsprüfung > Übersicht	**Konfiguration > Konfigurationsprüfung**	Ja
Konfiguration > Konfigurationsaudit > Audit-Vorlagen	**Konfiguration > Audit-Vorlagen**	Nein
Konfiguration > Konfigurationsaudit > Konfigurationshinweise	**Konfiguration > Konfigurationshinweise**	Nein

NetScaler-Lizenzierung > Pool-Lizenzierung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VORHERIGE BILDSCHIRMNAVIGATION	GEÄNDERTE BILDSCHIRMNAVIGATION	GIBT ES EINE ÄNDERUNG DER UNTERMENÜBEZEICHNUNG?
Pool-Lizenzierung > Durchsatzkapazitätslizenzen > Durchsatzkapazität	**Pool-Lizenzierung > Durchsatzkapazität**	Nein
Pool-Lizenzierung > Durchsatzkapazitätslizenzen > CPX-Lizenzen	**Pool-Lizenzierung > CPX-Lizenzen**	Nein
Pool-Lizenzierung > Durchsatzkapazitätslizenzen > CICO	**Pool-Lizenzierung > CICO**	Nein
Pool-Lizenzierung > Durchsatzkapazitätslizenzen > FIPS-Instanzen	**Pool-Lizenzierung > FIPS-Instanzen**	Nein
Pool-Lizenzierung > Selbstverwaltet > Informationen zum Lizenzablauf	**Pool-Lizenzierung > Informationen zum selbstverwalteten Ablauf**	Ja
Pool-Lizenzierung > Selbstverwaltet > Durchsatzkapazitätslizenzen > Selbstverwalteter Pool	**Pool-Lizenzierung > Selbstverwalteter Durchsatz**	Ja
Gepoolte Lizenzierung > Selbstverwaltet > Selbstverwaltete VCPU	**Gepoolte Lizenzierung > Selbstverwaltete VCPU**	Nein

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway > HDX Insight

VORHERIGE BILDSCHIRMNAVIGATION	GEÄNDERTE BILDSCHIRMNAVIGATION	GIBT ES EINE ÄNDERUNG DER UNTERMENÜBEZEICHNUNG?
HDX Insight > Lizenzen > SSL-VPN-Lizenzen	**HDX Insight > Lizenzen**	Ja

Einstellungen

Es gibt keine weiteren Änderungen unter **Einstellungen**, außer der Änderung der Untermenübezeichnung oder des Namens.

VORHERIGE BILDSCHIRMNAVIGATION	GEÄNDERTE BILDSCHIRMNAVIGATION	GIBT ES EINE ÄNDERUNG DER UNTERMENÜBEZEICHNUNG?
Einstellungen > Datenspeicherverwaltung	Es gibt keine Änderung in der Bildschirmnavigation.	Die Untermenübezeichnung wurde geändert in **Einstellungen > Datenspeicher**

Einklappbares Menü

Sie können das gesamte Menü durch Klicken auf ein Symbol einklappen oder erweitern.

Erweitertes Menü

Klicken Sie auf das Symbol **>>** im Bereich, um das gesamte Menü zu erweitern.

Eingeklapptes Menü

Klicken Sie im Bereich auf **Collapse <<**, um das gesamte Menü einzuklappen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Seitenleisten-Umschalter

Sie können den Bildschirmplatz optimieren, indem Sie die Sichtbarkeit der Seitenleiste umschalten. Klicken Sie auf die Umschalttaste in der Breadcrumb-Navigation, um die Seitenleiste auszublenden oder anzuzeigen.

Seitenleiste anzeigen

Seitenleiste ausblenden

Diese Option optimiert den Bildschirmbereich, indem die Seitenleiste ausgeblendet wird.

Als Startbildschirm festlegen

Die NetScaler Console GUI verfügt über ein Symbol neben dem Namen eines Untermenüs, das als Seite angezeigt wird. Das Startbildschirmsymbol ermöglicht es Ihnen, Ihre Landingpage festzulegen. Es erscheint nur, wenn Sie sich auf dieser spezifischen Seite befinden. Um die Seite von der Startseite zu entfernen, klicken Sie einfach erneut auf das Symbol.

Favoriten anheften

Die Funktion **Anheften** bietet einen schnelleren Zugriff auf Ihre bevorzugten Elemente. Um ein Menü oder Untermenü anzuheften, fahren Sie mit der Maus darüber und klicken Sie auf das Anheftsymbol, das neben dem Namen erscheint.

Angeheftete Menüs werden unter **ANGEHEFTET** in der Seitenleiste angezeigt, wodurch sie leicht zugänglich sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unkomplizierte Integration von NetScaler-Instanzen mithilfe von Console Advisory Connect

Mit dem Wachstum Ihrer hybriden Multi-Cloud (HMC)-Infrastruktur werden die Herausforderungen bei der Verwaltung, Überwachung, Analyse und Fehlerbehebung von NetScaler-Instanzen vielfältiger. Ein zentraler Controller, der Transparenz über Ihre gesamte Infrastruktur und alle darauf laufenden Anwendungen bietet, wird dringend benötigt.

In der heutigen Welt muss die Integration Ihrer Instanzen in einen zentralen Controller schnell, einfach und unkompliziert erfolgen. Diesem Bedarf Rechnung tragend, führt NetScaler Console einen neuen Onboarding-Workflow ein, der Ihnen eine schnellere Möglichkeit bietet, vollständige Transparenz über Ihre HMC-Bereitstellung zu erhalten.

Übersicht: Komponenten des NetScaler Console Onboarding-Workflows

Die Grundbausteine dieses Workflows sind zwei ADC-seitige Komponenten: NetScaler Service Connect und Call Home.

- **Console Advisory Connect**: Dies ist eine neue Funktion in NetScaler, die eine nahtlose Integration von NetScaler-Instanzen in NetScaler Console ermöglicht. Diese Funktion lässt die NetScaler-Instanz automatisch eine Verbindung mit NetScaler Console herstellen und System-, Nutzungs- und Telemetriedaten an NetScaler Console senden. Basierend auf diesen Daten liefert Ihnen NetScaler Console Einblicke und Empfehlungen zu Ihrer NetScaler-Infrastruktur. Dazu gehören die schnelle Identifizierung von Leistungsproblemen, hoher Ressourcennutzung und kritischen Fehlern.

  Console Advisory Connect ist auf den folgenden NetScaler-Versionen verfügbar:

  - NetScaler MPX- und VPX-Image-Version 12.1 57.18 und höher sowie 13.0 61.48 und höher. Weitere Informationen finden Sie unter (/de-de/citrix-adc/13/adm-service-connect.html).
  - NetScaler SDX-Version Image 12.1 58.14 und höher sowie 13.0 61.48 und höher. Weitere Informationen finden Sie unter (/de-de/sdx/13/adm-service-connect.html).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Call Home**: Dies ist eine bestehende Funktion in ADC, die die Instanzen regelmäßig überwacht und Daten automatisch auf den technischen Support-Server von Citrix hochlädt. Weitere Details finden Sie unter (/de-de/citrix-adc/13/system/configuring-call-home.html). Die von Call Home gesammelten Daten werden auch an NetScaler Console weitergeleitet, um diesen neuen Workflow zu ermöglichen.

Alle NetScaler-Instanzen mit Internetverbindung oder Call Home, oder Instanzen, die mit NetScaler Console Connect aktiviert sind, sind mit NetScaler Console verbunden. NetScaler Console beginnt, relevante Metriken von diesen NetScaler-Instanzen über den Call Home-Weg, den NetScaler Console Connect-Weg oder beides zu sammeln. Weitere Informationen finden Sie unter (/de-de/citrix-adc/13/data-governance.html) und (/de-de/sdx/13/data-governance.html).

Mithilfe dieser Daten erstellt NetScaler Console ein Inventar der NetScaler-Instanzen für jeden Kunden (eindeutige Organisations-ID), das Ihnen eine konsolidierte Liste Ihrer NetScaler-Instanzen anzeigt. NetScaler Console nutzt diese Daten auch, um Einblicke in Ihre NetScaler- und Gateway-Instanzen zu gewinnen, die aussagekräftige Einblicke in Ihre HMC-Bereitstellungen liefern, Probleme identifizieren und Maßnahmen zur Behebung der Probleme empfehlen. Bevor Sie die Probleme beheben können, müssen Sie die NetScaler-Instanzen in NetScaler Console integrieren.

Sie können **NetScaler- und Gateway-Instanzen zur Integration auswählen** aktivieren und die NetScaler-Instanzen auswählen, die Sie in NetScaler Console integrieren möchten. Nach dem Start werden Sie durch den Onboarding-Prozess geführt.

Der automatische Onboarding-Prozess nutzt Console Advisory Connect, was die Erfahrung automatisiert, nahtlos und schneller macht. Für NetScaler-Instanzen auf Versionen, die Console Advisory Connect und das automatische Onboarding nicht unterstützen, bietet NetScaler Console ein skriptbasiertes Onboarding, das ein halbautomatischer Prozess ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEISE

- Das automatische und skriptbasierte Onboarding verwendet einen integrierten Agenten. Dieser Workflow bietet Ihnen jedoch auch die Flexibilität, einen externen Agenten für das Onboarding zu verwenden. Sie können das externe agentenbasierte Onboarding verwenden, wenn Sie die gebündelte Lizenzierung oder die vollständige Analysesammlung in NetScaler Console nutzen möchten. Oder wenn Sie sowohl die gebündelte Lizenzierung als auch die vollständige Analysesammlung nutzen möchten. Der integrierte Agent unterstützt nur die Verwaltung und Überwachung.
- Die von Console Advisory Connect gesammelten Metriken werden direkt an den NetScaler Console Service-Endpunkt gesendet. Auch wenn der NetScaler ein verwalteter/erkannter NetScaler in NetScaler Console ist und ein externer Agent für diesen ADC konfiguriert wurde, werden die Metriken direkt vom NetScaler an den NetScaler Console Service-Endpunkt gesendet und nicht über den externen Agenten geleitet.

Ein kurzer Überblick über das Onboarding

Ihr erster Kontaktpunkt auf der Onboarding-Reise ist eine vom Produkt initiierte E-Mail. Hier ist ein kurzer Überblick über den Onboarding-Prozess:

1. Eine **vom NetScaler-Produkt initiierte E-Mail**: Sie erhalten eine E-Mail von NetScaler Console, die einige wichtige Einblicke in Ihre NetScaler-Infrastruktur zeigt und Sie einlädt, mit NetScaler Console zu beginnen. Klicken Sie in der E-Mail auf **Onboard to ADM Service**. Die Seite **Citrix Cloud** wird angezeigt.
2. Auf der Anmeldeseite von **Citrix Cloud™**:
    - Wenn Sie bereits ein Citrix Cloud-Kunde sind, melden Sie sich mit Ihren Anmeldeinformationen von **Citrix.com**, **My Citrix** oder **Citrix Cloud** bei Citrix Cloud an.
    - Wenn Sie noch kein Citrix Cloud-Kunde sind, registrieren Sie sich bei Citrix Cloud. Weitere Informationen finden Sie unter Registrierung für Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEISE

- Wenn Sie Teil mehrerer Organisations-IDs sind und eine der Organisations-IDs in Citrix Cloud ist, melden Sie sich mit Ihren vorhandenen Anmeldeinformationen an. Schließen Sie dann den Onboarding-Workflow für die neue Organisations-ID ab.
- Sie können die E-Mail-Benachrichtigungen, die Sie im Rahmen des Low-Touch-Onboarding-Workflows von Console Advisory Connect erhalten, aktivieren oder deaktivieren. Weitere Informationen finden Sie unter E-Mail-Einstellungen.

3. **NetScaler Console Willkommensseite**: Sie erhalten einen Überblick über NetScaler Console und seine Vorteile.
4. **Einblicke in Ihre NetScaler- und Gateway-Instanzen**: Sie erhalten detaillierte Einblicke in Ihre gesamte NetScaler-Infrastruktur, einschließlich Sicherheitsberatung (Ratschläge zu aktuellen NetScaler CVEs), Upgrade-Beratung (Ratschläge basierend auf EOM/EOL-Zeitplänen), Schlüsselmetriken, Trends und Hervorhebung der Probleme, die die NetScaler-Leistung und -Integrität beeinträchtigen, sowie Empfehlungen zur Behebung der Probleme.
5. **NetScaler- und Gateway-Instanzen zum Onboarding auswählen**: Sie erhalten eine konsolidierte Ansicht Ihres NetScaler-Inventars. Sie können auswählen, welche NetScaler-Instanzen Sie in NetScaler Console aufnehmen möchten.
6. **NetScaler-Instanzen in NetScaler Console aufnehmen**: Basierend auf den für das Onboarding ausgewählten NetScaler-Instanzen führt Sie NetScaler Console durch den Onboarding-Prozess. Standardmäßig ist der integrierte Agent für das automatische Onboarding ausgewählt.
7. **NetScaler Console GUI-Dashboard**: Nach Abschluss des Onboardings werden Sie zum NetScaler Console Instanz-Dashboard weitergeleitet.

Weitere Details zu jeder dieser Onboarding-Methoden finden Sie unter NetScaler-Instanzen mit NetScaler Console Connect onboarden.

NetScaler-Instanzen mithilfe von Console Advisory Connect einbinden

Dieses Dokument bietet eine Schritt-für-Schritt-Anleitung, die Ihnen den Einstieg in die NetScaler Console erleichtert. Bevor Sie beginnen, lesen Sie, wie die NetScaler Console einen neuen Onboarding-Workflow startet, der Ihnen einen schnelleren Weg bietet, vollständige Transparenz

© 1997–2026 Citrix Systems, Inc. All rights reserved.

über Ihre hybride Multi-Cloud (HMC)-Bereitstellung zu erhalten. Siehe Low-Touch-Onboarding von NetScaler-Instanzen mithilfe von NetScaler Console Connect.

Schritt 1: Erste Schritte

Sie erhalten eine E-Mail von der NetScaler Console, die einige wichtige Einblicke in Ihre NetScaler-Infrastruktur zeigt und Sie einlädt, mit der NetScaler Console zu beginnen.

1. Klicken Sie in der E-Mail auf **Onboard to ADM Service**. Die Seite **Citrix Cloud™** wird angezeigt.
2. Auf der Anmeldeseite von **Citrix Cloud**:
   - Wenn Sie bereits ein Citrix Cloud-Kunde sind, melden Sie sich bei Citrix Cloud mit Ihren Anmeldeinformationen für **Citrix.com**, **My Citrix** oder **Citrix Cloud** an.
   - Wenn Sie noch kein Citrix Cloud-Kunde sind, melden Sie sich bei Citrix Cloud an. Weitere Informationen finden Sie unter Anmeldung bei Citrix Cloud.

   HINWEISE

   - Wenn Sie Teil mehrerer Org-IDs sind und eine der Org-IDs in Citrix Cloud ist, melden Sie sich mit Ihren vorhandenen Anmeldeinformationen an. Schließen Sie dann den Onboarding-Workflow für die neue Org-ID ab.
   - Sie können die E-Mail-Benachrichtigungen aktivieren oder deaktivieren, die Sie im Rahmen des Consolve Advisory Connect-basierten Low-Touch-Onboarding-Workflows erhalten. Weitere Informationen finden Sie unter E-Mail-Einstellungen.
3. Auf der Landingpage der NetScaler Console nehmen Sie sich einen Moment Zeit, um zu lesen, warum Sie hier sind und welche Vorteile die Verwendung der NetScaler Console bietet.

HINWEIS

Die Erkenntnisse zur Sicherheitsberatung in der E-Mail basieren nur auf dem Scan der NetScaler-Build-Version. Umfassendere und schlüssigere Erkenntnisse zur Sicherheitsberatung erhalten Sie, nachdem Sie Ihre NetScaler-Instanzen in NetScaler Console integriert haben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Klicken Sie auf **Weiter**. Die Seite **Einblicke in Ihre NetScaler- und Gateway-Instanzen** wird geöffnet.

Die nächsten Schritte dienen als geführter Workflow, um Ihnen einen Einblick in die Möglichkeiten von NetScaler Console zu geben und Sie bei der nahtlosen Integration Ihrer NetScaler-Instanzen in NetScaler Console zu unterstützen.

Schritt 2: Einblicke in Ihre NetScaler- und Gateway-Instanzen

Diese Einblicksseite verwendet die über Call Home oder NetScaler Console Connect oder beides gesammelten Daten, um Einblicke in Ihre NetScaler-Instanzen zu geben. Diese Seite bietet Ihnen Einblicke in Ihre gesamte NetScaler-Infrastruktur, einschließlich Sicherheitsberatung (Hinweise zu aktuellen NetScaler-CVEs), Upgrade-Beratung (Hinweise basierend auf EOM/EOL-Zeitplänen), Schlüsselmetriken, Trends und hebt die Probleme hervor, die die NetScaler-Leistung und -Integrität beeinträchtigen, und empfiehlt Wege zur Behebung der Probleme. Diese Einblicke und Empfehlungen sind nur ein kleiner Vorgeschmack auf die Fülle der Vorteile und des Mehrwerts, die NetScaler Console zu bieten hat. Um viele weitere Vorteile und detaillierte Einblicke zu erhalten und die empfohlenen Aktionen ausführen zu können, müssen Sie die NetScaler-Instanzen in NetScaler Console integrieren.

Die Einblicke und Empfehlungen sind in die folgenden Typen kategorisiert:

- **Sicherheitsberatung**: Integrieren Sie NetScaler-Instanzen, um die CVE-Auswirkungsdetails auf Ihre NetScaler-Instanzen zu erhalten und die empfohlenen Abhilfemaßnahmen oder Mitigationen auszuführen.
- **Upgrade-Beratung**: Integrieren Sie NetScaler-Instanzen in NetScaler Console und aktualisieren Sie Ihre NetScaler-Instanzen, die EOM/EOL erreicht haben oder erreichen werden oder auf älteren Releases/Builds basieren.
- **Aktuelle Ereignisse**: Integrieren Sie NetScaler-Instanzen in NetScaler Console, um regelmäßig über 200 Ereignisse zu überwachen und Regeln zu erstellen, um per E-Mail, PagerDuty, Slack, ServiceNow benachrichtigt zu werden und entsprechende Maßnahmen zu ergreifen.
- **Ressourcennutzung – Trends und Anomalien**: Integrieren Sie NetScaler-Instanzen in NetScaler Console, um einen umfassenden Überblick über die Integrität der NetScaler-Instanz, Leistungsprobleme und Empfehlungen zur Behebung dieser Probleme zu erhalten. Sie können auch die prognostizierte CPU- und Speichernutzung für Ihre NetScaler-Instanzen bewerten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **NetScaler-Bereitstellungsanleitung**: Integrieren Sie NetScaler-Instanzen in NetScaler Console und konfigurieren Sie sie als HA-Paar mithilfe von Konfigurationsaufträgen in NetScaler Console.

1. **Sicherheitsberatung**: Die NetScaler Console Sicherheitsberatung warnt Sie vor Schwachstellen, die Ihre NetScaler-Instanzen gefährden, und empfiehlt Mitigationen und Abhilfemaßnahmen.

   HINWEIS:

   Die Erkenntnisse zur Sicherheitsberatung in der Onboarding-E-Mail und im geführten Workflow basieren nur auf dem Scan der NetScaler-Build-Version. Umfassendere und schlüssigere Erkenntnisse zur Sicherheitsberatung erhalten Sie, nachdem Sie Ihre NetScaler-Instanzen in NetScaler Console integriert haben. **Beispiel**: Wenn ein CVE sowohl einen Versionsscan als auch einen Konfigurationsscan für die Schwachstellenbewertung erfordert, zeigen die Onboarding-E-Mail und der geführte Workflow die Ergebnisse basierend auf dem Versionsscan an. Es kann also zu falsch positiven Ergebnissen kommen. Um eine schlüssigere und genauere Bewertung der Auswirkungen zu erhalten, integrieren Sie NetScaler in NetScaler Console. Nach dem Onboarding zeigt die NetScaler Console Sicherheitsberatung die Auswirkungsbewertung, welche anfällige NetScaler-Bewertung, basierend auf Versionsscan und Konfigurationsscan.

   Sie können die CVE-ID, den Schwachstellentyp und die betroffenen NetScaler-Instanzen überprüfen. Der CVE-ID-Link führt zum Sicherheitsbulletin-Artikel.

   ☐

   Die Empfehlung leitet Sie an, Ihre NetScaler-Instanzen in NetScaler Console zu integrieren, um weitere Details zu den CVE-Auswirkungen auf Ihre NetScaler-Instanzen zu erhalten und die empfohlenen Minderungs- oder Abhilfemaßnahmen auszuführen. Klicken Sie auf die betroffenen NetScaler-Instanzen, um die IP-Adressen der betroffenen Instanzen anzuzeigen.

   ☐

2. **Upgrade-Hinweis**: Verwenden Sie diesen Hinweis, um zu überprüfen, welche NetScaler-Instanzen sich dem EOM/EOL nähern oder auf älteren Builds basieren.

   Basierend auf diesen Erkenntnissen empfiehlt NetScaler Console, ein rechtzeitiges Upgrade vor EOM/EOL zu planen oder von den neuesten Funktionen und Korrekturen zu profitieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Um das Upgrade durchzuführen, müssen Sie Ihre NetScaler-Instanzen in NetScaler Console integrieren.

3. **Aktuelle Ereignisse**: Erhalten Sie Details zu einigen kritischen Fehlern, die auf den NetScaler-Instanzen aufgetreten sind, und eine Liste der NetScaler-Instanzen, auf denen die Fehler aufgetreten sind.

4. **Ressourcennutzung – Trends und Anomalien**: Finden Sie Erkenntnisse über eine hohe Ressourcennutzung für CPU, Arbeitsspeicher, HTTP-Durchsatz und SSL-Durchsatz. Für jede Erkenntnis schlägt NetScaler Console eine empfohlene Aktion vor. Um mehr Einblick in diese Erkenntnisse und Empfehlungen zu erhalten, müssen Sie Ihre NetScaler-Instanzen in NetScaler Console integrieren. Einige Vorteile nach dem Onboarding sind:

   - CPU: Vorhersage der CPU-Auslastung für die nächsten 24 Stunden in NetScaler Console.
   - Arbeitsspeicher: Vorhersage der Arbeitsspeicherauslastung für die nächsten 24 Stunden in NetScaler Console.
   - SSL-Durchsatz: Anzeige der SSL-Echtzeitoptimierung mit intelligenter App Analytics in NetScaler Console.
   - HTTP-Durchsatz: Beheben Sie Probleme mit der NetScaler-Durchsatzkapazität mit Infrastructure Analytics.

   - **Wichtige Metriken**: Erhalten Sie Details zu wichtigen Metriken bezüglich CPU, Arbeitsspeicher, HTTP-Durchsatz, SSL-Durchsatz und decken Sie anomale Trends in den Metriken auf.

5. **Bereitstellungsanleitung**: Erhalten Sie Einblick in NetScaler-Instanzen, die als eigenständige NetScaler bereitgestellt werden. NetScaler Console empfiehlt, diese NetScaler-Instanzen als HA-Paar für eine bessere Ausfallsicherheit zu konfigurieren. Dazu müssen Sie Ihre NetScaler-Instanzen in NetScaler Console integrieren und dann Wartungsaufträge verwenden, um die Instanzen als HA-Paar zu konfigurieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schritt 3: NetScaler- und Gateway-Instanzen zum Onboarding auswählen

Diese Seite zeigt alle NetScaler- und Gateway-Instanzen in Ihrer Umgebung an. Zeigen Sie die NetScaler- und Gateway-Instanzen an, die Sie in NetScaler Console integrieren möchten, wählen Sie sie aus und klicken Sie auf **Weiter**.

1. Zeigen Sie die NetScaler-Instanzen an, die Sie in NetScaler Console integrieren möchten, und wählen Sie sie aus.

   Wenn Sie Details zu einer Instanz benötigen, wie z. B. Geräteinformationen, NetScaler-Konfiguration, verfügbare NetScaler-Funktionen oder Lizenzinformationen, klicken Sie auf die IP-Adresse der Instanz unter der NetScaler-Instanz.

   Wenn Ihre Instanz nicht aufgeführt ist, verwenden Sie die Option **NetScaler nicht in der Liste gefunden** in der oberen rechten Ecke.

   Sie können auf drei Arten vorgehen: befolgen Sie die Schritte unter **NetScaler in die Liste aufnehmen** oder verwenden Sie die Option **Meinen NetScaler finden**. Wenn diese beiden Schritte nicht helfen, klicken Sie auf die Option **Konventionelle Methode verwenden**, die den Workflow überspringt und Sie auf dem traditionellen Weg des Onboardings von NetScaler-Instanzen führt.

   Für die Option **Meinen NetScaler finden** geben Sie die Details in die Pflichtfelder (Serien-ID, IP-Adresse der NetScaler-Instanz, Lizenzseriennummer und Fulfillment-ID) ein und suchen Sie.

Schritt 4: NetScaler-Instanzen in NetScaler Console integrieren

Sie können Ihre Instanzen über den integrierten Agenten (Standardoption) oder einen externen Agenten integrieren.

NetScaler-Instanzen mit einem integrierten Agenten integrieren

Die automatische und skriptbasierte Integration verwendet den integrierten Agenten, der standardmäßig eingestellt ist.

Automatische Integration: Sie wird nur auf den folgenden NetScaler-Versionen unterstützt:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler MPX- und VPX-Image-Version 12.1 57.18 und höher sowie 13.0 61.48 und höher
- SDX-Versions-Image 13.0 61.48 und höher sowie 12.1 58.14 und höher

Um eine andere NetScaler-Instanz auszuwählen, klicken Sie auf **Auswahl ändern**.

Von den insgesamt ausgewählten NetScaler-Instanzen können einige Instanzen für die automatische Integration in Frage kommen (basierend auf den Mindestversionskriterien). Sie können die Instanzen sehen, die für die automatische Integration in Frage kommen.

Sie können einen Testlauf der Integration durchführen, um sicherzustellen, dass die NetScaler-Instanz für die Integration bereit ist. Klicken Sie auf **Testen**, um den Testlauf zu starten. Weitere Informationen finden Sie unter Testen der Integrationsbereitschaft von NetScaler-Instanzen.

Wenn Sie die Integration ohne Testlauf durchführen möchten, geben Sie den NetScaler-Benutzernamen und das Kennwort ein. Die Anmeldeinformationen müssen NetScaler-Benutzer-Administratoranmeldeinformationen sein, und NetScaler Console verwendet diese Anmeldeinformationen, um NetScaler zu integrieren. Klicken Sie auf **Automatische Integration starten**, um Ihre NetScaler-Instanzen in NetScaler Console zu integrieren.

HINWEIS

Nachdem Sie die NetScaler-Anmeldeinformationen angegeben und das Geräteprofil erstellt haben, fordert die ADM-GUI den Benutzernamen und das Kennwort für jede NetScaler-Instanz nicht erneut an. Sie können jedoch das Profil aus der Dropdown-Liste **Geräteprofil** auswählen, um die NetScaler-Instanzen zu authentifizieren.

Das automatische Onboarding kann 2-5 Minuten dauern.

HINWEIS:

Wenn Sie nicht möchten, dass die NetScaler-Instanzen automatisch in NetScaler Console integriert werden, können Sie das automatische Onboarding deaktivieren und die skriptbasierte Option für das Onboarding verwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Skriptbasiertes Onboarding: Nachdem das automatische Onboarding abgeschlossen ist, können Sie die restlichen Instanzen mithilfe des skriptbasierten Onboardings integrieren. Verwenden Sie eine der folgenden Optionen:

- **Option 1**: Laden Sie das Skript herunter, entpacken Sie die Tar-Datei und führen Sie es auf einer der NetScaler-Instanzen mit dem in der Benutzeroberfläche angegebenen Befehl aus. Stellen Sie sicher, dass die NetScaler-Instanz, auf der Sie dieses Skript ausführen, über eine Netzwerkverbindung zu allen anderen ausgewählten NetScaler-Instanzen verfügt.
- **Option 2**: Melden Sie sich bei der CLI-Konsole jeder NetScaler-Instanz an und führen Sie die in der Benutzeroberfläche angegebenen Befehle aus. Weitere Informationen finden Sie in Schritt 7 im Dokument Konfigurieren des integrierten NetScaler-Agenten zur Verwaltung von Instanzen. Stellen Sie sicher, dass Sie für jede NetScaler-Instanz einen neuen eindeutigen Aktivierungscode generieren.

Nachdem Sie alle Ihre Instanzen integriert haben, klicken Sie auf **Zu NetScaler Console wechseln**, um zum Dashboard der NetScaler Console-Instanzverwaltungs-UI zu gelangen und die verschiedenen Funktionen zu erkunden.

HINWEIS

Wenn Sie ein neuer Kunde von NetScaler Console ohne NetScaler Console-Lizenz sind, ist Ihr Citrix-Servicekonto standardmäßig ein Express-Konto. Weitere Informationen zur Berechtigung für NetScaler Console-Konten finden Sie unter NetScaler Console-Ressourcen mit Express-Konto verwalten.

NetScaler-Instanzen mit einem externen Agenten integrieren

Sie können das externe agentenbasierte Onboarding verwenden, wenn Sie gebündelte Lizenzen oder die vollständige Analysesammlung in NetScaler Console oder beides (gebündelte Lizenzen und die vollständige Analysesammlung) nutzen möchten.

Führen Sie die folgenden Schritte aus:

1. Wählen Sie ein Geräteprofil aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Aus Sicherheitsgründen können Sie die Standard-NetScaler-Anmeldeinformationen (nsroot/nsroot) nicht für das Onboarding verwenden.

2. Wählen Sie einen externen Agenten aus und klicken Sie auf **Neuen Agenten einrichten**.
3. Wählen Sie eine der folgenden Umgebungen aus:

   - Amazon Web Services
   - Microsoft Azure
   - Google Cloud Platform
   - Vor Ort

Installieren Sie einen Agenten auf Ihrem lokalen Hypervisor

Wenn Sie **Vor Ort** auswählen, können Sie den Agenten auf den folgenden Hypervisoren installieren: Citrix Hypervisor™, VMware ESXi, Microsoft Hyper-V, Linux KVM Server.

1. Wählen Sie **Auf einem Hypervisor (Vor Ort)** aus und klicken Sie auf **Weiter**.
2. Wählen Sie den Hypervisor-Typ aus und laden Sie das Image herunter, zum Beispiel VMware ESXi.
3. Verwenden Sie die Dienst-URL und den Aktivierungscode, um den Agenten zu konfigurieren.

   Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren. Detaillierte Anweisungen zur Installation eines Agenten auf Ihrem lokalen Hypervisor finden Sie unter Installieren eines NetScaler-Agenten vor Ort
4. Klicken Sie auf **Agent registrieren**. Nach Abschluss klicken Sie auf **Fertig**, um zur NetScaler-Onboarding-Seite der NetScaler Console zurückzukehren.
5. Klicken Sie auf **Onboarding starten**. Nachdem Sie alle Ihre Instanzen integriert haben, klicken Sie auf **Instanz-Dashboard anzeigen**, um zum Instanzverwaltungs-UI-Dashboard der NetScaler Console zu gelangen und die verschiedenen Funktionen zu erkunden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Agenten in einer öffentlichen Cloud installieren

Sie können den Agenten in einer der folgenden Cloud-Umgebungen installieren:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

Weitere Informationen finden Sie in den folgenden Dokumenten:

- Agent in der Microsoft Azure Cloud installieren
- Agent auf AWS installieren
- Agent auf GCP installieren

Onboarding-Bereitschaft von NetScaler-Instanzen testen

Wenn Sie eine NetScaler-Instanz in die NetScaler Console aufnehmen möchten, können Sie testen, ob die Instanzen für das Onboarding bereit sind. Der Testlaufstatus zeigt Ihnen an, ob die Instanzen bereit sind oder überprüft werden müssen.

Klicken Sie auf **Testen**, um den diagnostischen Probelauf zu starten. Die Seite **Automatisches Onboarding testen** zeigt die Problemkategorie, den Status und die Empfehlung an.

Weitere Informationen finden Sie unter NetScaler-Diagnoseinformationen in der NetScaler Console-GUI anzeigen.

Wenn der NetScaler-Testlaufstatus den Status **Überprüfung erforderlich** aufweist, dann:

- Überprüfen Sie die NetScaler-Anmeldeinformationen im Geräteprofil.
- Die folgenden Endpunkte sind nicht erreichbar:
  - `adm.cloud.com`
  - `agent.adm.cloud.com`
  - `trust.citrixnetworkapi.net`
  - `download.citrixnetworkapi.net`

Wenn Probleme auftreten, wenn Sie den Test zur Onboarding-Bereitschaft ausführen, finden Sie Empfehlungen unter Fehlerbehebung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

E-Mail-Einstellungen

Der NetScaler Console-Dienst ermöglicht das Onboarding von NetScaler-Instanzen über den auf Advisory Console Connect basierenden Low-Touch-Onboarding-Workflow. Als Teil dieses Workflows erhalten Kunden produktinitiierte E-Mails vom NetScaler Console-Dienst. Sie können die E-Mail-Benachrichtigungen, die Sie im Rahmen des auf Advisory Console Connect basierenden Low-Touch-Onboarding-Workflows erhalten, aktivieren oder deaktivieren. Sie können die E-Mail-Benachrichtigungen auf folgende Weisen konfigurieren und verwalten:

- **E-Mails für alle Administratoren aktivieren** – Sie können die E-Mails für alle Administratoren in Ihrer Organisation aktivieren. Standardmäßig sind die E-Mails für alle Administratoren in der Organisation aktiviert.
- **E-Mails für ausgewählte Administratoren aktivieren/deaktivieren** – Sie können die E-Mail-Einstellungen anpassen, sodass nur bestimmte Administratoren in der Organisation E-Mails erhalten und die anderen Administratoren nicht.
- **E-Mails für alle Administratoren deaktivieren** – Sie können die E-Mails für alle Administratoren in Ihrer Organisation deaktivieren und stoppen.

E-Mail-Einstellungen konfigurieren

Sie können die E-Mail-Einstellungen konfigurieren und die E-Mails, die Sie im Rahmen des auf Console Advisory Connect basierenden Low-Touch-Onboarding-Workflows erhalten, aktivieren oder deaktivieren. Um die **E-Mail-Einstellungen** zu konfigurieren:

1. Klicken Sie in der produktinitiierten E-Mail auf **Onboard to ADM Service**. Die Seite **Citrix Cloud™** wird angezeigt.
2. Auf der Anmeldeseite von **Citrix Cloud**:
   - Wenn Sie ein bestehender Citrix Cloud-Kunde sind, melden Sie sich mit Ihren Anmeldeinformationen von Citrix.com, My Citrix oder Citrix Cloud bei Citrix Cloud an.
   - Wenn Sie kein bestehender Citrix Cloud-Kunde sind, registrieren Sie sich bei Citrix Cloud. Weitere Informationen finden Sie unter Registrieren Sie sich für Citrix Cloud.

   HINWEIS:

   Wenn Sie Teil mehrerer Organisations-IDs sind und eine der Organisations-IDs in Citrix Cloud ist, melden Sie sich mit Ihren vorhandenen Anmeldeinformationen an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die NetScaler Console-Landingpage wird angezeigt und bietet Ihnen einen Überblick über NetScaler Console und ihre Vorteile.

3. Klicken Sie auf der NetScaler Console-Landingpage auf **Weiter**.

   Die Seite **Insights zu Ihren NetScaler- und Gateway-Instanzen** wird angezeigt, auf der Sie Einblicke in Ihre gesamte NetScaler-Infrastruktur mit Empfehlungen erhalten können.

4. Klicken Sie auf der Seite **Insights zu Ihren NetScaler- und Gateway-Instanzen** auf **Weiter**.

   Die Seite **NetScaler- und Gateway-Instanzen zum Onboarding auswählen** wird angezeigt, auf der Sie eine Liste der NetScaler-Instanzen sehen, die Sie onboarden können, sowie zusätzliche Optionen wie **E-Mail-Einstellungen**.

5. Klicken Sie auf **E-Mail-Einstellungen**. Der Bereich **E-Mail-Einstellungen** wird angezeigt.

   ☐
   Sie können nun die E-Mail-Einstellungen konfigurieren, um E-Mails zu aktivieren oder zu deaktivieren.

HINWEIS:

Wenn Sie nur eine NetScaler-Instanz angebunden haben, erhalten Sie diese E-Mails nicht.

Wenn Sie sich bereits in der NetScaler Console GUI befinden und die E-Mail-Einstellungen konfigurieren möchten:

1. Navigieren Sie in der NetScaler Console GUI zu **Infrastructure > Instances** und klicken Sie dann auf **NetScaler**. Die Seite **NetScaler** wird angezeigt.
2. Klicken Sie auf der Seite **NetScaler** auf **Asset Inventory**.

   Die Seite **NetScaler- und Gateway-Instanzen zum Onboarding auswählen** wird angezeigt, um die Liste der angebundenen NetScaler-Instanzen und zusätzliche Optionen wie **E-Mail-Einstellungen** anzuzeigen.

3. Klicken Sie auf **E-Mail-Einstellungen**. Der Bereich **E-Mail-Einstellungen** wird angezeigt.

   ☐
   Sie können nun die E-Mail-Einstellungen konfigurieren, um E-Mails zu aktivieren oder zu deaktivieren.

E-Mails für alle Administratoren aktivieren

Standardmäßig sind die E-Mails für alle Administratoren in der Organisation aktiviert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So aktivieren oder abonnieren Sie die E-Mail-Benachrichtigungen als Teil des Console Advisory Connect-basierten Workflows:

1. Wählen Sie im Bereich **E-Mail-Einstellungen** die Option **E-Mails aktivieren** für alle Administratoren.

2. Klicken Sie auf **Speichern** und **Schließen**.

   Alle Administratoren in der Organisation sind jetzt abonniert und erhalten E-Mail-Benachrichtigungen als Teil des Console Advisory Connect-basierten Workflows.

E-Mails für bestimmte Administratoren in der Organisation aktivieren/deaktivieren

Sie können die E-Mail-Einstellungen anpassen, sodass nur bestimmte Administratoren in der Organisation E-Mails erhalten. Sie sehen die Liste der Administratoren, für die E-Mails aktiviert sind, auf der linken Seite und die Liste der Administratoren, für die E-Mails deaktiviert sind, auf der rechten Seite.

So deaktivieren Sie E-Mails für bestimmte Administratoren in der Organisation:

1. Suchen Sie die E-Mail-Adresse des Administrators in der Liste **Aktiviert**.
2. Klicken Sie auf die Schaltfläche Hinzufügen (**+**).

   Die E-Mail-Adresse des Administrators wird der Liste **Deaktiviert** hinzugefügt.
3. Klicken Sie auf **Speichern** und **Schließen**.

   Der Administrator ist jetzt abgemeldet, um keine E-Mail-Benachrichtigungen im Rahmen des Console Advisory Connect-basierten Workflows zu erhalten.

   HINWEIS:

   Wenn Sie E-Mails für mehrere Administratoren deaktivieren möchten, wählen Sie alle deren E-Mail-IDs in der Liste **Aktivierte** E-Mails aus und klicken Sie auf die Schaltfläche „Hinzufügen“ (**+**), um die E-Mail-IDs zur Liste **Deaktiviert** hinzuzufügen. Klicken Sie auf **Speichern** und **Schließen**.

Wenn Sie zuvor E-Mails für bestimmte oder alle Administratoren in Ihrer Organisation deaktiviert haben, können Sie E-Mails für alle Administratoren aktivieren. So aktivieren Sie E-Mails für bestimmte Administratoren in der Organisation:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Suchen Sie die E-Mail-Adresse des Administrators in der Liste **Deaktiviert**.
2. Klicken Sie auf die Schaltfläche „Entfernen“ (-). Sie sehen, dass die E-Mail-Adresse des Administrators aus der Liste **Deaktiviert** entfernt wurde.

3. Klicken Sie auf **Speichern** und **Schließen**.

   Der Administrator erhält nun E-Mails zum Onboarding. Der Administrator ist jetzt für den Empfang von E-Mail-Benachrichtigungen angemeldet.

   HINWEIS:

   Wenn Sie E-Mails für mehrere Administratoren aktivieren möchten, wählen Sie alle deren E-Mail-IDs in der Liste **Deaktivierte** E-Mails aus und klicken Sie auf die Schaltfläche „Entfernen“ (**-**), um die E-Mail-IDs zur Liste **Aktiviert** hinzuzufügen. Klicken Sie auf **Speichern** und **Schließen**.

E-Mails für alle Administratoren deaktivieren

Sie können diese Option auswählen, wenn Sie die E-Mails für alle Administratoren, die zu Ihrer Organisation gehören, deaktivieren oder stoppen möchten.

So deaktivieren oder abbestellen Sie den Empfang von E-Mails:

1. Wählen Sie im Bereich **E-Mail-Einstellungen** die Option **E-Mails für alle Administratoren deaktivieren**.

2. Klicken Sie auf **Speichern** und **Schließen**.

   Alle Administratoren in der Organisation sind jetzt abgemeldet und erhalten keine E-Mail-Benachrichtigungen mehr.

Beheben Sie Probleme mit dem Diagnosetool oder der NetScaler Console GUI

Hinweis

Das Diagnosetool ist nur für NetScaler-Instanzen anwendbar, die über das Console Advisory Connect-basierte Low-Touch-Onboarding integriert wurden oder integriert werden sollen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen finden Sie unter Low-Touch-Onboarding von NetScaler-Instanzen mithilfe von NetScaler Console Connect.
Wenn Sie eine NetScaler-Instanz in die NetScaler Console integrieren, können einige Probleme auftreten, die eine erfolgreiche Integration der NetScaler-Instanz verhindern. Als Administrator müssen Sie den Grund für den Fehler bei der Integration kennen. Sie können Diagnoseprüfungen mit dem Diagnosetool durchführen, wenn Sie:

- Probleme beim automatischen Onboarding oder skriptbasierten Onboarding auftreten
- Sicherstellen möchten, ob die NetScaler-Instanz für das Onboarding bereit ist
- Probleme bei bereits integrierten NetScaler-Instanzen analysieren möchten, die in der NetScaler Console GUI den Status „Down“ anzeigen

Wenn (/de-de/citrix-adc/13/adm-service-connect.html#how-to-enable-and-disable-citrix-adm-service-connect) auf der NetScaler-Instanz aktiviert ist, werden die Diagnosedetails automatisch an Citrix gesendet, und Sie können die Details in der (#view-pagecitrix-adc-generic-diagnostic-information-in-pageadm-product-name-long-gui) anzeigen. Wenn Console Advisory Connect nicht aktiviert ist, können Sie (#manually-use-the-diagnostic-tool).

Diagnosetool manuell verwenden

Das Diagnosetool ist als Teil des `mastools` (13.1-2.x oder höher) verfügbar und unter `/var/mastools/scripts` zugänglich. Sie können die `mastools` Version überprüfen, indem Sie den Befehl `cat /var/mastools/version.txt` in der NetScaler-Instanz ausführen.

So führen Sie das Diagnosetool aus:

1. Melden Sie sich mit einem SSH-Client bei der NetScaler-Instanz an.
2. Geben Sie „shell“ ein und drücken Sie die Eingabetaste, um in den Bash-Modus zu wechseln.
3. Geben Sie `cd /var/mastools/scripts` ein.
4. Geben Sie `sh mastools_diag` ein.

Das Tool startet und zeigt die Ergebnisse für die folgenden Diagnoseprüfungen an:

- **nscli**
- **DNS-Konfiguration**
- **Internetverbindung**
- **Instanz-zu-ADM-Verbindung**
- **Benutzerberechtigung**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn die Probleme auch nach der Fehlerbehebung weiterhin bestehen, können Sie den Support kontaktieren. Wenn Sie den Support kontaktieren, müssen Sie die Konfigurationsinformationen bereitstellen, die nach dem Ausführen des Diagnosetools angezeigt werden.

Das Folgende ist ein Beispiel für Diagnoseergebnisse für eine NetScaler-Instanz, die keine Probleme aufweist:

- **1** – Zeigt den Typ der Diagnoseprüfung an
- **2** – Zeigt die Ergebnisse der Diagnoseprüfung entweder in Grün oder in Rot an. Grün bedeutet, dass das Ergebnis erfolgreich ist, und Rot bedeutet, dass das Ergebnis nicht erfolgreich ist.
- **3** – Zeigt die NetScaler Console-Konfigurationsinformationen jedes Mal, wenn Sie das Diagnosetool ausführen, in Gelb an. Wenn Sie den NetScaler-Support kontaktieren möchten, müssen Sie diese Informationen bereitstellen.

Überprüfen Sie die Bereitschaft der NetScaler-Instanz für das Onboarding mit dem Diagnosetool

Bevor Sie die NetScaler-Instanz in NetScaler Console integrieren, können Sie die Bereitschaft der NetScaler-Instanz überprüfen, indem Sie das Diagnosetool auf der NetScaler-Instanz ausführen. Wenn die NetScaler-Instanz keine Probleme aufweist und bereit für das Onboarding ist, zeigt das Tool die Meldung **device not claimed on ADM** an.

Gerät nicht in NetScaler Console beansprucht(/en-us/netscaler-console-service/media/device-not-claimed.png)

NetScaler-Diagnoseinformationen in der NetScaler Console GUI anzeigen

Navigieren Sie zu **Infrastructure > Instances > NetScaler** und klicken Sie auf **Asset Inventory**, um die neu hinzugefügte Option **Onboarding Readiness** anzuzeigen, die den Onboarding-Bereitschaftsstatus der NetScaler-Instanz angibt, wie z. B. **Überprüfung erforderlich** oder **OK**.

- **Überprüfung erforderlich**. Die NetScaler-Instanz weist Probleme auf, die behoben werden müssen.
- **OK**. Die NetScaler-Instanz ist bereit für das Onboarding.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Wenn die **Onboarding Readiness** leer angezeigt wird, bedeutet dies, dass die NetScaler-Instanz nicht mit dem neuesten Image ausgeführt wird, das Diagnoseunterstützung bietet.

Wenn die NetScaler-Instanz Probleme aufweist, wird die Option **Überprüfung erforderlich** angezeigt, und Sie können darauf klicken, um weitere Details anzuzeigen.

Automatische Diagnosemeldung(/en-us/netscaler-console-service/media/auto-diagnostic-info.png)

Nachdem Sie auf **Überprüfung erforderlich** geklickt haben, zeigt die Seite **NetScaler Diagnostics Details** die Problemdetails an.

Details zum automatischen Diagnoseproblem(/en-us/netscaler-console-service/media/auto-diagnostic-issue.png)

- **Kategorie**. Gibt die Problemkategorie an.
- **Status**. Gibt den Problemstatus an, wie z. B. **Überprüfung erforderlich**, **OK** oder **Nicht zutreffend**.
- **Empfehlung**. Gibt die erforderliche Empfehlung zur Behebung des Problems an.

Nachdem Sie das Problem behoben haben, ändert sich der Status in der Onboarding Readiness zu **OK**.

Fehlerbehebung

Im Folgenden sind einige Probleme mit NetScaler-Instanzen und deren Schritte zur Fehlerbehebung aufgeführt:

Ungültiger Benutzername oder ungültiges Kennwort

Problemumgehung: Stellen Sie sicher, dass der im Administratorprofil angegebene Benutzername und das Kennwort korrekt sind. Wenn Sie das Kennwort der NetScaler-Instanz geändert haben, müssen Sie die Administratorprofile der Instanzen ändern. Weitere Informationen finden Sie unter Administratorprofil ändern.

DNS-Konfigurationsfehler

Problemumgehung: Stellen Sie sicher, dass DNS konfiguriert ist oder die DNS-IP-Adresse gültig ist. Weitere Informationen finden Sie unter DNS-Konfiguration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Keine Internetverbindung

Problemumgehung: Stellen Sie sicher, dass die Firewall-Einstellung den Internetzugang nicht blockiert und der erforderliche Proxy konfiguriert ist.

Keine Verbindung zum NetScaler Console-Endpunkt

Problemumgehung: Überprüfen Sie die Firewall-Einstellungen und stellen Sie sicher, dass die folgenden NetScaler Console-Endpunkte in der Firewall nicht blockiert sind:

```
ADM_GRP_EP = "adm.cloud.com"



ADM_AGENT_EP = "agent.adm.cloud.com"



ADM_TRUST_EP = "trust.citrixnetworkapi.net"



ADM_DOWNLOAD_EP = "download.citrixnetworkapi.net"
```

Wenn bei den Diagnoseprüfungen kein Problem gefunden wurde und das Verbindungsproblem weiterhin besteht, notieren Sie sich die NetScaler Console-Konfigurationsinformationen (in Gelb verfügbar) und wenden Sie sich an den NetScaler-Support.

Wenn Sie einen Testlauf durchführen, um sicherzustellen, dass die NetScaler-Instanz für das Onboarding bereit ist, können die folgenden Probleme auftreten:

Timeout des integrierten Agent-Testlaufs

Wenn die Ergebnisse des Probelaufs nicht innerhalb von 5 Minuten abgerufen werden, wird eine Timeout-Meldung angezeigt.

Empfehlung: Es wird empfohlen, zu überprüfen, ob die NetScaler-Instanz mit dem neuesten Image läuft, das Diagnoseunterstützung bietet. Außerdem wird in der Tabelle „Asset-Auswahl“ die Spalte „Onboarding-Bereitschaft“ leer angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Roter Umriss im Dropdown-Menü des Geräteprofils

Die NetScaler-Authentifizierung schlägt während des Probelaufs fehl, und im Dropdown-Menü des Geräteprofils wird ein roter Umriss angezeigt.

Empfehlung: Geben Sie die NetScaler-Benutzer-Admin-Anmeldeinformationen erneut ein, erstellen Sie das Geräteprofil und klicken Sie auf „Testen“, um den Probelauf erneut auszuführen.

Umstellung von einem integrierten Agenten auf einen externen Agenten

Möglicherweise haben Sie mit der Verwendung von NetScaler Console nur für die Verwaltung und Überwachung begonnen, und später möchten Sie möglicherweise andere Funktionen wie gepoolte Lizenzierung und Analysen nutzen. Dazu müssen Sie von dem integrierten Agenten zu einem externen Agenten wechseln.

Der integrierte Agent unterstützt nur Verwaltungs- und Überwachungsfunktionen. Für andere NetScaler Console-Funktionen wie gepoolte Lizenzierung und Analysen benötigen Sie einen externen Agenten. Dieses Dokument beschreibt die Schritte für die Umstellung von einem vorhandenen integrierten NetScaler Console-Agenten auf einen externen Hypervisor-basierten Agenten.

Bevor Sie beginnen

Installieren Sie einen externen Agenten, bevor Sie mit der Umstellung beginnen. Befolgen Sie das Verfahren im Thema Installieren eines NetScaler-Agenten vor Ort.

Umstellung von einem integrierten Agenten auf einen externen Agenten

Führen Sie die folgenden Schritte aus, um von einem integrierten Agenten zu einem externen Agenten zu wechseln:

1. Wählen Sie in der NetScaler Console-GUI unter **Infrastructure > Instances Dashboard > NetScaler** die NetScaler-Instanz aus und klicken Sie auf **Edit**.

2. Wählen Sie den Standort und den Agenten aus und klicken Sie auf **OK**.

3. Wählen Sie die Instanz erneut aus und klicken Sie auf **Select Action > Rediscover**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Informationen zum Erstellen eines Standorts in NetScaler Console und zum Hinzufügen des Agenten zum Standort finden Sie unter Instanzen hinzufügen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SAML als Identitätsanbieter mit NetScaler Console verbinden

NetScaler Console unterstützt die Verwendung von SAML (Security Assertion Markup Language) als Identitätsanbieter zur Authentifizierung von Administratoren und Abonnenten, die sich bei ihrer NetScaler Console anmelden. Sie können den SAML 2.0-Anbieter Ihrer Wahl mit Ihrem lokalen Active Directory (AD) verwenden.

Für die meisten SAML-Anbieter verwenden Sie die Informationen in diesem Artikel, um die SAML-Authentifizierung einzurichten. Wenn Sie die SAML-Authentifizierung mit Ihrem Azure AD verwenden möchten, haben Sie die Möglichkeit, die Citrix Cloud™ SAML SSO-App aus der Azure AD-App-Galerie zu verwenden.

Voraussetzungen

Die SAML-Authentifizierung mit NetScaler Console hat die folgenden Anforderungen:

- SAML-Anbieter, der SAML 2.0 unterstützt
- Lokale AD-Domäne
- Zwei Cloud Connectors, die an einem Ressourcenstandort bereitgestellt und Ihrer lokalen AD-Domäne beigetreten sind. Die Cloud Connectors werden verwendet, um sicherzustellen, dass Citrix Cloud mit Ihrem Ressourcenstandort kommunizieren kann.
- AD-Integration mit Ihrem SAML-Anbieter.

Cloud Connectors

Sie müssen mindestens zwei (2) Server haben, auf denen die Citrix Cloud Connector™-Software installiert werden kann. Es wird empfohlen, mindestens zwei Server für die Hochverfügbarkeit des Cloud Connectors zu haben. Diese Server müssen die folgenden Anforderungen erfüllen:

- Erfüllt die Systemanforderungen, die in den Cloud Connector Technical Details beschrieben sind.
- Es sind keine anderen Citrix-Komponenten installiert, ist kein AD-Domänencontroller und ist keine Maschine, die für Ihre Ressourcenstandortinfrastruktur kritisch ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Der Domäne beigetreten, in der sich Ihre Ressourcen befinden. Wenn Benutzer auf Ressourcen in mehreren Domänen zugreifen, müssen Sie mindestens zwei Cloud Connectors in jeder Domäne installieren.
- Mit einem Netzwerk verbunden, das die Ressourcen kontaktieren kann, auf die Abonnenten über Citrix Workspace zugreifen.
- Mit dem Internet verbunden.

Active Directory

Bevor Sie die SAML-Authentifizierung konfigurieren, führen Sie die folgenden Aufgaben aus:

- Die Felder Vorname, Nachname und E-Mail sind für die Benutzer in Active Directory obligatorisch, um Benutzer in die Okta-Instanz zu importieren.
- Stellen Sie sicher, dass Ihre Workspace-Abonnenten Benutzerkonten in Active Directory (AD) haben. Abonnenten ohne AD-Konten können sich nicht erfolgreich bei ihren Workspaces anmelden, wenn die SAML-Authentifizierung konfiguriert ist.
- Stellen Sie sicher, dass die Benutzereigenschaften in den AD-Konten Ihrer Abonnenten ausgefüllt sind. Citrix Cloud benötigt diese Eigenschaften, um den Benutzerkontext herzustellen, wenn sich Abonnenten bei Citrix Workspace anmelden. Wenn diese Eigenschaften nicht ausgefüllt sind, können sich Abonnenten nicht anmelden. Diese Eigenschaften umfassen:
  - E-Mail-Adresse
  - Anzeigename (optional)
  - Allgemeiner Name
  - SAM-Kontoname
  - Benutzerprinzipalname
  - Objekt-GUID
  - SID
- Verbinden Sie Ihr Active Directory (AD) mit Ihrem Citrix Cloud-Konto, indem Sie Cloud Connectors in Ihrem lokalen AD bereitstellen.
- Synchronisieren Sie Ihre AD-Benutzer mit dem SAML-Anbieter. Citrix Cloud benötigt die AD-Benutzerattribute für Ihre Workspace-Abonnenten, damit diese sich erfolgreich anmelden können.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SAML-SSO-Konfiguration

Navigieren Sie in einer Okta-Instanz zu **Directory integrations > Add Active Directory**.

Für eine erfolgreiche Integration muss der SAML-Identitätsanbieter Citrix Cloud bestimmte Active Directory-Attribute des Benutzers in der SAML-Assertion übermitteln. Insbesondere:

- Sicherheits-ID (SID)
- objectGUID (OID)
- Benutzerprinzipalname (UPN)
- E-Mail (E-Mail)

1. Melden Sie sich mit Administratoranmeldeinformationen bei Okta an.
2. Wählen Sie **Directory > Profile Editor** und dann das Profil **Okta User (default)** aus. Okta zeigt die Seite „Benutzerprofil“ an.

3. Wählen Sie unter **Attributes** die Option **Add Attributes** aus und fügen Sie die benutzerdefinierten Felder hinzu.

   - `cip_sid`
   - `cip_upn`
   - `cip_oid`
   - `cip_email`

   Klicken Sie auf **Speichern und weiteres hinzufügen** und wiederholen Sie den Vorgang, um 4 benutzerdefinierte Attribute zu erstellen.

   Sie können die folgenden Details anzeigen, nachdem Sie 4 benutzerdefinierte Attribute erstellt haben:

4. Ordnen Sie Active Directory-Attribute den benutzerdefinierten Attributen zu. Wählen Sie das von Ihnen verwendete Active Directory unter **Benutzer > Verzeichnisse** aus.
5. Bearbeiten Sie die Attributzuordnungen:

   a. Navigieren Sie in der Okta-Konsole zu **Verzeichnis > Profil-Editor**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Suchen Sie das `active_directory` Profil für Ihr AD. Dieses Profil könnte im Format „myDomain User“ bezeichnet sein, wobei „myDomain“ der Name Ihrer integrierten AD-Domäne ist.

c. Wählen Sie **Zuordnungen** aus. Die Seite **Benutzerprofilzuordnungen** für Ihre AD-Domäne wird angezeigt und die Registerkarte zum Zuordnen Ihres AD zu Okta-Benutzer ist ausgewählt.

d. Ordnen Sie in der Spalte **Okta-Benutzerprofil** die Active Directory-Attribute den von Ihnen erstellten benutzerdefinierten Attributen zu:

i. Wählen Sie für `cip_email` E-Mail aus der Spalte „Benutzerprofil“ für Ihre Domäne aus. Wenn ausgewählt, wird die Zuordnung als `appuser.email` angezeigt.

ii. Wählen Sie für `cip_sid` **objectSid** aus der Spalte „Benutzerprofil“ für Ihre Domäne aus. Wenn ausgewählt, wird die Zuordnung als `appuser.objectSid` angezeigt.

iii. Wählen Sie für `cip_upn` `userName` aus der Spalte **Benutzerprofil** für Ihre Domäne aus. Wenn ausgewählt, wird die Zuordnung als `appuser.userName` angezeigt.

iv. Wählen Sie für `cip_oid` `externalId` aus der Spalte **Benutzerprofil** für Ihre Domäne aus. Nach der Auswahl wird die Zuordnung als `appuser.externalId` angezeigt.

6. Melden Sie sich bei Citrix Cloud unter `https://citrix.cloud.com` an.
7. Wählen Sie im Citrix Cloud-Menü **Identitäts- und Zugriffsverwaltung** aus.
8. Suchen Sie **SAML 2.0** und klicken Sie auf **Verbinden**.

   Die Seite **SAML konfigurieren** wird angezeigt.

   Laden Sie die Datei `xml` herunter und öffnen Sie die Datei mit einem beliebigen Dateieditor. Sie müssen zu dieser Seite zurückkehren, nachdem Sie die weitere Konfiguration in Okta abgeschlossen haben.
9. Navigieren Sie in Okta zu **Application > Create App Integration**.
10. Klicken Sie auf der Seite **Add Application** auf **Create New App**.
11. Wählen Sie auf der Seite **Create a New Application Integration** die Option **SAML 2.0** aus und klicken Sie auf **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. Geben Sie Details wie App-Namen, App-Logo (optional) an, legen Sie die App-Sichtbarkeit fest und klicken Sie dann auf **Next**.
13. Auf der Registerkarte **Configuration SAML** müssen Sie die Details aus der heruntergeladenen Datei `xml` verwenden:

    a. Geben Sie die URL-Details für **Single sign-on URL** als `https://saml-internal.cloud.com/saml/acs` und **Audience URI (SP Entity ID)** als `https://saml-internal.cloud.com` an.

    HINWEIS:

    Bei externer Citrix Cloud muss die URL `https://saml.cloud.com/saml/acs` und `https://saml.cloud.com` anstelle der `https://saml-internal.cloud.com`-Domäne sein.

    b. Wählen Sie **Nicht spezifiziert** für **Name ID Format**.

    c. Wählen Sie **Okta-Benutzername** für **Anwendungsbenutzername**.

    d. Klicken Sie auf **Erweiterte Einstellungen anzeigen** und stellen Sie sicher, dass **Antwort** und **Assertion** mit **Signiert** ausgewählt sind.

    e. Fügen Sie **Attributanweisungen** hinzu, wie in der folgenden Abbildung gezeigt.

    f. Sie können alle anderen Optionen standardmäßig belassen und auf **Weiter** klicken.

    g. Wählen Sie **Ich bin ein Okta-Kunde, der eine interne App hinzufügt** und klicken Sie dann auf **Fertig stellen**.

14. Die Okta-Anwendung ist nun erstellt und klicken Sie auf **Setup-Anweisungen anzeigen**.

    Die Seite **Konfigurieren von SAML 2.0 für Testanwendungen** wird mit Details angezeigt, die Sie erneut in der Citrix Cloud hinzufügen müssen.

    Laden Sie das Zertifikat herunter, um es in die Citrix Cloud hochzuladen.

15. Sie müssen nun zur Seite **SAML konfigurieren** in Citrix Cloud zurückkehren und die restliche Konfiguration wie folgt abschließen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verwenden Sie das heruntergeladene Zertifikat und benennen Sie die Dateinamenerweiterung von `.cert` in `.crt` um, um es in Citrix Cloud hochzuladen.

16. Nachdem Sie das Zertifikat hochgeladen haben, verwenden Sie alle anderen Optionen, die standardmäßig eingestellt sind:

17. Als Nächstes müssen Sie sicherstellen, dass `appuser.userName` unter **Directory-integrations > Active Directory -> Provisiong > To okta** definiert ist.

    HINWEIS:

    Manchmal müssen Sie `user.cip_upn` anstelle von `appuser.cip_upn` verwenden. Stellen Sie sicher, dass Sie die Definition Ihrer Anwendung in der OKTA-Integration überprüfen, wie in diesem Bild gezeigt.

18. Sie müssen nun versuchen, Benutzer in Okta zu dieser SAML-Anwendung hinzuzufügen. Sie können Benutzer auf verschiedene Weisen zuweisen.

    Methode 1:

    a. Melden Sie sich bei Okta mit Administratoranmeldeinformationen an
    b. Navigieren Sie zu **Applications > Applications**
    c. Wählen Sie die SAML-Anwendung aus, die Sie erstellt haben
    d. Klicken Sie auf **Assign > Assign to People**

    e. Klicken Sie auf **Assign** und wählen Sie dann **Save and Go back**.
    f. Klicken Sie auf **Fertig**.

    Methode 2:

    a. Navigieren Sie zu **Applications > Applications**.
    b. Klicken Sie auf **Assign Users to App**.

    c. Wählen Sie die Anwendung und die Benutzer aus und klicken Sie dann auf **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Klicken Sie auf **Confirm Assignments**.

Methode 3:

a. Navigieren Sie zu **Directory > People**.

b. Wählen Sie einen beliebigen Benutzer.

c. Klicken Sie auf **Assign Applications** und weisen Sie dem Benutzer die SAML-Anwendung zu.

19. Melden Sie sich nach dem Zuweisen der Benutzer bei Citrix Cloud an.
20. Wählen Sie im Citrix Cloud-Menü **Identity and Access Management** aus.
21. Klicken Sie auf der Registerkarte **Administrators** auf **Add Administrator/group**.
22. Wählen Sie **Active Directory -** aus der Liste aus, wählen Sie die Domäne aus und klicken Sie dann auf **Weiter**.

23. Geben Sie die Zugriffsberechtigungen an.
24. Überprüfen Sie, ob alles korrekt ist, und klicken Sie auf **Send Invitiation**.
25. Auf der Registerkarte **Authentication** können Sie die Anmelde-URL für SAML 2.0 anzeigen. Es folgt ein Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Systemanforderungen

Bevor Sie NetScaler Console verwenden, müssen Sie die Softwareanforderungen, Browseranforderungen, Portinformationen, Lizenzinformationen und Einschränkungen überprüfen.

Unterstützte Browser

Um auf NetScaler Console zuzugreifen, muss Ihre Arbeitsstation über einen unterstützten Webbrowser verfügen.

Die folgenden Browser werden unterstützt.

WEBBROWSER	VERSION
Microsoft Edge	79 und höher
Google Chrome	51 und höher
Safari	10 und höher
Mozilla Firefox	52 und höher

Anforderungen an die Agent-Installation

Installieren und konfigurieren Sie einen Agenten in Ihrer Netzwerkumgebung, um die Kommunikation zwischen der NetScaler Console und den verwalteten Instanzen in Ihrem Rechenzentrum zu ermöglichen. In Ihrem lokalen Rechenzentrum können Sie einen Agenten auf Citrix XenServer, VMware ESXi, Microsoft Hyper-V und Linux KVM-Servern installieren.

Die Agent-Anforderungen sind die virtuellen Computerressourcen, die der Hypervisor für jeden Agenten bereitstellen muss. Die folgende Tabelle listet die Agent-Anforderungen auf, um alle Funktionen der NetScaler Console nutzen zu können:

KOMPONENTE	ANFORDERUNG
RAM	32 GB
Virtuelle CPU	8

© 1997–2026 Citrix Systems, Inc. All rights reserved.

KOMPONENTE	ANFORDERUNG
Speicherplatz	30 GB
Virtuelle Netzwerkschnittstellen	1
Durchsatz	1 Gbit/s

Die Agent-Anforderungen zur Nutzung der gepoolten oder flexiblen Lizenzierungsfunktion finden Sie unter Leichter Agent für gepoolte oder flexible Lizenzierung.

Sie können einen Agenten auch auf Microsoft Azure, AWS oder Google Cloud installieren. Citrix empfiehlt die Verwendung der folgenden virtuellen Maschinentypen von den jeweiligen Cloud-Marktplätzen, um alle NetScaler Console-Funktionen nutzen zu können:

CLOUD	AGENT-ANFORDERUNGEN	BEVORZUGTER VIRTUELLER MASCHINENTYP
AWS	8 virtuelle CPUs, 32 GB RAM und 30 GB Speicherplatz	`m4.2xlarge`
Microsoft Azure	8 virtuelle CPUs, 32 GB RAM und 30 GB Speicherplatz	`Standard_D8s_v3`
Google Cloud	8 virtuelle CPUs, 32 GB RAM und 30 GB Speicherplatz	`e2-standard-8`

HINWEISE:

Azure wird das Skalieren von Agents mit den Basis-Installer-Versionen 13.0 und 13.1 nach July 23, 2024 nicht mehr unterstützen.

Für NetScaler Agents:

- NetScaler Agents mit 8 virtuellen CPUs, 32 GB RAM und 30 GB Speicherplatz bleiben davon unberührt. Diese Agents können ohne Unterbrechungen aktualisiert werden.
- Bereitstellungen, die mit Version 14.1 begonnen wurden, bleiben ebenfalls unberührt.

Für Lightweight Agents:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Lightweight Agents mit 4 virtuellen CPUs, 8 GB RAM und 30 GB Speicherplatz, die die Basis-Installer-Versionen 13.0 oder 13.1 verwenden, können nach dem Deprecation-Datum nicht mehr skaliert werden (CPU oder RAM erhöhen).
- Um die Lightweight Agents in Zukunft zu skalieren, stellen Sie einen neuen Agent mit der neuesten Version bereit.

Anweisungen zur Installation eines Agents finden Sie unter den folgenden Links:

- Installieren eines Agents in Microsoft Azure Cloud.
- Installieren eines Agents in AWS.
- Installieren eines Agents in Google Cloud.

Lightweight Agent für gepoolte oder flexible Lizenzierung

Wenn Sie die NetScaler Console nur für die gepoolte oder flexible Lizenzierung verwenden möchten, können Sie einen Agent mit geringeren Spezifikationen verwenden, wie in der folgenden Tabelle aufgeführt:

KOMPONENTE	ANFORDERUNG
RAM	8 GB
Virtuelle CPU	4
Speicherplatz	30 GB

Solche Agents mit geringeren Spezifikationen (Lightweight) werden nur auf NetScaler Console unterstützt.

Citrix empfiehlt die Verwendung der folgenden virtuellen Maschinentypen von den jeweiligen Cloud-Marktplätzen, um nur die Funktion für gepoolte Lizenzen zu nutzen:

CLOUD	AGENT-ANFORDERUNGEN	BEVORZUGTER VIRTUELLER MASCHINENTYP
AWS	4 virtuelle CPU, 8 GB RAM und 30 GB Speicherplatz	`m4.xlarge`. Dieser Instanztyp bietet 4 virtuelle CPUs, 16 GB RAM und 30 GB Speicherplatz. Citrix empfiehlt diesen Instanztyp,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CLOUD	AGENT-ANFORDERUNGEN	BEVORZUGTER VIRTUELLER MASCHINENTYP
		da er die meisten Agent-Anforderungen unter den bestehenden Instanztypen erfüllt.
Microsoft Azure	4 virtuelle CPUs, 8 GB RAM und 30 GB Speicherplatz	`Standard_F4s_v2`
Google Cloud	4 virtuelle CPUs, 8 GB RAM und 30 GB Speicherplatz	`e2-standard-4`

HINWEIS

Sie müssen die standardmäßigen Planungsaufträge deaktivieren, indem Sie zu **Settings > Global Settings > Configurable Features** navigieren.

Unterstützte Ports

Für die Kommunikation zwischen NetScaler-Instanzen und dem Agenten öffnen Sie die erforderlichen Ports.

Ports für den NetScaler-Agenten

Diese Tabelle erläutert die erforderlichen Ports, die auf dem Agenten geöffnet sein müssen.

PORT	TYP	DETAILS	KOMMUNIKATIONS RICHTUNG
80/443	TCP	Für die NITRO-Kommunikation vom NetScaler Console-Dienst zu NetScaler.	NetScaler-Agent zu NetScaler und NetScaler zu NetScaler-Agent
4739	UDP	Für die AppFlow-Kommunikation von NetScaler zum	NetScaler zu NetScaler-Agent

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYP	DETAILS	KOMMUNIKATIONS RICHTUNG
		NetScaler Console-Dienst.	
162	UDP	Zum Empfangen von SNMP-Ereignissen von der NetScaler-Instanz an den NetScaler Console-Dienst.	NetScaler zu NetScaler-Agent
514	UDP	Um Syslog-Nachrichten von der NetScaler-Instanz an den NetScaler Console-Dienst zu empfangen.	NetScaler an NetScaler-Agent
5563	TCP	Dieser Port ist erforderlich, damit der NetScaler Console Collector-Dienst ausgeführt werden kann. Zum Empfangen von NetScaler-Metriken (Zählern) von der NetScaler-Instanz an NetScaler Console.	NetScaler an NetScaler-Agent
5557/5558	TCP	Für die Logstream-Kommunikation (für WAF-Sicherheitsverletzungen, Web Insight und HDX Insight) von NetScaler an den NetScaler Console-Dienst.	NetScaler an NetScaler-Agent

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYP	DETAILS	KOMMUNIKATIONS RICHTUNG
27000 und 7279	TCP	Lizenzports für die Kommunikation zwischen NetScaler-Agent und NetScaler-Instanz. Diese Ports werden auch für NetScaler Pooled Licenses verwendet.	NetScaler an NetScaler-Agent
5140	UDP	Port zum Empfangen von NetScaler Gateway-Telemetriedaten	NetScaler zu NetScaler-Agent

Ports für NetScaler-Instanzen

Diese Tabelle erläutert die erforderlichen Ports, die auf NetScaler-Instanzen geöffnet sein müssen.

PORT	TYP	DETAILS	KOMMUNIKATIONS RICHTUNG
80/443	TCP	Für die NITRO-Kommunikation von NetScaler Console zur NetScaler-Instanz.	NetScaler-Agent zu NetScaler und NetScaler zu NetScaler-Agent
22	TCP	Für die SSH-Kommunikation zwischen dem Agenten und NetScaler. **Hinweis:** Dieser Port wird auch für die NetScaler-Telemetrie verwendet.	NetScaler-Agent zu NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PORT	TYP	DETAILS	KOMMUNIKATIONS RICHTUNG
Kein reservierter Port	ICMP	Zur Erkennung der Netzwerk-Erreichbarkeit zwischen NetScaler-Agent und NetScaler-Instanzen.	NetScaler-Agent zu NetScaler
161	UDP	Zum Abrufen von Ereignissen von NetScaler-Instanzen.	NetScaler-Agent zu NetScaler

Ports für den integrierten NetScaler-Agenten

Diese Tabelle erläutert die erforderlichen Ports, die für den integrierten NetScaler-Agenten benötigt werden.

PORT	TYP	DETAILS	KOMMUNIKATIONS RICHTUNG
443	TCP	Für die NITRO-Kommunikation von NetScaler Console zur NetScaler-Instanz.	NetScaler Console zum integrierten NetScaler-Agent und integrierter NetScaler-Agent zu NetScaler Console

HINWEIS:

Der Endpunkt des NetScaler Console-Dienstes ist derselbe wie die „Dienst-URL“, die beim Versuch, den Agenten zu registrieren, generiert wird. Der Agent verwendet die Dienst-URL, um die NetScaler Console zu finden.

Stellen Sie sicher, dass die folgenden Endpunkt-URLs zugelassen sind:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DIENST	GOVERNMENT CLOUD	JAPAN	ANDERE REGIONEN (APEC, EU UND USA)
Download-Dienst	`download.adm.cloud.us`	`download.citrixnetworkapi.net`	`download.citrixnetworkapi.net`
Vertrauensdienst	`*.citrixnetworkapi.us`	`*.citrixnetworkapi.jp`	`*.citrixnetworkapi.net`
	`trust.citrixworkspacesapi.us`	`trust.citrixworkspacesapi.jp`	`trust.citrixworkspacesapi.net`
Dienst-URLs	`*.agent.adm.cloud.us`	`*.agent.adm.citrixcloud.jp`	`*.agent.adm.cloud.com`
	`*.adm.cloud.us`	`*.adm.citrixcloud.jp`	`*.adm.cloud.com`
	`adm.cloud.us`	`adm.citrixcloud.jp`	`adm.cloud.com`
Citrix Cloud-Konnektivität	`citrix.cloud.us`	`citrix.citrixcloud.jp`	`citrix.cloud.com`
	`accounts.cloud.us`	`accounts.citrixcloud.jp`	`accounts.cloud.com`

Anforderungen für die NetScaler Console Analytics-Lösung

Erforderliche Mindestversionen von Citrix Virtual Apps and Desktops

NETSCALER CONSOLE-FUNKTION	CITRIX VIRTUAL APPS AND DESKTOPS-VERSION
HDX Insight	Citrix Virtual Apps and Desktops 7.0 und höher

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Die NetScaler Gateway-Funktion (als Access Gateway Enterprise für die Versionen 9.3 und 10.x bezeichnet) muss auf der NetScaler-Instanz verfügbar sein. NetScaler Console unterstützt keine eigenständigen Access Gateway Standard Appliances.

NetScaler Console kann Berichte für Anwendungen generieren, die auf einer Citrix Virtual App oder einem Desktop veröffentlicht sind und über Citrix Workspace aufgerufen werden. Diese Funktion hängt jedoch vom Betriebssystem ab, auf dem Citrix Workspace installiert ist. Derzeit analysiert ein NetScaler den ICA-Datenverkehr nicht für Anwendungen oder Desktops, die über Citrix Workspace aufgerufen werden, das auf iOS- oder Android-Betriebssystemen ausgeführt wird.

Unterstützte Thin Clients für HDX™ Insight

NetScaler Console unterstützt die folgenden Thin Clients zur Überwachung von NetScaler-Instanzen, die auf Softwareversion 11.0 Build 65.31 und höher ausgeführt werden:

- Dell Wyse Windows-basierte Thin Clients
- Dell Wyse Linux-basierte Thin Clients
- Dell Wyse ThinOS-basierte Thin Clients
- 10ZiG Ubuntu-basierte Thin Clients

NetScaler-Instanzlizenz für HDX Insight erforderlich

Die von NetScaler Console für HDX Insight gesammelten Daten hängen von der Version und den installierten Lizenzen der überwachten NetScaler-Instanzen ab. HDX Insight-Berichte werden nur für NetScaler Premium- und Enterprise-Appliances angezeigt, die unter Softwareversion 10.5 und höher ausgeführt werden.

NetScaler-Lizenz/ Dauer	5 Minuten	1 Stunde	1 Tag	1 Woche	1 Monat
Standard	Nein	Nein	Nein	Nein	Nein
Erweitert	Ja	Ja	Nein	Nein	Nein

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Premium	Ja	Ja	Ja	Ja	Ja

Unterstützte Betriebssysteme und Citrix Workspace-Versionen

Die folgende Tabelle listet die von NetScaler Console unterstützten Betriebssysteme und die derzeit mit jedem System unterstützten Citrix Workspace-Versionen auf:

BETRIEBSSYSTEM	CITRIX WORKSPACE-VERSION
Windows	4.0 Standard Edition
Linux	13.0.265571 und höher
Mac	11.8, Build 238301 und höher
HTML5	1.5
Chrome-App	1.5

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lizenzen

Ab NetScaler Console Service Release 14.1-21.x wird das Konzept der lizenzierten VIPs entfernt. Eine unbegrenzte Anzahl von VIPs ist jetzt im NetScaler Console Service verfügbar. Sie müssen keine NetScaler Console Virtual Server-Lizenzen mehr erwerben, da die VIP-Lizenz-SKU in Kürze das End of Sale (EOS) und End of Renewal (EOR) erreichen wird.

Die Änderungen am NetScaler® Console Service-Speicher sind wie folgt:

- Die NetScaler Console Service-Speicher-SKU wird in Kürze das End of Sale (EOS) und End of Renewal (EOR) erreichen.
- Der standardmäßige NetScaler Console Service-Speicheranspruch beträgt jetzt 5 GB.
- Jeder in der Vergangenheit erworbene NetScaler Console Service-Speicher wird bis zum Ende der Laufzeit berücksichtigt.
- Alle in der Vergangenheit erworbenen NetScaler Console VIP-Lizenzen, die Ihnen einen proportionalen Anspruch auf NetScaler Console Service-Speicher gewährten, werden bis zum Ende der Laufzeit berücksichtigt.
- Wenn Sie ein anderes Paket erwerben, das Ihnen einen höheren NetScaler Console-Speicheranspruch gewährt, wird der standardmäßige 5-GB-Speicher angepasst, um dem Anspruch zu entsprechen.

HINWEIS:

Wenn Sie zuvor einen virtuellen Server erworben haben, gelten 500 MB Speicher pro virtuellem Server bis zum Ende der Abonnementlaufzeit.

NetScaler-Lizenzierung für NetScaler Console-Funktionen erforderlich

Die folgende Tabelle listet die NetScaler-Lizenzen auf, die zur Nutzung einiger NetScaler Console-Funktionen erforderlich sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETSCALER CONSOLE-FUNKTIONSGRUPPE	NETSCALER CONSOLE-FUNKTIONEN	NETSCALER- UND GATEWAY-LIZENZANFORDERUNG
Analysen	HDX Insight	Advanced (Berichterstellung < 1 Stunde) Premium (Berichterstellung = Unbegrenzt)
Analysen	Security Insight	Premium (oder) Advanced mit App Firewall-Lizenz
Analysen	Gateway Insight	Advanced (Berichterstellung < 1 Stunde) Premium (Berichterstellung = Unbegrenzt)
Anwendungen	Anwendungsstatistiken (App-Dashboard, App-Sicherheits-Dashboard)	NetScaler Web App Firewall-bezogene Informationen auf dem App-Dashboard und dem App-Sicherheits-Dashboard erfordern eine Premium- (oder) Advanced-Lizenz mit App Firewall
Anwendungen	API-Gateway	Premium- (oder) Advanced-Lizenz
Anwendungen	StyleBooks	N/A
Anwendungen	Bestandsverwaltung – Infrastruktur-Dashboard, Instanzgruppen, Instanz-Dashboards und Sites	N/A
Anwendungen	Ereignisverwaltung und Syslog	N/A
Anwendungen	Konfigurationsaufträge, Konfigurationsprüfung und Konfigurationsberatung	N/A

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETSCALER CONSOLE-FUNKTIONSGRUPPE	NETSCALER CONSOLE-FUNKTIONEN	NETSCALER- UND GATEWAY-LIZENZANFORDERUNG
Anwendungen	Netzwerkberichterstattung (Instanzebene)	N/A
Anwendungen	Netzwerkberichterstattung (auf virtueller Serverebene)	N/A
Anwendungen	Netzwerkfunktionen (Einfache Sichtbarkeit und Verwaltung von virtuellen Servern, Diensten, Dienstgruppen, Servern)	N/A
Anwendungen	SSL-Zertifikatsverwaltung (auf Instanzebene)	N/A
Anwendungen	SSL-Zertifikatsverwaltung (auf virtueller Serverebene)	N/A
System	RBAC und externe Authentifizierung (auf Instanzebene)	N/A
System	RBAC und externe Authentifizierung (auf virtueller Serverebene)	N/V

Ablaufprüfungen für Abonnements virtueller Server anzeigen

Sie können den Status der installierten Lizenzen mit dem Ablaufdatum und dem zulässigen Speichergrenzwert für die Lizenzen in NetScaler Console anzeigen.

So zeigen Sie den Status der Lizenzen an:

1. Navigieren Sie zu **Einstellungen > Analytics-Konfiguration**.
2. Im Abschnitt **Berechtigungen** können Sie die folgenden Details anzeigen:
   - **Berechtigter Speicher:** Speichergrenzwert der Lizenz.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Tage bis zum Ablauf:** Anzahl der verbleibenden Tage bis zum Ablauf der Lizenz.

Den Typ der auf den virtuellen Servern aktivierten Analysen anzeigen

Nachdem Sie AppFlow® auf den ausgewählten virtuellen Servern aktiviert haben, können Sie den Typ der Analysen, die auf den lizenzierten virtuellen Servern oder virtuellen Servern von Drittanbietern aktiviert sind, auf der Seite **Abonnements** anzeigen.

1. Navigieren Sie zu **Einstellungen > Analytics-Konfiguration**.
2. Wählen Sie im Abschnitt **Zusammenfassung der Analysen virtueller Server** den Typ der lizenzierten virtuellen Server aus.
3. Auf der Seite für lizenzierte virtuelle Server wird die Liste der lizenzierten virtuellen Server angezeigt. Auf dieser Seite zeigt die Spalte **Analysestatus** den Typ der auf den virtuellen Servern aktivierten Analysen an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade-Empfehlung

Als Netzwerkadministrator verwalten Sie möglicherweise viele NetScaler-Instanzen, die auf verschiedenen NetScaler-Versionen in der NetScaler Console ausgeführt werden. Die Überwachung des Lebenszyklus jeder NetScaler-Instanz kann eine mühsame Aufgabe sein. Sie müssen die NetScaler-Produktmatrix besuchen, um die NetScaler-Instanzen zu identifizieren, die das End of Life (EOL) oder End of Maintenance (EOM) erreichen oder erreicht haben. Planen Sie dann deren Upgrade.

Um diesen Prozess zu erleichtern, hilft Ihnen die Upgrade-Empfehlung der NetScaler Console, den Lebenszyklus Ihrer NetScaler-Instanzen auf folgende Weisen zu überwachen:

- Identifiziert Instanzen, die EOL oder EOM erreichen oder erreicht haben. So können Sie NetScaler-Upgrades vor dem EOL- oder EOM-Datum planen.
- Hebt die Instanzen hervor, die nicht auf der neuesten Version oder dem neuesten Build sind. Sie können diese Instanzen auf die neueste Version oder den neuesten Build aktualisieren. Mit diesem Upgrade erhalten Sie Updates zu neuen Funktionen und behobenen Problemen.
- Hebt die Instanzen hervor, die nicht auf bevorzugten NetScaler-Builds basieren. Einige Organisationen haben möglicherweise bevorzugte NetScaler-Builds für ihre Instanzen. In der NetScaler Console können Sie den bevorzugten Build festlegen für Ihre Organisation, abhängig von Build-Stabilität, Funktionen und anderen Überlegungen. Überprüfen und aktualisieren Sie dann die Instanzen, die nicht auf bevorzugten Builds basieren. Instanzen, die die bevorzugten Builds ausführen, werden mit einem Sternsymbol gekennzeichnet.
- Hebt Instanzen hervor, die auf den beliebtesten Versionen oder Builds laufen. Instanzen, die die beliebten Builds ausführen, werden mit einem Bandsymbol gekennzeichnet.

Die Upgrade-Empfehlung bietet Links zu den entsprechenden Versionshinweisen. Mit diesen Informationen können Sie einen NetScaler-Build für das Upgrade überprüfen und auswählen. Sie können dann einen Wartungsauftrag erstellen, um NetScaler-Instanzen von der Seite „Upgrade-Empfehlung“ zu aktualisieren.

WICHTIG

Die Upgrade-Empfehlung überwacht nur das EOL von NetScaler-Softwareversionen. Sie überprüft nicht das EOL von NetScaler-Appliances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade-Empfehlung anzeigen

Navigieren Sie zu **Infrastruktur > Instanz-Empfehlung > Upgrade-Empfehlung** und zeigen Sie die folgenden Informationen an:

- Gesamtzahl der NetScaler-Instanzen.
- Instanzen, die das End of Life erreichen.
- Instanzen, die das End of Maintenance erreichen.
- Instanzen in älterer Build-Version.
- Instanzen nicht in bevorzugter Build-Version.
- End-of-Life- und End-of-Maintenance-Daten für die verschiedenen NetScaler-Releases.

Die Seite **Upgrade Advisory** gruppiert die NetScaler-Instanzen nach ihren Releases. Der Link **Release Notes** führt Sie zu den spezifischen NetScaler-Versionshinweisen. Überprüfen Sie neue Funktionen, behobene und bekannte Probleme, bevor Sie ein Upgrade durchführen. Sie können mehrere NetScaler-Instanzen über verschiedene Releases hinweg gleichzeitig für ein Upgrade auswählen. Wenn Sie mit einem Upgrade fortfahren, wird ein Upgrade-Job erstellt. Siehe NetScaler-Instanzen aktualisieren.

Bevorzugte Builds festlegen

Als Administrator können Sie einen bevorzugten NetScaler-Build für die Organisation definieren. Gehen Sie wie folgt vor, um den bevorzugten Build festzulegen:

1. Klicken Sie unter **Infrastructure > Instance Advisory > Upgrade Advisory** auf **Settings**.
2. Wählen Sie das bevorzugte Release und den Build aus.

   In diesem Beispiel sind die bevorzugten Builds `13.0-58.30` und `13.0-67.39`.
3. Klicken Sie auf **Speichern**.

NetScaler-Instanzen aktualisieren

Führen Sie auf der Seite **Upgrade Advisory** nach Ihrer Überprüfung die folgenden Schritte aus, um die erforderlichen NetScaler-Instanzen zu aktualisieren:

1. Wählen Sie die Instanz-Builds aus, die Sie aktualisieren möchten, und klicken Sie auf **Select instances to upgrade**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Wählen Sie die NetScaler-Instanz aus, die Sie aktualisieren möchten, und klicken Sie auf **Zum Upgrade-Workflow fortfahren**.

   Dieser Workflow erstellt einen Upgrade-Job.

3. Wählen Sie auf der Registerkarte **Instanz auswählen**,

   a. Geben Sie einen Namen für den Upgrade-Job an.

   b. (Optional) Wenn Sie weitere Instanzen hinzufügen möchten, klicken Sie auf **Instanzen hinzufügen**.

   c. Klicken Sie auf **Weiter**.

4. Wählen Sie auf der Registerkarte **Image auswählen** ein NetScaler-Image aus der Image-Bibliothek oder lokal oder vom Gerät aus.

   - **Aus Image-Bibliothek auswählen**: Wählen Sie ein NetScaler-Image aus der Liste aus. Diese Option listet alle NetScaler-Images auf, die auf der NetScaler-Download-Website verfügbar sind.

     Die NetScaler-Software-Images zeigen die bevorzugten Builds mit dem Sternsymbol an. Und die am häufigsten heruntergeladenen Builds mit dem Lesezeichensymbol.

   - **Lokal oder vom Gerät auswählen**: Sie können das Image von Ihrem lokalen Computer oder dem NetScaler-Gerät hochladen. Wenn Sie NetScaler-Gerät auswählen, zeigt die NetScaler Console-GUI die Instanzdateien an, die sich in `/var/mps/mps_images` befinden. Wählen Sie das Image aus der NetScaler Console-GUI aus.

   - **Image-Upload auf NetScaler überspringen, wenn das ausgewählte Image bereits verfügbar ist** – Diese Option prüft, ob das ausgewählte Image in NetScaler verfügbar ist. Der Upgrade-Job überspringt das Hochladen eines neuen Images und verwendet das in NetScaler verfügbare Image.

   - **Software-Image nach erfolgreichem Upgrade von NetScaler bereinigen** – Diese Option löscht das hochgeladene Image in der NetScaler-Instanz nach dem Instanz-Upgrade.

   Klicken Sie auf **Weiter**, um die Vorab-Upgrade-Validierung für die ausgewählten Instanzen zu starten.

5. Die Registerkarte **Pre-upgrade validation** zeigt die fehlgeschlagenen Instanzen an. Sie können die fehlgeschlagenen Instanzen entfernen und auf **Next** klicken.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Festplattenspeicherprüfung**: Wenn Sie auf einer Instanz nicht genügend Festplattenspeicher haben, können Sie den Festplattenspeicher überprüfen und bereinigen. Siehe, NetScaler-Festplattenspeicher bereinigen.
- **Richtlinienprüfung**: Wenn NetScaler Console nicht unterstützte klassische Richtlinien findet, können Sie diese Richtlinien entfernen, um einen Upgrade-Job zu erstellen.

HINWEIS:

Wenn Sie die Cluster-IP-Adresse angeben, führt die NetScaler Console die Vor-Upgrade-Validierung nur auf der angegebenen Instanz und nicht auf den anderen Clusterknoten durch.

6. Optional können Sie auf der Registerkarte **Custom scripts** die Skripte angeben, die vor und nach einem Instanz-Upgrade ausgeführt werden sollen.

   Weitere Informationen finden Sie unter Benutzerdefinierte Skripte verwenden.

7. Wählen Sie unter **Schedule Task** eine der folgenden Optionen aus:

   - **Jetzt aktualisieren** – Der Upgrade-Job wird sofort ausgeführt.
   - **Später planen** – Wählen Sie diese Option, um diesen Upgrade-Job später auszuführen. Geben Sie das **Ausführungsdatum** und die **Startzeit** an, zu der Sie die Instanzen aktualisieren möchten.

   Wenn Sie ein NetScaler Hochverfügbarkeitspaar in zwei Phasen aktualisieren möchten, wählen Sie „Zweistufiges Upgrade für Knoten in HA durchführen“.

   Weitere Informationen finden Sie unter NetScaler Hochverfügbarkeitspaar aktualisieren.

8. Geben Sie auf der Registerkarte **Create Job** die folgenden Details an:

   Wenn Sie den Upgrade-Auftrag planen, können Sie angeben, wann Sie das Image auf eine Instanz hochladen möchten:

   - **Jetzt hochladen**: Wählen Sie diese Option, um das Image sofort hochzuladen. Der Upgrade-Auftrag wird jedoch zum geplanten Zeitpunkt ausgeführt.
   - **Zum Zeitpunkt der Ausführung hochladen**: Wählen Sie diese Option, um das Image zum Zeitpunkt der Ausführung des Upgrade-Auftrags hochzuladen.

Weitere Informationen zu den anderen Optionen finden Sie unter NetScaler-Upgrade-Optionen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sicherheitsberatung

Eine sichere, geschützte und widerstandsfähige Infrastruktur ist die Lebensader jeder Organisation. Organisationen müssen neue Common Vulnerabilities and Exposures (CVEs) verfolgen und die Auswirkungen von CVEs auf ihre Infrastruktur bewerten. Sie müssen auch die Behebung verstehen und planen, um die Schwachstellen zu beheben.

Die Funktion „Sicherheitsberatung“ in NetScaler Console ermöglicht Ihnen Folgendes:

- Analysieren Sie Ihre NetScaler-Konfigurationseinstellungen, um Fehlkonfigurationen, Schwachstellen oder Abweichungen von Best Practices zu identifizieren, die Ihr System Angriffen aussetzen könnten.
- Verfolgen Sie neue Common Vulnerabilities and Exposures (CVEs), bewerten Sie die Auswirkungen von CVEs, verstehen Sie die Behebung und beheben Sie die Schwachstellen.
- Überprüfen Sie die Integrität Ihrer NetScaler-Build-Dateien.

Landingpage für Sicherheitsberatung

Die Landingpage für Sicherheitsberatung bietet einen umfassenden Überblick über die Sicherheitslage Ihrer NetScaler-Bereitstellung. Die Benutzeroberfläche wurde verbessert und so konzipiert, dass sie Administratoren und Sicherheitsexperten sofortige Einblicke in den allgemeinen Zustand und den Schwachstellenstatus ihrer NetScaler-Infrastruktur bietet.

NetScaler Console bietet drei Arten von Sicherheitsberatungen:

- **Empfehlungen für sichere Konfigurationen** — Ermöglicht Ihnen die Konfiguration von NetScaler-Instanzen gemäß Best Practices.
- **Erkennung von Common Vulnerabilities and Exposures (CVEs)** — Ermöglicht Ihnen die Identifizierung der CVEs, die Ihre NetScaler-Instanzen gefährden, und empfiehlt Abhilfemaßnahmen.
- **Überwachung der Dateintegrität** — Ermöglicht Ihnen die Feststellung, ob Änderungen oder Ergänzungen an Ihren NetScaler-Build-Dateien vorgenommen wurden.

Das NetScaler Console Sicherheitsberatungs-Dashboard enthält auch Folgendes:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Gesamtschweregrad der Sicherheitslage** — Repräsentiert den Status der Sicherheitslage und wird basierend auf dem maximalen Schweregrad der drei Arten von Beratungen berechnet. Der Status kann einer der folgenden sein:
  - **Kritisch**: Es wurden mehrere Beobachtungen mit kritischem Schweregrad erkannt, die mit höchster Dringlichkeit behoben werden müssen.
  - **Hoch**: Es wurden kritische Schwachstellen oder Fehlkonfigurationen erkannt, die sofort behoben werden müssen. Obwohl nicht so dringend wie kritische Befunde, stellen diese Probleme ein erhebliches Risiko für die Sicherheit und Stabilität dar.
  - **Mittel**: Wichtige Sicherheitsbeobachtungen, die zeitnah behoben werden müssen. Diese Probleme stellen keine unmittelbare, kritische Bedrohung dar, könnten aber potenziell ausgenutzt werden oder zu schwerwiegenderen Problemen führen, wenn sie unbeachtet bleiben.
  - **Niedrig**: Kleinere Sicherheitsprobleme oder Verstöße gegen Best Practices, die kein erhebliches Sicherheitsrisiko darstellen. Obwohl sie keine unmittelbare Bedrohung sind, ist es dennoch ratsam, diese Probleme zu beheben, um die allgemeine Sicherheitslage zu verbessern.
- **Letzter Scan** – Das Datum des letzten Scans. Die im Dashboard bereitgestellten Daten basieren auf den Ergebnissen des letzten Scans.
- **Nächster geplanter Scan** – Das Datum des nächsten geplanten Systemscans.
- **Häufigkeit geplanter Scans** – Die Häufigkeit, mit der die Systemscans ausgeführt werden.
- **Jetzt scannen** – Ermöglicht einen On-Demand-Scan, mit dem Sie die Instanzen jederzeit und nach Bedarf außerhalb des Systemscan-Zeitplans scannen können.
- **Scanverlauf** – Bietet eine historische Ansicht aller Scans, die auf Ihren NetScaler-Instanzen ausgeführt wurden.
- **Betroffene NetScaler** – Listet die betroffenen NetScaler-Instanzen auf.
- **Einstellungen** – Ermöglicht die Konfiguration der Systemscan-Einstellungen und die Festlegung von Benachrichtigungen für Ereignisse nach Ihren Bedürfnissen.

Mit den im Dashboard verfügbaren Informationen können Sie kritische Schwachstellen, Empfehlungen für sichere Konfigurationen einschließlich Abhilfemaßnahmen und Links zu relevanter Dokumentation schnell identifizieren.

Die Landingpage ermöglicht es Ihnen, Probleme nach Kritikalität und NetScaler-IP-Adresse zu filtern. Wenn ein bestimmter Kritikalitätsgrad ausgewählt ist, werden nur NetScaler-Instanzen dieses Schweregrads angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

In der GUI oder im Bericht zur **Sicherheitsberatung** werden möglicherweise nicht alle CVEs angezeigt, und Sie sehen möglicherweise nur ein CVE. Klicken Sie als Workaround auf **Jetzt scannen** und wählen Sie **CVE** aus, um einen On-Demand-Scan auszuführen. Nachdem der Scan abgeschlossen ist, werden alle relevanten CVEs (ca. 15) in der Benutzeroberfläche oder im Bericht angezeigt.-->

Empfehlungen für sichere Konfigurationen

Die Registerkarte **Empfehlungen für sichere Konfigurationen** bietet eine detaillierte, instanzbezogene Analyse von Konfigurationsbeobachtungen, die Benutzern umsetzbare Erkenntnisse liefern soll. Weitere Informationen finden Sie unter Empfehlungen für sichere Konfigurationen.

CVE-Erkennung

Die CVE-Erkennung konzentriert sich hauptsächlich auf die Identifizierung und Behebung von Sicherheitslücken. Weitere Informationen finden Sie unter CVE-Erkennung.

Überwachung der Dateintegrität

Die Überwachung der Dateintegrität prüft auf unbefugte oder bösartige Änderungen an den Kerndateien einer NetScaler-Instanz. Sie ist ein wichtiger Bestandteil der Sicherheitsberatung. Weitere Informationen finden Sie unter Überwachung der Dateintegrität.

Jetzt scannen

Sie können die Instanzen jederzeit nach Bedarf scannen und auch die Arten der Scans auswählen, die Sie basierend auf Ihren Sicherheitsanforderungen ausführen möchten.

Führen Sie die folgenden Schritte aus, um den Scan auszuführen:

1. Klicken Sie auf **Jetzt scannen**.

2. Wählen Sie die Arten von Scans aus, die Sie ausführen möchten.

   - Empfehlungen für Sicherheitskonfigurationen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- CVE-Erkennung
- Überwachung der Dateintegrität

3. Klicken Sie auf **Jetzt scannen**. Sobald der Scan abgeschlossen ist, werden die überarbeiteten Sicherheitsdetails im Sicherheitsberatungs-Dashboard angezeigt.

Scan-Verlauf

Klicken Sie auf **Scan-Verlauf**, um alle historischen Scans anzuzeigen, die auf Ihren NetScaler-Instanzen ausgeführt wurden.

Sie können den Scantyp (On-Demand-Scan oder System-Scan), die Start- und Endzeit des Scans, den Gesamtscanstatus anzeigen und die Details jedes Scans im CSV- oder PDF-Format herunterladen.

Betroffene NetScaler

Der Abschnitt **Betroffene NetScaler** listet alle NetScaler-Instanzen auf, die von den Sicherheitskonfigurationen, CVEs und Überprüfungen der Dateisystemintegrität betroffen sind.

Sie können auch auf die Zahl unter **SICHERE EMPFEHLUNGSKONFIGURATION**, **CVE-ERKENNUNG** oder **DATEIINTEGRITÄTSÜBERWACHUNG** klicken, um weitere Details anzuzeigen. Das Folgende ist ein Beispielbild zu Ihrer Referenz.

Einstellungen

Als Administrator können Sie Citrix Cloud-Benachrichtigungen erhalten, die Ihnen mitteilen, wie viele NetScaler-Instanzen CVE-anfällig sind. Um zu konfigurieren, wann und wie Sie Benachrichtigungen erhalten möchten, klicken Sie auf das Einstellungssymbol in der oberen rechten Ecke der Sicherheitsberatungsseite.

Sie können die folgenden Aktionen ausführen:

- Wählen Sie die Art der Ereignisse aus, für die Sie die Benachrichtigung erhalten müssen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wählen Sie aus, wie Sie benachrichtigt werden möchten. Zum Beispiel per E-Mail, Slack, PagerDuty.
- Wählen Sie die Art des Scans aus, der in Systemscans enthalten sein muss. Standardmäßig ist nur der CVE-Scan für den Systemscan aktiviert.
- Deaktivieren Sie den benutzerdefinierten Scan für Sicherheitsempfehlungen.

Sie können auch die Art der Scans konfigurieren, die in den Systemscans enthalten sein müssen.

HAFTUNGSAUSSCHLUSS:

Bitte beachten Sie, dass NetScaler File Integrity Monitoring („die Funktion“) nicht in der Lage ist, alle Techniken, Taktiken oder Verfahren (TTPs) zu erkennen, die Bedrohungsakteure beim Angriff auf relevante Umgebungen verwenden können. Bedrohungsakteure ändern TTPs und Infrastruktur häufig, und daher kann die Funktion in Bezug auf bestimmte Bedrohungen einen begrenzten oder gar keinen forensischen Wert haben. Es wird Ihnen dringend empfohlen, die Dienste erfahrener forensischer Ermittler in Anspruch zu nehmen, um Ihre Umgebung im Zusammenhang mit möglichen Bedrohungen zu bewerten.

Dieses Dokument und die darin enthaltenen Informationen werden im Ist-Zustand bereitgestellt. Cloud Software Group, Inc. übernimmt keine ausdrücklichen oder stillschweigenden Garantien oder Zusicherungen bezüglich des Dokuments oder seines Inhalts, einschließlich, aber nicht beschränkt auf die Fehlerfreiheit dieses Dokuments oder der darin enthaltenen Informationen oder die Erfüllung von Bedingungen der Marktgängigkeit oder Eignung für einen bestimmten Zweck.

Empfehlungen für eine sichere Konfiguration

Die NetScaler-Beratung für sichere Konfigurationen dient als umfassender Leitfaden, der Expertenempfehlungen und spezifische Anweisungen zur Verbesserung der Sicherheitslage von NetScaler-Konfigurationen bietet. Mit dieser Funktion können Sie Ihre ADC-Infrastruktur (Application Delivery Controller) vor potenziellen Schwachstellen und sich entwickelnden Cyberbedrohungen schützen. Durch die sorgfältige Befolgung der empfohlenen Richtlinien können Sie Risiken proaktiv mindern, die Systemresilienz verbessern und eine robuste Verteidigung gegen unbefugten Zugriff und böswillige Aktivitäten aufrechterhalten.

Diese Funktion scannt nicht nur die NetScaler-Konfiguration auf potenzielle Schwachstellen, sondern schlägt auch proaktiv präzise Befehle zur Behebung dieser Konfigurationen vor. Die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Netzwerkadministratoren können Sicherheitslücken schnell identifizieren und die notwendigen Änderungen implementieren, um ihre NetScaler-Bereitstellung zu stärken.

Die Registerkarte **Empfehlungen für sichere Konfigurationen** bietet eine umfassende Ansicht, die sorgfältig nach Schweregrad kategorisiert ist, was einen priorisierten Ansatz zur Behebung potenzieller Konfigurationsschwachstellen ermöglicht.

Priorisierung nach Schweregrad

Die Kategorisierung nach Schweregrad ermöglicht es Benutzern, ihre Anstrengungen effizient zu verteilen. Beobachtungen werden typischerweise in Stufen wie folgt klassifiziert:

- **Kritisch**: Probleme, die ein unmittelbares und erhebliches Risiko für die Sicherheit und Integrität der NetScaler-Instanz darstellen. Diese Probleme müssen mit höchster Dringlichkeit behoben werden.
- **Hoch**: Konfigurationen, die bei Ausnutzung zu erheblichen Sicherheitsverletzungen führen könnten und sofortige Aufmerksamkeit erfordern.
- **Mittel**: Beobachtungen, die auf potenzielle Schwachstellen oder Fehlkonfigurationen hinweisen. Obwohl diese Probleme nicht kritisch sind, könnten sie zu einem größeren Sicherheitsvorfall beitragen, wenn sie unbeachtet bleiben.
- **Niedrig**: Kleinere Empfehlungen oder Best Practices, die die allgemeine Sicherheitslage verbessern. Diese Probleme stellen keine unmittelbare Bedrohung dar.

Vorteile einer detaillierten Ansicht auf Instanzebene

- **Gezielte Behebung**: Anstelle allgemeiner Ratschläge erhalten Benutzer spezifische Empfehlungen, die auf jede einzelne NetScaler-Instanz zugeschnitten sind, um eine präzise und effektive Behebung zu gewährleisten.
- **Reduzierte Angriffsfläche**: Durch die systematische Behebung beobachteter Fehlkonfigurationen können Unternehmen ihre Angriffsfläche erheblich reduzieren und die Wahrscheinlichkeit erfolgreicher Exploits minimieren.
- **Einhaltung von Vorschriften**: Die detaillierten Beobachtungen können Unternehmen dabei helfen, Konfigurationen zu identifizieren und zu korrigieren, die gegen regulatorische Compliance-Standards verstoßen könnten (z. B. DSGVO, HIPAA, PCI DSS).
- **Verbesserte Sicherheitslage**: Die proaktive Identifizierung und Behebung von Konfigurationsschwächen führt zu einer stärkeren allgemeinen Sicherheitslage und einer verbesserten Widerstandsfähigkeit gegen Cyberbedrohungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Betriebliche Effizienz**: Durch die Bereitstellung klarer und umsetzbarer Erkenntnisse optimiert das System den Sicherheitssanierungsprozess und spart Zeit und Ressourcen.

Sie können **auswählen**, welche Beobachtungen Sie zuerst angehen möchten, basierend auf Ihren Prioritäten, Ihrer Risikobereitschaft und den verfügbaren Ressourcen. Diese Flexibilität stellt sicher, dass die dringendsten Sicherheitsbedenken unverzüglich angegangen werden, während gleichzeitig die notwendigen Informationen bereitgestellt werden, um im Laufe der Zeit eine umfassende Konfigurationshärtung zu erreichen. Diese Option ermöglicht es Sicherheitsadministratoren, fundierte Entscheidungen zu treffen und entschlossene Maßnahmen zum Schutz ihrer NetScaler-Bereitstellungen zu ergreifen.

Die Freitext-Suchfunktion ermöglicht es Ihnen, die Ergebnisse anhand verschiedener wichtiger Kennungen einzugrenzen. Sie können beispielsweise effizient nach einer Instanz anhand ihres eindeutigen Hostnamens suchen, was eine direkte Methode zur Lokalisierung eines bestimmten Geräts bietet. Alternativ bietet die Suche nach IP-Adresse eine weitere präzise Möglichkeit, Instanzen zu finden, was besonders in netzwerkzentrierten Umgebungen nützlich ist.

Über die grundlegende Identifizierung hinaus unterstützt die Suche auch das Filtern nach dem NetScaler-Modell. Dies bedeutet, dass Sie Modelle wie MPX, SDX oder VPX angeben können, um nur Instanzen anzuzeigen, die zu einer bestimmten Hardware- oder Softwarekategorie gehören. Sie können die Suche auch nach dem Schweregrad verfeinern, sodass Sie Instanzen basierend auf ihrer Kritikalität priorisieren können, von Informationsmeldungen bis hin zu kritischen Warnungen.

Konfigurationsempfehlungen beheben

Sobald Sie die Konfigurationsbeobachtungen bewertet und festgelegt haben, welche Maßnahmen erfordern, wird eine umfassende Ansicht der empfohlenen Konfigurationen präsentiert. Das System zeigt dann eine spezielle Seite an, wie im folgenden Bild gezeigt, die die auf Ihre Auswahl zugeschnittenen Abhilfeschritte anzeigt. Wenn Sie sich beispielsweise dafür entscheiden, nur kritische Schweregradprobleme für eine bestimmte NetScaler-Instanz (in diesem speziellen Szenario die Instanz mit der IP-Adresse 10.102.56.45) zu beheben, wird die Seite dynamisch mit den relevanten, hochpriorisierten Empfehlungen gefüllt, um den Abhilfeprozess effektiv zu steuern.

Konfigurationsempfehlungen können in zwei Typen unterteilt werden:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Empfehlungen, die eine Benutzereingabe erfordern**: Diese Kategorie umfasst Konfigurationsvorschläge, die spezifische, kontextbezogene Informationen oder Entscheidungen vom NetScaler-Administrator oder Sicherheitsteam erfordern. Dies sind typischerweise Szenarien, in denen ein generischer Standardwert möglicherweise nicht angemessen ist oder in denen die optimale Einstellung von der einzigartigen Betriebsumgebung, den Sicherheitsrichtlinien oder den Anwendungsanforderungen abhängt. Im Folgenden sind einige Beispiele für Empfehlungen aufgeführt:
    - **Definieren spezifischer IP-Adressen oder IP-Bereiche**: Zum Beispiel das Konfigurieren von Firewall-Regeln, um den Datenverkehr nur von vertrauenswürdigen internen Subnetzen oder spezifischen Client-IP-Adressen zuzulassen. Das System kann diese eindeutigen Netzwerkdetails nicht ableiten.
    - **Festlegen benutzerdefinierter Portnummern**: Obwohl für viele Dienste Standardports existieren, können Anwendungen aus Sicherheits- oder Betriebsgründen so konfiguriert werden, dass sie nicht standardmäßige Ports verwenden. Der Netzwerkadministrator muss die Portnummern angeben.
    - **Angeben von Hostnamen oder Domänennamen**: Beim Konfigurieren von SSL-Zertifikaten, virtuellen Lastausgleichsservern oder Content-Switching-Richtlinien müssen die genauen Hostnamen oder Domänennamen, die die NetScaler-Instanz bedient oder mit denen sie interagiert, vom Benutzer bereitgestellt werden.
    - **Bereitstellen von Authentifizierungsserverdetails**: Die Integration von NetScaler mit externen Authentifizierungssystemen wie LDAP, RADIUS, SAML oder OAuth erfordert, dass der Benutzer Server-IP-Adressen, gemeinsame Geheimnisse, Verzeichnispfade und andere protokollspezifische Details eingibt.
    - **Einrichten spezifischer URL-Rewriting- oder Content-Switching-Richtlinien**: Die genauen URLs, Muster und Zielorte für diese erweiterten Funktionen sind sehr spezifisch für die Anwendungsarchitektur und müssen vom Benutzer definiert werden.
    - **Auswirkungen**: Diese Empfehlungen erfordern oft ein tieferes Verständnis der spezifischen Anforderungen der Bereitstellung, der Sicherheitsrichtlinien und der Netzwerktopologie. Fehler bei der Benutzereingabe können zu Dienstunterbrechungen oder Sicherheitslücken führen, was die Notwendigkeit einer sorgfältigen Planung und Validierung unterstreicht. Automatisierte Tools oder Skripte, die diese implementieren, fordern typischerweise die notwendigen Parameter an oder lesen sie aus einer Konfigurationsdatei.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Empfehlungen, die keine Benutzereingabe erfordern**: Diese Kategorie umfasst Konfigurationsvorschläge, die universell angewendet werden können oder standardmäßige Best Practices beinhalten, die nicht von einzigartigen Umgebungsvariablen abhängen. Dies sind oft grundlegende Sicherheitsverbesserungen oder Leistungsoptimierungen, die bei den meisten NetScaler-Bereitstellungen von Vorteil sind. Im Folgenden sind einige Beispiele für Empfehlungen aufgeführt:
  - **Deaktivieren schwacher Chiffren oder Protokolle**: Es wird empfohlen, SSL/TLS-Versionen wie SSLv3 oder TLS 1.0 oder spezifische schwache Chiffrenuites (z. B. RC4, 3DES) zu deaktivieren, da diese bekannte Schwachstellen darstellen und ihre Entfernung eine universelle Best Practice für die Sicherheit ist. Das System benötigt keine spezifische Eingabe, um zu wissen, welche Chiffren schwach sind.
  - **Aktivieren von HTTP Strict Transport Security (HSTS)**: Dies ist eine Richtlinie, die von Webbrowsern durchgesetzt wird, um nur über sichere HTTPS-Verbindungen mit einem Server zu interagieren. Die Aktivierung ist ein standardmäßiger Schritt zur Sicherheitserhärtung.
  - **Festlegen sicherer Cookie-Flags (z. B. `Secure`, `HttpOnly`)**: Diese Flags erhöhen die Sicherheit von Session-Cookies, indem sie verhindern, dass diese über unverschlüsselte Kanäle übertragen oder über clientseitige Skripte aufgerufen werden. Ihre Anwendung ist eine allgemeine Empfehlung.
  - **Aktivieren gängiger Sicherheits-Header**: Header wie X-Frame-Options, X-Content-Type-Options und Content-Security-Policy (mit einer standardmäßigen sicheren Richtlinie) können ohne spezifische Benutzereingabe empfohlen werden, da sie die clientseitige Sicherheit universell verbessern.
  - **Implementierung einer standardmäßigen Ratenbegrenzung für gängige Angriffe**: Während benutzerdefinierte Ratenbegrenzungen möglicherweise eine Eingabe erfordern, könnte eine Empfehlung zur Anwendung einer allgemeinen Ratenbegrenzung auf gängige Angriffsvektoren (z. B. übermäßige fehlgeschlagene Anmeldeversuche) als Basislinie anwendbar sein.
  - **Konfigurieren optimaler Puffergrößen oder Timeouts**: Allgemeine Leistungsempfehlungen bezüglich interner Puffergrößen oder Verbindungs-Timeouts, die eher durch die Systemarchitektur als durch spezifische Anwendungslogik bestimmt werden.
  - **Sicherstellen angemessener Protokollierungsstufen für Sicherheitsereignisse**: Eine Empfehlung, ein bestimmtes Protokollierungsniveau für sicherheitsrelevante Ereignisse sicherzustellen, ist eine allgemeine Best Practice für Auditing und Incident Response.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Auswirkungen**: Diese Empfehlungen eignen sich oft hervorragend für die Automatisierung oder für Basislinien-Konfigurationsskripte, da sie einheitlich auf mehrere NetScaler-Instanzen angewendet werden können, ohne dass eine manuelle Intervention für spezifische Details erforderlich ist. Sie tragen zu einer starken Sicherheitsposition bei, indem sie gängige Schwachstellen beheben und weithin akzeptierte Standards durchsetzen.

Zusammenfassend lässt sich sagen, dass die Klassifizierung von Konfigurationsempfehlungen basierend auf den Anforderungen an die Benutzereingabe den Implementierungsprozess optimiert. Empfehlungen, die eine Eingabe erfordern, verlangen eine sorgfältige Datenerfassung und Validierung durch den Benutzer, während Empfehlungen, die keine Eingabe erfordern, oft als standardmäßige Sicherheitsbaselines oder durch automatisierte Bereitstellungsmechanismen angewendet werden können.

Sobald ein Benutzer entschieden hat, welche Konfiguration behandelt werden soll, übernimmt der bestehende Konfigurationsauftrags-Workflow die Aufgabe, die Konfigurationsänderungen zu übertragen.

Hier ist zum Beispiel ein Beispiel für eine Konfigurationsempfehlung, die Benutzereingaben erfordert. Man kann Konfigurationswerte einzeln eingeben oder eine Datei hochladen, die die Konfigurationswerte enthält, wie im folgenden Bild gezeigt.

Konfigurationsauftrag erstellen(/en-us/netscaler-console-service/media/create-config-job.png)

CVE-Erkennung

NetScaler erkennt CVEs, indem es Instanzversionen, Konfigurationen und Systemdateien scannt, um Schwachstellen zu identifizieren. Es verwendet ein aktualisiertes CVE-Repository und bietet eine detaillierte Auswirkungsanalyse und Vorschläge zur Behebung.

Der Abschnitt **CVE-Erkennung** im Dashboard **Sicherheitsberatung** listet Folgendes auf:

- Anzahl der erkannten CVEs
- Anzahl der betroffenen NetScaler-Instanzen
- Datum des letzten Scans
- Betroffene NetScaler-Instanzen, kategorisiert nach den Schweregraden Kritisch, Hoch, Mittel und Niedrig

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Als Administrator können Sie NetScaler erlauben, die periodisch geplanten Systemscans auszuführen, oder Sie können bei Bedarf On-Demand-Scans ausführen.

- **Systemscan** – Scannt standardmäßig alle verwalteten Instanzen. NetScaler Console entscheidet über Datum und Uhrzeit der Systemscans, und Sie können diese nicht ändern.
- **On-Demand-Scan** – Sie können die Instanzen bei Bedarf manuell scannen. Wenn seit dem letzten Systemscan viel Zeit vergangen ist, können Sie einen On-Demand-Scan ausführen, um die aktuelle Sicherheitslage zu beurteilen. Oder scannen Sie nach der Anwendung einer Behebung, um die überarbeitete Lage zu beurteilen. Um den On-Demand-Scan auszuführen, klicken Sie in der Sicherheitsberatung auf **Jetzt scannen**.

Sie können auf den Abschnitt **CVE-Erkennung** klicken, um detaillierte Informationen anzuzeigen.

Der Abschnitt **CVE-Erkennung** hat zwei Ansichten:

- Instanzansicht
- CVE-Ansicht

Instanzansicht

Die Instanzansicht enthält die Registerkarten **Betroffene Instanzen** und **CVE-Repository**.

Die Registerkarte **Betroffene Instanzen** zeigt die Liste der betroffenen NetScaler-Instanzen an.

Die betroffenen Instanzen werden basierend auf den folgenden Formfaktoren kategorisiert:

- MPX und VPX
- SDX
- CPX
- BLX

Sie können die Instanzen auch basierend auf den folgenden Kriterien suchen:

- Erkannte CVE
- Hostname
- Modell
- NetScaler-Instanz
- Status

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Tabelle zeigt die folgenden Details:

- NetScaler IP-Adresse
- Hostname
- NetScaler Modellnummer
- Status des NetScaler
- Softwareversion und Build
- Liste der CVEs, die den NetScaler betreffen.

Die meisten CVEs erfordern ein Upgrade als Abhilfemaßnahme, während andere ein Upgrade und einen zusätzlichen Schritt als Abhilfemaßnahme erfordern.

- Informationen zur Behebung von CVE-2020-8300 finden Sie unter Schwachstellen für CVE-2020-8300 beheben.
- Informationen zu CVE-2021-22927 und CVE-2021-22920 finden Sie unter Schwachstellen für CVE-2021-22927 und CVE-2021-22920 beheben.
- Informationen zu CVE CVE-2021-22956 finden Sie unter Schwachstellen für CVE-2021-22956 identifizieren und beheben
- Informationen zu CVE CVE-2022-27509 finden Sie unter Schwachstellen für CVE-2022-27509 beheben

HINWEIS

Wenn Ihre NetScaler-Instanzen Anpassungen aufweisen, lesen Sie Überlegungen zum Upgrade für angepasste NetScaler-Konfigurationen, bevor Sie ein NetScaler-Upgrade planen.

Sie können die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, die den Fix enthalten. Führen Sie zum Upgrade einen der folgenden Schritte aus:

- **Upgrade-Workflow** – Wählen Sie eine Instanz aus und klicken Sie auf **Proceed to upgrade workflow** (Mit Upgrade-Workflow fortfahren).
- **Konfigurationsauftrags-Workflow** – Wählen Sie eine Instanz aus und klicken Sie auf **Configuration job workflow** (Konfigurationsauftrags-Workflow).

Der Upgrade-Workflow startet und der anfällige NetScaler wird automatisch als Ziel-NetScaler eingetragen. Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.

HINWEIS:

- Die Releases 13.0, 12.1, 12.0, 11.0, 10.5 und niedrigere Versionen haben bereits das End of Life (EOL) erreicht. Wenn Ihre NetScaler-Instanzen auf einer dieser Releases laufen, aktualisieren Sie auf eine unterstützte Release.
- Die Release und der Build, auf die Sie aktualisieren möchten, liegen in Ihrem Ermessen. Beachten Sie die Hinweise in der Spalte „Behebung“, um zu erfahren, welche Release und Builds den Sicherheitsfix enthalten. Wählen Sie dementsprechend eine unterstützte Release und einen Build aus, die noch nicht das End of Life erreicht haben.

Um zur CVE-Ansicht zu wechseln, klicken Sie auf **Switch to CVE View** (Zur CVE-Ansicht wechseln).

CVE-Ansicht

Die CVE-Ansicht zeigt die Ergebnisse aller CVEs, die Ihre Infrastruktur betreffen, und alle betroffenen NetScaler-Instanzen an und schlägt Abhilfemaßnahmen vor. Sie können diese Informationen verwenden, um Abhilfemaßnahmen zur Behebung von Sicherheitsrisiken anzuwenden.

Die Tabelle mit der Anzahl der CVEs, die sich auf die NetScaler-Instanzen auswirken, enthält die folgenden Details.

- **CVE-ID**: Die ID des CVE, der sich auf die Instanzen auswirkt.
- **Veröffentlichungsdatum**: Das Datum, an dem das Sicherheitsbulletin für diesen CVE veröffentlicht wurde.
- **Schweregrad**: Der Schweregrad (hoch/mittel/kritisch) und die Punktzahl. Um die Punktzahl anzuzeigen, bewegen Sie den Mauszeiger über den Schweregrad.
- **Schwachstellentyp**: Der Typ der Schwachstelle für diese CVE.
- **Betroffene NetScaler-Instanzen**: Die Anzahl der Instanzen, die von der CVE-ID betroffen sind. Beim Überfahren mit der Maus wird die Liste der NetScaler-Instanzen angezeigt.
- **Behebung**: Die verfügbaren Behebungsmaßnahmen, die (üblicherweise) ein Upgrade der Instanz oder die Anwendung von Konfigurationspaketen sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dieselbe Instanz kann von mehreren CVEs betroffen sein. Diese Tabelle hilft Ihnen zu sehen, wie viele Instanzen von einer bestimmten CVE oder mehreren ausgewählten CVEs betroffen sind. Um die IP-Adresse der betroffenen Instanz zu überprüfen, fahren Sie mit der Maus über NetScaler-Details unter **Betroffene NetScaler-Instanzen**. Um die Details der betroffenen Instanz zu überprüfen, klicken Sie unten in der Tabelle auf **Betroffene Instanzen anzeigen**. Sie können auch Spalten in der Tabelle hinzufügen oder entfernen, indem Sie auf das Pluszeichen klicken.

CVE-Repository

Sowohl die Instanzansicht als auch die CVE-Ansicht enthalten die Registerkarte **CVE-Repository**. Diese Registerkarte bietet eine detaillierte Ansicht aller NetScaler-bezogenen CVEs, die Citrix seit Dezember 2019 angekündigt hat und die Ihre NetScaler-Infrastruktur beeinträchtigen könnten.

- CVE-IDs
- Schwachstellentyp
- Veröffentlichungsdatum
- Schweregrad
- Behebung
- Links zu Sicherheitsbulletins

Sie können diese Ansicht verwenden, um die CVEs im Bereich der Sicherheitsberatung zu verstehen und mehr über die CVE zu erfahren. Informationen zu nicht unterstützten CVEs finden Sie unter Nicht unterstützte CVEs in der Sicherheitsberatung.

Wichtige Hinweise

- Das Security Advisory unterstützt keine NetScaler-Builds, die das Ende der Lebensdauer (EOL) erreicht haben. Wir empfehlen Ihnen, ein Upgrade auf die von NetScaler unterstützten Builds oder Versionen durchzuführen.
- Für die CVE-Erkennung unterstützte Instanzen: alle NetScaler (SDX, MPX, VPX) und Gateway.
- Für die Dateiintegritätsüberwachung unterstützte Instanzen: MPX-, VPX-Instanzen und Gateway.
- Unterstützte CVEs: Alle CVEs nach Dezember 2019.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Die Erkennung und Behebung von Schwachstellen, die das NetScaler Gateway-Plug-in für Windows betreffen, wird vom NetScaler Console Security Advisory nicht unterstützt. Informationen zu nicht unterstützten CVEs finden Sie unter Nicht unterstützte CVEs im Security Advisory.

- Das NetScaler Console Security Advisory berücksichtigt keine Art von Fehlkonfiguration der Funktionen bei der Identifizierung der Schwachstelle.
- Das NetScaler Console Security Advisory unterstützt nur die Identifizierung und Behebung der CVEs. Es unterstützt nicht die Identifizierung und Behebung der Sicherheitsbedenken, die im Sicherheitsartikel hervorgehoben werden.
- Umfang der NetScaler-, Gateway-Releases: Die Funktion ist auf Haupt-Builds beschränkt. Das Security Advisory schließt keine speziellen Builds in seinen Umfang ein.
    - Das Security Advisory wird in der Admin-Partition nicht unterstützt.
- Die folgenden Scan-Typen sind für CVEs verfügbar:
    - **Versions-Scan**: Dieser Scan erfordert, dass NetScaler Console die Version einer NetScaler-Instanz mit den Versionen und Builds vergleicht, für die der Fix verfügbar ist. Dieser Versionsvergleich hilft dem NetScaler Console Security Advisory zu erkennen, ob der NetScaler für die CVE anfällig ist. Wenn beispielsweise eine CVE in einem NetScaler-Release und Build xx.yy behoben ist, betrachtet das Security Advisory alle NetScaler-Instanzen auf Builds, die kleiner als xx.yy sind, als anfällig. Der Versions-Scan wird heute im Security Advisory unterstützt.
    - **Konfigurations-Scan**: Dieser Scan erfordert, dass NetScaler Console ein für den CVE-Scan spezifisches Muster mit der NetScaler-Konfigurationsdatei (`nsconf`) abgleicht. Wenn das spezifische Konfigurationsmuster in der NetScaler ns.conf-Datei vorhanden ist, wird die Instanz für diese CVE als anfällig betrachtet. Dieser Scan wird typischerweise zusammen mit dem Versions-Scan verwendet. Der Konfigurations-Scan wird heute im Security Advisory unterstützt.
    - **Benutzerdefinierter Scan**: Dieser Scan erfordert, dass NetScaler Console eine Verbindung zur verwalteten NetScaler-Instanz herstellt, ein Skript darauf überträgt und das Skript ausführt. Die Skriptausgabe hilft NetScaler Console zu erkennen, ob der NetScaler für die CVE anfällig ist. Beispiele hierfür sind die Ausgabe spezifischer Shell-Befehle, die Ausgabe spezifischer CLI-Befehle, bestimmte Protokolle sowie das Vorhandensein oder

© 1997–2026 Citrix Systems, Inc. All rights reserved.

der Inhalt bestimmter Verzeichnisse oder Dateien. Für CVEs, die benutzerdefinierte Scans erfordern, wird das Skript jedes Mal ausgeführt, wenn Ihr geplanter oder On-Demand-Scan läuft. Erfahren Sie mehr über die gesammelten Daten und Optionen für spezifische benutzerdefinierte Scans in der Security Advisory-Dokumentation für diese CVE.

- Scans beeinträchtigen den Produktionsdatenverkehr auf NetScaler nicht und ändern keine NetScaler-Konfiguration auf NetScaler.
- Der Sicherheitshinweis der NetScaler Console unterstützt keine CVE-Minderung. Wenn Sie eine Minderung (temporäre Problemumgehung) auf die NetScaler-Instanz angewendet haben, identifiziert die NetScaler Console die NetScaler-Instanz weiterhin als anfällige NetScaler-Instanz, bis Sie die Behebung abgeschlossen haben.
- Für die FIPS-Instanzen wird der CVE-Scan nicht unterstützt.

Dateiintegritätsüberwachung

Die Dateiintegritätsüberwachung ermöglicht es Ihnen, festzustellen, ob Änderungen oder Ergänzungen an Ihrem NetScaler-Dateisystem vorgenommen wurden. Diese Funktion bewertet die Integrität von NetScaler-Dateien, indem sie den binären Hash-Wert Ihres aktuellen NetScaler-Builds mit dem ursprünglichen binären Hash vergleicht, der mit demselben NetScaler-Build verknüpft ist.

Der Abschnitt **Dateiintegritätsüberwachung** im Dashboard **Sicherheitsberatung** listet Folgendes auf:

- Anzahl der erkannten Probleme
- Anzahl der betroffenen NetScaler-Instanzen
- Datum des letzten Scans
- Betroffene NetScaler-Instanzen, kategorisiert nach den Schweregraden Kritisch, Hoch, Mittel und Niedrig
- Betroffene NetScaler-Instanzen, die Probleme mittels binärer Signierung und Verifizierung gemeldet haben

Als Administrator können Sie NetScaler erlauben, die regelmäßig geplanten Systemscans auszuführen, oder Sie können bei Bedarf On-Demand-Scans ausführen.

- **Systemscan** – Scannt standardmäßig alle verwalteten Instanzen. NetScaler Console legt Datum und Uhrzeit der Systemscans fest, die standardmäßig deaktiviert sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **On-Demand-Scan** – Sie können den Scan bei Bedarf manuell auslösen. Um den On-Demand-Scan auszuführen, klicken Sie im Sicherheitsberatungs-Dashboard auf **Jetzt scannen**.

Sie können auf den Abschnitt **Dateiintegritätsüberwachung** klicken, um detaillierte Informationen anzuzeigen.

Von der Konsole erkannt

Die Registerkarte **Von der Konsole erkannt** listet die betroffenen NetScaler-Instanzen auf, indem sie den binären Hash des aktuellen Builds mit dem ursprünglichen Build-Hash vergleicht, um geänderte oder neu hinzugefügte Dateien zu erkennen. Die Tabelle zeigt die folgenden Details an:

- IP-Adresse – Die IP-Adresse der betroffenen Instanzen.
- Scan-Status – Zeigt Scan-Fehlerergebnisse an.
- Vorhandene Datei geändert – Die Liste der vorhandenen Dateien, die geändert wurden.
- Neue Dateien hinzugefügt – Die Liste der neu hinzugefügten Dateien.
- Scan-Zeit – Die Zeit des letzten Scans.
- Hostname – Der Hostname des betroffenen NetScaler.
- Modell – Der Modellname des betroffenen NetScaler.

Scan-Fehlerergebnisse werden in der Haupt-Dashboard-Ansicht angezeigt, sodass Sie nicht auf die einzelnen Scan-Ergebnisse oder Zeilenelemente klicken müssen, um auf Fehlerdetails zuzugreifen. Alle Integritätsprobleme, wie z. B. Hash-Fehlpaarungen oder Scan-Fehler, werden in einem klaren, zugänglichen Format auf dem Dashboard dargestellt, wodurch Sie Probleme schnell identifizieren und verstehen können.

Klicken Sie auf die Zahlen unter **Vorhandene Dateien geändert** und **Neue Dateien hinzugefügt**, um Details anzuzeigen.

Sie können eine benutzerdefinierte Positivliste erstellen und bestimmte Dateien von Scans zur Dateintegritätsüberwachung ausschließen. Indem Sie definieren, welche Dateien vom Scan ausgeschlossen werden sollen, können Sie die Überwachung optimieren und unnötige Warnmeldungen für vertrauenswürdige Dateien reduzieren.

So schließen Sie bestimmte Dateien von Scans zur Dateintegritätsüberwachung aus:

1. Klicken Sie auf **Dateien/Verzeichnisse ausschließen**.
2. Wählen Sie die erforderlichen Dateien oder Verzeichnisse aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

oder

Klicken Sie auf **Dateien/Verzeichnisse hinzufügen**, um neue Dateien hinzuzufügen. Sie können Standard-Shell-Glob-Muster hinzufügen und alle Pfade ausschließen, die den definierten Kriterien entsprechen. Wenn ein Verzeichnis hinzugefügt wird, werden alle seine Dateien vom Scan ausgeschlossen. Klicken Sie auf **Hinzufügen**.

Sie können auch eine Suche durchführen, um bestimmte Dateien oder Ordner zu finden. Sie können die Pfade der Ausschlussliste auch finden, indem Sie einen Teil einer Datei oder eines Ordners in die Suchleiste unter der Option `path` eingeben. Die Suchfunktion erleichtert die Verwaltung und Überprüfung ausgeschlossener Pfade.

Wenn Sie die Dateien nicht vom Scan ausschließen möchten, können Sie die erforderlichen Dateien oder Verzeichnisse auswählen und auf **Dateien/Verzeichnisse entfernen** klicken. Die angegebenen Dateien oder Verzeichnisse werden in den nächsten geplanten Scan einbezogen.

Dateien vom Scan ausschließen(/en-us/netscaler-console-service/media/exclude-files-directories.png)

Wichtige Hinweise

- Für die Dateintegritätsüberwachung unterstützte Instanzen: MPX-, VPX-Instanzen und Gateway.
- Der folgende Scan ist für die Dateintegritätsüberwachung verfügbar:
  - **Scan zur Dateintegritätsüberwachung**: Dieser Scan erfordert, dass die NetScaler Console eine Verbindung zur verwalteten NetScaler-Instanz herstellt. Die NetScaler Console vergleicht die Hash-Werte, indem sie ein Skript in NetScaler ausführt und die aktuellen binären Hash-Werte für die NetScaler-Systemdateien sammelt. Nach dem Vergleich liefert die NetScaler Console das Ergebnis mit der Gesamtzahl der geänderten vorhandenen Dateien und der Gesamtzahl der neu hinzugefügten Dateien. Als Administrator können Sie sich für weitere Untersuchungen der Scan-Ergebnisse an die digitale Forensik Ihrer Organisation wenden.
- Die folgende Liste enthält nicht unterstützte Plattformen: BLX

Vom Gerät gemeldet

Die Registerkarte **Vom Gerät gemeldet** listet die NetScaler-Instanzen auf, die Probleme bei der binären Signierung und Verifizierung gemeldet haben. Mit dieser Verifizierung wird die digitale Signatur jeder Datei validiert, um die Authentizität zu bestätigen und Manipulationen zu erkennen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Sie betroffene Instanzen sehen, können Sie die digitalen forensischen Aktivitäten Ihrer Organisation fortsetzen. Die Tabelle listet die betroffenen NetScaler-Instanzen zusammen mit weiteren Details wie Hostname, hinzugefügtem Binärprogramm und geändertem Binärprogramm auf. Sie können auf **Details** der entsprechenden Instanz klicken, um detaillierte Informationen anzuzeigen.

Abschnitt zur Dateintegritätsüberwachung(/en-us/netscaler-console-service/media/device-reported.png)

Erkennung von Kompromittierungsindikatoren in NetScaler Console

Die Funktion zur Erkennung von Kompromittierungsindikatoren (IoC) in NetScaler Console ist darauf ausgelegt, zu erkennen, ob Ihre NetScaler-Appliances möglicherweise aufgrund einer Schwachstelle betroffen sind.

Wenn es CVE-Ereignisse gibt, ist eine der ersten Sorgen, dass bösartige Akteure die Schwachstelle ausnutzen konnten. Ein Exploit verursacht katastrophale Schäden für das Geschäft eines Kunden, und daher ist es entscheidend, solche Vorfälle sofort zu erkennen. Kompromittierungsindikatoren wurden in der Vergangenheit für NetScaler über Supportkanäle verteilt, was den Kundenbedürfnissen entspricht, aber mit zusätzlichem Aufwand verbunden ist, den Supportprozess des Erstellens eines Tickets und des Gesprächs mit einem Supportmitarbeiter zu durchlaufen, was manchmal nicht ideal sein mag. Die Funktion zur Erkennung von Kompromittierungsindikatoren in NetScaler Console ist darauf ausgelegt, den aktuellen supportorientierten Prozess abzukürzen und einem Kunden bei einer schnellen Bewertung seiner NetScaler-Infrastruktur zu helfen.

Voraussetzungen

Diese Funktion erfordert, dass Sie Telemetriedaten zur Produktnutzung senden. Weitere Informationen zur NetScaler-Telemetrie finden Sie unter `<https://docs.netscaler.com/de-de/netscaler-application-delivery-management-software/current-release/ns-telemetry.html>`.

Vorteile

- Sie können Scans zur Kompromittierungserkennung von der Seite **Sicherheitshinweise** der NetScaler Console ausführen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Der Scan liefert eines der folgenden Ergebnisse:
  - **Potenziell kompromittiert** – Wenn die Erkennungslogik eine potenzielle Kompromittierung für eine CVE erkannt hat.
  - **Keine Kompromittierung erkannt** – Wenn die Erkennungslogik keine Kompromittierung erkannt hat.
  - **Übersprungen** – Wenn der Scan für eine bestimmte NetScaler-Instanz manuell übersprungen wurde.
  - **Ausführung fehlgeschlagen** – Wenn der Scan nicht erfolgreich ausgeführt wurde.
  - **Ausführung läuft** – Wenn der Scan läuft.
- Die IoC-Logik wird ständig aktualisiert, wenn weitere IoCs entdeckt werden. In einem solchen Fall zeigt die Startseite an, dass ein Update verfügbar ist.
- Sobald ein Update für die IoC-Erkennungslogik verfügbar ist, können Sie es auf der Landingpage sehen.

  Dashboard für Kompromittierungsindikatoren(/en-us/netscaler-console-service/media/indicators-of-compromise-dashboard.png)
- Ergebnisse älterer Scans werden gespeichert und können jederzeit eingesehen werden.

  Verlauf der Dokumente zu Kompromittierungsindikatoren(/en-us/netscaler-console-service/media/indicators-of-comprimise-scan-history.png)
- Die Lösung verwendet eine Hub-and-Spoke-Architektur, bei der ein zentraler Cloud-Dienst Assets von einem sicheren Cloud-Speicherort aufnimmt und diese auf den Zielgeräten installiert.

HINWEIS:

Die IoC-Informationen umfassen nicht alle Techniken, Taktiken oder Verfahren („TTPs“), die Bedrohungsakteure verwenden könnten, wenn sie relevante Umgebungen angreifen. Außerdem ändern Bedrohungsakteure TTPs und Infrastruktur häufig. Aus diesen und anderen Gründen können die IoC-Informationen von begrenztem forensischem Wert sein und tatsächliche Kompromittierungen möglicherweise nicht identifizieren. Es wird empfohlen, die Dienste erfahrener forensischer Ermittler in Anspruch zu nehmen, um Ihre Umgebung zu bewerten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwachstellen beheben

NetScaler erkennt CVEs und bietet entsprechende Behebungsvorschläge. Dieses Thema listet die vorgeschlagenen Behebungen für die folgenden CVEs auf:

- Schwachstellen für CVE-2026-88771 beheben
- Schwachstellen für CVE-2026-88772 beheben
- Schwachstellen für CVE-2026-88773 beheben
- Schwachstellen für CVE-2026-88774 beheben
- Schwachstellen für CVE-2026-88775 beheben
- Schwachstellen für CVE-2026-88776 beheben
- Schwachstellen für CVE-2026-88777 beheben
- Schwachstellen für CVE-2026-88778 beheben
- Schwachstellen für CVE-2026-19490 beheben
- Schwachstellen für CVE-2026-19489 beheben
- Schwachstellen für CVE-2026-13474 beheben
- Schwachstellen für CVE-2026-10817 beheben
- Schwachstellen für CVE-2026-10816 beheben
- Schwachstellen beheben für CVE-2026-8655
- Schwachstellen beheben für CVE-2026-8452
- Schwachstellen beheben für CVE-2026-8451
- Schwachstellen beheben für CVE-2026-4368
- Schwachstellen beheben für CVE-2026-3055
- Schwachstellen beheben für CVE-2025-12101
- Schwachstellen beheben für CVE-2025-8424
- Schwachstellen beheben für CVE-2025-7776
- Schwachstellen beheben für CVE-2025-7775
- Schwachstellen beheben für CVE-2025-6543
- Schwachstellen beheben für CVE-2025-5349
- Schwachstellen beheben für CVE-2025-5777
- Schwachstellen beheben für CVE-2024-8535

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Schwachstellen beheben für CVE-2020-8300
- Schwachstellen beheben für CVE-2021-22927 und CVE-2021-22920
- Schwachstellen für CVE-2021-22956 identifizieren und beheben(/de-de/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2021-22956.html)
- Schwachstellen für CVE-2022-27509 identifizieren und beheben(/de-de/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2022-27509.html)

Schwachstellen für CVE-2026-88771 identifizieren und beheben

Klicken Sie im NetScaler Console® Security Advisory Dashboard auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2026-88771. Die Liste der NetScaler-Instanzen, die von CVE-2026-88771 betroffen sind, wird angezeigt.

Weitere Informationen zum Security Advisory Dashboard finden Sie unter Sicherheitshinweis.

HINWEIS:

Es kann einige Stunden dauern, bis der Systemscan des Sicherheitshinweissystems abgeschlossen ist und die Auswirkungen von CVE-2026-88771 im Sicherheitshinweismodul angezeigt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2026-88771 beheben

Für von CVE-2026-88771 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits ausgefüllt sind.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Auftrags.

Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwachstellen für CVE-2026-88772 identifizieren und beheben

Klicken Sie im Sicherheitsberatungs-Dashboard von NetScaler Console® auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2026-88772. Die Liste der NetScaler-Instanzen, die von CVE-2026-88772 betroffen sind, wird angezeigt.

Weitere Informationen zum Sicherheitsberatungs-Dashboard finden Sie unter Sicherheitsberatung.

HINWEIS:

Es kann einige Stunden dauern, bis der Systemscan des Sicherheitsberatungsdienstes abgeschlossen ist und die Auswirkungen von CVE-2026-88772 im Sicherheitsberatungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2026-88772 beheben

Für von CVE-2026-88772 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, bei dem Sie die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren müssen, die den Fix enthalten.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird mit den bereits ausgefüllten anfälligen NetScaler-Instanzen geöffnet.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

Schwachstellen für CVE-2026-88773 identifizieren und beheben

Im NetScaler Console® Sicherheitswarnungs-Dashboard klicken Sie auf **CVE-Erkennung**. Auf der Registerkarte **Betroffene Instanzen** suchen Sie nach CVE-2026-88773. Die Liste der NetScaler-Instanzen, die von CVE-2026-88773 betroffen sind, wird angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sicherheitswarnungs-Dashboard für CVE-2026-sep(/en-us/netscaler-console-service/media/security-advisory-cve-2026-sep.png)

Weitere Informationen zum Sicherheitswarnungs-Dashboard finden Sie unter Sicherheitswarnung.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitswarnungssystems abgeschlossen ist und die Auswirkungen von CVE-2026-88773 im Sicherheitswarnungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2026-88773 beheben

Für von CVE-2026-88773 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

In der GUI, unter **CVE-Erkennung > Betroffene Instanzen**, wählen Sie die Instanzen aus und klicken Sie auf **Mit Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird mit den bereits ausgefüllten anfälligen NetScaler-Instanzen geöffnet.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

Dieser Schritt kann gleichzeitig für alle anfälligen NetScaler-Instanzen durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

Schwachstellen für CVE-2026-88774 identifizieren und beheben

Klicken Sie im NetScaler Console® Security Advisory Dashboard auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2026-88774. Die Liste der NetScaler-Instanzen, die von CVE-2026-88774 betroffen sind, wird angezeigt.

Weitere Informationen zum Security Advisory Dashboard finden Sie unter Sicherheitshinweis.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Es kann einige Stunden dauern, bis der Systemscan des Sicherheitshinweissystems abgeschlossen ist und die Auswirkungen von CVE-2026-88774 im Sicherheitshinweismodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2026-88774 beheben

Für von CVE-2026-88774 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, die den Fix enthalten.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird mit den bereits ausgefüllten anfälligen NetScaler-Instanzen geöffnet.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Auftrags.

Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

Schwachstellen für CVE-2026-88775 identifizieren und beheben

Klicken Sie im Sicherheitsberatungs-Dashboard von NetScaler Console® auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2026-88775. Die Liste der NetScaler-Instanzen, die von CVE-2026-88775 betroffen sind, wird angezeigt.

Weitere Informationen zum Sicherheitsberatungs-Dashboard finden Sie unter Sicherheitsberatung.

HINWEIS:

Es kann einige Stunden dauern, bis der Systemscan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2026-88775 im Sicherheitsberatungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CVE-2026-88775 beheben

Für von CVE-2026-88775 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits ausgefüllt sind.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

Schwachstellen für CVE-2026-88776 identifizieren und beheben

Im NetScaler Console® Sicherheitswarnungs-Dashboard klicken Sie auf **CVE-Erkennung**. Auf der Registerkarte **Betroffene Instanzen** suchen Sie nach CVE-2026-88776. Die Liste der NetScaler-Instanzen, die von CVE-2026-88776 betroffen sind, wird angezeigt.

Sicherheitswarnungs-Dashboard für CVE-2026-sep(/en-us/netscaler-console-service/media/security-advisory-cve-2026-sep.png)

Weitere Informationen zum Sicherheitswarnungs-Dashboard finden Sie unter Sicherheitswarnung.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitswarnungssystems abgeschlossen ist und die Auswirkungen von CVE-2026-88776 im Sicherheitswarnungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2026-88776 beheben

Für von CVE-2026-88776 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits ausgefüllt sind.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

Dieser Schritt kann gleichzeitig für alle anfälligen NetScaler-Instanzen durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

Schwachstellen für CVE-2026-88777 identifizieren und beheben

Im NetScaler Console® Sicherheitsberatungs-Dashboard klicken Sie auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2026-88777. Die Liste der NetScaler-Instanzen, die von CVE-2026-88777 betroffen sind, wird angezeigt.

Sicherheitsberatungs-Dashboard für CVE-2026-sep(/en-us/netscaler-console-service/media/security-advisory-cve-2026-sep.png)

Weitere Informationen zum Sicherheitsberatungs-Dashboard finden Sie unter Sicherheitsberatung.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2026-88777 im Sicherheitsberatungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2026-88777 beheben

Für von CVE-2026-88777 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits ausgefüllt sind.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dieser Schritt kann gleichzeitig für alle anfälligen NetScaler-Instanzen durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

Schwachstellen für CVE-2026-88778 beheben

Im NetScaler Console Security Advisory Dashboard unter **Aktuelle CVEs** `<number of>` **NetScaler-Instanzen sind von CVEs betroffen** sehen Sie alle Instanzen, die aufgrund von CVE-2026-88778 anfällig sind. Um die Details der von den CVEs betroffenen Instanzen zu überprüfen, wählen Sie CVE-2026-88778 aus und klicken Sie auf **Betroffene Instanzen anzeigen**.

CVE-2026-88778 beheben

Für von CVE-2026-88778 betroffene NetScaler-Instanzen ist die Behebung ein zweistufiger Prozess. In der GUI unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen** sehen Sie Schritt 1 und 2.

Die beiden Schritte umfassen:

1. Aktualisieren der anfälligen NetScaler-Instanzen auf eine Version und einen Build, der den Fix enthält.
2. Anwenden der erforderlichen Konfigurationsbefehle mithilfe der anpassbaren integrierten Konfigurationsvorlage in Konfigurationsaufträgen.

Unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen** sehen Sie zwei separate Workflows für diesen zweistufigen Behebungsprozess: **Mit Upgrade-Workflow fortfahren** und **Mit Konfigurationsauftrags-Workflow fortfahren**.

Schritt 1: Aktualisieren der anfälligen NetScaler-Instanzen

Um die anfälligen Instanzen zu aktualisieren, wählen Sie die Instanzen aus und klicken Sie auf **Mit Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits ausgefüllt sind.

Weitere Informationen zur Verwendung von NetScaler Console zum Aktualisieren von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Dieser Schritt kann gleichzeitig für alle anfälligen NetScaler-Instanzen durchgeführt werden.

Schritt 2: Konfigurationsbefehle anwenden

Nachdem Sie die betroffenen Instanzen aktualisiert haben, wählen Sie im Fenster `<number of>` **NetScaler-Instanzen, die von CVEs betroffen sind** die von CVE-2026-88778 betroffene Instanz aus und klicken Sie auf **Mit dem Konfigurationsauftrags-Workflow fortfahren**. Der Workflow umfasst die folgenden Schritte.

1. Anpassen der Konfiguration.
2. Überprüfen der automatisch ausgefüllten betroffenen Instanzen.
3. Eingaben für Variablen für den Auftrag angeben.
4. Überprüfen der endgültigen Konfiguration mit ausgefüllten Variableneingaben.
5. Ausführen des Auftrags.

Beachten Sie den folgenden Punkt, bevor Sie eine Instanz auswählen und auf **Mit dem Konfigurationsauftrags-Workflow fortfahren** klicken:

- Nur für mehrere NetScaler-Instanzen, die von CVE-2026-88778 betroffen sind: Sie können Konfigurationsaufträge auf allen Instanzen gleichzeitig ausführen. Zum Beispiel haben Sie NetScaler 1, NetScaler 2 und NetScaler 3, und alle sind nur von CVE-2026-88778 betroffen. Wählen Sie alle diese Instanzen aus und klicken Sie auf **Mit dem Konfigurationsauftrags-Workflow fortfahren**, und die integrierte Konfigurationsvorlage wird automatisch unter **Konfiguration auswählen** ausgefüllt.

Schritt 1: Konfiguration auswählen

Im Konfigurationsauftrags-Workflow wird die integrierte Konfigurationsbasistabelle automatisch unter **Konfiguration auswählen** ausgefüllt.

Schritt 2: Instanz auswählen

Die betroffene Instanz wird automatisch unter **Instanzen auswählen** ausgefüllt. Wählen Sie die Instanz aus. Klicken Sie auf **Weiter**. Im nächsten Schritt zeigen Sie eine Vorschau der Konfigurationen an. Klicken Sie auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Für NetScaler-Instanzen im Cluster-Modus unterstützt NetScaler Console mithilfe der Sicherheitsberatung das Ausführen des Konfigurationsauftrags nur auf dem Cluster Configuration Coordinator (CCO)-Knoten. Führen Sie die Befehle auf Nicht-CCO-Knoten separat aus.

Schritt 3: Konfiguration ausführen

Klicken Sie auf **Fertig stellen**, um den Konfigurationsauftrag auszuführen.

Nachdem der Auftrag ausgeführt wurde, wird er unter **Infrastructure > Configuration > Configuration Jobs** angezeigt.

Nachdem Sie die beiden Korrekturschritte für alle anfälligen NetScaler-Instanzen abgeschlossen haben, können Sie einen On-Demand-Scan ausführen, um die überarbeitete Sicherheitslage anzuzeigen.

Schwachstellen für CVE-2026-19490 identifizieren und beheben

Klicken Sie im Sicherheitsberatungs-Dashboard der NetScaler Console® auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2026-19490. Die Liste der NetScaler-Instanzen, die von CVE-2026-19490 betroffen sind, wird angezeigt.

Weitere Informationen zum Sicherheitsberatungs-Dashboard finden Sie unter Sicherheitsberatung.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2026-19490 im Sicherheitsberatungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2026-19490 beheben

Für von CVE-2026-19490 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, die den Fix enthalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits ausgefüllt sind.

Weitere Informationen zur Verwendung der NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Auftrags.

Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

Schwachstellen für CVE-2026-19489 identifizieren und beheben

Klicken Sie im Sicherheitsberatungs-Dashboard von NetScaler Console® auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2026-19489. Die Liste der NetScaler-Instanzen, die von CVE-2026-19489 betroffen sind, wird angezeigt.

Weitere Informationen zum Sicherheitsberatungs-Dashboard finden Sie unter Sicherheitsberatung.

HINWEIS:

Es kann einige Stunden dauern, bis der Systemscan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2026-19489 im Sicherheitsberatungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2026-19489 beheben

Für von CVE-2026-19489 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits ausgefüllt sind.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Auftrags.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

Schwachstellen für CVE-2026-13474 identifizieren und beheben

Im NetScaler Console Sicherheitswarnungs-Dashboard, unter **Aktuelle CVEs >** `<number of>` **NetScaler-Instanzen sind von allgemeinen Schwachstellen und Expositionen (CVEs) betroffen**, sehen Sie alle Instanzen, die von dieser spezifischen CVE betroffen sind. Um die Details der von CVE-2026-13474 betroffenen Instanzen zu überprüfen, wählen Sie **CVE-2026-13474** aus und klicken Sie auf **Betroffene Instanzen anzeigen**.

Das Fenster `<number of>` **NetScaler-Instanzen, die von CVEs betroffen sind** wird angezeigt. Hier sehen Sie die Anzahl und Details der NetScaler-Instanzen, die von CVE-2026-13474 betroffen sind.

Weitere Informationen zum Sicherheitswarnungs-Dashboard finden Sie unter Sicherheitswarnung.

CVE-2026-13474 beheben

Für von CVE-2026-13474 betroffene NetScaler-Instanzen ist die Behebung ein zweistufiger Prozess. In der GUI, unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen**, sehen Sie Schritt 1 und Schritt 2.

Die beiden Schritte umfassen:

1. Aktualisieren der anfälligen NetScaler-Instanzen auf eine Version und einen Build, der den Fix enthält.
2. Anwenden der erforderlichen Konfigurationsbefehle mithilfe der anpassbaren integrierten Konfigurationsvorlage in Konfigurationsaufträgen.

Unter **Aktuelle CVEs > NetScaler-Instanzen, die von CVEs betroffen sind**, sehen Sie zwei separate Workflows für diesen zweistufigen Behebungsprozess: **Workflow für Upgrade fortsetzen** und **Workflow für Konfigurationsauftrag fortsetzen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schritt 1: Betroffene NetScaler-Instanzen aktualisieren

Um die anfälligen Instanzen zu aktualisieren, wählen Sie die Instanzen aus und klicken Sie auf **Workflow für Upgrade fortsetzen**. Der Upgrade-Workflow wird mit den bereits ausgefüllten anfälligen NetScaler-Instanzen geöffnet.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

Schritt 2: Konfigurationsbefehle anwenden

Nachdem Sie die betroffenen Instanzen aktualisiert haben, wählen Sie im Fenster `<number of>` **NetScaler-Instanzen, die von CVEs betroffen sind** die von CVE-2026-13474 betroffene Instanz aus und klicken Sie auf **Mit dem Konfigurations-Job-Workflow fortfahren**. Der Workflow umfasst die folgenden Schritte:

1. Anpassen der Konfiguration.
2. Überprüfen der automatisch ausgefüllten betroffenen Instanzen.
3. Angeben von Eingabevariablen für den Job.
4. Überprüfen der endgültigen Konfiguration mit ausgefüllten Variablenwerten.
5. Ausführen des Jobs.

Beachten Sie die folgenden Punkte, bevor Sie eine Instanz auswählen und auf **Mit dem Konfigurations-Job-Workflow fortfahren** klicken:

- Für mehrere NetScaler-Instanzen, die nur von CVE-2026-13474 betroffen sind, können Sie Konfigurations-Jobs auf allen Instanzen gleichzeitig ausführen. Wenn beispielsweise NetScaler 1, NetScaler 2 und NetScaler 3 nur von CVE-2026-13474 betroffen sind, wählen Sie alle diese Instanzen aus und klicken Sie auf **Mit dem Konfigurations-Job-Workflow fortfahren**. Die integrierte Konfigurationsvorlage wird automatisch unter **Konfiguration auswählen** ausgefüllt.

Schritt 1: Konfiguration auswählen

Im Konfigurations-Job-Workflow wird die integrierte Basiskonfigurationsvorlage automatisch unter **Konfiguration auswählen** ausgefüllt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schritt 2: Instanz auswählen

Die betroffene Instanz wird automatisch unter **Instanzen auswählen** vorab ausgefüllt. Wählen Sie die Instanzen aus und klicken Sie auf **Weiter**. Im nächsten Schritt zeigen Sie die Konfigurationen in der Vorschau an und klicken Sie auf **Weiter**.

HINWEIS:

Für NetScaler-Instanzen im Cluster-Modus unterstützt NetScaler Console mithilfe der Sicherheitsberatung das Ausführen des Konfigurationsauftrags nur auf dem Cluster Configuration Coordinator (CCO)-Knoten. Führen Sie die Befehle auf Nicht-CCO-Knoten separat aus.

Schritte zur Behebung für CVE-2026-13474(/en-us/netscaler-console-service/media/cve-2026-13474-remediation-step-2.png)

Schritt 3: Konfiguration ausführen

Klicken Sie auf **Fertig stellen**, um den Konfigurationsauftrag auszuführen.

Schritte zur Behebung für CVE-2026-13474(/en-us/netscaler-console-service/media/cve-2026-13474-remediation-step-3.png)

Nachdem der Auftrag ausgeführt wurde, wird er unter **Infrastructure > Configuration > Configuration Jobs** angezeigt.

Nachdem Sie die beiden Behebungsschritte für alle anfälligen NetScaler-Instanzen abgeschlossen haben, führen Sie einen On-Demand-Scan aus, um die überarbeitete Sicherheitslage anzuzeigen.

Schwachstellen für CVE-2026-10817 identifizieren und beheben

Im NetScaler Console® Sicherheitsberatungs-Dashboard klicken Sie auf **CVE-Erkennung**. Auf der Registerkarte **Betroffene Instanzen** suchen Sie nach CVE-2026-10817. Die Liste der NetScaler-Instanzen, die von CVE-2026-10817 betroffen sind, wird angezeigt.

Sicherheitsberatungs-Dashboard für CVE-2026-10817(/en-us/netscaler-console-service/media/security-advisory-cve-2026-10817.png)

Weitere Informationen zum Sicherheitsberatungs-Dashboard finden Sie unter Sicherheitsberatung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Es kann ein paar Stunden dauern, bis der Scan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2026-10817 im Sicherheitsberatungsmodul widerspiegelt. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2026-10817 beheben

Für von CVE-2026-10817 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

In der GUI wählen Sie unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken auf **Mit Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits vorausgefüllt sind.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

Dieser Schritt kann auf einmal für alle anfälligen NetScaler-Instanzen durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

Schwachstellen für CVE-2026-10816 identifizieren und beheben

Klicken Sie im NetScaler Console® Security Advisory Dashboard auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2026-10816. Die Liste der NetScaler-Instanzen, die von CVE-2026-10816 betroffen sind, wird angezeigt.

Weitere Informationen zum Security Advisory Dashboard finden Sie unter Sicherheitshinweis.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitshinweissystems abgeschlossen ist und die Auswirkungen von CVE-2026-10816 im Sicherheitshinweismodul angezeigt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CVE-2026-10816 beheben

Für von CVE-2026-10816 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird mit den bereits ausgefüllten anfälligen NetScaler-Instanzen geöffnet.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Jobs.

Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

Schwachstellen für CVE-2026-8655 identifizieren und beheben

Klicken Sie im Sicherheitsberatungs-Dashboard von NetScaler Console® auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2026-8655. Die Liste der NetScaler-Instanzen, die von CVE-2026-8655 betroffen sind, wird angezeigt.

Weitere Informationen zum Sicherheitsberatungs-Dashboard finden Sie unter Sicherheitsberatung.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitsberatungssystems abgeschlossen ist und die Auswirkungen von CVE-2026-8655 im Sicherheitsberatungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2026-8655 beheben

Für von CVE-2026-8655 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, die den Fix enthalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird mit den bereits ausgefüllten anfälligen NetScaler-Instanzen geöffnet.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

Schwachstellen für CVE-2026-8452 identifizieren und beheben

Klicken Sie im NetScaler Console® Security Advisory Dashboard auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2026-8452. Die Liste der NetScaler-Instanzen, die von CVE-2026-8452 betroffen sind, wird angezeigt.

Weitere Informationen zum Security Advisory Dashboard finden Sie unter Security Advisory.

HINWEIS:

Es kann einige Stunden dauern, bis der Systemscan des Security Advisory abgeschlossen ist und die Auswirkungen von CVE-2026-8452 im Security Advisory-Modul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2026-8452 beheben

Für von CVE-2026-8452 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, die den Fix enthalten.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits vorausgefüllt sind.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

Schwachstellen für CVE-2026-8451 identifizieren und beheben

Klicken Sie im NetScaler Console® Security Advisory Dashboard auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2026-8451. Die Liste der NetScaler-Instanzen, die von CVE-2026-8451 betroffen sind, wird angezeigt.

Weitere Informationen zum Security Advisory Dashboard finden Sie unter Security Advisory.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Security Advisory Systems abgeschlossen ist und die Auswirkungen von CVE-2026-8451 im Security Advisory Modul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2026-8451 beheben

Für von CVE-2026-8451 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird mit den bereits ausgefüllten anfälligen NetScaler-Instanzen geöffnet.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig durchgeführt werden. Weitere Informationen finden Sie unter CVE-Erkennung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwachstellen für CVE-2026-4368 identifizieren und beheben

Im NetScaler Console® Sicherheitswarnungs-Dashboard klicken Sie auf **CVE Detection**. Auf der Registerkarte **Impacted Instances** suchen Sie nach CVE-2026-4368. Die Liste der NetScaler-Instanzen, die von CVE-2026-4368 betroffen sind, wird angezeigt.

Sicherheitswarnungs-Dashboard für CVE-2026-4368(/en-us/netscaler-console-service/media/security-advisory-cve-2026-4368.png)

Weitere Informationen zum Sicherheitswarnungs-Dashboard finden Sie unter Security Advisory.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitswarnungssystems abgeschlossen ist und die Auswirkungen von CVE-2026-4368 im Sicherheitswarnungsmodul widerspiegelt. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Scan-Now** klicken.

CVE-2026-4368 beheben

Für von CVE-2026-4368 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

In der GUI wählen Sie unter **CVE Detection > Impacted Instances** die Instanzen aus und klicken auf **Proceed to upgrade workflow**. Der Upgrade-Workflow öffnet sich, wobei die anfälligen NetScaler-Instanzen bereits ausgefüllt sind.

WICHTIG

Wenn Ihre anfälligen NetScaler-Instanzen die Datei /etc/httpd.conf in das Verzeichnis /nsconfig kopiert haben, siehe Upgrade considerations for customized NetScaler configurations bevor Sie ein NetScaler-Upgrade planen.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Create a NetScaler upgrade job.

Behebungsworkflow(/en-us/netscaler-console-service/media/remediation-workflow-cve-2026-4368.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwachstellen für CVE-2026-3055 identifizieren und beheben

Klicken Sie im NetScaler Console® Sicherheitswarnungs-Dashboard auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2026-3055. Die Liste der NetScaler-Instanzen, die von CVE-2026-3055 betroffen sind, wird angezeigt.

Weitere Informationen zum Sicherheitswarnungs-Dashboard finden Sie unter Sicherheitswarnung.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitswarnungssystems abgeschlossen ist und die Auswirkungen von CVE-2026-3055 im Sicherheitswarnungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2026-3055 beheben

Für von CVE-2026-3055 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird mit den bereits ausgefüllten anfälligen NetScaler-Instanzen geöffnet.

WICHTIG

Wenn Ihre anfälligen NetScaler-Instanzen die Datei /etc/httpd.conf in das Verzeichnis /nsconfig kopiert haben, siehe Upgrade-Überlegungen für angepasste NetScaler-Konfigurationen bevor Sie das NetScaler-Upgrade planen.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwachstellen für CVE-2025-12101 identifizieren und beheben

Klicken Sie im Sicherheitswarnungs-Dashboard von NetScaler Console auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2025-12101. Die Liste der NetScaler®-Instanzen, die von CVE-2025-12101 betroffen sind, wird angezeigt.

Weitere Informationen zum Sicherheitswarnungs-Dashboard finden Sie unter Sicherheitswarnung.

HINWEIS:

Es kann einige Stunden dauern, bis der Systemscan der Sicherheitswarnung abgeschlossen ist und die Auswirkungen von CVE-2025-12101 im Sicherheitswarnungsmodul angezeigt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2025-12101 beheben

Für von CVE-2025-12101 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits ausgefüllt sind.

WICHTIG

Wenn Ihre anfälligen NetScaler-Instanzen die Datei /etc/httpd.conf in das Verzeichnis /nsconfig kopiert haben, lesen Sie Überlegungen zum Upgrade für angepasste NetScaler-Konfigurationen, bevor Sie ein NetScaler-Upgrade planen.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Auftrags.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwachstellen für CVE-2025-8424 identifizieren und beheben

Klicken Sie im NetScaler Console Security Advisory Dashboard auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2025-8424. Die Liste der NetScaler-Instanzen, die von CVE-2025-8424 betroffen sind, wird angezeigt.

Security Advisory Dashboard für CVE-2025-8424(/en-us/netscaler-console-service/media/security-advisory-cve-2025-8424.png)

Weitere Informationen zum Security Advisory Dashboard finden Sie unter Sicherheitshinweis.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitshinweis-Systems abgeschlossen ist und die Auswirkungen von CVE-2025-8424 im Sicherheitshinweis-Modul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2025-8424 beheben

Für von CVE-2025-8424 betroffene NetScaler®-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits vorausgefüllt sind.

WICHTIG

Wenn Ihre anfälligen NetScaler-Instanzen die Datei /etc/httpd.conf in das Verzeichnis /nsconfig kopiert haben, lesen Sie Überlegungen zum Upgrade für angepasste NetScaler-Konfigurationen bevor Sie ein NetScaler-Upgrade planen.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

Behebungs-Workflow(/en-us/netscaler-console-service/media/remediation-workflow-cve-2025-8424.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwachstellen für CVE-2025-7776 identifizieren und beheben

Klicken Sie im NetScaler Console Sicherheitswarnungs-Dashboard auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2025-7776. Die Liste der NetScaler-Instanzen, die von CVE-2025-7776 betroffen sind, wird angezeigt.

Sicherheitswarnungs-Dashboard für CVE-2025-7776(/en-us/netscaler-console-service/media/security-advisory-cve-2025-7776.png)

Weitere Informationen zum Sicherheitswarnungs-Dashboard finden Sie unter Sicherheitswarnung.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitswarnungssystems abgeschlossen ist und die Auswirkungen von CVE-2025-7776 im Sicherheitswarnungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2025-7776 beheben

Für von CVE-2025-7776 betroffene NetScaler®-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits ausgefüllt sind.

WICHTIG

Wenn Ihre anfälligen NetScaler-Instanzen die Datei /etc/httpd.conf in das Verzeichnis /nsconfig kopiert haben, siehe Upgrade-Überlegungen für angepasste NetScaler-Konfigurationen, bevor Sie ein NetScaler-Upgrade planen.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Job erstellen.

Behebungs-Workflow(/en-us/netscaler-console-service/media/remediation-workflow-cve-2025-7776.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwachstellen für CVE-2025-7775 identifizieren und beheben

Klicken Sie im NetScaler Console Security Advisory Dashboard auf **CVE-Erkennung**. Suchen Sie auf der Registerkarte **Betroffene Instanzen** nach CVE-2025-7775. Die Liste der NetScaler-Instanzen, die von CVE-2025-7775 betroffen sind, wird angezeigt.

Weitere Informationen zum Security Advisory Dashboard finden Sie unter Security Advisory.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Security Advisory Systems abgeschlossen ist und die Auswirkungen von CVE-2025-7775 im Security Advisory Modul angezeigt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2025-7775 beheben

Für von CVE-2025-7775 betroffene NetScaler®-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, die den Fix enthalten.

Wählen Sie in der GUI unter **CVE-Erkennung > Betroffene Instanzen** die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird mit den bereits ausgefüllten anfälligen NetScaler-Instanzen geöffnet.

WICHTIG

Wenn Ihre anfälligen NetScaler-Instanzen die Datei /etc/httpd.conf in das Verzeichnis /nsconfig kopiert haben, lesen Sie Upgrade-Überlegungen für angepasste NetScaler-Konfigurationen, bevor Sie ein NetScaler-Upgrade planen.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Jobs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwachstellen für CVE-2025-6543 identifizieren und beheben

Im NetScaler Console Sicherheitswarnungs-Dashboard, unter **Aktuelle CVEs** `<number of>` **NetScaler-Instanzen sind von CVEs betroffen**, können Sie alle Instanzen sehen, die aufgrund von CVE-2025-6543 anfällig sind. Um die Details der von den CVEs betroffenen Instanzen zu überprüfen, wählen Sie CVE-2025-6543 aus und klicken Sie auf **Betroffene Instanzen anzeigen**.

Sicherheitswarnungs-Dashboard für CVE-2025-6543(/en-us/netscaler-console-service/media/security-advisory-cve-2025-6543.png)

HINWEIS:

Um den Grund für die NetScaler-Schwachstelle zu verstehen, laden Sie den CSV-Bericht im Tab **Scan-Protokolle** in der Sicherheitswarnung herunter.

Das Fenster `<number of>` **NetScaler-Instanzen, die von CVEs betroffen sind** wird angezeigt. Im folgenden Screenshot sehen Sie die Anzahl und Details der NetScaler-Instanzen, die von CVE-2025-6543 betroffen sind.

Instanzen, die von CVE-2025-6543 betroffen sind(/en-us/netscaler-console-service/media/cve-2025-6543-impacted-instance.png)

Weitere Informationen zum Sicherheitswarnungs-Dashboard finden Sie unter Sicherheitswarnung.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitswarnungssystems abgeschlossen ist und die Auswirkungen von CVE-2025-6543 im Sicherheitswarnungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2025-6543 beheben

Für von CVE-2025-6543 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält. In der GUI, unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen**, sehen Sie den Schritt zur Behebung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unter **Aktuelle CVEs > NetScaler-Instanzen, die von CVEs betroffen sind**, sehen Sie den folgenden Workflow für diesen einstufigen Behebungsprozess, der **Mit dem Upgrade-Workflow fortfahren** lautet.

Um die anfälligen Instanzen zu aktualisieren, wählen Sie die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird mit den bereits ausgefüllten anfälligen NetScaler-Instanzen geöffnet.

WICHTIG

Wenn Ihre anfälligen NetScaler-Instanzen die Datei /etc/httpd.conf in das Verzeichnis /nsconfig kopiert haben, siehe Upgrade-Überlegungen für angepasste NetScaler-Konfigurationen, bevor Sie ein NetScaler-Upgrade planen.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter NetScaler-Upgrade-Auftrag erstellen.

Schwachstellen für CVE-2025-5349 identifizieren und beheben

Im NetScaler Console Security Advisory Dashboard, unter **Aktuelle CVEs** `<number of>` **NetScaler-Instanzen sind von CVEs betroffen**, sehen Sie alle Instanzen, die aufgrund von CVE-2025-5349 anfällig sind. Um die Details der von den CVEs betroffenen Instanzen zu überprüfen, wählen Sie CVE-2025-5349 aus und klicken Sie auf **Betroffene Instanzen anzeigen**.

Security Advisory Dashboard für CVE-2025-5349(/en-us/netscaler-console-service/media/security-advisory-cve-2025-5349.png)

HINWEIS:

Um den Grund für die NetScaler-Schwachstelle zu verstehen, laden Sie den CSV-Bericht auf der Registerkarte **Scan-Protokolle** im Security Advisory herunter.

Das Fenster `<number of>` **NetScaler-Instanzen, die von CVEs betroffen sind** wird angezeigt. Im folgenden Screenshot sehen Sie die Anzahl und Details der NetScaler-Instanzen, die von CVE-2025-5349 betroffen sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instanzen, die von CVE-2025-5349 betroffen sind(/en-us/netscaler-console-service/media/cve-2025-5349-impacted-instance.png)

Weitere Informationen zum Security Advisory Dashboard finden Sie unter Security Advisory.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Security Advisory Systems abgeschlossen ist und die Auswirkungen von CVE-2025-5349 im Security Advisory Modul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2025-5349 beheben

Für von CVE-2025-5349 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält. In der GUI, unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen**, sehen Sie den Schritt zur Behebung.

Unter **Aktuelle CVEs > NetScaler-Instanzen, die von CVEs betroffen sind**, sehen Sie den folgenden Workflow für diesen einstufigen Behebungsprozess, nämlich **Mit dem Upgrade-Workflow fortfahren**.

Um die anfälligen Instanzen zu aktualisieren, wählen Sie die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits vorausgefüllt sind.

WICHTIG

Wenn Ihre anfälligen NetScaler-Instanzen die Datei /etc/httpd.conf in das Verzeichnis /nsconfig kopiert haben, lesen Sie Upgrade-Überlegungen für angepasste NetScaler-Konfigurationen bevor Sie ein NetScaler-Upgrade planen.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Auftrags.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwachstellen für CVE-2025-5777 beheben

Im NetScaler Console Sicherheitswarnungs-Dashboard, unter **Aktuelle CVEs** `<number of>` **NetScaler-Instanzen sind von CVEs betroffen**, sehen Sie alle Instanzen, die aufgrund von CVE-2025-5777 anfällig sind. Um die Details der von den CVEs betroffenen Instanzen zu überprüfen, wählen Sie CVE-2025-5777 aus und klicken Sie auf **Betroffene Instanzen anzeigen**.

HINWEIS:

Um den Grund für die NetScaler-Schwachstelle zu verstehen, laden Sie den CSV-Bericht im Tab **Scan-Protokolle** unter Sicherheitswarnung herunter.

Das Fenster `<number of>` **NetScaler-Instanzen, die von CVEs betroffen sind** wird angezeigt. Im folgenden Screenshot sehen Sie die Anzahl und Details der NetScaler-Instanzen, die von CVE-2025-5777 betroffen sind.

Weitere Informationen zum Sicherheitswarnungs-Dashboard finden Sie unter Sicherheitswarnung.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitswarnungssystems abgeschlossen ist und die Auswirkungen von CVE-2025-5777 im Sicherheitswarnungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2025-5777 beheben

Für von CVE-2025-5777 betroffene NetScaler-Instanzen ist die Behebung ein zweistufiger Prozess. In der GUI, unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen**, sehen Sie Schritt 1 und 2.

Die beiden Schritte umfassen:

1. Aktualisierung der anfälligen NetScaler-Instanzen auf eine Version und einen Build, der den Fix enthält.
2. Anwenden der erforderlichen Konfigurationsbefehle mithilfe der anpassbaren integrierten Konfigurationsvorlage in Konfigurationsaufträgen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unter **Aktuelle CVEs > NetScaler-Instanzen, die von CVEs betroffen sind** sehen Sie zwei separate Workflows für diesen zweistufigen Behebungsprozess: **Mit dem Upgrade-Workflow fortfahren** und **Mit dem Konfigurationsauftrags-Workflow fortfahren**.

Schritt 1: Aktualisieren Sie die anfälligen NetScaler-Instanzen

Um die anfälligen Instanzen zu aktualisieren, wählen Sie die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits ausgefüllt sind.

Weitere Informationen zur Verwendung von NetScaler Console zum Aktualisieren von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Auftrags.

HINWEIS:

Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig durchgeführt werden.

Schritt 2: Konfigurationsbefehle anwenden

Nachdem Sie die betroffenen Instanzen aktualisiert haben, wählen Sie im Fenster `<number of>` **NetScaler-Instanzen, die von CVEs betroffen sind** die von CVE-2025-5777 betroffene Instanz aus und klicken Sie auf **Mit dem Konfigurationsauftrags-Workflow fortfahren**. Der Workflow umfasst die folgenden Schritte.

1. Anpassen der Konfiguration.
2. Überprüfen der automatisch ausgefüllten betroffenen Instanzen.
3. Ausführen des Auftrags.

Beachten Sie die folgenden Punkte, bevor Sie eine Instanz auswählen und auf **Mit dem Konfigurationsauftrags-Workflow fortfahren** klicken:

- Für eine NetScaler-Instanz, die von mehreren CVEs betroffen ist (z. B. CVE-2020-8300, CVE-2021-22927, CVE-2021-22920, CVE-2021-22956 und CVE-2025-5777): Wenn Sie die Instanz auswählen und auf **Mit dem Konfigurationsauftrags-Workflow fortfahren** klicken, wird die integrierte Konfigurationsvorlage nicht automatisch unter **Konfiguration auswählen** ausgefüllt. Sie müssen die entsprechende Konfigurationsauftragsvorlage unter **Sicherheitsberatungsvorlage** manuell in den Konfigurationsauftragsbereich auf der rechten Seite ziehen und ablegen.
- Für mehrere NetScaler-Instanzen, die nur von CVE-2025-5777 betroffen sind: Sie können Konfigurationsaufträge für alle Instanzen gleichzeitig ausführen. Wenn Sie beispielsweise

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler 1, NetScaler 2 und NetScaler 3 haben und alle nur von CVE-2025-5777 betroffen sind, wählen Sie alle diese Instanzen aus und klicken Sie auf **Mit dem Konfigurationsauftrags-Workflow fortfahren**, und die integrierte Konfigurationsvorlage wird automatisch unter **Konfiguration auswählen** ausgefüllt.

- Für mehrere NetScaler-Instanzen, die von CVE-2025-5777 und einer oder mehreren anderen CVEs (wie CVE-2020-8300, CVE-2021-22927 und CVE-2021-22920) betroffen sind und für die eine Behebung nacheinander auf jeden NetScaler angewendet werden muss: Wenn Sie diese Instanzen auswählen und auf **Proceed to configuration job workflow** klicken, wird eine Fehlermeldung angezeigt, die Sie darauf hinweist, den Konfigurationsjob nacheinander auf jedem NetScaler auszuführen.

Schritt 1: Konfiguration auswählen

Im Workflow für Konfigurationsjobs wird die integrierte Konfigurationsbasistabelle automatisch unter **Select configuration** ausgefüllt.

Schritt 2: Instanz auswählen

Die betroffene Instanz wird automatisch unter **Select Instances** ausgefüllt. Wählen Sie die Instanz aus. Wenn diese Instanz Teil eines HA-Paares ist, wählen Sie **Execute on Secondary Nodes**. Klicken Sie auf **Next**.

HINWEIS:

Für NetScaler-Instanzen im Cluster-Modus, die Sicherheitswarnungen verwenden, unterstützt die NetScaler Console das Ausführen des Konfigurationsjobs nur auf dem Cluster Configuration Coordinator (CCO)-Knoten. Führen Sie die Befehle auf Nicht-CCO-Knoten separat aus.

Schritt 3: Job ausführen

Klicken Sie auf **Finish**, um den Konfigurationsjob auszuführen.

Nachdem der Job ausgeführt wurde, wird er unter **Infrastructure > Configuration > Configuration Jobs** angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nachdem Sie die beiden Behebungsschritte für alle anfälligen NetScaler-Instanzen abgeschlossen haben, können Sie einen On-Demand-Scan ausführen, um die überarbeitete Sicherheitslage zu sehen.

Schwachstellen für CVE-2024-8535 beheben

Im NetScaler Console Sicherheitswarnungs-Dashboard, unter **Aktuelle CVEs > `<number of>`** NetScaler-Instanzen sind von allgemeinen Schwachstellen und Expositionen (CVEs) betroffen, können Sie alle Instanzen sehen, die aufgrund dieser spezifischen CVE anfällig sind. Um die Details der von CVE-2024-8535 betroffenen Instanzen zu überprüfen, wählen Sie CVE-2024-8535 aus und klicken Sie auf **Betroffene Instanzen anzeigen**.

Sicherheitswarnungs-Dashboard für CVE-2024-8535(/en-us/netscaler-console-service/media/security-advisory-cve-2024-8435.png)

Das Fenster `<number of>` NetScaler-Instanzen, die von CVEs betroffen sind, wird angezeigt. Hier sehen Sie die Anzahl und Details der NetScaler-Instanzen, die von CVE-2024-8535 betroffen sind.

Instanzen, die von CVE-2020-8300 betroffen sind(/en-us/netscaler-console-service/media/cve-2024-8535-impacted-instance.png)

Weitere Informationen zum Sicherheitswarnungs-Dashboard finden Sie unter Sicherheitswarnung.

HINWEIS

Es kann einige Zeit dauern, bis der Scan des Sicherheitswarnungssystems abgeschlossen ist und die Auswirkungen von CVE-2024-8535 im Sicherheitswarnungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

CVE-2024-8535 beheben

Für von CVE-2024-8535 betroffene NetScaler-Instanzen ist die Behebung ein zweistufiger Prozess. In der GUI, unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen**, sehen Sie Schritt 1 und 2.

Behebungsschritte für CVE-2024-8535(/en-us/netscaler-console-service/media/remediate-steps-CVE-2024-8535.png)

Die beiden Schritte umfassen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Aktualisieren der anfälligen NetScaler-Instanzen auf eine Version und einen Build, der den Fix enthält.
2. Anwenden der erforderlichen Konfigurationsbefehle mithilfe der anpassbaren integrierten Konfigurationsvorlage in Konfigurationsaufträgen.

Unter **Aktuelle CVEs > NetScaler**-Instanzen, die von CVEs betroffen sind, sehen Sie zwei separate Workflows für diesen zweistufigen Behebungsprozess: nämlich **Zum Upgrade-Workflow fortfahren** und **Zum Konfigurationsauftrags-Workflow fortfahren**.

Schritt 1: Die anfälligen NetScaler-Instanzen aktualisieren

Um die anfälligen Instanzen zu aktualisieren, wählen Sie die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits ausgefüllt sind.

Weitere Informationen zur Verwendung von NetScaler Console zum Aktualisieren von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Auftrags.

HINWEIS:

Dieser Schritt kann auf einmal für alle anfälligen NetScaler-Instanzen durchgeführt werden.

Schritt 2: Konfigurationsbefehle anwenden

Nachdem Sie die betroffenen Instanzen aktualisiert haben, wählen Sie im Fenster `<number of>` **NetScaler-Instanzen, die von CVEs betroffen sind** die von CVE-2024-8535 betroffene Instanz aus und klicken Sie auf **Mit dem Konfigurationsauftrags-Workflow fortfahren**.

Beachten Sie die folgenden Punkte, bevor Sie eine Instanz auswählen und auf **Mit dem Konfigurationsauftrags-Workflow fortfahren** klicken:

- Für eine NetScaler-Instanz, die von mehreren CVEs betroffen ist (z. B. CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 und CVE-2021-22956): Wenn Sie die Instanz auswählen und auf **Mit dem Konfigurationsauftrags-Workflow fortfahren** klicken, wird die integrierte Konfigurationsvorlage nicht automatisch unter **Konfiguration auswählen** ausgefüllt. Ziehen Sie die entsprechende Konfigurationsauftragsvorlage unter **Sicherheitsberatungsvorlage** manuell in den Konfigurationsauftragsbereich auf der rechten Seite.
- Für mehrere NetScaler-Instanzen, die nur von CVE-2024-8535 betroffen sind, können Sie Konfigurationsaufträge auf allen Instanzen gleichzeitig ausführen. Sie haben beispielsweise

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler 1, NetScaler 2 und NetScaler 3, und alle sind nur von CVE-2024-8535 betroffen. Wählen Sie alle diese Instanzen aus und klicken Sie auf **Mit dem Konfigurationsauftrags-Workflow fortfahren**, und die integrierte Konfigurationsvorlage wird automatisch unter **Konfiguration auswählen** ausgefüllt.

- Für mehrere NetScaler-Instanzen, die von CVE-2024-8535 und einem oder mehreren anderen CVEs betroffen sind (z. B. CVE-2020-8300, CVE-2021-22927 und CVE-2021-22920), bei denen die Behebung nacheinander auf jeden NetScaler angewendet werden muss: Wenn Sie diese Instanzen auswählen und auf **Mit dem Konfigurationsauftrags-Workflow fortfahren** klicken, wird eine Fehlermeldung angezeigt, die Sie darauf hinweist, den Konfigurationsauftrag nacheinander auf jedem NetScaler auszuführen.

Schritt 1: Konfiguration auswählen

Im Konfigurationsauftrags-Workflow wird die integrierte Konfigurationsbasistabelle automatisch unter **Konfiguration auswählen** ausgefüllt.

Schritt 2: Instanz auswählen

Die betroffene Instanz wird unter **Instanzen auswählen** automatisch ausgefüllt. Wählen Sie die Instanz aus. Wenn diese Instanz Teil eines HA-Paares ist, wählen Sie **Auf sekundären Knoten ausführen**. Klicken Sie auf **Weiter**.

Instanz auswählen(/en-us/netscaler-console-service/media/select-instance-cve-2021-22956.png)

HINWEIS:

Für NetScaler-Instanzen im Cluster-Modus, die Sicherheitswarnungen verwenden, unterstützt die NetScaler Console das Ausführen des Konfigurationsauftrags nur auf dem Cluster Configuration Coordinator (CCO)-Knoten. Führen Sie die Befehle auf Nicht-CCO-Knoten separat aus.

Schritt 3: Variablenwerte angeben

In diesem Schritt muss keine Variable angegeben werden. Wählen Sie **Gemeinsame Variablenwerte für alle Instanzen** aus und klicken Sie auf **Weiter**.

Schritt 4: Konfiguration in der Vorschau anzeigen

Zeigt die in die Konfiguration eingefügten Variablenwerte in der Vorschau an und klicken Sie auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Auftrag in der Vorschau anzeigen(/en-us/netscaler-console-service/media/preview-job-cve-2024-8535.png)

Schritt 5: Auftrag ausführen

Klicken Sie auf **Fertig stellen**, um den Konfigurationsauftrag auszuführen.

Konfigurationsauftrag ausführen(/en-us/netscaler-console-service/media/run-job-cve-2021-22956.png)

Nachdem der Auftrag ausgeführt wurde, wird er unter **Infrastruktur > Konfiguration > Konfigurationsaufträge** angezeigt.

Nachdem Sie die beiden Korrekturschritte für alle anfälligen NetScaler-Instanzen abgeschlossen haben, können Sie einen On-Demand-Scan ausführen, um die überarbeitete Sicherheitslage zu sehen.

Schwachstellen für CVE-2020-8300 beheben

Im NetScaler Console Sicherheitswarnungs-Dashboard, unter **Aktuelle CVEs > `<number of>` NetScaler-Instanzen sind von CVEs betroffen**, sehen Sie alle Instanzen, die von dieser spezifischen CVE betroffen sind. Um die Details der von CVE-2020-8300 betroffenen Instanzen zu überprüfen, wählen Sie **CVE-2020-8300** aus und klicken Sie auf **Betroffene Instanzen anzeigen**.

Sicherheitswarnungs-Dashboard für CVE-2020-8300(/en-us/netscaler-console-service/media/security-advisory-2020-8300.png)

HINWEIS

Weitere Informationen zum Sicherheitswarnungs-Dashboard finden Sie unter Sicherheitswarnung.

Das Fenster `<number of>` **NetScaler-Instanzen, die von CVEs betroffen sind** wird angezeigt. Hier sehen Sie die Anzahl und Details der von CVE-2020-8300 betroffenen NetScaler-Instanzen.

Von CVE-2020-8300 betroffene Instanzen(/en-us/netscaler-console-service/media/2020-8300-impacted-instances.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CVE-2020-8300 beheben

Für von CVE-2020-8300 betroffene NetScaler-Instanzen ist die Behebung ein zweistufiger Prozess. In der GUI, unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen**, sehen Sie Schritt 1 und 2.

Schritte zur Behebung(/en-us/netscaler-console-service/media/remediate-steps.png)

Die beiden Schritte umfassen:

1. Aktualisieren der anfälligen NetScaler-Instanzen auf eine Version und einen Build, der die Korrektur enthält.
2. Anwenden der erforderlichen Konfigurationsbefehle mithilfe der anpassbaren integrierten Konfigurationsvorlage in Konfigurationsaufträgen. Führen Sie diesen Schritt für jede anfällige NetScaler-Instanz einzeln aus und schließen Sie alle SAML-Aktionen und SAML-Profile für diese NetScaler-Instanz ein.

Unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen** sehen Sie zwei separate Workflows für diesen zweistufigen Behebungsprozess: **Workflow zum Upgrade fortsetzen** und **Workflow zum Konfigurationsauftrag fortsetzen**.

Workflows zur Behebung(/en-us/netscaler-console-service/media/remediation-workflows.png)

Schritt 1: Anfällige NetScaler-Instanzen aktualisieren

Um die anfälligen Instanzen zu aktualisieren, wählen Sie die Instanzen aus und klicken Sie auf **Proceed to upgrade workflow**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits ausgefüllt sind.

Weitere Informationen zur Verwendung von NetScaler Console zum Aktualisieren von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Auftrags.

HINWEIS

Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig durchgeführt werden.

Schritt 2: Konfigurationsbefehle anwenden

Nachdem Sie die betroffenen Instanzen aktualisiert haben, wählen Sie im Fenster `<number of>` **NetScaler-Instanzen, die von CVEs betroffen sind** eine von CVE-2020-8300 betroffene Instanz

© 1997–2026 Citrix Systems, Inc. All rights reserved.

aus und klicken Sie auf **Proceed to configuration job workflow**. Der Workflow umfasst die folgenden Schritte.

1. Anpassen der Konfiguration.
2. Überprüfen der automatisch ausgefüllten betroffenen Instanzen.
3. Angeben von Eingaben für Variablen für den Auftrag.
4. Überprüfen der endgültigen Konfiguration mit ausgefüllten Variableneingaben.
5. Ausführen des Auftrags.

Beachten Sie die folgenden Punkte, bevor Sie eine Instanz auswählen und auf **Proceed to configuration job workflow** klicken:

- Für eine NetScaler-Instanz, die von mehreren CVEs betroffen ist (z. B. CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 und CVE-2021-22956): Wenn Sie die Instanz auswählen und auf **Proceed to configuration job workflow** klicken, wird die integrierte Konfigurationsvorlage nicht automatisch unter „Konfiguration auswählen“ ausgefüllt. Ziehen Sie die entsprechende Konfigurationsauftragsvorlage unter **Security Advisory Template** manuell in den Konfigurationsauftragsbereich auf der rechten Seite.
- Für mehrere NetScaler-Instanzen, die nur von CVE-2021-22956 betroffen sind: Sie können Konfigurationsaufträge auf allen Instanzen gleichzeitig ausführen. Wenn Sie beispielsweise NetScaler 1, NetScaler 2 und NetScaler 3 haben und alle nur von CVE-2021-22956 betroffen sind. Wählen Sie alle diese Instanzen aus und klicken Sie auf **Weiter zum Konfigurationsauftrags-Workflow**, und die integrierte Konfigurationsvorlage wird unter **Konfiguration auswählen** automatisch ausgefüllt. Beachten Sie das bekannte Problem NSADM-80913 in den Versionshinweisen.
- Für mehrere NetScaler-Instanzen, die von CVE-2021-22956 und einer oder mehreren anderen CVEs (wie CVE-2020-8300, CVE-2021-22927 und CVE-2021-22920) betroffen sind, bei denen die Behebung nacheinander auf jeden NetScaler angewendet werden muss: Wenn Sie diese Instanzen auswählen und auf **Weiter zum Konfigurationsauftrags-Workflow** klicken, wird eine Fehlermeldung angezeigt, die Sie auffordert, den Konfigurationsauftrag nacheinander auf jedem NetScaler auszuführen.

Schritt 1: Konfiguration auswählen

Im Konfigurationsauftrags-Workflow wird die integrierte Konfigurationsvorlage unter **Konfiguration auswählen** automatisch ausgefüllt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Führen Sie für jede betroffene NetScaler-Instanz nacheinander einen separaten Konfigurationsauftrag aus und schließen Sie alle SAML-Aktionen und SAML-Profile für diesen NetScaler ein. Wenn Sie beispielsweise zwei anfällige NetScaler-Instanzen haben, die jeweils zwei SAML-Aktionen und zwei SAML-Profile aufweisen, müssen Sie diesen Konfigurationsauftrag zweimal ausführen. Einmal pro NetScaler, wobei alle seine SAML-Aktionen und SAML-Profile abgedeckt werden.

NETSCALER 1	NETSCALER2
Auftrag 1: zwei SAML-Aktionen + zwei SAML-Profile	Auftrag 2: zwei SAML-Aktionen + zwei SAML-Profile

Geben Sie dem Auftrag einen Namen und passen Sie die Vorlage an die folgenden Spezifikationen an. Die integrierte Konfigurationsvorlage ist nur eine Gliederung oder Basisvorlage. Passen Sie die Vorlage basierend auf Ihrer Bereitstellung an die folgenden Anforderungen an:

a. **SAML-Aktionen und ihre zugehörigen Domänen**

Je nach Anzahl der SAML-Aktionen, die Sie in Ihrer Bereitstellung haben, müssen Sie die Zeilen 1–3 replizieren und die Domänen für jede SAML-Aktion anpassen.

Wenn Sie beispielsweise zwei SAML-Aktionen haben, wiederholen Sie die Zeilen 1–3 zweimal und passen Sie die Variablendefinitionen entsprechend für jede SAML-Aktion an.

Und wenn Sie N Domänen für eine SAML-Aktion haben, müssen Sie die Zeile `bind patset $saml_action_patset$ “$saml_action_domain1$”` mehrmals manuell eingeben, um sicherzustellen, dass die Zeile N-mal für diese SAML-Aktion erscheint. Und ändern Sie die folgenden Variablendefinitionsnamen:

- `saml_action_patset`: ist die Konfigurationsvorlagenvariable und stellt den Wert des Namens des Mustersatzes (Patset) für die SAML-Aktion dar. Sie können den tatsächlichen Wert in Schritt 3 des Konfigurationsauftrags-Workflows angeben. Siehe den Abschnitt Schritt 3: Variablenwerte angeben in diesem Dokument.
- `saml_action_domain1`: ist die Konfigurationsvorlagenvariable und stellt den Domänennamen für diese spezifische SAML-Aktion dar. Sie können den tatsächlichen Wert in Schritt 3 des Konfigurationsauftrags-Workflows angeben. Siehe den Abschnitt Schritt 3: Variablenwerte angeben in diesem Dokument.

Um alle SAML-Aktionen für ein Gerät zu finden, führen Sie den Befehl `show samlaction` aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **SAML-Profile und ihre zugehörigen URLs**

Je nach Anzahl der SAML-Profile in Ihrer Bereitstellung replizieren Sie die Zeilen 4–6. Passen Sie die URLs für jedes SAML-Profil an.

Wenn Sie beispielsweise zwei SAML-Profile haben, geben Sie die Zeilen 4–6 zweimal manuell ein und passen Sie die Variablendefinitionen entsprechend für jede SAML-Aktion an.

Und wenn Sie N Domänen für eine SAML-Aktion haben, müssen Sie die Zeile `bind patset $saml_profile_patset$ “$saml_profile_url1$”` mehrmals manuell eingeben, um sicherzustellen, dass die Zeile N-mal für dieses SAML-Profil erscheint. Und ändern Sie die folgenden Variablendefinitionsnamen:

- `saml_profile_patset`: ist die Konfigurationsvorlagenvariable und stellt den Wert des Namens des Mustersatzes (Patset) für das SAML-Profil dar. Sie können den tatsächlichen Wert in Schritt 3 des Konfigurationsauftrags-Workflows angeben. Siehe den Abschnitt Schritt 3: Variablenwerte angeben in diesem Dokument.
- `saml_profile_url1`: ist die Konfigurationsvorlagenvariable und stellt den Domänennamen für dieses spezifische SAML-Profil dar. Sie können den tatsächlichen Wert in Schritt 3 des Konfigurationsauftrags-Workflows angeben. Siehe den Abschnitt Schritt 3: Variablenwerte angeben in diesem Dokument.

Um alle SAM-Profile für ein Gerät zu finden, führen Sie den Befehl `show samlidpProfile` aus.

Schritt 2: Instanz auswählen

Die betroffene Instanz wird unter **Instanzen auswählen** automatisch ausgefüllt. Wählen Sie die Instanz aus und klicken Sie auf **Weiter**.

Instanz auswählen(/en-us/netscaler-console-service/media/select-instance.png)

Schritt 3: Variablenwerte angeben

Geben Sie die Variablenwerte ein.

- `saml_action_patset`: einen Namen für die SAML-Aktion hinzufügen
- `saml_action_domain1`: eine Domäne im Format `https://<example1.com>/` eingeben
- `saml_action_name`: den Namen der SAML-Aktion eingeben, für die Sie den Job konfigurieren

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `saml_profile_patset`: einen Namen für das SAML-Profil hinzufügen
- `saml_profile_url1`: die URL in diesem Format `https://<example2.com>/cgi/samlauth` eingeben
- `saml_profile_name`: den Namen des SAML-Profils eingeben, für das Sie den Job konfigurieren

HINWEIS

Bei URLs ist die Erweiterung nicht immer `cgi/samlauth`. Es hängt davon ab, welche Drittanbieter-Autorisierung Sie haben, und dementsprechend müssen Sie die Erweiterung angeben.

Variablen angeben(/en-us/netscaler-console-service/media/specify-variables.png)

Schritt 4: Konfiguration in der Vorschau anzeigen

Zeigt die in die Konfiguration eingefügten Variablenwerte in der Vorschau an und klicken Sie auf **Weiter**.

Schritt 5: Auftrag ausführen

Klicken Sie auf **Fertig stellen**, um den Konfigurationsauftrag auszuführen.

Nachdem der Auftrag ausgeführt wurde, wird er unter **Infrastructure > Configuration > Configuration Jobs** angezeigt.

Nachdem Sie die beiden Korrekturschritte für alle anfälligen NetScaler-Instanzen abgeschlossen haben, können Sie einen On-Demand-Scan ausführen, um die überarbeitete Sicherheitslage anzuzeigen.

Hinweise zum NetScaler Console Express-Konto

Das NetScaler Console Express-Konto verfügt über eingeschränkte Funktionen, die unter anderem auf zwei Konfigurationsaufträge beschränkt sind. Weitere Informationen zum NetScaler Console Express-Konto finden Sie unter NetScaler Console-Ressourcen mit Express-Konto verwalten. Für die CVE-2020-8300-Behebung müssen Sie so viele Konfigurationsaufträge ausführen, wie Sie anfällige NetScaler-Instanzen haben. Wenn Sie also ein Express-Konto haben und mehr als zwei Konfigurationsaufträge ausführen müssen, befolgen Sie diese Problemumgehung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Problemumgehung: Führen Sie zwei Konfigurationsaufträge für zwei anfällige NetScaler-Instanzen aus und löschen Sie dann beide Aufträge, um die nächsten beiden Aufträge für die nächsten beiden anfälligen NetScaler-Instanzen auszuführen. Fahren Sie damit fort, bis Sie alle anfälligen Instanzen abgedeckt haben. Bevor Sie die Aufträge löschen, können Sie den Bericht zur späteren Bezugnahme herunterladen. Um den Bericht herunterzuladen, wählen Sie unter **Network > Jobs** die Aufträge aus und klicken Sie unter **Actions** auf **Download**.

Beispiel: Wenn Sie sechs anfällige NetScaler-Instanzen haben, führen Sie jeweils zwei Konfigurationsaufträge auf zwei anfälligen Instanzen aus und löschen Sie dann beide Konfigurationsaufträge. Wiederholen Sie diesen Schritt noch zweimal. Am Ende hätten Sie sechs Konfigurationsaufträge für jeweils sechs NetScaler-Instanzen ausgeführt. In der NetScaler Console-Benutzeroberfläche unter **Infrastructure > Jobs** sehen Sie nur die letzten beiden Konfigurationsaufträge.

Szenario

In diesem Szenario sind drei NetScaler-Instanzen anfällig für CVE-2020-8300, und Sie müssen alle Instanzen beheben. Gehen Sie wie folgt vor:

1. Führen Sie ein Upgrade aller drei NetScaler-Instanzen durch, indem Sie die Schritte im Abschnitt **Upgrade einer Instanz** in diesem Dokument befolgen.
2. Wenden Sie den Konfigurations-Patch nacheinander auf einen NetScaler an, indem Sie den Workflow für Konfigurationsaufträge verwenden. Beachten Sie die Schritte im Abschnitt **Konfigurationsbefehle anwenden** in diesem Dokument.

Der anfällige NetScaler 1 hat die folgende Konfiguration:

ZWEI SAML-AKTIONEN	ZWEI SAML-PROFILE

Wählen Sie NetScaler 1 aus und klicken Sie auf **Mit dem Konfigurationsauftrags-Workflow fortfahren**. Die integrierte Vorlage wird automatisch ausgefüllt. Geben Sie anschließend einen Auftragsnamen ein und passen Sie die Vorlage gemäß der angegebenen Konfiguration an.

Die folgenden Tabellen listen die Variablendefinitionen für angepasste Parameter auf.

Tabelle 1. Variablendefinitionen für SAML-Aktion

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETSCALER-KONFIGURATION	VARIABLENDEFINITION FÜR PATSET	VARIABLENDEFINITION FÜR SAML-AKTIONSNAME	VARIABLENDEFINITION FÜR DOMÄNE
SAML-Aktion 1 hat eine Domäne	saml_action_patset1	saml_action_name1	saml_action_domain 1
SAML-Aktion 2 hat zwei Domänen	saml_action_patset2	saml_action_name2	saml_action_domain 2, saml_action_domain 3

Tabelle 2. Variablendefinitionen für SAML-Profil

NETSCALER-KONFIGURATION	VARIABLENDEFINITION FÜR PATSET	VARIABLENDEFINITION FÜR SAML-PROFILNAME	VARIABLENDEFINITION FÜR URL
SAML-Profil 1 hat eine URL	saml_profile_patset1	saml_profile_name1	saml_profile_url1
SAML-Profil 2 hat zwei URLs	saml_profile_patset2	saml_profile_name2	saml_profile_url2, saml_profile_url3

Wählen Sie unter **Instanzen auswählen** NetScaler 1 aus und klicken Sie auf **Weiter**. Das Fenster **Variablenwerte angeben** wird angezeigt. In diesem Schritt müssen Sie Werte für alle im vorherigen Schritt definierten Variablen angeben.

- [ ] Überprüfen Sie als Nächstes die Variablen.

Klicken Sie auf **Weiter** und dann auf **Fertig stellen**, um den Auftrag auszuführen.

Nachdem der Auftrag ausgeführt wurde, wird er unter **Infrastructure > Configuration > Configuration Jobs** angezeigt.

Nachdem Sie die beiden Korrekturschritte für NetScaler 1 abgeschlossen haben, führen Sie die gleichen Schritte aus, um NetScaler 2 und NetScaler 3 zu korrigieren. Nachdem die Korrektur abgeschlossen ist, können Sie einen On-Demand-Scan ausführen, um die überarbeitete Sicherheitslage anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwachstellen für CVE-2021-22927 und CVE-2021-22920 beheben

Im NetScaler Console Sicherheitswarnungs-Dashboard, unter **Aktuelle CVEs > `<number of>` NetScaler-Instanzen sind von CVEs betroffen**, sehen Sie alle Instanzen, die aufgrund von CVE-2021-22927 und CVE-2021-22920 anfällig sind. Um die Details der von diesen beiden CVEs betroffenen Instanzen zu überprüfen, wählen Sie eine oder mehrere CVEs aus und klicken Sie auf **Betroffene Instanzen anzeigen**.

HINWEIS

Es kann einige Stunden dauern, bis der Scan des Sicherheitswarnungssystems abgeschlossen ist und die Auswirkungen von CVE-2021-22927 und CVE-2021-22920 im Sicherheitswarnungsmodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken. Weitere Informationen zum Sicherheitswarnungs-Dashboard finden Sie unter Sicherheitswarnung.

Das Fenster **`<number of>` NetScaler-Instanzen, die von CVEs betroffen sind** wird angezeigt. Im folgenden Screenshot sehen Sie die Anzahl und Details der NetScaler-Instanzen, die von CVE-2021-22927 und CVE-2021-22920 betroffen sind.

CVE-2021-22927 und CVE-2021-22920 beheben

Für von CVE-2021-22927 und CVE-2021-22920 betroffene NetScaler-Instanzen ist die Behebung ein zweistufiger Prozess. In der GUI, unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen**, sehen Sie Schritt 1 und 2.

Die beiden Schritte umfassen:

1. Aktualisieren der anfälligen NetScaler-Instanzen auf eine Version und einen Build, der die Korrektur enthält.
2. Anwenden der erforderlichen Konfigurationsbefehle mithilfe der anpassbaren integrierten Konfigurationsvorlage in Konfigurationsaufträgen. Führen Sie diesen Schritt für jede anfällige NetScaler-Instanz einzeln aus und schließen Sie alle SAML-Aktionen für diese NetScaler-Instanz ein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Überspringen Sie Schritt 2, wenn Sie bereits Konfigurationsaufträge auf der NetScaler-Instanz für CVE-2020-8300 ausgeführt haben.

Unter **Aktuelle CVEs> NetScaler-Instanzen, die von CVEs betroffen sind**, sehen Sie zwei separate Workflows für diesen zweistufigen Behebungsprozess: nämlich **Workflow für das Upgrade fortsetzen** und **Workflow für den Konfigurationsauftrag fortsetzen**.

Schritt 1: Aktualisieren Sie die anfälligen NetScaler-Instanzen

Um die anfälligen Instanzen zu aktualisieren, wählen Sie die Instanzen aus und klicken Sie auf **Workflow für das Upgrade fortsetzen**. Der Upgrade-Workflow wird geöffnet, wobei die anfälligen NetScaler-Instanzen bereits vorausgefüllt sind.

Weitere Informationen zur Verwendung von NetScaler Console zum Aktualisieren von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Auftrags.

HINWEIS

Dieser Schritt kann für alle anfälligen NetScaler-Instanzen gleichzeitig durchgeführt werden.
Hinweis

Nachdem Sie Schritt 1 für alle NetScaler-Instanzen abgeschlossen haben, die für CVE-2021-22920 und CVE-2021-22927 anfällig sind, führen Sie einen On-Demand-Scan durch. Die aktualisierte Sicherheitslage unter **Aktuelle CVEs** hilft Ihnen zu verstehen, ob die NetScaler-Instanzen immer noch für eine dieser CVEs anfällig sind. Anhand der neuen Lage können Sie auch überprüfen, ob Sie Konfigurationsaufträge ausführen müssen. Wenn Sie die entsprechenden Konfigurationsaufträge bereits auf die NetScaler-Instanz für CVE-2020-8300 angewendet haben und die NetScaler-Instanz nun aktualisiert haben, wird die Instanz nach dem On-Demand-Scan nicht mehr als anfällig für CVE-2020-8300, CVE-2021-22920 und CVE-2021-22927 angezeigt.

Schritt 2: Konfigurationsbefehle anwenden

Nachdem Sie die betroffenen Instanzen aktualisiert haben, wählen Sie im Fenster `<number of>` **NetScaler-Instanzen, die von CVEs betroffen sind** eine Instanz aus, die von CVE-2021-22927

© 1997–2026 Citrix Systems, Inc. All rights reserved.

und CVE-2021-22920 betroffen ist, und klicken Sie auf **Workflow für den Konfigurationsauftrag fortsetzen**. Der Workflow umfasst die folgenden Schritte.

1. Anpassen der Konfiguration.
2. Überprüfen der automatisch ausgefüllten betroffenen Instanzen.
3. Eingaben für Variablen für den Auftrag angeben.
4. Überprüfen der endgültigen Konfiguration mit ausgefüllten Variableneingaben.
5. Ausführen des Auftrags.

Beachten Sie die folgenden Punkte, bevor Sie eine Instanz auswählen und auf **Proceed to configuration job workflow** klicken:

- Für eine NetScaler-Instanz, die von mehreren CVEs betroffen ist (z. B. CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 und CVE-2021-22956): Wenn Sie die Instanz auswählen und auf **Proceed to configuration job workflow** klicken, wird die integrierte Konfigurationsvorlage unter „Select configuration“ nicht automatisch ausgefüllt. Ziehen Sie die entsprechende Konfigurationsauftragsvorlage unter **Security Advisory Template** manuell in den Konfigurationsauftragsbereich auf der rechten Seite.
- Für mehrere NetScaler-Instanzen, die nur von CVE-2021-22956 betroffen sind: Sie können Konfigurationsaufträge auf allen Instanzen gleichzeitig ausführen. Wenn Sie beispielsweise NetScaler 1, NetScaler 2 und NetScaler 3 haben und alle nur von CVE-2021-22956 betroffen sind, wählen Sie alle diese Instanzen aus und klicken Sie auf **Proceed to configuration job workflow**. Die integrierte Konfigurationsvorlage wird dann unter **Select configuration** automatisch ausgefüllt. Siehe das bekannte Problem NSADM-80913 in den Versionshinweisen.
- Für mehrere NetScaler-Instanzen, die von CVE-2021-22956 und einer oder mehreren anderen CVEs betroffen sind (z. B. CVE-2020-8300, CVE-2021-22927 und CVE-2021-22920), und bei denen die Behebung nacheinander auf jeden NetScaler angewendet werden muss: Wenn Sie diese Instanzen auswählen und auf **Proceed to configuration job workflow** klicken, erscheint eine Fehlermeldung, die Sie auffordert, den Konfigurationsauftrag nacheinander auf jedem NetScaler auszuführen.

Schritt 1: Konfiguration auswählen

Im Workflow des Konfigurationsauftrags wird die integrierte Basiskonfigurationsvorlage unter **Select configuration** automatisch ausgefüllt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Wenn die in Schritt 2 für die Anwendung von Konfigurationsbefehlen ausgewählte NetScaler-Instanz anfällig für CVE-2021-22927, CVE-2021-22920 und auch CVE-2020-8300 ist, wird die Basiskonfigurationsvorlage für CVE-2020-8300 automatisch ausgefüllt. Die CVE-2020-8300-Vorlage ist eine Obermenge der Konfigurationsbefehle, die für alle drei CVEs erforderlich sind. Passen Sie diese Basiskonfigurationsvorlage an die Bereitstellung und die Anforderungen Ihrer NetScaler-Instanz an.

Sie müssen für jede betroffene NetScaler-Instanz nacheinander einen separaten Konfigurationsauftrag ausführen und alle SAML-Aktionen für diesen NetScaler einschließen. Wenn Sie beispielsweise zwei anfällige NetScaler-Instanzen mit jeweils zwei SAML-Aktionen haben, müssen Sie diesen Konfigurationsauftrag zweimal ausführen. Einmal pro NetScaler, wobei alle seine SAML-Aktionen abgedeckt werden.

NETSCALER 1	NETSCALER 2
Auftrag 1: zwei SAML-Aktionen	Auftrag 2: zwei SAML-Aktionen

Geben Sie dem Auftrag einen Namen und passen Sie die Vorlage an die folgenden Spezifikationen an. Die integrierte Konfigurationsvorlage ist nur ein Entwurf oder eine Basisvorlage. Passen Sie die Vorlage basierend auf Ihrer Bereitstellung an die folgenden Anforderungen an:

a. **SAML-Aktionen und ihre zugehörigen Domänen**

Je nach der Anzahl der SAML-Aktionen, die Sie in Ihrer Bereitstellung haben, müssen Sie die Zeilen 1–3 replizieren und die Domänen für jede SAML-Aktion anpassen.

Wenn Sie beispielsweise zwei SAML-Aktionen haben, wiederholen Sie die Zeilen 1–3 zweimal und passen Sie die Variablendefinitionen entsprechend für jede SAML-Aktion an.

Und wenn Sie N Domänen für eine SAML-Aktion haben, müssen Sie die Zeile `bind patset $saml_action_patset$ “$saml_action_domain1$”` mehrmals manuell eingeben, um sicherzustellen, dass die Zeile N-mal für diese SAML-Aktion erscheint. Und ändern Sie die folgenden Variablendefinitionsnamen:

- `saml_action_patset`: ist die Konfigurationsvorlagenvariable und stellt den Wert des Namens des Mustersatzes (Patset) für die SAML-Aktion dar. Sie können den tatsächlichen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wert in Schritt 3 des Konfigurationsauftrags-Workflows angeben. Siehe den Abschnitt Schritt 3: Variablenwerte angeben in diesem Dokument.

- `saml_action_domain1`: ist die Konfigurationsvorlagenvariable und stellt den Domänennamen für diese spezifische SAML-Aktion dar. Sie können den tatsächlichen Wert in Schritt 3 des Konfigurationsauftrags-Workflows angeben. Siehe den Abschnitt Schritt 3: Variablenwerte angeben in diesem Dokument.

Um alle SAML-Aktionen für ein Gerät zu finden, führen Sie den Befehl `show samlaction` aus.

Schritt 2: Instanz auswählen

Die betroffene Instanz wird unter **Instanzen auswählen** automatisch ausgefüllt. Wählen Sie die Instanz aus und klicken Sie auf **Weiter**.

Schritt 3: Variablenwerte angeben

Geben Sie die Variablenwerte ein.

- `saml_action_patset`: Geben Sie einen Namen für die SAML-Aktion ein
- `saml_action_domain1`: Geben Sie eine Domäne im Format `https://<example1.com>/` ein
- `saml_action_name`: Geben Sie den Namen der SAML-Aktion ein, für die Sie den Auftrag konfigurieren

Schritt 4: Konfiguration in der Vorschau anzeigen

Zeigt die in die Konfiguration eingefügten Variablenwerte in der Vorschau an und klicken Sie auf **Weiter**.

Schritt 5: Auftrag ausführen

Klicken Sie auf **Fertig stellen**, um den Konfigurationsauftrag auszuführen.

Nachdem der Auftrag ausgeführt wurde, wird er unter **Infrastruktur > Konfiguration > Konfigurationsaufträge** angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nachdem Sie die beiden Korrekturschritte für alle anfälligen NetScaler-Instanzen abgeschlossen haben, können Sie einen On-Demand-Scan ausführen, um den überarbeiteten Sicherheitsstatus anzuzeigen.

Szenario

In diesem Szenario sind zwei NetScaler-Instanzen anfällig für CVE-2021-22920, und Sie müssen alle Instanzen beheben. Gehen Sie wie folgt vor:

1. Aktualisieren Sie alle drei NetScaler-Instanzen, indem Sie die Schritte im Abschnitt „Eine Instanz aktualisieren“ in diesem Dokument befolgen.
2. Wenden Sie den Konfigurations-Patch nacheinander auf jeden NetScaler an, indem Sie den Workflow für Konfigurationsaufträge verwenden. Die Schritte finden Sie im Abschnitt „Konfigurationsbefehle anwenden“ in diesem Dokument.

Der anfällige NetScaler 1 hat zwei SAML-Aktionen:

- SAML-Aktion 1 hat eine Domäne
- SAML-Aktion 2 hat zwei Domänen

Wählen Sie NetScaler 1 aus und klicken Sie auf **Mit dem Workflow für Konfigurationsaufträge fortfahren**. Die integrierte Basisschablone wird automatisch ausgefüllt. Geben Sie anschließend einen Auftragsnamen ein und passen Sie die Schablone gemäß der angegebenen Konfiguration an.

Die folgende Tabelle listet die Variablendefinitionen für angepasste Parameter auf.

Tabelle. Variablendefinitionen für SAML-Aktion

NETSCALER-KONFIGURATION	VARIABLENDEFINITION FÜR PATSET	VARIABLENDEFINITION FÜR SAML-AKTIONSNAME	VARIABLENDEFINITION FÜR DOMÄNE
SAML-Aktion 1 hat eine Domäne	saml_action_patset1	saml_action_name1	saml_action_domain 1
SAML-Aktion 2 hat zwei Domänen	saml_action_patset2	saml_action_name2	saml_action_domain 2, saml_action_domain 3

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wählen Sie unter **Instanzen auswählen** NetScaler 1 aus und klicken Sie auf **Weiter**. Das Fenster **Variablenwerte angeben** wird angezeigt. In diesem Schritt müssen Sie Werte für alle im vorherigen Schritt definierten Variablen angeben.

- Als Nächstes überprüfen Sie die Variablen.
- Klicken Sie auf **Weiter** und dann auf **Fertig stellen**, um den Auftrag auszuführen.

Nachdem der Auftrag ausgeführt wurde, wird er unter **Infrastruktur > Konfiguration > Konfigurationsaufträge** angezeigt.

Nachdem die beiden Korrekturschritte für NetScaler 1 abgeschlossen sind, führen Sie die gleichen Schritte aus, um NetScaler 2 und NetScaler 3 zu korrigieren. Nachdem die Korrektur abgeschlossen ist, können Sie einen On-Demand-Scan ausführen, um die überarbeitete Sicherheitslage zu sehen.

Schwachstellen für CVE-2021-22956 identifizieren und beheben

Im NetScaler Console Security Advisory Dashboard, unter **Aktuelle CVEs > `<number of>`** NetScaler-Instanzen sind von allgemeinen Schwachstellen und Expositionen (CVEs) betroffen, können Sie alle Instanzen sehen, die aufgrund dieser spezifischen CVE anfällig sind. Um die Details der von CVE-2021-22956 betroffenen Instanzen zu überprüfen, wählen Sie CVE-2021-22956 aus und klicken Sie auf **Betroffene Instanzen anzeigen**.

Security Advisory Dashboard für CVE-2021-22927 und CVE-2021-22920(/en-us/netscaler-console-service/media/security-advisory-cve-2021-22956.png)

Das Fenster „`<number of>` NetScaler-Instanzen, die von CVEs betroffen sind“ wird angezeigt. Hier sehen Sie die Anzahl und Details der NetScaler-Instanzen, die von CVE-2021-22956 betroffen sind.

Von CVE-2020-8300 betroffene Instanzen(/en-us/netscaler-console-service/media/cve-2021-22956-impacted-instance.png)

Weitere Informationen zum Security Advisory Dashboard finden Sie unter Security Advisory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Es kann einige Zeit dauern, bis der Systemscan des Security Advisory abgeschlossen ist und die Auswirkungen von CVE-2021-22956 im Security Advisory Modul widerspiegelt. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

Von CVE-2021-22956 betroffene Instanzen identifizieren

CVE-2021-22956 erfordert einen benutzerdefinierten Scan, bei dem die NetScaler Console eine Verbindung zur verwalteten NetScaler-Instanz herstellt und ein Skript an die Instanz übermittelt. Das Skript wird auf der NetScaler-Instanz ausgeführt und überprüft die Apache-Konfigurationsdatei (`httpd.conf file`) und die Parameter für maximale Clientverbindungen (`maxclient`), um festzustellen, ob eine Instanz anfällig ist oder nicht. Die Informationen, die das Skript mit der NetScaler Console teilt, sind der Schwachstellenstatus in Boolesch (wahr oder falsch). Das Skript gibt der NetScaler Console auch eine Liste der Zählungen für max_clients für verschiedene Netzwerkschnittstellen zurück, z. B. Local Host, NSIP und SNIP mit Verwaltungszugriff. Einen detaillierten Bericht dieser Liste finden Sie in der CSV-Datei, die Sie von der Registerkarte **Scan-Protokolle** auf der Seite **Security Advisory** herunterladen können.

Dieses Skript wird jedes Mal ausgeführt, wenn Ihre geplanten oder On-Demand-Scans ausgeführt werden. Nach Abschluss des Scans wird das Skript von der NetScaler-Instanz gelöscht.

CVE-2021-22956 beheben

Für von CVE-2021-22956 betroffene NetScaler-Instanzen ist die Behebung ein zweistufiger Prozess. In der GUI, unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen**, sehen Sie Schritt 1 und 2.

Schritte zur Behebung für CVE-2021-22927 und CVE-2021-22920(/en-us/netscaler-console-service/media/remediate-steps-cve-2021-22956.png)

Die beiden Schritte umfassen:

1. Aktualisieren der anfälligen NetScaler-Instanzen auf eine Version und einen Build, der den Fix enthält.
2. Anwenden der erforderlichen Konfigurationsbefehle mithilfe der anpassbaren integrierten Konfigurationsvorlage in Konfigurationsaufträgen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unter Aktuelle CVEs > NetScaler-Instanzen, die von CVEs betroffen sind, sehen Sie zwei separate Workflows für diesen zweistufigen Behebungsprozess: „Workflow für Upgrade fortsetzen“ und „Workflow für Konfigurationsauftrag fortsetzen“.

Schritt 1: Aktualisieren der anfälligen NetScaler-Instanzen

Um die anfälligen Instanzen zu aktualisieren, wählen Sie die Instanzen aus und klicken Sie auf **Workflow für Upgrade fortsetzen**. Der Upgrade-Workflow wird mit den bereits ausgefüllten anfälligen NetScaler-Instanzen geöffnet.

Weitere Informationen zur Verwendung von NetScaler Console zum Aktualisieren von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Auftrags.

HINWEIS:

Dieser Schritt kann gleichzeitig für alle anfälligen NetScaler-Instanzen durchgeführt werden.

Schritt 2: Konfigurationsbefehle anwenden

Nachdem Sie die betroffenen Instanzen aktualisiert haben, wählen Sie im Fenster `<number of>` **NetScaler-Instanzen, die von CVEs betroffen sind** die von CVE-2021-22956 betroffene Instanz aus und klicken Sie auf **Workflow für Konfigurationsauftrag fortsetzen**. Der Workflow umfasst die folgenden Schritte.

1. Anpassen der Konfiguration.
2. Überprüfen der automatisch ausgefüllten betroffenen Instanzen.
3. Angeben von Eingaben für Variablen für den Auftrag.
4. Überprüfen der endgültigen Konfiguration mit ausgefüllten Variableneingaben.
5. Ausführen des Jobs.

Beachten Sie die folgenden Punkte, bevor Sie eine Instanz auswählen und auf **Proceed to configuration job workflow** klicken:

- Für eine NetScaler-Instanz, die von mehreren CVEs betroffen ist (z. B. CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 und CVE-2021-22956): Wenn Sie die Instanz auswählen und auf **Proceed to configuration job workflow** klicken, wird die integrierte Konfigurationsvorlage nicht automatisch unter „Select configuration“ ausgefüllt. Ziehen Sie die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

entsprechende Konfigurationsjob-Vorlage unter **Security Advisory Template** manuell in den Konfigurationsjob-Bereich auf der rechten Seite.

- Für mehrere NetScaler-Instanzen, die nur von CVE-2021-22956 betroffen sind: Sie können Konfigurationsjobs auf allen Instanzen gleichzeitig ausführen. Sie haben beispielsweise NetScaler 1, NetScaler 2 und NetScaler 3, und alle sind nur von CVE-2021-22956 betroffen. Wählen Sie alle diese Instanzen aus und klicken Sie auf **Proceed to configuration job workflow**, und die integrierte Konfigurationsvorlage wird automatisch unter **Select configuration** ausgefüllt.
- Für mehrere NetScaler-Instanzen, die von CVE-2021-22956 und einem oder mehreren anderen CVEs betroffen sind (z. B. CVE-2020-8300, CVE-2021-22927 und CVE-2021-22920), und bei denen die Behebung nacheinander auf jeden NetScaler angewendet werden muss: Wenn Sie diese Instanzen auswählen und auf **Proceed to configuration job workflow** klicken, wird eine Fehlermeldung angezeigt, die Sie darauf hinweist, den Konfigurationsjob nacheinander auf jedem NetScaler auszuführen.

Schritt 1: Konfiguration auswählen

Im Konfigurationsjob-Workflow wird die integrierte Konfigurationsbasistabelle automatisch unter **Select configuration** ausgefüllt.

Schritt 2: Instanz auswählen

Die betroffene Instanz wird automatisch unter **Select Instances** ausgefüllt. Wählen Sie die Instanz aus. Wenn diese Instanz Teil eines HA-Paares ist, wählen Sie **Execute on Secondary Nodes**. Klicken Sie auf **Next**.

HINWEIS:

Für NetScaler-Instanzen im Cluster-Modus, die Sicherheitswarnungen verwenden, unterstützt die NetScaler Console das Ausführen des Konfigurationsjobs nur auf dem Cluster Configuration Coordinator (CCO)-Knoten. Führen Sie die Befehle auf Nicht-CCO-Knoten separat aus.

Schritt 3: Variablenwerte angeben

Geben Sie die Variablenwerte ein.

Variablen angeben(/en-us/netscaler-console-service/media/specify-variables-cve-2021-22956.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wählen Sie eine der folgenden Optionen, um Variablen für Ihre Instanzen anzugeben:

Gemeinsame Variablenwerte für alle Instanzen: Geben Sie einen gemeinsamen Wert für die Variable `max_client` ein.

Eingabedatei für Variablenwerte hochladen: Klicken Sie auf **Eingabeschlüsseldatei herunterladen**, um eine Eingabedatei herunterzuladen. Geben Sie in der Eingabedatei Werte für die Variable `max_client` ein und laden Sie die Datei dann auf den NetScaler Console-Server hoch.

HINWEIS:

Für beide oben genannten Optionen ist der empfohlene Wert `max_client` 30. Sie können den Wert entsprechend Ihrem aktuellen Wert festlegen. Er sollte jedoch nicht Null sein und kleiner oder gleich dem in der Datei `/etc/httpd.conf` festgelegten max_client sein. Sie können den aktuellen Wert, der in der Apache HTTP Server-Konfigurationsdatei `/etc/httpd.conf` festgelegt ist, überprüfen, indem Sie die Zeichenfolge `MaxClients` in der NetScaler-Instanz suchen.

Schritt 4: Konfiguration in der Vorschau anzeigen

Zeigt die in die Konfiguration eingefügten Variablenwerte in der Vorschau an und klicken Sie auf **Weiter**.

Auftrag in der Vorschau anzeigen(/en-us/netscaler-console-service/media/preview-job-cve-2021-22956.png)

Schritt 5: Auftrag ausführen

Klicken Sie auf **Fertig stellen**, um den Konfigurationsauftrag auszuführen.

Konfigurationsauftrag ausführen(/en-us/netscaler-console-service/media/run-job-cve-2021-22956.png)

Nachdem der Auftrag ausgeführt wurde, wird er unter **Infrastruktur > Konfiguration > Konfigurationsaufträge** angezeigt.

Nachdem Sie die beiden Korrekturschritte für alle anfälligen NetScaler-Instanzen abgeschlossen haben, können Sie einen On-Demand-Scan ausführen, um die überarbeitete Sicherheitslage zu sehen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwachstellen für CVE-2022-27509 identifizieren und beheben

Im Dashboard für Sicherheitshinweise der NetScaler Console, unter **Aktuelle CVEs** `<number of>` **NetScaler-Instanzen sind von CVEs betroffen**, können Sie alle Instanzen sehen, die aufgrund von CVE-2022-27509 anfällig sind. Um die Details der von den CVEs betroffenen Instanzen zu überprüfen, wählen Sie CVE-2022-27509 aus und klicken Sie auf **Betroffene Instanzen anzeigen**.

HINWEIS

Um den Grund für die NetScaler-Schwachstelle zu verstehen, laden Sie den CSV-Bericht auf der Registerkarte „Scan-Protokolle“ unter „Sicherheitshinweise“ herunter.

Das Fenster `<number of>` **NetScaler-Instanzen, die von CVEs betroffen sind** wird angezeigt. Im folgenden Screenshot sehen Sie die Anzahl und Details der NetScaler-Instanzen, die von CVE-2022-27509 betroffen sind.

Weitere Informationen zum Dashboard für Sicherheitshinweise finden Sie unter Sicherheitshinweise.

HINWEIS

Es kann einige Stunden dauern, bis der Scan des Sicherheitshinweissystems abgeschlossen ist und die Auswirkungen von CVE-2022-27509 im Sicherheitshinweismodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, starten Sie einen On-Demand-Scan, indem Sie auf **Jetzt scannen** klicken.

Von CVE-2022-27509 betroffene Instanzen identifizieren

CVE-2022-27509 erfordert eine Kombination aus benutzerdefiniertem Scan und Versionsscan. Im Rahmen des benutzerdefinierten Scans stellt die NetScaler Console eine Verbindung zur verwalteten NetScaler-Instanz her und überträgt ein Skript an die Instanz. Das Skript wird auf der NetScaler-Instanz ausgeführt und bestimmt, ob die Instanz anfällig ist. Dieses Skript wird jedes Mal ausgeführt, wenn Ihr geplanter oder On-Demand-Scan läuft.

Nach Abschluss des Scans wird das Skript von der NetScaler-Instanz gelöscht.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können diese benutzerdefinierten Scans für Sicherheitshinweise auch abwählen. Weitere Informationen zu den Einstellungen für benutzerdefinierte Scans und zum Abwählen benutzerdefinierter Scans finden Sie im Abschnitt **Benutzerdefinierte Scaneinstellungen konfigurieren** auf der Seite **Sicherheitshinweise**.

CVE-2022-27509 beheben

Für von CVE-2022-27509 betroffene NetScaler-Instanzen ist die Behebung ein einstufiger Prozess, und Sie müssen die anfälligen NetScaler-Instanzen auf eine Version und einen Build aktualisieren, der den Fix enthält. In der GUI, unter **Aktuelle CVEs > NetScaler-Instanzen sind von CVEs betroffen**, sehen Sie den Schritt zur Behebung.

Unter **Aktuelle CVEs> NetScaler-Instanzen, die von CVEs betroffen sind**, sehen Sie den folgenden Workflow für diesen einstufigen Behebungsprozess, der **Mit dem Upgrade-Workflow fortfahren** lautet.

Um die anfälligen Instanzen zu aktualisieren, wählen Sie die Instanzen aus und klicken Sie auf **Mit dem Upgrade-Workflow fortfahren**. Der Upgrade-Workflow wird mit den bereits ausgefüllten anfälligen NetScaler-Instanzen geöffnet.

WICHTIG

Wenn Ihre anfälligen NetScaler-Instanzen die Datei /etc/httpd.conf in das Verzeichnis / nsconfig kopiert haben, siehe Überlegungen zum Upgrade für angepasste NetScaler-Konfigurationen bevor Sie ein NetScaler-Upgrade planen.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Erstellen eines NetScaler-Upgrade-Jobs.

Nicht unterstützte CVEs im Sicherheits-Advisory

Das NetScaler Console Sicherheits-Advisory verfolgt alle neuen Common Vulnerabilities and Exposures (CVEs) und bewertet die Auswirkungen von CVEs auf die Infrastruktur. Sie können die Empfehlungen überprüfen und entsprechende Maßnahmen ergreifen. Es gibt jedoch einige CVEs, die nicht unterstützt werden, und die Erkennung und Behebung der Schwachstellen liegen außerhalb des Geltungsbereichs des NetScaler Console Sicherheits-Advisory.

- **CVE-2022-21827**:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CVE-2022-21827 betrifft das NetScaler Gateway Plug-in für Windows in unterstützten Versionen vor 21.9.1.2.

Die Erkennung und Behebung von Schwachstellen, die das NetScaler Gateway Plug-in für Windows betreffen, wird von der NetScaler Console nicht unterstützt. Auch können Schwachstellen des NetScaler Gateway Plug-ins nicht durch Überprüfungen auf NetScaler-Seite, durch Überprüfung der NetScaler-Version oder durch Überprüfung der NetScaler-Konfiguration bewertet werden. Die Erkennung und Behebung für dieses CVE kann nur basierend auf der Version des NetScaler Gateway Plug-ins für Windows bewertet werden, das auf dem Client bereitgestellt ist.

Daher liegen die Erkennung und Behebung dieser Schwachstelle außerhalb des Geltungsbereichs des NetScaler Console Sicherheits-Advisory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Einrichtung

Nachdem die Ersteinrichtung abgeschlossen ist, müssen Sie bestimmte Einstellungen konfigurieren, um die Verwaltung Ihrer Bereitstellung vollständig zu starten.

- Hinzufügen mehrerer Agenten. Die Anzahl der zu installierenden Agenten hängt von der Anzahl der verwalteten Instanzen in einem Rechenzentrum oder in der Cloud und dem Gesamtdurchsatz ab. Citrix empfiehlt, mindestens einen Agenten für jedes Rechenzentrum zu installieren.
- Hinzufügen von Instanzen. Sie können Instanzen entweder bei der erstmaligen Einrichtung der NetScaler Console (/de-de/netscaler-console-service/getting-started.html) oder zu einem späteren Zeitpunkt hinzufügen. Sie müssen Instanzen zum Dienst hinzufügen, um deren Verwaltung und Überwachung zu starten. Nachdem Sie mehrere Agenten installiert haben, müssen Sie Instanzen hinzufügen und diese den Agenten zuordnen.
- Analytics aktivieren. Um Analysedaten für Ihren Anwendungsdatenverkehr anzuzeigen, müssen Sie die Analytics-Funktion auf den virtuellen Servern aktivieren, die Datenverkehr für die spezifischen Anwendungen empfangen.
- Konfigurieren von Syslog auf Instanzen. Sie können die auf Ihren NetScaler-Instanzen generierten Syslog-Ereignisse überwachen, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Nachrichten an die NetScaler Console umgeleitet werden. Um Syslog-Ereignisse zu überwachen, müssen Sie zuerst die NetScaler Console als Syslog-Server für Ihre NetScaler-Instanz konfigurieren.
- Konfigurieren der rollenbasierten Zugriffssteuerung. NetScaler Console bietet eine detaillierte, rollenbasierte Zugriffssteuerung (RBAC), mit der Sie Zugriffsberechtigungen basierend auf den Rollen einzelner Benutzer in Ihrem Unternehmen erteilen können.
- Konfigurieren der Analytics-Einstellungen. Sie können bestimmte Einstellungen konfigurieren, um eine optimale Erfahrung mit der Analytics-Funktion zu gewährleisten. Sie können beispielsweise die Dauer angeben, für die Sie historische Analysedaten speichern möchten, und Sie können auch Schwellenwerte und Warnungen festlegen, um die gewünschten Analysemetriken zu überwachen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hinzufügen mehrerer Agents

Die Anzahl der zu installierenden Agents hängt von der Anzahl der verwalteten Instanzen in einem Rechenzentrum und dem Gesamtdurchsatz ab. Citrix empfiehlt, mindestens einen Agent für jedes Rechenzentrum zu installieren.

Sie können nur einen Agent installieren, wenn Sie sich zum ersten Mal beim Dienst anmelden. Um mehrere Agents hinzuzufügen, schließen Sie zuerst die Ersteinrichtung ab und navigieren Sie dann zu **Infrastruktur > Instanzen > Agents** und klicken Sie auf **Agent einrichten**.

Laden Sie das Image für den erforderlichen Hypervisor herunter und installieren Sie den Agent, indem Sie die Anweisungen unter Erste Schritte befolgen. Stellen Sie sicher, dass Sie die Dienst-URL und den Aktivierungscode, die auf dem Bildschirm angezeigt werden, kopieren, da Sie die Dienst-URL und den Aktivierungscode bei der Installation des Agents auf Ihrem Hypervisor eingeben müssen. Der Agent verwendet die Dienst-URL, um den Dienst zu finden, und den Aktivierungscode, um sich beim Dienst zu registrieren.

Sie können dasselbe Image verwenden, um mehrere Agents in Ihrem Hypervisor zu installieren. Sie können jedoch nicht denselben Aktivierungscode für mehrere Agents verwenden. Nachdem Sie einen Agent installiert haben, generieren Sie den Aktivierungscode für den nächsten Agent erneut. Sie können einen neuen Aktivierungscode generieren, indem Sie zu **Infrastruktur > Instanzen > Agents** navigieren und auf **Aktivierungscode generieren** klicken.

Nachdem der Agent erfolgreich installiert und registriert wurde, überprüfen Sie den Agent-Status in der Dienst-GUI und fügen Sie Instanzen hinzu.

HINWEIS

Sie können einen Agent auch in der Microsoft Azure Cloud oder AWS Cloud installieren. Das Agent-Image ist auf dem jeweiligen Cloud-Marktplatz verfügbar.

- Anweisungen zur Installation eines Agents in der Microsoft Azure Cloud finden Sie unter Installieren eines NetScaler-Agents in der Microsoft Azure Cloud.
- Anweisungen zur Installation eines Agents in AWS finden Sie unter Installieren eines NetScaler-Agents in AWS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Agenten für die Bereitstellung an mehreren Standorten konfigurieren

Agenten fungieren als Vermittler zwischen der NetScaler Console und den erkannten Instanzen in verschiedenen Rechenzentren und öffentlichen Clouds. NetScaler Console unterstützt Agenten-Failover innerhalb eines Rechenzentrums oder einer öffentlichen Cloud.

Die Installation von Agenten bietet folgende Vorteile:

- Die konfigurierten Instanzen senden die unverarbeiteten Daten direkt an den Agenten statt an die NetScaler Console. Der Agent führt die erste Ebene der Datenverarbeitung durch und sendet die verarbeiteten Daten im komprimierten Format zur Speicherung an die NetScaler Console.
- Agenten und Instanzen befinden sich im selben Rechenzentrum oder in derselben Cloud, sodass die Datenverarbeitung schneller erfolgt.
- Das Clustering der Agenten ermöglicht eine Neuverteilung der NetScaler-Instanzen bei Agenten-Failover. Wenn ein Agent an einem Standort ausfällt, wechselt der Datenverkehr von NetScaler-Instanzen zu einem anderen verfügbaren Agenten am selben Standort.

Architektur

Die folgende Abbildung zeigt NetScaler-Instanzen, die auf mehreren Agenten in einem Rechenzentrum und einer öffentlichen Cloud konfiguriert sind, um Agenten-Failover zu erreichen:

Die öffentliche Cloud verfügt über vier NetScaler-Instanzen und zwei Agenten. Das Unternehmensrechenzentrum verfügt ebenfalls über vier NetScaler-Instanzen und zwei Agenten. Jeder Agent ist mit zwei NetScaler-Instanzen konfiguriert.

Die Agenten empfangen Daten direkt von den konfigurierten Instanzen. Nachdem der Agent die Daten empfangen hat, verarbeitet er sie und sendet sie in einem komprimierten Format an die NetScaler Console. Agenten kommunizieren über einen sicheren Kanal mit dem NetScaler Console-Server.

In der öffentlichen Cloud tritt ein Agenten-Failover auf, wenn **Agent 1** inaktiv wird (DOWN-Status). Die NetScaler Console verteilt die NetScaler-Instanzen von **Agent 1** auf **Agent 2** neu. Die Instanz-Neuverteilung erfolgt in einem Unternehmensrechenzentrum, wenn einer der Agenten im Rechenzentrum ausfällt.

Informationen zur Installation eines Agenten finden Sie unter Einen NetScaler-Agenten installieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Agenten-Failover

Das Agenten-Failover kann an einem Standort auftreten, der zwei oder mehr registrierte Agenten hat. Wenn ein Agent an diesem Standort inaktiv wird (DOWN-Status), verteilt die NetScaler Console die NetScaler-Instanzen des inaktiven Agenten auf andere aktive Agenten um.

WICHTIG

- Agent-Failover berücksichtigt keine CPX-Instanzen.
- Stellen Sie sicher, dass die Agent-Failover-Funktion in Ihrem Konto aktiviert ist. Informationen zum Aktivieren dieser Funktion finden Sie unter NetScaler Console-Funktionen aktivieren oder deaktivieren.
- Wenn ein Agent ein Skript ausführt, stellen Sie sicher, dass dieses Skript auf allen Agenten am Standort vorhanden ist. Daher kann der geänderte Agent das Skript nach dem Agent-Failover ausführen.

So weisen Sie einem Agenten in der NetScaler Console-GUI einen Standort zu:

1. Navigieren Sie zu **Infrastruktur > Instanzen > Agenten**.
2. Wählen Sie einen Agenten aus, den Sie einem Standort zuweisen möchten.
3. Geben Sie den Standort aus der Liste an. Wenn Sie einen neuen Standort hinzufügen möchten, klicken Sie auf **Hinzufügen**.
4. Klicken Sie auf **Speichern**.

Um ein Agent-Failover zu erreichen, wählen Sie die Agenten einzeln aus und weisen Sie sie demselben Standort zu.

Beispielsweise sind zwei Agenten 10.106.1xx.2x und 10.106.1xx.7x am Standort Bangalore zugewiesen und betriebsbereit. Wenn ein Agent inaktiv wird, erkennt NetScaler Console dies und zeigt den Status als „Down“ an.

Wenn ein Agent an einem Standort inaktiv wird (Status „Down“), wartet NetScaler Console einige Minuten, bis der Agent aktiv wird (Status „Up“). Bleibt der Agent inaktiv, verteilt NetScaler Console die Instanzen automatisch auf die verfügbaren Agenten am selben Standort. Diese Umverteilung kann etwa 10-15 Minuten dauern.

NetScaler Console löst alle 30 Minuten eine Instanzumverteilung aus, um die Last unter den aktiven Agenten am Standort auszugleichen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Instanzen werden Agenten am selben Standort für Trap-Ziel, Syslog-Server und Analysen zugewiesen und automatisch neu konfiguriert.

Agent-Upgrade-Einstellungen konfigurieren

In NetScaler Console werden Agents, die auf Softwareversion 12.0 Build 507.110 und höher ausgeführt werden, von NetScaler Console automatisch auf neuere und empfohlene Versionen aktualisiert. Der Agent wird entweder aktualisiert, wenn eine neue Version verfügbar ist, oder zu einem von Ihnen festgelegten Zeitpunkt.

Sie können die aktuelle Version und die empfohlene Version Ihrer Agents anzeigen, indem Sie zu **Infrastructure > Instances > Agents** navigieren.

Standardmäßig wird ein Agent automatisch aktualisiert, wenn eine neuere Version verfügbar ist. Sie können jedoch ein Upgrade für jeden der Agents planen.

Während des Upgrades kann es zu einer Ausfallzeit von etwa fünf Minuten kommen.

So konfigurieren Sie die Agent-Upgrade-Einstellungen:

1. Navigieren Sie zu **Infrastructure > Instances > Agents**, klicken Sie auf **Settings**.

2. Geben Sie an, wann das Upgrade für jeden Agenten beginnen soll.

   Sie können eine der folgenden Optionen verwenden, um den Agenten zu aktualisieren:

   - Automatisiertes Upgrade – Wählen Sie **Auto-Upgrade**, damit der Agent aktualisiert wird, wenn ein neues Agent-Image verfügbar ist. Wenn Sie keinen Wert eingeben, ist **Auto-Upgrade** standardmäßig ausgewählt.
   - Legen Sie eine bestimmte Zeit fest: Geben Sie die Uhrzeit (im Format hh:mm) ein und wählen Sie die Zeitzone aus, zu der NetScaler Console den Agenten automatisch aktualisieren soll.

   Sie können auf **Copy to All** klicken, um dieselbe Upgrade-Zeit auf alle Agents anzuwenden.

3. Klicken Sie auf **Save**.

   Diese Einstellungen bleiben für zukünftige Agent-Upgrades bestehen, bis Sie die Einstellungen ändern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Agent manuell aktualisieren

In einigen Szenarien werden die Agents möglicherweise nicht automatisch aktualisiert und laufen weiterhin auf einer älteren Version. In solchen Szenarien müssen Sie den Agent manuell aktualisieren. Sie können überprüfen, ob der Agent auf der neuesten Version läuft, indem Sie zu **Infrastructure > Instances > Agents** navigieren und den Build unter **Version** überprüfen. Wenn Sie ein Download-Symbol sehen, läuft der Agent auf einer älteren Version.

So aktualisieren Sie den externen Agent manuell:

1. Laden Sie unter **Infrastructure > Instances > Agents** den neuesten Build herunter, indem Sie auf das Download-Symbol klicken, das in der Version verfügbar ist.
2. Kopieren Sie das Agent-Paket (`build-masagent.tgz`) mit einem FTP-Client an den `/var/mps/mps_agent_images/latest` Speicherort des Agents.
3. Melden Sie sich mit einem SSH-Client beim NetScaler-Agent an.
4. Entpacken Sie das Agent-Paket.

   `cd /var/mps/mps_agent_images/latest`

   `tar -xzvf build-masagent.tgz`
5. Führen Sie `./installmasagent` aus

Der Installationsvorgang beginnt, und der Agent wird nach Abschluss des Upgrades neu gestartet.

So aktualisieren Sie den integrierten Agent manuell:

Navigieren Sie zu **Infrastructure > Instances > NetScaler** und scrollen Sie nach rechts, um die **Build-in agent version** anzuzeigen. Wenn Sie ein Download-Symbol sehen, läuft der Agent auf einer älteren Version.

1. Unter **Infrastructure > Instances > NetScaler** laden Sie den neuesten Build herunter, indem Sie auf das Download-Symbol klicken, das in der Version verfügbar ist.
2. Kopieren Sie mit einem FTP-Client das mastools-Paket an den Speicherort `/var/mastools directory`.
3. Melden Sie sich mithilfe eines SSH-Clients bei NetScaler an.
4. Führen Sie `/var/mastools/scripts/mastoolsd stop` aus.
5. Führen Sie `tar xvzf <package_name_with_path> -C /var/mastools` aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Sie müssen `package_name_with_path` durch den genauen Pfad Ihres Paketspeicherorts ersetzen.

6. Führen Sie `/bin/sh /var/mastools/scripts/admautoreg/admautoregd_ctl restart_if_running` aus.
7. Führen Sie `/var/mastools/scripts/mastoolsd restart` aus.

Dual-NIC-Unterstützung auf NetScaler Console

Sie können zwei NICs auf einem Agent konfigurieren. Mit der Dual-NIC-Architektur kann der Agent Folgendes tun:

- Kommunikation zwischen dem Agent und NetScaler-Instanzen herstellen – Sie können die erste NIC verwenden, um den über die NetScaler Console empfangenen und gesendeten Datenverkehr zu isolieren und auch, um zwischen der NetScaler Console und ihren verwalteten NetScaler-Instanzen in einem anderen Netzwerk zu kommunizieren.
- Kommunikation zwischen dem Agent und der NetScaler Console herstellen – Sie können die zweite NIC verwenden, um die NetScaler Console, die sich in einem Netzwerk befindet, zu verwalten und administrative Aufgaben auszuführen.

HINWEIS

Sie können die Funktionalität und Konfiguration beider NICs nicht austauschen.

In diesem Szenario können Sie als Administrator Folgendes tun:

- IP-Adresse für den Datenverkehr zwischen NetScaler Console und ihren verwalteten NetScaler-Instanzen konfigurieren.
- IP-Adresse für die Verwaltung der NetScaler Console-Software konfigurieren, um alle administrativen Aufgaben in der Software auszuführen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Es ist nicht zwingend erforderlich, Dual-NICs für einen Agent zu konfigurieren. Dies ist optional und nur erforderlich, wenn der Datenverkehr zwischen Agent, NetScaler Console-Dienst und NetScaler-Instanzen getrennt werden muss.

Voraussetzungen

- Stellen Sie sicher, dass Sie den NetScaler-Agent auf dem Hypervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM oder VMware ESXi) bereitgestellt und konfiguriert haben.
- Stellen Sie sicher, dass Sie die zweite NIC auf dem Hypervisor (Citrix Hypervisor™, Microsoft Hyper-V, Linux KVM oder VMware ESXi) hinzugefügt haben.

Informationen zum Zuweisen einer IP-Adresse zu einer NIC auf einem Citrix Hypervisor und zum Erstellen einer sekundären Schnittstelle finden Sie unter Zuweisen einer IP-Adresse zu einer NIC.

IPV4-NIC-Netzwerkadressen ändern

1. Öffnen Sie eine SSH-Verbindung zur NetScaler-Agent-Konsole mit einem SSH-Client wie PuTTY.
2. Melden Sie sich mit den Anmeldeinformationen **nsrecover/nsroot** an und wechseln Sie zur Shell-Eingabeaufforderung.
3. Führen Sie den Befehl **ifconfig** aus. Sie sehen die Details der beiden NICs, die Sie konfiguriert haben -

   - NIC 1 – Für die Kommunikation zwischen Agent und NetScaler Communication
   - NIC 2 – Für die Kommunikation zwischen Agent und NetScaler Console

   ☐
4. Führen Sie den Befehl **networkconfig** aus. Es erscheint ein Menü, mit dem Sie die IPV4-Netzwerkadressen festlegen oder ändern können.

   ☐

   HINWEIS:

   Die Netzwerkadresse der zweiten NIC kann mehrere IP-Werte annehmen.
5. Wählen Sie einen Menüpunkt zum Ändern aus. Speichern und beenden Sie die Einstellungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instanzen hinzufügen

Sie können Instanzen entweder bei der erstmaligen Einrichtung der NetScaler Console (/de-de/netscaler-console-service/getting-started.html) oder später hinzufügen.

Instanzen sind NetScaler-Appliances oder virtuelle Appliances, die Sie über NetScaler Console erkennen, verwalten und überwachen möchten. Sie können die folgenden NetScaler-Appliances und virtuellen Appliances zu NetScaler Console hinzufügen:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway
- Citrix Secure Web Gateway™

Um Instanzen hinzuzufügen, müssen Sie entweder den Hostnamen oder die IP-Adresse jeder NetScaler-Instanz oder einen Bereich von IP-Adressen angeben.

Geben Sie ein Instanzprofil an, das NetScaler Console für den Zugriff auf die Instanz verwenden kann. Dieses Instanzprofil enthält den Benutzernamen und das Kennwort der Instanzen, die Sie dem Dienst hinzufügen möchten. Für jeden Instanztyp ist ein Standardprofil verfügbar. Zum Beispiel ist das ns-root-profile das Standardprofil für NetScaler-Instanzen. Die Standard-Administratoranmeldeinformationen von NetScaler definieren dieses Profil. Wenn Sie die Standard-Administratoranmeldeinformationen Ihrer Instanzen geändert haben, können Sie benutzerdefinierte Instanzprofile für diese Instanzen definieren. Wenn Sie die Anmeldeinformationen einer Instanz ändern, nachdem die Instanz erkannt wurde, müssen Sie das Instanzprofil bearbeiten oder ein Profil erstellen und die Instanz dann erneut erkennen.

Sie können nach dem Hinzufügen der Instanzen in der NetScaler Console auf die GUIs der NetScaler-Instanzen über die NetScaler Console zugreifen. Um von der NetScaler Console auf die NetScaler-Instanzen zuzugreifen, müssen Sie mit dem Citrix-Netzwerk verbunden sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

- Um in einem Cluster konfigurierte NetScaler-Instanzen hinzuzufügen, müssen Sie entweder die Cluster-IP-Adresse oder einen der einzelnen Knoten in der Cluster-Einrichtung angeben. In der NetScaler Console repräsentiert die Cluster-IP-Adresse jedoch den Cluster.
- Bei NetScaler-Instanzen, die als HA-Paar eingerichtet sind, wird die andere Instanz im Paar automatisch hinzugefügt, wenn Sie eine Instanz hinzufügen.
- Um sicherzustellen, dass der NetScaler-Benutzer alle Berechtigungen besitzt, weisen Sie dem Benutzer in NetScaler Superuser-Berechtigungen zu. Weitere Informationen finden Sie unter Benutzer, Benutzergruppen und Befehlsrichtlinien

So erstellen Sie ein NetScaler®-Profil

Ein NetScaler-Profil enthält den Benutzernamen, das Kennwort, die Kommunikationsports und die Authentifizierungstypen der Instanzen, die Sie NetScaler Console hinzufügen möchten. Für jeden Instanztyp ist ein Standardprofil verfügbar. Zum Beispiel ist `nsroot` das Standardprofil für NetScaler-Instanzen. Das Standardprofil wird unter Verwendung der Standard-NetScaler-Administratoranmeldeinformationen definiert. Wenn Sie die Standard-Administratoranmeldeinformationen Ihrer Instanzen geändert haben, können Sie benutzerdefinierte Instanzprofile für diese Instanzen definieren. Wenn Sie die Anmeldeinformationen einer Instanz ändern, nachdem die Instanz erkannt wurde, müssen Sie das Instanzprofil bearbeiten oder ein Profil erstellen und die Instanz dann erneut erkennen.

Sie können ein NetScaler-Profil auf der Seite **Instanz** oder beim Hinzufügen oder Ändern einer Instanz erstellen.

HINWEIS:

Stellen Sie sicher, dass Sie das Superadministrator-Konto verwenden, um ein Instanzprofil zu erstellen.

So erstellen Sie ein NetScaler-Profil auf der Seite „Instanz“:

1. Navigieren Sie zu **Infrastruktur > Instanzen**.
2. Wählen Sie eine Instanz aus. Zum Beispiel NetScaler.
3. Wählen Sie auf der NetScaler-Seite unter **Aktion auswählen** die Option **Profile** aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Wählen Sie auf der Seite **Admin-Profile** die Option **Hinzufügen**.
5. Führen Sie auf der Seite **NetScaler-Profil erstellen** die folgenden Schritte aus:

   a. **Profilname**: Geben Sie einen Profilnamen für die NetScaler-Instanz an.

   b. **Benutzername**: Geben Sie einen Benutzernamen an, um sich bei der NetScaler-Instanz anzumelden.

   c. **Passwort**: Geben Sie ein Passwort an, um sich bei der NetScaler-Instanz anzumelden.

   d. **SSH-Port**: Geben Sie den Port für die SSH-Kommunikation zwischen NetScaler Console und der NetScaler-Instanz an.

   e. **HTTP-Port**: Geben Sie den Port für die HTTP-Kommunikation zwischen NetScaler Console und der NetScaler-Instanz an.

   HINWEIS:

   Der Standard-HTTP-Port ist 80. Sie können auch den nicht standardmäßigen oder angepassten HTTP-Port angeben, den Sie in Ihrer NetScaler CPX-Instanz konfiguriert haben. Der angepasste HTTP-Port kann nur für die Kommunikation zwischen NetScaler Console und NetScaler CPX verwendet werden.

   f. **HTTPS-Port**: Geben Sie den Port für die HTTPS-Kommunikation zwischen NetScaler Console und der NetScaler-Instanz an.

   HINWEIS:

   Der Standard-HTTPS-Port ist 443. Sie können auch den nicht standardmäßigen oder angepassten HTTPS-Port angeben, den Sie in Ihrer NetScaler CPX-Instanz konfiguriert haben. Der angepasste HTTPS-Port kann nur für die Kommunikation zwischen NetScaler Console und NetScaler CPX verwendet werden.

   g. **Globale Einstellungen für die NetScaler-Kommunikation verwenden**: Wählen Sie diese Option, wenn Sie die Systemeinstellungen für die Kommunikation zwischen NetScaler Console und der NetScaler-Instanz verwenden möchten, andernfalls wählen Sie entweder HTTP oder HTTPS.

   h. **SNMP-Version**: Wählen Sie entweder **SNMPv2** oder **SNMPv3** und gehen Sie wie folgt vor:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. Wenn Sie SNMPv2 auswählen, geben Sie den **Community**-Namen für die Authentifizierung an.

ii. Wenn Sie SNMPv3 auswählen, geben Sie den **Sicherheitsnamen** und die **Sicherheitsstufe** an. Wählen Sie basierend auf der Sicherheitsstufe den **Authentifizierungstyp** und den **Datenschutztyp** aus.

> **HINWEIS:**
>
> Für NetScaler SDX wird nur **SNMPv2** unterstützt.

i. **Timeout-Einstellungen**: Geben Sie die Zeit an, die NetScaler Console warten muss, bevor eine Verbindungsanfrage an die NetScaler-Instanz nach einem Neustart gesendet wird.

j. Wählen Sie **Erstellen**.

So fügen Sie eine NetScaler-Instanz zu NetScaler Console hinzu

> **HINWEIS**
>
> Führen Sie diese Aufgabe aus, um alle anderen NetScaler-Instanzen außer der NetScaler CPX-Instanz hinzuzufügen.

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler**. Wählen Sie unter **Instances** den Typ der Instanz aus, die Sie hinzufügen möchten (z. B. NetScaler VPX), und klicken Sie auf **Hinzufügen**.
2. Wählen Sie eine der folgenden Optionen aus:

   - **Geräte-IP-Adresse eingeben** – Geben Sie für NetScaler-Instanzen eine der folgenden Optionen an:

     - Hostname
     - IP-Adresse oder NAT-IP jeder NetScaler-Instanz
     - Bereich von IP-Adressen

     Geben Sie beispielsweise einen oder mehrere Hostnamen, IP-Adressen oder NAT-IPs und/oder einen Bereich von IP-Adressen (z. B. 10.10.20.10-10.10.20.45) durch Kommas getrennt ein. Das Eingabeformat für die Erkennung von NAT-HA-Instanzen ist 10.10.20.10#10.10.20.32 (NAT-IP-Adresse beider NetScaler HA-Instanzen).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Aus Datei importieren** – Laden Sie von Ihrem lokalen System eine Textdatei hoch, die die IP-Adressen aller Instanzen enthält, die Sie hinzufügen möchten.

3. (Optional) Wählen Sie **Gerätehinzufügung bei erstmaligem Anmeldefehler aktivieren**. Mit dieser Option können Sie die Instanz auch ohne gültige Anmeldeinformationen hinzufügen.
4. Wählen Sie unter **Profilname** das entsprechende Instanzprofil aus, oder erstellen Sie ein Profil, indem Sie auf das **+**-Symbol klicken.
5. Wählen Sie unter **Site** den Standort aus, an dem die Instanz hinzugefügt werden soll.
6. Wählen Sie unter **Agent** den Agenten aus, dem Sie die Instanzen zuordnen möchten, und klicken Sie dann auf **OK**.

   Wenn in Ihrer NetScaler Console nur ein Agent konfiguriert ist, wird dieser Agent standardmäßig ausgewählt.

So fügen Sie eine NetScaler CPX-Instanz in NetScaler Console hinzu

1. Navigieren Sie zu **Infrastructure > Instances**. Wählen Sie unter **Instances** die Option **NetScaler** und dann die Registerkarte CPX aus.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie eine der folgenden Optionen aus:

   - **Geräte-IP-Adresse eingeben**. Geben Sie entweder den Hostnamen oder die IP-Adresse jeder Instanz oder einen Bereich von IP-Adressen an.
   - **Aus Datei importieren**. Laden Sie von Ihrem lokalen System eine Textdatei hoch, die die IP-Adressen aller Instanzen enthält, die Sie hinzufügen möchten.

4. (Optional) Wählen Sie **Gerätehinzufügung bei erstmaligem Anmeldefehler aktivieren**. Mit dieser Option können Sie die Instanz auch ohne gültige Anmeldeinformationen hinzufügen.
5. Geben Sie im Feld **Routable IP/Docker IP** die IP-Adresse ein. Die IP-Adresse kann entweder die NetScaler CPX-Instanz (sofern erreichbar) oder der Docker-Host sein.
6. Wählen Sie im Feld **Profilname** das entsprechende Instanzprofil aus, oder erstellen Sie ein Profil, indem Sie auf das +-Symbol klicken.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Wenn Sie ein Profil erstellen, stellen Sie sicher, dass Sie die HTTP-, HTTPS-, SSH- und SNMP-Portdetails des Hosts angeben. Sie können auch den Bereich der Ports angeben, die vom Host im Feld Startport und Anzahl der Ports veröffentlicht werden.

7. Wählen Sie optional den Standort aus, an dem Sie die CPX-Instanz bereitstellen möchten. Sie können auch einen Standort erstellen, indem Sie auf **Hinzufügen** klicken.
8. Wählen Sie, falls verfügbar, den Agenten aus der Liste der Agenten aus.
9. Klicken Sie auf **OK**, um den Prozess des Hinzufügens von Instanzen zur NetScaler Console zu starten.

HINWEIS

Wenn Sie eine Instanz erneut ermitteln möchten, führen Sie die folgenden Schritte aus:

a. Navigieren Sie zu **Infrastructure > Instances > NetScaler** > **CPX**.
b. Wählen Sie die Instanz aus, die Sie erneut ermitteln möchten.
c. Klicken Sie in der Liste **Aktion auswählen** auf **Erneut ermitteln**.

So fügen Sie eine eigenständige NetScaler BLX-Instanz in NetScaler Console hinzu

Eine eigenständige NetScaler BLX-Instanz ist eine einzelne Instanz, die auf dem dedizierten Host-Linux-Server ausgeführt wird.

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler**.
2. Klicken Sie auf der Registerkarte **BLX** auf **Hinzufügen**.
3. (Optional) Wählen Sie **Gerätehinzufügung bei erstmaligem Anmeldefehler aktivieren**. Mit dieser Option können Sie die Instanz auch ohne gültige Anmeldeinformationen hinzufügen.
4. Wählen Sie die Option **Eigenständig** aus der Liste **Instanztyp** aus.
5. Geben Sie im Feld **IP-Adresse** die IP-Adresse der BLX-Instanz an.
6. Geben Sie im Feld **Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die BLX-Instanz gehostet wird.
7. Wählen Sie in der Liste **Profilname** das entsprechende Profil für eine BLX-Instanz aus, oder erstellen Sie ein Profil.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Um ein Profil zu erstellen, klicken Sie auf **Hinzufügen**.

WICHTIG

Stellen Sie sicher, dass Sie den korrekten Host-Benutzernamen und das Passwort des Linux-Servers im Profil angegeben haben.

8. Wählen Sie in der Liste **Site** die Site aus, der Sie eine Instanz hinzufügen möchten.

   Wenn Sie eine Site hinzufügen möchten, klicken Sie auf **Hinzufügen**.

9. Wählen Sie in der Liste **Agent** den Agenten aus, dem Sie die Instanz zuordnen möchten.

   Wenn nur ein Agent auf Ihrer NetScaler Console konfiguriert ist, wird dieser Agent standardmäßig ausgewählt.

10. Klicken Sie auf **OK**.

So fügen Sie hochverfügbare NetScaler BLX-Instanzen in NetScaler Console hinzu

Die hochverfügbaren NetScaler BLX-Instanzen, die auf verschiedenen Host-Linux-Servern ausgeführt werden. Ein Linux-Server kann nicht mehr als eine BLX-Instanz hosten.

1. Klicken Sie auf der Registerkarte **BLX** auf **Hinzufügen**.
2. (Optional) Wählen Sie **Gerätehinzufügung bei erstmaligem Anmeldefehler aktivieren**. Mit dieser Option können Sie die Instanz auch ohne gültige Anmeldeinformationen hinzufügen.
3. Wählen Sie die Option **Hochverfügbarkeit** aus der Liste **Instanztyp**.
4. Geben Sie im Feld **IP-Adresse** die IP-Adresse der BLX-Instanz an.
5. Geben Sie im Feld **Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die BLX-Instanz gehostet wird.
6. Geben Sie im Feld **Peer-IP-Adresse** die IP-Adresse der Peer-BLX-Instanz an.
7. Geben Sie im Feld **Peer-Host-IP-Adresse** die IP-Adresse des Linux-Servers an, auf dem die Peer-BLX-Instanz gehostet wird.
8. Wählen Sie in der Liste **Profilname** das entsprechende Profil für eine BLX-Instanz aus oder erstellen Sie ein Profil.

   Um ein Profil zu erstellen, klicken Sie auf **Hinzufügen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG

Stellen Sie sicher, dass Sie den korrekten Host-Benutzernamen und das Passwort des Linux-Servers im Profil angegeben haben.

9. Wählen Sie in der Liste **Site** die Site aus, der Sie eine Instanz hinzufügen möchten.

   Wenn Sie eine Site hinzufügen möchten, klicken Sie auf **Hinzufügen**.

10. Wählen Sie in der Liste **Agent** den Agenten aus, dem Sie die Instanz zuordnen möchten.

    Wenn nur ein Agent in Ihrer NetScaler Console konfiguriert ist, wird dieser Agent standardmäßig ausgewählt.

11. Klicken Sie auf **OK**.

So greifen Sie über die NetScaler Console auf eine Instanz-GUI zu

1. Navigieren Sie zu **Infrastructure > Instances** > **NetScaler**.
2. Wählen Sie den Instanztyp aus, auf den Sie zugreifen möchten (z. B. VPX, MPX, CPX, SDX oder BLX).
3. Klicken Sie auf die erforderliche NetScaler IP-Adresse oder den Hostnamen.

Die Instanz-IP-Adressen geben den Bereitstellungstyp mit den folgenden Notationen an:

- Bei Hochverfügbarkeitspaaren: **P** – Primärserver und **S** – Sekundärserver.
- **C**-Cluster
- **A**-Autoscale™-Gruppe

Wenn eine Instanz keine Notation hat, handelt es sich um eine eigenständige Bereitstellung.

Die GUI der ausgewählten Instanz wird in einem Pop-up-Fenster angezeigt.

Instanzwarnungen beheben

Ein Warnzeichen erscheint auf der Instanz aus folgenden Gründen:

- **Anmeldung fehlgeschlagen** – Wenn Sie eine Instanz ohne gültige Anmeldeinformationen hinzufügen, wird sie im Status DOWN mit der Warnung „Anmeldung fehlgeschlagen“

© 1997–2026 Citrix Systems, Inc. All rights reserved.

angezeigt. Geben Sie die korrekten Anmeldeinformationen an, um die Instanz in der NetScaler Console zu verwalten.

Wenn die Instanz nicht lizenziert ist, erscheint die Option **Lizenz**, wenn Sie die Instanz auswählen. Klicken Sie auf **Lizenz**, um die Lizenz aus dem Lizenzpool auf eine Instanz anzuwenden.

- **Nicht lizenzierte Instanz mit HTTPS-Profil** – Wenn eine nicht lizenzierte Instanz nur eine HTTPS-Verbindung verwendet, wenden Sie die Lizenz über die NetScaler GUI auf eine Instanz an.

Konfigurieren von Syslog auf Instanzen

Das Syslog-Protokoll bietet einen Transport, der es den NetScaler-Instanzen ermöglicht, Ereignisbenachrichtigungen an die NetScaler Console zu senden, die als Collector oder Syslog-Server für diese Nachrichten konfiguriert ist.

Sie können die auf Ihren NetScaler-Instanzen generierten Syslog-Ereignisse überwachen, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Nachrichten an die NetScaler Console umgeleitet werden. Um Syslog-Ereignisse zu überwachen, müssen Sie zunächst die NetScaler Console als Syslog-Server für Ihre NetScaler-Instanz konfigurieren. Nachdem die Instanz konfiguriert wurde, werden alle Syslog-Nachrichten an die NetScaler Console umgeleitet, sodass diese Protokolle dem Benutzer strukturiert angezeigt werden können.

Syslog verwendet das User Datagram Protocol (UDP), Port 514, für die Kommunikation, und da UDP ein verbindungsloses Protokoll ist, sendet es keine Bestätigung an die Instanzen zurück. Die Syslog-Paketgröße ist auf 1024 Byte begrenzt und enthält die folgenden Informationen:

- Einrichtung
- Schweregrad
- Hostname
- Zeitstempel
- Nachricht

In der NetScaler Console müssen Sie die Einrichtung und die Protokollschweregrade auf den Instanzen konfigurieren.

- **Einrichtung** – Syslog-Nachrichten werden grob nach den Quellen kategorisiert, die sie generieren. Diese Quellen können das Betriebssystem, der Prozess oder eine Anwendung sein. Diese Kategorien werden als Einrichtungen bezeichnet und durch ganze Zahlen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

dargestellt. Zum Beispiel wird 0 für Kernel-Nachrichten verwendet, 1 für Nachrichten auf Benutzerebene, 2 für das Mailsystem und so weiter. Die lokalen Einrichtungen (von local0 bis local7) sind nicht reserviert und stehen zur allgemeinen Verwendung zur Verfügung. Daher können Prozesse und Anwendungen, die keine vorab zugewiesenen Einrichtungswerte haben, an eine der acht lokalen Einrichtungen geleitet werden.

- **Schweregrad** – Die Quelle oder Einrichtung, die die Syslog-Nachricht generiert, gibt auch den Schweregrad der Nachricht mit einer einstelligen ganzen Zahl an, wie unten gezeigt:

```
1 - Emergency: System is unusable.


2 - Alert: Action must be taken immediately.


3 - Critical: Critical conditions.


4 - Error: Error conditions.


5 - Warning: Warning conditions.


6 - Notice: Normal but significant condition.


7 - Informational: Informational messages.


8 - Debug: Debug-level messages.
```

So konfigurieren Sie Syslog auf NetScaler-Instanzen:

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > Instanzen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Wählen Sie die NetScaler-Instanz aus, von der die Syslog-Nachrichten gesammelt und in der NetScaler Console angezeigt werden sollen.
3. Wählen Sie in der Dropdown-Liste **Aktion** die Option **Syslog konfigurieren**.
4. Klicken Sie auf **Aktivieren**.
5. Wählen Sie in der Dropdown-Liste **Facility** eine lokale oder benutzerdefinierte Facility aus.
6. Wählen Sie die erforderliche Protokollstufe für die Syslog-Meldungen.
7. Klicken Sie auf **OK**.

Dadurch werden alle Syslog-Befehle in der NetScaler-Instanz konfiguriert, und NetScaler Console beginnt, die Syslog-Meldungen zu empfangen. Sie können die Meldungen anzeigen, indem Sie zu **Infrastruktur > Ereignisse > Syslog-Meldungen** navigieren.

Logstream-Übersicht

NetScaler-Instanzen generieren AppFlow-Datensätze und sind ein zentraler Kontrollpunkt für den gesamten Anwendungsdatenverkehr im Rechenzentrum. **IPFIX** und **Logstream** sind die Protokolle, die diese AppFlow-Datensätze von NetScaler-Instanzen an NetScaler Console übertragen. Weitere Informationen finden Sie unter AppFlow.

- **IPFIX** ist ein offener Standard der Internet Engineering Task Force (IETF), der in RFC 5101 definiert ist. **IPFIX** verwendet das UDP-Protokoll, ein unzuverlässiges Transportprotokoll, das für den Datenfluss in eine Richtung verwendet wird. Da IPFIX das UDP-Protokoll verwendet, führt die Einhaltung des IPFIX-Standards zu einem höheren Ressourcenverbrauch in NetScaler Console.
- **Logstream** ist ein Citrix-eigenes Protokoll, das als einer der Transportmodi verwendet wird, um die Analyse-Protokolldaten effizient von NetScaler-Instanzen an NetScaler Console zu übertragen. **Logstream** verwendet das zuverlässige TCP-Protokoll und benötigt weniger Ressourcen bei der Verarbeitung der Daten.

Für NetScaler zwischen **11.1 Build 47.14 und 11.1 Build 62.8** ist **Logstream** der Standard-Transportmodus zum Aktivieren von Web Insight (HTTP), und IPFIX ist der einzige Transportmodus zum Aktivieren anderer Insights. Für NetScaler-Versionen ab **12.0 bis zur neuesten Version** können Sie entweder **Logstream** oder **IPFIX** als Transportmodus auswählen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Die Version und der Build von NetScaler Console müssen **gleich oder höher** sein als die Version und der Build Ihres NetScaler. Wenn Sie beispielsweise NetScaler 12.1 Build 50.28/50.31 installiert haben, stellen Sie sicher, dass Sie NetScaler Console 12.1 Build 50.39 oder höher installiert haben.

Logstream als Transportmodus aktivieren

1. Navigieren Sie zu **Infrastruktur > Instanzen**, und wählen Sie die NetScaler-Instanz aus, für die Sie Analysen aktivieren möchten.
2. Wählen Sie aus der Liste **Aktion auswählen** die Option **Analysen konfigurieren** aus.

3. Wählen Sie die virtuellen Server aus und klicken Sie dann auf **Sicherheit & Analysen aktivieren**.

4. Im Fenster **Sicherheit & Analysen aktivieren**:

   a. Wählen Sie die Insight-Typen aus (Web Insight oder WAF-Sicherheitsverletzungen oder Bot-Sicherheitsverletzungen)

   b. Wählen Sie **Logstream** als Transportmodus

   HINWEIS

   Für NetScaler zwischen **11.1 Build 47.14 und 11.1 Build 62.8** ist **Logstream** der Standardtransportmodus zum Aktivieren von Web Insight (HTTP), und IPFIX ist der einzige Transportmodus zum Aktivieren anderer Insights. Für NetScaler-Versionen ab **12.0 bis zur neuesten Version** können Sie entweder **Logstream** oder **IPFIX** als Transportmodus auswählen.

   c. Der Ausdruck ist standardmäßig wahr

   d. Klicken Sie auf **Analysen speichern**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

- Für Administratorpartitionen wird nur **Web Insight** unterstützt
- Für virtuelle Server wie Cache-Umleitung, Authentifizierung und GSLB können Sie keine Analysen aktivieren. Eine Fehlermeldung wird angezeigt.

Die folgende Tabelle beschreibt die Funktionen von NetScaler Console, die **Logstream** als Transportmodus unterstützen:

FUNKTION	IPFIX	LOGSTREAM
Web Insight	•	•
Bot-Sicherheitsverletzungen	Nicht unterstützt	•
WAF-Sicherheitsverletzungen	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Nicht unterstützt	•
CR Insight	•	•
IP-Reputation	•	•
AppFirewall	•	•
Client-seitige Messung	•	•
Syslog/Auditlog	•	•

So weisen Sie delegierten Administratorbenutzern weitere Berechtigungen zu

Wenn der erste Benutzer Ihrer Organisation sich bei NetScaler Console anmeldet, werden diesem Benutzer die Super-Admin-Berechtigungen zugewiesen. Jeder nachfolgende Benutzer, der sich anmeldet, erhält standardmäßig eine delegierte Administratorrolle. Ein delegierter Administrator hat

© 1997–2026 Citrix Systems, Inc. All rights reserved.

keine Berechtigung, Aufgaben im Zusammenhang mit der Benutzerverwaltung oder RBAC-Einstellungen anzuzeigen und auszuführen.

Sie können einem delegierten Administrator jedoch Super-Admin-Berechtigungen oder bestimmte Nicht-Super-Admin-Rollen zuweisen, damit der Administrator Aufgaben im Zusammenhang mit der Benutzerverwaltung ausführen kann.

Detaillierte Informationen zur rollenbasierten Zugriffssteuerung finden Sie unter Konfigurieren der rollenbasierten Zugriffssteuerung.

Zuweisen von Super-Admin-Berechtigungen zu einem delegierten Administrator

Um einem delegierten Administrator Super-Admin-Berechtigungen zuzuweisen, muss ein Super-Administrator die Standard-Administratorgruppe einem delegierten Administratorbenutzer zuweisen. Führen Sie die folgenden Aufgaben aus:

1. Melden Sie sich als Super-Administrator bei NetScaler Console an.
2. Navigieren Sie zu **Account** > **User Administration** > **Users**.
3. Wählen Sie den Benutzernamen des delegierten Administrators aus und klicken Sie auf **Edit**.
4. Weisen Sie die Gruppe **\<*tenant*_*name*\>_admin_group** dem delegierten Administrator zu und klicken Sie auf **OK**. Im folgenden Bild wird beispielsweise „example_admin_group“ einem delegierten Administratorbenutzer zugewiesen.

Zuweisen einer benutzerdefinierten Rolle zu einem delegierten Administrator

Um einem delegierten Administrator eine benutzerdefinierte Rolle zuzuweisen, muss der Super-Administrator eine Gruppe, Rolle und Richtlinie erstellen und diese dem delegierten Administratorbenutzer zuweisen. Dadurch wird sichergestellt, dass der delegierte Administrator nur die erforderlichen Berechtigungen besitzt. Führen Sie die folgenden Aufgaben aus:

1. Melden Sie sich als Super-Administrator bei NetScaler Console an.
2. Navigieren Sie zu **Account** > **User Administration** > **Access Policies**. Wählen Sie **Add**, um eine Zugriffsrichtlinie mit den erforderlichen Berechtigungen für den delegierten Administrator zu erstellen. In diesem Beispiel wird eine Zugriffsrichtlinie `custompolicy` erstellt, die Lesezugriff auf die Einstellungen der Benutzerverwaltung ermöglicht.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Rollen**. Wählen Sie **Hinzufügen**, um eine Rolle zu erstellen und diese Rolle an die Zugriffsrichtlinie zu binden, die Sie im vorherigen Schritt erstellt haben. In diesem Beispiel wird eine Rolle `customrole` erstellt und an die Zugriffsrichtlinie `custompolicy` gebunden.

4. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Gruppen**. Wählen Sie **Hinzufügen**, um eine Gruppe zu erstellen und diese Gruppe an die Rolle zu binden, die Sie im vorherigen Schritt erstellt haben. In diesem Beispiel wird die Gruppe „custom group“ erstellt und an die Rolle „custom role“ gebunden.

5. Navigieren Sie zu **Konto** > **Benutzerverwaltung** > **Benutzer**
6. Wählen Sie den Benutzernamen des delegierten Administrators und klicken Sie auf **Bearbeiten**.
7. Weisen Sie dem delegierten Administrator die Gruppe zu, die Sie im vorherigen Schritt erstellt haben. In diesem Beispiel wird dem delegierten Administrator die Gruppe `customgroup` zugewiesen.

Integration mit der ServiceNow-Instanz

Als NetScaler-Administrator verwenden Sie ServiceNow möglicherweise als primäres IT-Anforderungs- und Supportsystem. Sie müssen Tickets oder Incidents für kritische NetScaler-Ereignisse erstellen, um diese zu untersuchen, zu verfolgen und zu beheben.

Sie können die Ticketerstellung in ServiceNow mithilfe von NetScaler Console und dem Citrix ITSM-Konnektor für ServiceNow automatisieren. Um diese Automatisierung zu starten, binden Sie den Citrix ITSM-Adapterdienst ein, um Ereignisse zu empfangen und relevante Incidents in ServiceNow zu erstellen. Weitere Informationen zu den Vorbereitungs- und Integrationsschritten finden Sie unter Erste Schritte im Citrix ITSM Adapter Service.

Nach der erfolgreichen Integration konfigurieren Sie die automatische Generierung von ServiceNow-Incidents in NetScaler Console. Führen Sie die Schritte aus, um zu überprüfen, ob ServiceNow-Tickets automatisch generiert werden.

1. Melden Sie sich bei NetScaler Console an.
2. Navigieren Sie zu **Einstellungen > Benachrichtigungen** und wählen Sie **ServiceNow** aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Wählen Sie das ServiceNow-Profil aus der Liste aus.
4. Klicken Sie auf **Testen**, um ein ServiceNow-Ticket automatisch zu generieren und die Konfiguration zu überprüfen.

   Wenn Sie ServiceNow-Tickets in der NetScaler Console-GUI anzeigen möchten, wählen Sie **ServiceNow-Tickets** aus.

Wenn Sie NetScaler Console in ServiceNow integrieren, können Sie die Generierung von ServiceNow-Incidents für Folgendes automatisieren:

- Alle NetScaler-Ereignisse
- SSL-Zertifikate, die bald ablaufen
- Die Lizenzablaufereignisse der NetScaler Console

Und Sie können auch die Ereignisrichtlinien der NetScaler Console anpassen.

ServiceNow-Vorfälle für alle NetScaler-Ereignisse generieren

In NetScaler Console können Sie Regeln konfigurieren, um automatisch ein Ticket in ServiceNow für bestimmte Ereignisse zu erstellen. NetScaler Console generiert automatisch ein ServiceNow-Ticket für Ereignisse wie:

- Virtuelle Server fallen aus oder sind außer Betrieb.
- Der Ressourcenverbrauch überschreitet den Schwellenwert.
- Die Lizenz auf einer NetScaler-Instanz läuft ab.

Das automatisch generierte Ticket in ServiceNow enthält die erforderlichen Details zur Nachverfolgung und Fehlerbehebung des Problems. Sie können die Benachrichtigungen über ein oder mehrere Netzwerkgeräte von einer einzigen ServiceNow-Konsole aus verwalten. Weisen Sie es dann dem Administrator zur weiteren Analyse zu.

Sie können eine Ereignisregel in der NetScaler Console erstellen, indem Sie zu **Infrastructure > Events > Rules** navigieren. Weitere Informationen finden Sie unter ServiceNow-Benachrichtigungen senden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ServiceNow-Vorfälle für SSL-Zertifikate generieren, die bald ablaufen

Wenn ein SSL-Zertifikat auf NetScaler-Instanzen bald abläuft, generiert NetScaler Console automatisch ein ServiceNow-Ticket. Auf diese Weise können Sie die bevorstehenden Ablauf-Tickets für SSL-Zertifikate im Voraus in Ihrem ServiceNow-Dashboard überprüfen.

Informationen zum Senden von ServiceNow-Benachrichtigungen für den Ablauf eines SSL-Zertifikats finden Sie unter Ablauf des SSL-Zertifikats.

ServiceNow-Vorfälle für den Ablauf der NetScaler Console-Lizenz generieren

In NetScaler Console können Sie die Regeln konfigurieren, um automatisch ein Ticket in ServiceNow für bestimmte NetScaler Console-Lizenzablaufereignisse zu erstellen.

Informationen zum Senden von ServiceNow-Benachrichtigungen für den Ablauf der NetScaler Console-Lizenz finden Sie unter Ablauf der NetScaler Console-Lizenz.

NetScaler Console-Ereignisrichtlinien anpassen

Sie können Richtlinien definieren, um zu steuern, wie ServiceNow die NetScaler Console-Ereignisse basierend auf Ereignisattributen verarbeitet. Legen Sie die NetScaler Console-Ereignisrichtlinien im Citrix ITSM connector fest. Sie können entscheiden, wie ein Vorfall in ADM generiert, verarbeitet und gemeldet werden soll. Führen Sie dann die folgenden Aktionen über ITSM aus:

- Vorfälle ignorieren
- Vorfälle auf dem Dashboard anzeigen
- Vorfälle erstellen

Weitere Informationen finden Sie unter NetScaler Console Ereignisrichtlinien anpassen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Umsetzbare Aufgaben und Empfehlungen

HINWEIS:

- Die Registerkarte **To Do** wird in **Recommendations** umbenannt. Unter **Recommendations** können Sie weiterhin die vorhandenen Aufgaben überprüfen und auf **Guide Me** klicken, um die Aufgabe abzuschließen.
- Die Registerkarte **Archive** ist nicht mehr verfügbar. Stattdessen können Sie eine Empfehlung aus der Liste **Dismiss** (Verwerfen).

Möglicherweise haben Sie Hunderte von erkannten NetScaler-Instanzen und mehrere virtuelle Server (Anwendungen) von jeder Instanz konfiguriert. Als Administrator müssen Sie sicherstellen, dass alle NetScaler-Instanzen und Ihre Anwendungen effizient verwaltet werden, um Erkenntnisse für eine bessere Priorisierung und Fehlerbehebung zu erhalten.

Wenn Sie Ihre Infrastruktur weiter ausbauen, müssen Sie sich möglicherweise auch auf die kritischen Probleme konzentrieren, die sich auf Ihre Instanzen und Anwendungen auswirken und Ihre sofortige Aufmerksamkeit erfordern. Sie müssen auch sicherstellen, dass Ihre NetScaler Console-Bereitstellung effizient, sicher und konform ist. Basierend auf Ihrer aktuellen Auslastung und Ihrem Abonnement können Sie mit der Funktion **Tasks** in NetScaler Console sowohl umsetzbare **Tasks** anzeigen, die sofortiges Handeln erfordern, als auch **Recommendations**, um eine effiziente Bereitstellung zu gewährleisten.

Als Administrator können Sie mithilfe dieser umsetzbaren **Tasks** und **Recommendations** Folgendes tun:

- Erhalten Sie sofortige Transparenz bei Beobachtungen oder Problemen, die Ihr sofortiges Handeln erfordern.
- Konfigurieren Sie Benachrichtigungen, um eine Benachrichtigung zu erhalten, sobald NetScaler Console Aufgaben erkennt, und ergreifen Sie proaktiv Maßnahmen.
- Erreichen Sie eine effiziente Bereitstellung von NetScaler Console und NetScaler-Instanzen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Reduzieren Sie den entscheidenden Zeit- und Arbeitsaufwand bei der Identifizierung kritischer Probleme.
- Stellen Sie sicher, dass Sie alle Funktionen von NetScaler Console nutzen, aktivieren Sie die Produkterkennung und die vom Produkt empfohlenen Funktionen für eine effiziente Verwaltung der Bereitstellung.

Klicken Sie in der NetScaler Console-GUI auf **Tasks**, um sowohl **Tasks** als auch **Recommendations** anzuzeigen.

- **Tasks** – Ermöglicht Ihnen die Anzeige einer Liste von Aufgaben, die Ihre sofortige Aufmerksamkeit und Ihr Handeln erfordern. Wenn Sie Ihre Infrastruktur erweitern, könnten einige kritische Probleme unbemerkt bleiben, die zu einer Sicherheitsverletzung führen. Zum Beispiel erfordern NetScaler-Instanzen mit CVEs sofortige Aufmerksamkeit, und Sie müssen sofort Maßnahmen ergreifen, um sicherzustellen, dass die Instanzen in der empfohlenen Build- und Version ausgeführt werden. In **Tasks** können Sie diese Erkenntnisse sofort erhalten. Basierend auf Ihrer aktuellen Auslastung können Sie insgesamt 5 Aufgaben anzeigen. Die Aufgaben werden basierend auf dem Schweregrad (Critical und Medium) angezeigt.

- **Empfehlungen** – Bietet bestimmte Empfehlungen basierend auf Ihrer aktuellen Nutzung, um Ihre NetScaler Console-Bereitstellung zu verbessern. Sie können die Option **Guide Me** verwenden, um jede Empfehlung abzuschließen. Jede Empfehlung, die Sie mit der Option **Guide Me** abschließen, wird nach „Abgeschlossen“ verschoben. Sie können auch Empfehlungen ablehnen, die dann unter die Kategorie **Abgelehnt** verschoben werden. Um Ihre abgelehnten Empfehlungen anzuzeigen, verwenden Sie den Filter **Nach Status** und wählen Sie **Abgelehnt** aus, um diese abgelehnten Empfehlungen anzuzeigen.

  Sie können auch den **Nach Kategorie filtern** verwenden, um bestimmte Empfehlungen basierend auf den Kategorien (Infrastruktur, Anwendung und Sicherheit) zu filtern. Alternativ können Sie auch die **Suchleiste** verwenden und die ersten Zeichen eingeben, um die Aufgabe einzugrenzen.

Aufgaben

Unter **Aufgaben** können Sie die folgenden 4 Aufgaben anzeigen, abhängig von Ihrer aktuellen NetScaler Console-Bereitstellung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Abgelaufene SSL-Zertifikate** – Bietet Informationen zu den abgelaufenen SSL-Zertifikaten, die in Ihrer NetScaler Console installiert sind. Wählen Sie diese Aufgabe aus, um die folgenden Registerkarten anzuzeigen:

  - **Nicht verwendete Zertifikate löschen**: Zeigt die Zertifikate an, die in keiner NetScaler-Instanz verwendet werden. Um die Aufgabe abzuschließen, überprüfen Sie die nicht verwendeten Zertifikate, wählen Sie das Zertifikat aus und klicken Sie auf **Anzeigen und Löschen**.

    Empfohlene Aktion: Sie werden zu **Infrastruktur > SSL-Dashboard > SSL-Zertifikate – Abgelaufen** weitergeleitet. Um ein Zertifikat zu löschen, klicken Sie auf **Löschen**. Wenn Sie das Zertifikat aktualisieren möchten, wählen Sie das Zertifikat aus und klicken Sie auf **Aktualisieren**. Weitere Informationen finden Sie unter So aktualisieren Sie ein installiertes Zertifikat.

  - **Zertifikate aktualisieren**: Zeigt die bereits abgelaufenen Zertifikate an. Um die Aufgabe abzuschließen, überprüfen Sie die Zertifikate, wählen Sie das Zertifikat aus und klicken Sie auf **Anzeigen und Aktualisieren**.

    Empfohlene Aktion: Sie werden zu **Infrastruktur > SSL-Dashboard > SSL-Zertifikate – Abgelaufen** weitergeleitet. Wählen Sie das Zertifikat aus und klicken Sie auf **Aktualisieren** oder **Löschen**. Weitere Informationen finden Sie unter So aktualisieren Sie ein installiertes Zertifikat.

- **Ablaufende SSL-Zertifikate** – Bietet Informationen zu den SSL-Zertifikaten, die bald ablaufen.

  Empfohlene Aktion: Wählen Sie diese Aufgabe aus, um Registerkarten basierend auf der Gesamtzahl der Tage vor dem Ablaufdatum anzuzeigen. Um die Aufgabe abzuschließen, wählen Sie das Zertifikat aus der Registerkarte aus und klicken Sie auf **Anzeigen und Aktualisieren**. Sie werden zur entsprechenden Seite in **Infrastruktur > SSL-Dashboard** weitergeleitet. Wählen Sie das Zertifikat aus und klicken Sie auf **Aktualisieren**. Weitere Informationen finden Sie unter So aktualisieren Sie ein installiertes Zertifikat.

- **Konfigurationsabweichungen** – Bietet Informationen zu den Konfigurationsabweichungen (gespeicherter vs. laufender Unterschied und Vorlage vs. laufender Unterschied) in den NetScaler-Instanzen. Wählen Sie diese Aufgabe aus, um die folgenden Registerkarten anzuzeigen:

  - **Instanzen mit nicht gespeicherter Konfiguration**: Sie können Instanzen anzeigen, die die nicht gespeicherte Konfiguration aufweisen. Um die Aufgabe abzuschließen, wählen Sie die Instanz aus und klicken Sie auf **Konfiguration anzeigen und speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Empfohlene Aktion: Sie werden zu **Infrastructure > Configuration > Configuration Audit > Audit Reports** weitergeleitet und können die Instanzen anzeigen, die nicht gespeicherte Konfigurationen haben. Klicken Sie auf **Konfiguration speichern**, um diese Aufgabe abzuschließen. Weitere Informationen finden Sie in der Dokumentation.

- **Instanzen mit Abweichungen von der Vorlage**: Sie können Instanzen anzeigen, die Vorlagenabweichungen aufweisen. Um die Aufgabe abzuschließen, wählen Sie die Instanz aus und klicken Sie auf **Befehle anzeigen und ausführen**.

  Empfohlene Aktion: Sie werden zu **Infrastructure > Configuration > Configuration Audit > Audit Reports** weitergeleitet und können die Instanzen anzeigen, die Vorlagenabweichungen aufweisen. Befolgen Sie die Dokumentation, um die Aufgabe abzuschließen.

- **Sicherheitshinweis** – Bietet Informationen zu den CVEs, die Ihre NetScaler-Instanzen betreffen. Wählen Sie diese Aufgabe aus, um die folgenden Registerkarten anzuzeigen:

  - **Erkannte CVEs**: Zeigt die erkannten CVEs und die NetScaler-Instanzen an, die von den CVEs betroffen sind. Um diese Aufgabe abzuschließen, wählen Sie eine CVE aus und klicken Sie auf **Anzeigen und Beheben**.

    Empfohlene Aktion: Sie werden zur Seite **Sicherheitshinweis** unter **Infrastructure > Instance Advisory > Security Advisory** weitergeleitet. Befolgen Sie die Dokumentation, um die Aufgabe abzuschließen.

  - **Betroffene Instanzen**: Zeigt die NetScaler-Instanzen an, die von CVEs betroffen sind. Um die Aufgabe abzuschließen, wählen Sie die Instanz aus und klicken Sie auf **Anzeigen und Beheben**.

    Empfohlene Aktion: Sie werden zur Seite **Sicherheitshinweis** unter **Infrastructure > Instance Advisory > Security Advisory** weitergeleitet. Befolgen Sie die Dokumentation, um die Aufgabe abzuschließen.

- **Upgrade-Hinweis**: Bietet Informationen zu Ihren NetScaler®-Instanzen, die innerhalb von 90 Tagen das End of Life (EOL) oder End of Maintenance (EOM) erreicht haben oder kurz davor stehen.

  Empfohlene Aktion: Klicken Sie auf **Aktion ausführen** und aktualisieren Sie die Instanzen auf einen empfohlenen Build.

- **SSL A+-Bewertungs-Upgrade**: Bietet Informationen zu Ihren Anwendungen, die nicht mit einer A+-Bewertung konform sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Empfohlene Aktion: Wählen Sie die Anwendungen aus der Liste aus und klicken Sie auf **Auf A+ aktualisieren**.

Nach erfolgreichem Upgrade wird folgende Erfolgsmeldung angezeigt:

Nachdem das Upgrade abgeschlossen ist, werden die Anwendungsdetails aus der Aufgabe entfernt.

Hinweise:

- Je nach Anzahl der ausgewählten Anwendungen kann die Dauer des Upgrade-Abschlussprozesses variieren.
- Nachdem Sie einen Upgrade-Prozess initiiert haben, wird empfohlen, einen weiteren Upgrade-Prozess zu initiieren, nachdem der laufende abgeschlossen ist.
- Sie können den Status des Upgrade-Prozesses auch unter **Infrastructure > Configuration > Configuration Jobs** einsehen.
- Wenn der Upgrade-Prozess nicht erfolgreich ist, können Sie den Status unter **Infrastructure > Configuration > Configuration Jobs** einsehen. Sie können den Upgrade-Prozess erneut aus der Aufgabe initiieren.
- Wenn Sie ein Bulk-Upgrade durchführen und eine oder mehrere Anwendungen nicht aktualisiert werden können, können Sie nur die Details dieser fehlgeschlagenen Anwendungen in der Aufgabe einsehen. Sie können den Upgrade-Prozess erneut initiieren, um ihn abzuschließen.

HINWEIS:

- Sie können die folgende Seite anzeigen, wenn Ihre NetScaler Console keine ausstehenden Aufgaben hat:

- In einigen Szenarien erfolgen die Prüfungen auf allen Instanzen, und es kann zusätzliche Zeit in Anspruch nehmen, alle Aufgaben zu laden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Empfehlungen

Die folgende Tabelle beschreibt die Empfehlungen, die Sie in der NetScaler Console GUI einsehen können:

HINWEIS

Für die gebündelte Lizenzierung erhalten Sie Empfehlungen basierend auf Ihren bestehenden Berechtigungen für die gebündelte Lizenzierung.

NAME DER EMPFEHLUNG	WANN IST DIE AUFGABE IN DER GUI SICHTBAR?
NetScaler-Instanz hinzufügen	Nachdem Sie sich bei NetScaler Console angemeldet haben und wenn keine NetScaler-Instanz erkannt wurde.
Fügen Sie einen externen Agenten hinzu, um die maximalen Funktionen in NetScaler Console zu nutzen.	Wenn kein externer Agent konfiguriert ist. Sie können mit einem integrierten Agenten beginnen. Ein externer Agent ist jedoch erforderlich, um alle Funktionen wie Analysen, gebündelte Lizenzierung usw. zu nutzen.
Registrieren Sie einen NetScaler von einem integrierten Agenten bei einem externen Agenten.	Nachdem Sie sich über den Service Connect-Workflow bei NetScaler Console angemeldet haben, werden die NetScaler-Instanzen über den integrierten Agenten hinzugefügt. Sie können diese NetScaler-Instanzen bei einem externen Agenten registrieren, um alle Funktionen wie Analysen, gebündelte Lizenzierung usw. zu nutzen.
Möchten Sie die Bandbreite auf Ihrem NetScaler neu zuweisen? Es ist ganz einfach!	Wenn die gebündelten Lizenzen in der NetScaler-GUI zugewiesen sind und diese NetScaler-Instanzen in NetScaler Console erkannt werden, können Sie die Neuzuweisung über NetScaler Console vornehmen.
Aktivieren Sie den granularen rollenbasierten Zugriff für Ihre wichtigsten Unternehmensbenutzer.	Wenn die rollenbasierte Zugriffssteuerung (RBAC) in NetScaler Console noch nicht konfiguriert ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME DER EMPFEHLUNG	WANN IST DIE AUFGABE IN DER GUI SICHTBAR?
Konfigurieren Sie Regeln und verpassen Sie keine kritischen Ereignisse auf Ihren NetScaler-Instanzen.	Wenn eine benutzerdefinierte Ereignisregel noch nicht konfiguriert ist.
Müssen Sie mehrere Anwendungen und deren Leistung überwachen? Erstellen Sie einfach eine benutzerdefinierte Anwendung.	Wenn die benutzerdefinierte App noch nicht konfiguriert ist.
Benachrichtigen Sie und verpassen Sie nie wieder kritische Ereignisse in Ihren Anwendungen.	Wenn die Aktionsrichtlinie nicht für App-Score-Abweichung, Server-Verarbeitungszeit, Client-Netzwerklatenz, Server-Netzwerklatenz oder Antwortzeit konfiguriert ist.
Vermeiden Sie Anwendungsausfälle und verpassen Sie nie ablaufende SSL-Zertifikate in einer Anwendung.	Wenn keine Warnungen oder Benachrichtigungen für die ablaufenden SSL-Zertifikate konfiguriert sind.
Sicherheitshinweis – Halten Sie Ihre NetScaler-Instanzen mit CVEs und Gegenmaßnahmen auf dem neuesten Stand.	Wenn die NetScaler-Instanzen von CVEs betroffen sind.
Konfigurieren Sie eine Unternehmensrichtlinie und überwachen Sie Abweichungen.	Wenn die SSL-Unternehmenseinstellungen nicht geändert wurden oder noch Standardeinstellungen sind.
Wiederholen Sie Aufgaben manuell? Erstellen Sie Konfigurationsaufträge und wenden Sie diese auf mehrere NetScaler-Instanzen an.	Wenn die Aufgabe **Konfigurationsauftrag** noch nicht konfiguriert ist.
Verwalten und überwachen Sie Ihren Instanz-Score, indem Sie benutzerdefinierte Indikatoren Ihrer Wahl auswählen.	Wenn die Standardeinstellungen und Schwellenwerte in den **Instanz-Score-Einstellungen** nicht geändert wurden.
Verfolgen Sie Ihren Anwendungs-Score, indem Sie benutzerdefinierte Indikatoren Ihrer Wahl auswählen	Wenn die App-Score-Komponenten im App-Dashboard standardmäßig verwendet werden und keine Anpassungen vorgenommen wurden.
Private IP-Blöcke hinzufügen, um Client-Anfragen in der Geo-Karte zu visualisieren	Wenn IP-Blöcke nicht konfiguriert sind. Sie können IP-Blöcke zum Zuordnen und Visualisieren von Client-Anfragen auf einer

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NAME DER EMPFEHLUNG	WANN IST DIE AUFGABE IN DER GUI SICHTBAR?
	Geo-Karte basierend auf ihren privaten IPs/ Bereich erstellen.
Abonnieren und exportieren Sie Ihre AppSec-Verletzungen in Echtzeit nach Splunk	Wenn die Splunk-Integration in NetScaler Console noch nicht konfiguriert ist.
Passen Sie den Standardschwellenwert an oder erstellen Sie einen neuen Schwellenwert für Ihre Kubernetes-Dienste	Wenn nur Standardschwellenwerte im Dienstgraphen verwendet werden und kein einfacher oder doppelter Schwellenwert auf die Dienste angewendet wird.
Konfigurieren Sie proaktiv Benachrichtigungsprofile und erhalten Sie Benachrichtigungen an Ihren Kommunikationszielen	Wenn ein Benachrichtigungsprofil noch nicht konfiguriert ist.
Planen Sie wiederkehrende Exporte und erhalten Sie Benachrichtigungen zu den Infrastrukturdetails	Wenn noch keine Exportzeitpläne unter **Infrastruktur > Instanzen** konfiguriert sind.
Sie verwenden ServiceNow und möchten es in ADM integrieren?	Wenn die ServiceNow-Integration in NetScaler Console noch nicht konfiguriert ist.
Automatisieren Sie die Verwaltung von SSL-Zertifikaten mit Venafi und ADM	Wenn der Venafi-Server noch nicht in der NetScaler Console konfiguriert ist.
Verlängern Sie Ihre Pooled-Lizenz, bevor sie abläuft.	Wenn Ihre bestehende Lizenz in 30 Tagen abläuft.
Beginnen Sie mit der Pooled-Lizenzierung, indem Sie Ihre erworbene gepoolte Bandbreite NetScaler-Instanzen zuweisen.	Wenn Sie noch nicht mit der Zuweisung Ihrer gepoolten Lizenzberechtigungen begonnen haben.
Erwägen Sie den Kauf weiterer gepoolter Bandbreitenkapazität.	Wenn Sie 90 % oder mehr Ihrer gepoolten Bandbreitenberechtigung genutzt haben.
Ihre aktuelle gepoolte Bandbreitenberechtigung wird nicht ausreichend genutzt. Überprüfen Sie dies und erwägen Sie, mehr zuzuweisen.	Wenn die Auslastung Ihrer gepoolten Lizenzzuweisung weniger als 70 % beträgt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wie verwende ich den „Guide me“-Workflow und schließe die Empfehlung ab?

Angenommen, Sie möchten Regeln für ein beliebiges Ereignis konfigurieren. Klicken Sie für die folgende Aufgabe auf **Guide me**:

Nachdem Sie auf **Guide me** geklickt haben, werden Sie zu **Infrastructure > Events > Rules** weitergeleitet. Klicken Sie auf **Add**, um eine Regel zu erstellen. Weitere Informationen finden Sie unter Ereignisregeln erstellen.

Nachdem Sie die Regelerstellung abgeschlossen haben, ist die Empfehlung abgeschlossen und wird nach **Completed** verschoben.

Wenn Sie eine Empfehlung später abschließen möchten, können Sie auf ähnliche Weise **Dismiss** aus der Liste auswählen, und sie wird nach **Dismissed** verschoben.

Empfehlung verwerfen(/en-us/netscaler-console-service/media/dismiss-recommendation.png)

Benachrichtigungen konfigurieren

Sie können Benachrichtigungen konfigurieren und erhalten, wann immer NetScaler Console offene Aufgaben identifiziert, die Ihr sofortiges Handeln erfordern. Wenn Sie keine Benachrichtigungen konfiguriert haben, können Sie oben rechts auf **Benachrichtigung konfigurieren** klicken.

Benachrichtigung(/en-us/netscaler-console-service/media/create-notification.png)

Auf der Seite **Benachrichtigungen** können Sie Profile für **E-Mail** und **Slack** konfigurieren und dann auf **Speichern** klicken, um Benachrichtigungen zu erhalten. Für jeden Benachrichtigungstyp zeigt die NetScaler Console GUI die konfigurierte Verteilerliste oder das Profil an. Die NetScaler Console sendet Benachrichtigungen an die ausgewählte Verteilerliste oder das Profil.

Häufig gestellte Fragen

1. **Guide me** zeigt keine Tooltips an und leitet nur die Benutzeroberfläche um? Was kann ich tun, um dies zu beheben?

   Dieses Problem kann auftreten, wenn Ihre Firewall Pendo FQDN blockiert. Lesen Sie Pendo für Ihr Unternehmen aktivieren und stellen Sie sicher, dass der FQDN in der Firewall zugelassen ist. Das Zulassen von Pendo FQDN ermöglicht es **Guide me**, Tooltips anzuzeigen. Sie können den **Guide me**-Workflow optimal nutzen, wenn Pendo verfügbar ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Welche Art von Empfehlungen gibt es für Administratoren?

   Derzeit beziehen sich die Empfehlungen auf Bereitstellungen, die Administratoren bei Konfigurations- und Einrichtungsaufgaben unterstützen, um die Bereitstellung effizienter zu gestalten. Es ermöglicht auch eine bessere Produktentdeckung, und Administratoren können ohne Vorkenntnisse oder ohne zu wissen, ob die Funktion in NetScaler Console existiert, erfahren, was eine Aufgabe bewirkt und wie sie helfen kann.

3. Was passiert, wenn ich eine Empfehlung verwerfe?

   Die Empfehlungen, die Sie verwerfen, werden in **Verworfen** verschoben. Sie können diese Empfehlungen später abschließen.

4. Wird die Empfehlung als **Abgeschlossen** markiert, wenn ich einen Guide me starte und ihn mittendrin abbreche?

   Nein, die Empfehlung wird erst abgeschlossen, wenn die Aktion gespeichert oder abgeschlossen wurde.

5. Kann ich suchen oder filtern?

   Ja! Sie können die Suchleiste verwenden oder bestimmte Aufgaben eingrenzen, indem Sie die Kategorie aus der Liste auswählen.

6. Erhalte ich Aufgaben, um auf dynamische Ereignisse zu reagieren?

   Ja! Derzeit können Sie insgesamt 4 umsetzbare Aufgaben anzeigen. Weitere Informationen finden Sie unter Aufgaben.

7. Werden alle umsetzbaren Aufgaben und über 20 Empfehlungen angezeigt, auch wenn ich keine NetScaler-Instanzen in der NetScaler Console hinzugefügt habe?

   Nein. Sie müssen sowohl NetScaler-Instanzen als auch virtuelle Server in der NetScaler Console verfügbar haben, um alle Aufgaben und Empfehlungen anzuzeigen.

8. Wie oft werden die Aufgaben aktualisiert?

   Wenn Sie im linken Navigationsbereich auf **Aufgaben** klicken, werden sie aktualisiert und sind mit dem neuesten Status verfügbar. Die Details werden abgerufen und aktualisiert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ein einheitliches Dashboard zur Anzeige wichtiger Instanz-Metrikdetails

In NetScaler Console können Sie verschiedene Einblicke in die Nutzung und Leistung von Anwendungen, die NetScaler-Infrastruktur, Sicherheitsverletzungen (Bot und WAF) und so weiter anzeigen. Als Administrator müssen Sie möglicherweise zu verschiedenen Optionen in der NetScaler Console-GUI navigieren, um mehrere Einblicke anzuzeigen. Zum Beispiel, um die virtuellen Server (Anwendungen) und NetScaler-Instanz-Einblicke zu überprüfen:

- Sie müssen zuerst zu **Applications > Dashboard** navigieren, um Einblicke für Anwendungen anzuzeigen.
- Dann müssen Sie zu **Infrastructure > Infrastructure Analytics** navigieren, um Einblicke für NetScaler-Instanzen anzuzeigen.

Für ein besseres Überwachungserlebnis ist es notwendig, dass Sie über ein Privileg verfügen, das eine Übersicht über alle erforderlichen Einblicke enthält. Navigieren Sie zu **Overview > Dashboard**, um ein Single-Pane-Dashboard mit einer Übersicht über die wichtigsten Metrikdetails basierend auf den folgenden Kategorien zu visualisieren:

- Anwendungen
- NetScaler-Infrastruktur
- Anwendungssicherheit
- Gateway
- API-Analysen

Anwendungen

Unter **Anwendungen** können Sie Folgendes anzeigen:

- **Anwendungszustand** – Bietet eine Übersicht über Anwendungen, die sich im Status **Down** und **Out-of-Service** befinden, und basierend auf ihrem Status wie **Kritisch**, **In Überprüfung**, **Gut** und **Nicht zutreffend**. Klicken Sie auf **Alle Anwendungen anzeigen**, um Details im App-Dashboard anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Golden Signal Anomalien** – Bietet eine Übersicht über Anwendungen, die Serverfehler und Antwortzeitanomalien aufweisen. Klicken Sie auf **Details anzeigen**, um weitere Informationen zu erhalten.
- **Anwendungskonfigurationsoptimierung** – Bietet eine Übersicht über alle Anwendungen, die Leistungsprobleme aufweisen. Klicken Sie auf **Mehr anzeigen**, um Problemdetails im App-Dashboard anzuzeigen.
- **SSL-Zertifikate** – Bietet einen Überblick über SSL-Zertifikate und deren Gültigkeit. Klicken Sie auf **SSL-Zertifikate verwalten**, um weitere Informationen im SSL-Dashboard anzuzeigen.
- **Optimierung der Anwendungs-SSL-Konfiguration** – Bietet einen Überblick über alle Anwendungen mit SSL-bezogenen Problemen. Klicken Sie auf **Mehr anzeigen**, um Details zu den Problemen anzuzeigen.

NetScaler-Infrastruktur

Unter **NetScaler-Infrastruktur** können Sie die folgenden wichtigen Metriken zu NetScaler-Instanzen anzeigen:

- **NetScaler-Instanzzustand** – Bietet einen Überblick über die Gesamtzahl der NetScaler-Instanzen basierend auf dem Instanz-Score.
- **NetScaler-Instanzen, die von CVEs betroffen sind** – Bietet einen Überblick über die Gesamtzahl der NetScaler-Instanzen, die von Common Vulnerabilities and Exposures (CVEs) betroffen sind. Weitere Informationen finden Sie unter Sicherheitshinweis.
- **NetScaler-Instanzprobleme** – Bietet einen Überblick über NetScaler-Instanzprobleme, abhängig von der Problemkategorie. Weitere Informationen finden Sie unter Infrastruktur-Analysen.
- **Zusammenfassung des NetScaler-Instanz-Upgrades** – Bietet einen Überblick über die Gesamtzahl der NetScaler-Instanzen, die nicht auf dem neuesten Build sind. Klicken Sie auf **NetScaler-Instanzen-Dashboard anzeigen**, um weitere Informationen zu erhalten.

Anwendungssicherheit

Bietet einen Überblick über die insgesamt betroffenen Anwendungen und die insgesamt gemeldeten Verstöße (Bot und WAF) für den ausgewählten Zeitraum. Klicken Sie auf **Sicherheits-Dashboard anzeigen**, um die Details zu Sicherheits- und Bot-Verstößen anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway

Bietet einen Überblick über die Gesamtzahl der aktiven Gateway-Benutzer, der aktiven ICA®-Benutzer und der aktiven ICA-Verbindungen. Sie können auch Fehler, Benutzeranmeldedetails und eine geografische Karte anzeigen, die Details zu den Benutzerstandorten liefert.

API-Analysen

Bietet einen Überblick über die Leistung und Nutzung der über NetScaler Console konfigurierten API-Endpunkte. Sie können Folgendes anzeigen:

- Verteilung der Anwendungs- und Serverantwortzeit für API-Endpunkte.
- Endpunkte mit hoher Anwendungs- und Serverantwortzeit.

Dashboard anpassen

Sie können die Option **Dashboard bearbeiten** verwenden und die Dashboard-Ansicht nach Ihren Wünschen anpassen. Mit der Option **Dashboard bearbeiten** können Sie:

- Widgets ziehen
- Das gesamte Widget entfernen (Anwendungen, NetScaler-Infrastruktur, Gateway oder Anwendungssicherheit).
- Die kleineren Widgets entfernen, die unter jedem Widget vorhanden sind.
- Klicken Sie auf **Widget hinzufügen** und wählen Sie die erforderlichen Schlüsselmetriken aus, die Sie unter jedem Widget anzeigen möchten.

- Auf Standard zurücksetzen
- Auf zuletzt gespeicherten Stand zurücksetzen

Nachdem Sie Änderungen vorgenommen haben, klicken Sie auf **Speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

- Standardmäßig werden alle Widgets angezeigt. Wenn Sie das Dashboard anpassen, die Änderungen speichern und dann erneut die Option **Auf Standard zurücksetzen** verwenden, werden alle Widgets dem Dashboard hinzugefügt.
- Die Option **Auf letzte gespeicherte Version zurücksetzen** lädt die zuvor gespeicherte Konfiguration.

Agentendetails anzeigen

Im vereinheitlichten Dashboard können Sie eine Übersicht der Agentendetails visualisieren. Unter **Übersicht > Dashboard**, neben dem **Agentenstatus**, können Sie die folgenden Status anzeigen, die Ihnen die Analyse der gesamten Agentenverfügbarkeit ermöglichen:

- **Alle verfügbar**. Zeigt an, dass alle Agenten aktiv und betriebsbereit sind.
- **Alle nicht verfügbar**. Zeigt an, dass alle Agenten ausgefallen und nicht zugänglich sind.
- **nicht verfügbar**. Zeigt an, dass einige Agenten ausgefallen und nicht zugänglich sind.
- **Alle außer Betrieb**. Zeigt an, dass alle Agenten außer Betrieb sind.
- **außer Betrieb**. Zeigt an, dass einige Agenten außer Betrieb sind.
- **Externer Agent nicht gefunden**. Zeigt an, dass kein Agent (über Hypervisoren) konfiguriert ist.

Klicken Sie auf **Details anzeigen**, um eine Übersicht der Agentendetails wie die Gesamtzahl der integrierten Agenten, die Gesamtzahl der externen Agenten, Agenten-IP, Status, Systemauslastung, Diagnoseprüfungen usw. zu visualisieren.

Filter erstellen und anwenden

Sie können Filter anwenden und Einblicke nur für die ausgewählten Instanzen oder Anwendungen in den folgenden Bereichen anzeigen:

- Anwendungen
- NetScaler-Infrastruktur
- Anwendungssicherheit

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Standardmäßig sind alle Anwendungen ausgewählt. Sie können einen benutzerdefinierten Filter über das Dashboard erstellen, indem Sie auf das Filtersymbol in der Kachel klicken.

Im Fenster **Anwendungen filtern**:

1. Wählen Sie **Neuen Filter erstellen**.
2. Geben Sie einen Filternamen nach Ihrer Wahl ein.
3. Klicken Sie auf **Anwendungen auswählen** und fügen Sie alle erforderlichen Anwendungen für den Filter hinzu. Wenn Sie Anwendungen auswählen, können Sie auch die Filter (**Anwendungsname** und **Typ**) verwenden und dann Anwendungen auswählen.

4. Klicken Sie auf **Filter erstellen und anwenden**.

Der Filter ist nun erstellt und angewendet. Sie können weitere Filter erstellen, indem Sie dieselbe Prozedur befolgen. Nachdem Sie Filter erstellt haben, können Sie Filter über die Liste **Filter aus vorhandenen Filtern auswählen** auswählen und anwenden.

Filter bearbeiten

Sie können einen Filter bearbeiten, indem Sie den Filter aus der Liste auswählen und auf **Bearbeiten** klicken. Mit der Bearbeitungsoption können Sie Anwendungen hinzufügen oder entfernen und den Filter anschließend aktualisieren.

Um einen Filter zu löschen, wählen Sie den Filter aus der Liste aus und klicken Sie auf **Löschen**.

HINWEIS

Wenn Sie einen Filter mit Anwendungen erstellen und eine der Anwendungen im App-Dashboard gelöscht wird, werden die Anwendungsdetails sofort aus dem Unified Dashboard entfernt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benutzerdefinierte Dashboards erstellen, um wichtige Metrikdetails der Instanz anzuzeigen

Ähnlich wie beim einheitlichen Dashboard (**Übersicht > Dashboard**) können Sie Instanzmetrikdetails nach Ihrer Wahl anzeigen, indem Sie benutzerdefinierte Dashboards erstellen. Sie können bis zu 30 Dashboards erstellen, indem Sie für jedes Dashboard einen eindeutigen Namen verwenden. Als Administrator ermöglicht Ihnen diese Verbesserung, mehrere Dashboards zu erstellen und nur die erforderlichen Instanzinformationen zu überwachen.

Betrachten Sie zum Einstieg, dass Sie die wichtigsten Metriken für **Anwendungen** und **Anwendungssicherheit** überwachen möchten:

1. Navigieren Sie zu **Übersicht > Benutzerdefiniertes Dashboard**.
2. Klicken Sie auf **+**, um ein neues Dashboard zu erstellen.

   Auf der Seite **Benutzerdefiniertes Dashboard erstellen**:

   a. **Name des benutzerdefinierten Dashboards** – Geben Sie einen eindeutigen Namen für das Dashboard an.

   b. **Beschreibung** – Geben Sie eine kurze Beschreibung an, um zusätzliche Details zu erhalten.

   c. **Widget zum Dashboard hinzufügen** – In diesem Beispiel besteht die Anforderung darin, Widgets für Anwendungen und Anwendungssicherheit hinzuzufügen. Wählen Sie die Widgets aus, die Sie aus den Kategorien **Anwendung** und **Anwendungssicherheit** überwachen möchten.

   d. **Anwendungsfilter** – Standardmäßig wird der Filter auf alle Anwendungen angewendet. Sie können auch einen Filter erstellen und nur bestimmte Anwendungen auswählen. Weitere Informationen finden Sie unter Filter erstellen und anwenden.

   e. Klicken Sie auf **Speichern**.

Das Dashboard wurde erfolgreich erstellt. Ähnlich können Sie bis zu 20 Dashboards erstellen und Kategorien nach Ihrer Wahl auswählen, indem Sie für jedes Dashboard einen eindeutigen Namen angeben.

Nachdem Sie ein benutzerdefiniertes Dashboard erstellt haben, können Sie die folgenden Optionen verwenden:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Bearbeiten**: Sie können das Dashboard bearbeiten, indem Sie weitere Widgets hinzufügen oder Widgets entfernen, Filter anwenden und so weiter.
- **Umbenennen**: Sie können den Dashboard-Namen ändern.
- **Löschen**: Sie können das Dashboard löschen.

  Optionen für benutzerdefiniertes Dashboard(/en-us/netscaler-console-service/media/custom-dashboard-options.png)

Weitere Optionen im Dashboard

Im benutzerdefinierten Dashboard, das Sie erstellt haben, können Sie die folgenden Optionen verwenden:

Weitere Optionen(/en-us/netscaler-console-service/media/custom-dashboard-more-options.png)

- **Konfiguration bearbeiten**: Sie können diese Option auch verwenden, um das Dashboard zu bearbeiten, indem Sie weitere Widgets hinzufügen oder Widgets entfernen, Filter anwenden und so weiter.
- **Layout bearbeiten**: Sie können diese Option verwenden, um das Dashboard zusätzlich anzupassen.
  - Sie können auswählen, nach oben, unten zu verschieben oder zu löschen.

    Nach oben oder unten verschieben oder löschen(/en-us/netscaler-console-service/media/custom-dashboard-move-options.png)
  - In den Widgets können Sie jedes Widget löschen, indem Sie die Option „Löschen“ auswählen.

    Widgets löschen(/en-us/netscaler-console-service/media/delete-widgets.png)
  - Ziehen Sie die Widgets, um sie zu platzieren, wo immer Sie möchten.
  - Erhöhen oder verringern Sie die Widget-Größe, um eine bessere Sichtbarkeit für bestimmte Einblicke zu erhalten.

    ▢

Nachdem Sie Änderungen vorgenommen haben, klicken Sie auf **Speichern**, um das aktualisierte Dashboard anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dashboard für andere Benutzer freigeben

Sie können das Dashboard für andere Benutzer freigeben. Wählen Sie ein vorhandenes Dashboard aus und klicken Sie auf **Freigeben**. Geben Sie den Benutzernamen ein und klicken Sie auf **Einladen**, um das Dashboard freizugeben. Der zugewiesene Benutzer kann das Dashboard im schreibgeschützten Modus anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

API-Sicherheit

APIs oder Anwendungsprogrammierschnittstellen sind Sätze von Regeln, Protokollen und Tools, die es verschiedenen Softwareanwendungen oder Systemen ermöglichen, miteinander zu kommunizieren. APIs spielen eine wichtige Rolle beim Schutz sensibler Daten, indem sie Zugriffskontrollen, Authentifizierung und Verschlüsselung durchsetzen und so sicherstellen, dass nur autorisierte Entitäten vertrauliche Informationen sicher zugreifen und übertragen können.

APIs dienen als Backend-Framework für mobile und Webanwendungen. Daher ist es entscheidend, die sensiblen Daten zu schützen, die sie übertragen. API-Sicherheit bezieht sich auf die Praxis, Angriffe auf APIs zu verhindern oder abzumildern.

Bei der API-Sicherheit fungiert ein Gateway als Einstiegspunkt für alle Anfragen an Ihre API-Endpunkte. Und es gewährleistet einen sicheren und zuverlässigen Zugriff auf alle API-Endpunkte und Microservices in Ihrem System.

Führen Sie die folgenden Schritte aus, um Ihre APIs zu sichern:

- Eine API-Definition erstellen oder hochladen
- Eine API-Instanz bereitstellen
- Richtlinien zu einer API-Bereitstellung hinzufügen

Die folgende Abbildung beschreibt, wie die API-Sicherheit in NetScaler Console die Client-Anfrage empfängt und die Antwort von den Backend-API-Diensten sendet:

HINWEIS:

In NetScaler Console ist diese Funktion für Benutzer mit Premium-Lizenzen verfügbar.

Vorteile der API-Sicherheit

Die API-Sicherheit bietet Ihnen die folgenden Vorteile:

- **Sichert Ihre API-Endpunkte**: Die API-Sicherheit fügt eine Sicherheitsebene hinzu und schützt Ihre API-Endpunkte und Backend-API-Server vor Angriffen wie:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Pufferüberlauf
- SQL-Injection
- Cross-Site-Scripting
- Denial of Service (DoS)

- **Überwacht und verbessert die API-Leistung**: Die API-Sicherheit bietet Dienste wie SSL-Offloading, Authentifizierung, Autorisierung, Ratenbegrenzung und mehr. Diese Dienste erhöhen die API-Leistung und deren Verfügbarkeit.

  Die API-Analysen bieten Ihnen Einblick in Ihre API-Leistungsmetriken und Bedrohungen für Ihre API-Endpunkte. Weitere Informationen finden Sie unter API-Analysen anzeigen.
- **Verwaltet den API-Verkehr**: Die API-Sicherheit abstrahiert die Komplexität Ihrer Backend-API-Infrastruktur.
- **Ermittelt API-Endpunkte**: Die API-Sicherheit ermittelt die API-Endpunkte in Ihrer Organisation und fügt sie der Seite **API-Erkennung** hinzu.

Berechtigungen für die API-Sicherheitskonfiguration und -verwaltung erteilen

Als Administrator können Sie eine Zugriffsrichtlinie erstellen, um Benutzerberechtigungen für die API-Sicherheitskonfiguration und -verwaltung zu erteilen. Die Benutzerberechtigungen können Anzeigen, Hinzufügen, Bearbeiten und Löschen umfassen. Gehen Sie wie folgt vor, um Berechtigungen zu erteilen:

1. Navigieren Sie zu **Einstellungen > Benutzer & Rollen > Zugriffsrichtlinien**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie unter **Zugriffsrichtlinien erstellen** einen Richtliniennamen und die Beschreibung an.
4. Erweitern Sie im Feld **Berechtigungen** erweitern **Anwendungen** und dann **API-Sicherheit**.
5. Wählen Sie die erforderlichen **API-Sicherheitsseiten** aus. Wählen Sie dann die Berechtigungen aus, die Sie erteilen möchten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

Stellen Sie sicher, dass Sie Berechtigungen für die Funktionen erteilen, die für die Verwendung einer API-Sicherheit erforderlich sind. Wenn Sie beispielsweise Benutzerzugriff auf die Seite **Bereitstellungen** gewähren, benötigen die folgenden Funktionen ebenfalls Benutzerzugriff:

- StyleBooks
- IPAM
- Lastausgleich (Unter **Netzwerkfunktionen**)
- Inhaltswechsel (Unter **Netzwerkfunktionen**)
- Geräte-API-Proxy (Unter **API**)

Weitere Informationen zu Zugriffsrichtlinien finden Sie unter Zugriffsrichtlinien auf NetScaler Console konfigurieren.

API-Definition erstellen oder hochladen

Eine API-Definition ist ein Dokument, das eine API unter Verwendung der OpenAPI-Spezifikationsstandards beschreibt. Diese Definition kann API-Ressourcenpfade und Methoden zu deren Betrieb enthalten. Sie können API-Definitionen zu NetScaler Console hinzufügen und sie dann auf einem API-Gateway (NetScaler) bereitstellen.

Sie können API-Definitionen auf eine der folgenden Arten erstellen:

- Swagger OAS-Spezifikationsdatei hochladen
- Eigene API-Definition erstellen

HINWEIS:

Derzeit unterstützt NetScaler Console das Parsen von OAS-Spezifikationsdateien, die **Swagger 2.0** oder **OpenAPI 3.0.1** verwenden.

OAS-Spezifikation hochladen

Sie können die OAS-Spezifikation in die NetScaler Console-GUI hochladen.

1. Navigieren Sie zu **Security > API Security > API Definitions**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Klicken Sie auf **Add**.
3. Wählen Sie **Upload OAS Specification**.

   HINWEIS:

   Stellen Sie sicher, dass die OAS-Spezifikationsdatei im YAML- oder JSON-Format vorliegt. Und diese Datei darf keine externen Referenzen enthalten.

4. Suchen Sie eine OAS-Spezifikation auf Ihrem lokalen Computer und laden Sie sie in NetScaler Console hoch.

API-Definition erstellen

Sie können Ihre eigene API-Definition in der NetScaler Console-GUI erstellen.

1. Navigieren Sie zu **Security > API Security > API Definitions**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie **Eigene Definition erstellen** aus und geben Sie Folgendes an:

   - **Name** – Ein Name für die API-Definition.
   - **API-Definition** – Eine Definition muss Titel, Version, Basispfad und Host enthalten. Sie können einen Domänennamen oder eine IP-Adresse im Feld **Host** angeben.
   - **API-Ressourcen** – Fügen Sie Ihrer Definition mehrere API-Ressourcen hinzu. Jede Ressource hat einen Pfad und eine unterstützte Methode. Klicken Sie auf **Hinzufügen**. Die Ressource wird der Tabelle **Hinzugefügte Ressourcen** hinzugefügt. Klicken Sie auf **Löschen**, um eine API-Ressource zu löschen.

   ☐

4. Klicken Sie auf **Erstellen**.

API-Definitionen anzeigen

Auf der Seite **API-Definitionen** wird die hochgeladene Definition aufgelistet. Klicken Sie auf **Anzeigen**, um die folgenden Details der API-Definition anzuzeigen:

- **Name** – Zeigt den Namen einer API-Definition an.
- **API-Definition** – Zeigt Titel, Version, Basispfad und Host einer Definition an.
- **API-Ressourcen** – Listet die API-Ressourcen in einer API-Definition und deren Methoden zur Bedienung auf.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Eine API-Instanz bereitstellen

Um eine API-Instanz bereitzustellen, benötigen Sie einen API-Proxy. Ein API-Proxy ist ein virtueller Front-End-Server, auf dem die API-Sicherheit (NetScaler-Instanz) den API-Verkehr von API-Clients empfängt. Die API-Clients können Browser, mobile Anwendungen usw. sein.

Sie können einen API-Proxy mit verschiedenen API-Bereitstellungen teilen. In einer Organisation mit vielen API-Diensten können Sie für jeden API-Dienst einen separaten API-Proxy erstellen. Oder Sie können einen API-Proxy erstellen und ihn mit API-Instanzen für verschiedene API-Dienste teilen.

Beispielsweise werden die beiden API-Dienste `app1` und `app2` auf derselben API-Sicherheit bereitgestellt und verwenden denselben virtuellen Front-End-Server. Sie möchten beiden API-Diensten dieselbe virtuelle IP-Adresse und SSL-Zertifikatsinformationen bereitstellen. In diesem Fall können Sie einen API-Proxy mit den erforderlichen Informationen hinzufügen und ihn mit separaten Bereitstellungen teilen. So können API-Dienste auf verschiedenen Bereitstellungen Anfragen über den gemeinsam genutzten API-Proxy empfangen.

Führen Sie als Administrator die folgenden Schritte aus, um eine API-Instanz bereitzustellen:

1. Einen API-Proxy hinzufügen.
2. Eine API-Instanz mithilfe des API-Proxys bereitstellen.

Einen API-Proxy hinzufügen

Führen Sie die folgenden Schritte aus, um einen API-Proxy hinzuzufügen:

1. Gehen Sie zu **Security > API Security > API Proxy > Add**.
2. Geben Sie Folgendes an:
    - **Proxy Name** – Ein Name für einen API-Proxy.
    - **Target NetScaler Instance** – Wählen Sie eine NetScaler-Instanz aus, die als API-Gateway fungiert.
    - **IP address** – Eine IP-Adresse des virtuellen Servers, der API-Dienste hostet.
    - **Port** – Eine Portnummer des virtuellen Servers, der API-Dienste hostet.
    - **Protokoll** – Legen Sie ein Protokoll fest, je nach Art des Datenverkehrs, den Sie auf dem API-Proxy empfangen möchten (HTTP oder HTTPS).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **TLS-Sicherheitsprofil** – Wählen Sie „Hoch“ oder „Mittel“ aus der Liste aus. Wenn Sie „Hoch“ auswählen, wird dies dem SSL-Profil mit der Bewertung A+ auf einer NetScaler-Instanz zugeordnet.
- **Zertifikatsspeicher** – Wählen Sie das SSL-Zertifikat für die API-Sicherheit aus. Der NetScaler-Agent-Zertifikatsspeicher hilft Ihnen, Ihre SSL-Zertifikate an einem Ort zu speichern und zu verwalten.

  Im NetScaler-Agent-Zertifikatsspeicher können Sie SSL-Zertifikate im NetScaler-Agent speichern und diese während der NetScaler-Konfiguration wiederverwenden.

  HINWEIS:

  Wenn Ihre vorhandenen Bereitstellungen das SSL-Zertifikat oder den Schlüssel verwenden, die sich nicht im NetScaler-Agent-Zertifikatsspeicher befinden, müssen Sie das Zertifikat und den Schlüssel mit demselben Namen zum Speicher hinzufügen.

- **Dienst-FQDN** – Ein vollqualifizierter Domänenname, unter dem Ihre API-Dienste gehostet werden. Zum Beispiel: `api.example.com`

Alternativ können Sie ein IPAM-Netzwerk auswählen, um die IP-Adresse zuzuweisen. Um die zugewiesene IP-Adresse aus dem IPAM-Netzwerk anzuzeigen, navigieren Sie zu **Einstellungen > IPAM**. Weitere Informationen zu IPAM finden Sie unter IPAM konfigurieren.

3. Klicken Sie auf **Speichern**, um die Bereitstellungskonfiguration zu speichern.

   Wenn Sie diesen API-Proxy für die API-Sicherheit bereitstellen möchten, klicken Sie auf **Speichern und bereitstellen**.

Nach dem Hinzufügen eines API-Proxys stellen Sie eine API-Instanz bereit.

Bereitstellen einer API-Instanz mithilfe des API-Proxys

Führen Sie die folgenden Schritte aus, um eine API-Instanz bereitzustellen:

1. Navigieren Sie zu **Sicherheit > API-Sicherheit > Bereitstellungen**.
2. Klicken Sie auf **Hinzufügen**.
3. Unter **Bereitstellungsgrundlagen** Info,
   a. Geben Sie den **Bereitstellungsnamen** an.
   b. Wählen Sie unter **API-Definitionen** die erforderliche API-Definition aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Wählen Sie den **API-Proxy** aus, den Sie mit dieser Bereitstellung verwenden möchten.

4. Klicken Sie unter **Upstream-Dienste** auf **Hinzufügen**, um Back-End- (Ursprungs-) API-Server hinzuzufügen, an die Sie den API-Datenverkehr ausleiten möchten. Sie können einen Upstream-Dienst mit seinem Domänennamen oder seiner IP-Adresse konfigurieren.

   Sie können SNIP-Adresse und Netzmaskendetails bei der Bereitstellung einer API-Instanz angeben. Die NetScaler-Instanz verwendet die angegebene SNIP-Adresse, um mit den Upstream-Diensten (Back-End) zu kommunizieren. Die angegebene SNIP-Adresse wird zur Quell-IP-Adresse für den an Upstream-Dienste gesendeten ausgehenden Datenverkehr. Sie können auch IPAM verwenden, um SNIP-Adresse und Netzmaske zu konfigurieren. Wenn Sie die SNIP-Adresse nicht konfigurieren, wird die Standard-SNIP-Adresse der NetScaler-Instanz zur Quell-IP-Adresse für die Upstream-Dienste.

   HINWEIS:

   Standardmäßig sind die Optionen für SNIP-Adresse und Netzmaske optional. Wenn Sie jedoch eine dieser Optionen angeben, müssen Sie auch die andere Option angeben.

   a. Geben Sie einen Namen für einen Upstream-Dienst an.

   b. Geben Sie die Domäne an.

   c. Geben Sie unter **Dienste** eine IP-Adresse und einen Portwert an. Um weitere IP-Adressen hinzuzufügen, klicken Sie auf **Neue Zeile hinzufügen**.

   d. Klicken Sie auf **Hinzufügen**.

5. Geben Sie unter **Routing** die folgenden Details an, um den eingehenden API-Datenverkehr basierend auf dem Ressourcenpfadpräfix weiterzuleiten:

   a. Geben Sie den Routennamen an.

   b. Wählen Sie eine **API-Ressource** aus, um eine API-Anfrage zu empfangen.

      HINWEIS:

      Sie können auch den benutzerdefinierten Pfad oder das Pfadpräfix angeben.

   c. Wählen Sie einen **Upstream-Dienst** aus der Liste aus, an den Sie den API-Datenverkehr übertragen möchten.

6. Klicken Sie auf **Speichern**, um die Bereitstellungskonfiguration zu speichern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Sie die Konfiguration für die API-Sicherheit bereitstellen möchten, klicken Sie auf **Speichern und bereitstellen**.

API-Analysen aktivieren

Im Folgenden sind die Voraussetzungen aufgeführt, um Analysen für eine Bereitstellung zu aktivieren:

- Stellen Sie sicher, dass virtuelle Server **lizenziert** sind.
- Stellen Sie sicher, dass der Analysestatus **Deaktiviert** ist.
- Stellen Sie sicher, dass virtuelle Server den Status **UP** haben.

Um die API-Analysen für eine Bereitstellung zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie unter **Security > API Security > Deployments** die Bereitstellung aus, für die Sie die API-Analysen aktivieren möchten.
2. Klicken Sie auf **Analysen aktivieren**.
3. Wählen Sie auf der Seite **Analysen für die Bereitstellung konfigurieren** den virtuellen Server aus und klicken Sie auf **Analysen aktivieren**.
4. Im Fenster **Analysen aktivieren**:
    a. Wählen Sie den Insight-Typ aus (Web Insight, Security Insight, Bot Insight)
    b. Wählen Sie **Logstream** oder **IPFIX** als Transportmodus aus.

        Weitere Informationen zu IPFIX und Logstream finden Sie unter Logstream-Übersicht.

        Der Ausdruck ist standardmäßig wahr.
    c. Klicken Sie auf **OK**.

NetScaler Console aktiviert Analysen auf den ausgewählten virtuellen Servern.

Richtlinien zu einer API-Bereitstellung hinzufügen

Sie können verschiedene Sicherheitsrichtlinien für Ihren API-Datenverkehr konfigurieren. Diese Konfiguration erfordert, dass Sie die Kriterien für die Datenverkehrsauswahl und die für eine Richtlinie erforderlichen Parameter angeben. Führen Sie die folgenden Schritte aus, um einer API-Definition eine Richtlinie hinzuzufügen:

1. Navigieren Sie zu **Security > API Security > Policies**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Klicken Sie auf **Add**.
3. Geben Sie den Namen für eine Richtliniengruppe an.
4. Wählen Sie ein **Deployment** aus der Liste aus.
5. Wählen Sie einen **Upstream Service** aus der Liste aus, für den Sie Richtlinien konfigurieren möchten.
6. Klicken Sie auf **Add**, um Datenverkehrsselektoren und einen Richtlinientyp auszuwählen.

   Traffic selector – Die Kriterien für die Datenverkehrsauswahl umfassen API-Ressourcenpfade oder Pfadpräfixe, Methoden und Richtlinien.

   Sie können eine der folgenden Optionen verwenden, um Kriterien für die Datenverkehrsauswahl anzugeben:

   - **API Resources** – Wählen Sie eine API-Ressource und ihre Methoden aus, für die Sie eine Richtlinie anwenden möchten. Sie können API-Ressourcen und -Methoden mit einem Schlüsselwort suchen.

     In diesem Beispiel werden die API-Ressourcen mit `/user` aufgelistet, die die Methode `POST` haben.

   - **Custom Rule** – Auf dieser Registerkarte können Sie benutzerdefinierte Pfadpräfixe und mehrere Methoden angeben.

     Die konfigurierte Richtlinie gilt für eine eingehende API-Anfrage, die der benutzerdefinierten Regel für die API-Datenverkehrsauswahl entspricht.

     In diesem Beispiel gilt die Richtlinie **No-Auth** für die API-Ressourcen, die das Präfix `/bill` und die Methode `GET` haben.

   Wählen Sie unter **Richtlinie** eine Richtlinie aus der Liste aus, die Sie auf die ausgewählte API-Ressource und -Methode anwenden möchten. Weitere Informationen zu den einzelnen Richtlinien finden Sie unter Richtlinientypen.
7. Optional können Sie Richtlinientypen verschieben, um eine Priorität festzulegen. Die Richtlinientypen mit höherer Priorität werden zuerst angewendet.
8. Klicken Sie auf **Speichern**, um eine Richtlinie hinzuzufügen. Wenn Sie die Richtlinie sofort anwenden möchten, klicken Sie auf **Speichern & Anwenden**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Richtlinientypen

Beim Konfigurieren einer API-Richtlinie können Sie die folgenden Richtlinien auswählen, die Sie auf die API-Ressource und -Methode anwenden möchten:

- **Authentifizierung und Autorisierung**
- **Ratenbegrenzung**
- **WAF**
- **BOT**
- **Header-Umschreibung**
- **URI-Pfad-Umschreibung**
- **Verweigern**

HINWEIS:

Informationen zur Verwaltung der API-Sicherheit mithilfe von APIs finden Sie unter Verwenden von APIs zur Verwaltung der API-Sicherheit.

Authentifizierung und Autorisierung

API-Ressourcen werden auf einem Anwendungs- oder API-Server gehostet. Wenn Sie Zugriffsbeschränkungen für solche API-Ressourcen erzwingen möchten, können Sie die Authentifizierungs- und Autorisierungsrichtlinien verwenden. Diese Richtlinien überprüfen, ob die eingehende API-Anfrage über die erforderliche Berechtigung für den Zugriff auf die Ressource verfügt.

Verwenden Sie die folgenden Richtlinien, um die Authentifizierung und Autorisierung für die ausgewählten API-Ressourcen zu definieren:

`No-Auth`

Verwenden Sie diese Richtlinie, um die Authentifizierung für den ausgewählten Datenverkehr zu überspringen.

`Auth-Basic`

Diese Richtlinie gibt an, dass die lokale Authentifizierung mit dem HTTP-Standardauthentifizierungsschema verwendet werden soll. Um die lokale Authentifizierung zu verwenden, müssen Sie Benutzerkonten auf dem NetScaler erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OAuth

OAuth erfordert einen externen Identitätsanbieter, um einen Client mithilfe von OAuth2 zu authentifizieren und ein Zugriffstoken auszustellen. Wenn der Client dieses Token als Zugangsdaten an ein API-Gateway übermittelt, wird das Token basierend auf den konfigurierten Werten validiert.

- **JWKS URI** – Die URL eines Endpunkts, der JWKs (JSON Web Key) zur JWT-Verifizierung (JSON Web Token) enthält
- **Aussteller** – Die Identität (normalerweise eine URL) des Authentifizierungsservers.
- **Zielgruppe** – Die Identität des Dienstes oder der Anwendung, für die das Token gültig ist.
- **Zu speichernde Claims** – Die Zugriffsberechtigungen werden als eine Reihe von Claims und erwarteten Werten dargestellt. Geben Sie die Claim-Werte im CSV-Format an.
- **Introspect URI** – Eine Introspektions-Endpunkt-URL des Authentifizierungsservers. Diese URL wird verwendet, um undurchsichtige Zugriffstoken zu überprüfen. Weitere Informationen zu diesen Token finden Sie unter OAuth configuration for opaque access tokens.

  Nachdem Sie die **Introspect URI** angegeben haben, geben Sie die **Client Id** und das **Client Secret** an, um auf den Authentifizierungsserver zuzugreifen.
- **Zulässige Algorithmen** – Diese Option ermöglicht es Ihnen, bestimmte Algorithmen in den eingehenden Token einzuschränken. Standardmäßig sind alle unterstützten Methoden erlaubt. Sie können jedoch die erforderlichen Algorithmen für den ausgewählten Datenverkehr überprüfen.

Bei erfolgreicher Validierung gewährt API Security dem Client Zugriff.

WICHTIG:

Wenn Sie eine OAuth- oder **Auth-Basic**-Richtlinie für die ausgewählten API-Ressourcen konfigurieren, konfigurieren Sie die **No Auth**-Richtlinie für die verbleibenden API-Ressourcen. Diese Konfiguration zeigt explizit an, dass Sie die Authentifizierung für die verbleibenden Ressourcen überspringen möchten.

Autorisierung

Diese Richtlinie überprüft die erforderlichen Berechtigungen für den Zugriff auf eine API-Ressource. Die Zugriffsrechte werden als eine Reihe von Claims und erwarteten Werten dargestellt. Um diese Richtlinie zu konfigurieren, wählen Sie **Add a new Claim** und geben Sie Folgendes an:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Claim-Name
- Claim-Werte

WICHTIG:

API Security erfordert sowohl Authentifizierungs- als auch Autorisierungsrichtlinien für den API-Verkehr. Daher müssen Sie eine Autorisierungsrichtlinie mit einer Authentifizierungsrichtlinie konfigurieren. Die Authentifizierungsrichtlinie kann OAuth oder `Auth-Basic` sein.

Auch wenn Sie keine Autorisierungsprüfungen haben, müssen Sie eine Autorisierungsrichtlinie mit leeren Claims erstellen. Andernfalls wird die Anfrage mit einem 403-Fehler abgelehnt.

Ratenbegrenzung

Geben Sie die maximale Last an, die der ausgewählten API-Ressource zugewiesen wird. Mit dieser Richtlinie können Sie die API-Verkehrsrate überwachen und vorbeugende Maßnahmen ergreifen. Um diese Richtlinie zu konfigurieren, geben Sie Folgendes an:

- **HTTP-Header-Name** – Dies ist ein Datenverkehrsselektorschlüssel, der den Datenverkehr filtert, um die API-Anfragen zu identifizieren. Die Ratenbegrenzungsrichtlinie wird nur auf solche API-Anfragen angewendet und überwacht diese.
- **Header-Werte** – Diese Header-Werte werden für den genannten Headernamen durch Kommas getrennt.
- **Schwellenwert** – Die maximale Anzahl von Anfragen, die im angegebenen Intervall zugelassen werden können. Wenn Sie **Header-Werte** angegeben haben, gilt dieser Schwellenwert für jeden Header-Wert.

  Beispiel-1:

  Wenn Sie Header-Werte (`"key1","key2","key3"`) für den Headernamen `x-api-key` angeben und den Schwellenwert auf `80` festlegen, gilt der festgelegte Schwellenwert für jeden Header-Wert.

  Beispiel-2:

  Wenn Sie unterschiedliche Schwellenwerte für jeden Header-Wert angeben möchten, erstellen Sie separate Ratenbegrenzungsrichtlinien mit demselben HTTP-Headernamen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Richtlinie-1**: Geben Sie Header-Werte (`"key1","key2"`) für den Headernamen `x-api-key` an und legen Sie den Schwellenwert auf `80` fest.
- **Richtlinie-2**: Geben Sie Header-Werte (`"key3"`) für den Headernamen `x-api-key` an und legen Sie den Schwellenwert auf `30` fest.

Wenn Sie keinen Header-Wert angeben, gilt der Schwellenwert für den angegebenen HTTP-Headernamen.

- **Zeitscheibe** – Das in Mikrosekunden angegebene Intervall. Während dieses Intervalls werden die Anfragen anhand der konfigurierten Grenzwerte überwacht. Standardmäßig ist sie auf 1000 Mikrosekunden (1 Millisekunde) eingestellt.
- **Begrenzungstyp** – Der Modus, wie Sie die Ratenbegrenzungsrichtlinie anwenden möchten. Sie können den Begrenzungstyp **Burst** oder **Smooth** auswählen.
- **Aktion** – Definiert eine Aktion, die Sie für den Datenverkehr ausführen möchten, der den Schwellenwert überschreitet. Sie können eine der folgenden Aktionen angeben:
  - **DROP**: Löscht die Anfragen, die die konfigurierten Datenverkehrsgrenzwerte überschreiten.
  - **RESET**: Setzt die Verbindung für die Anfragen zurück.
  - **REDIRECT**: Leitet den Datenverkehr an die konfigurierte redirect_url um.
  - **RESPOND**: Antwortet mit der Standardantwort (`429 Too many requests`).

WAF

Diese Richtlinie verhindert Sicherheitsverletzungen, Datenverlust und mögliche unbefugte Änderungen an Websites, die auf sensible Geschäfts- oder Kundeninformationen zugreifen.

Bevor Sie eine WAF-Richtlinie konfigurieren, erstellen Sie ein WAF-Profil in NetScaler Console mithilfe von StyleBooks.

Unter **WAF-Profilname** wählen oder geben Sie das von Ihnen erstellte WAF-Profil an.

Bot

Diese Richtlinie identifiziert schlechte Bots und schützt Ihre Appliance vor fortgeschrittenen Sicherheitsangriffen.

Bevor Sie eine BOT-Richtlinie konfigurieren, erstellen Sie ein BOT-Profil in NetScaler Console mithilfe von StyleBooks.

Unter **Bot-Profilname** geben Sie das von Ihnen erstellte BOT-Profil an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Header-Umschreibung

Diese Richtlinie hilft Ihnen, den Header von API-Anfragen und -Antworten zu ändern. Wenn Sie den Wert im HTTP-Header ersetzen möchten, geben Sie Folgendes an:

- **HTTP-Header-Name**: Der Feldname, den Sie im Anforderungsheader ändern möchten.

  Beispiel: `Host`
- **Header-Wert**: Optional, die Wertzeichenfolge, die Sie im angegebenen Headernamen ändern möchten.

  Beispiel: `sample.com`
- **Neuer Header-Wert**: Der neue Wert, der den angegebenen Header-Wert ersetzt.

  Wenn kein **Header-Wert** angegeben ist, ersetzt er jeden empfangenen Wert durch den angegebenen Wert für den **HTTP-Header-Namen**.

  Beispiel: `example.com`

In diesem Beispiel ersetzt die Header-Rewrite-Richtlinie `sample.com` durch `example.com` im Feld `Host` einer API-Anfrage.

URI-Pfad-Umschreibung

Diese Richtlinie hilft Ihnen, den URI-Pfad von API-Anfragen und -Antworten zu ändern. Wenn Sie ein Segment im URI-Pfad ersetzen möchten, fügen Sie eine Regel hinzu, um eines der folgenden Dinge zu tun:

- **Pfadsegment ersetzen** – Wenn Sie diesen Aktionstyp auswählen, geben Sie Folgendes an:
  - **Aktuelles Pfadsegment** – Das Pfadsegment, das Sie ersetzen möchten.
  - **Neues Pfadsegment** – Neues Pfadsegment, das nur das aktuelle Pfadsegment ersetzt.

  Um beispielsweise ein Gebietsschema im URI-Pfad von Englisch nach Chinesisch zu ändern, geben Sie `/de-de/` unter **Aktuelles Pfadsegment** an. Und geben Sie `/zh-zh` unter **Neues Pfadsegment** an. Es ersetzt nur das Pfadsegment und behält den restlichen URI-Pfad bei.
- **Vollständigen Pfad ersetzen** – Dieser Aktionstyp ersetzt den URI-Pfad von API-Anfragen und -Antworten vollständig durch den angegebenen Pfad. Wenn Sie `/example.html` unter **Neues Pfadsegment** angeben, wird der URI-Pfad einer API-Anfrage oder -Antwort in den angegebenen Pfad geändert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Pfadsegment entfernen** – Diese Aktion entfernt das angegebene Segment aus dem URI. Um beispielsweise das englische Gebietsschema aus dem URI-Pfad zu entfernen, geben Sie `/de-de/` unter **Aktuelles Pfadsegment** an.
- **Pfadsegment einfügen** – Diese Aktion fügt das angegebene Segment in den URI-Pfad ein. Um diese Regel anzuwenden, geben Sie die Position an, an der Sie das Segment einfügen möchten. Und welches Segment Sie einfügen möchten.

  Wenn Sie beispielsweise ein Segment direkt nach einem Text einfügen möchten, gehen Sie wie folgt vor:

  a. Geben Sie die Position an, an der Sie ein neues Segment einfügen möchten.
  b. Geben Sie unter **Aktuelles Pfadsegment** den Text an, nach dem ein neues Segment hinzugefügt werden soll.
  c. Geben Sie unter **Neues Pfadsegment** das Segment an, das Sie hinzufügen möchten.

Verweigern

Diese Richtlinie hilft Ihnen, API-Anfragen daran zu hindern, Ihre API-Ressourcen zu erreichen.

API-Analysen anzeigen

API-Analysen ermöglichen Einblick in den API-Datenverkehr. Diese Analysen ermöglichen es IT-Administratoren, API-Instanzen und Endpunkte zu überwachen, die von einem API-Gateway bereitgestellt werden. Sie bieten eine integrierte, regelmäßige Überwachung von API-Anfragen.

Bevor Sie API-Analysen überwachen, stellen Sie sicher, dass Sie Folgendes abgeschlossen haben:

1. Eine API-Definition hinzufügen
2. Eine API-Definition bereitstellen
3. Eine Richtlinie zu einer API-Definition hinzufügen
4. Lizenz auf API-Instanzen anwenden
5. Web Insight auf API-Instanzen aktivieren

In **API Analytics** können Sie die Antwortzeit von API-Instanzen und Endpunkten überwachen, die als Teil von API-Definitionen hinzugefügt wurden. Es zeigt auch die von API-Instanzen und Endpunkten verbrauchte Bandbreite an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Standardmäßig zeigt das Dashboard API-Analysen für die letzte Stunde an. Sie können eine Dauer auswählen, um API-Analysen für dieses Intervall anzuzeigen. Klicken Sie auf **Mehr anzeigen** auf jeder Kachel, um die gesamte Liste anzuzeigen. In dieser Ansicht können Sie API-Instanzen und Endpunkte anhand ihrer Teilnamen suchen, mit Ausnahme der Kachel **Geo-Standorte**.

API-Endpunktverteilung

Dieses Diagramm zeigt die Verteilung der Anwendungs- und Server-Antwortzeit für API-Endpunkte. Sie können einen API-Endpunkt identifizieren, der eine sehr hohe Antwortzeit aufweist, und die notwendigen Maßnahmen ergreifen.

Die API-Endpunkte erscheinen in einer der folgenden Farben, abhängig von ihren Antwortzeitlimits:

- **Grün** – wenn die Antwortzeit weniger als 30 Millisekunden beträgt.
- **Orange** – wenn die Antwortzeit zwischen 30 und 100 Millisekunden liegt.
- **Rot** – wenn die Antwortzeit mehr als 100 Millisekunden beträgt.

API-Instanzen

Die Kachel **API-Instanzen** zeigt die wichtigsten API-Instanzen mit hoher Anwendungs- und Server-Antwortzeit an.

Wählen Sie eine API-Instanz aus, um deren Leistungs-, Nutzungs- und Sicherheitsdetails anzuzeigen. Die ausgewählte API-Instanz zeigt die folgenden Informationen an:

- Anzahl der API-Endpunkte
- Anzahl der Anfragen
- Anwendungs- und Server-Antwortzeit
- Verbrauchte Bandbreite
- Authentifizierungsfehler

API-Endpunkte

Die Kachel **API-Endpunkte** zeigt die wichtigsten Endpunkte mit hoher Anwendungs- und Server-Antwortzeit an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wählen Sie einen API-Endpunkt aus, um Leistungs-, Nutzungs- und Sicherheitsdetails anzuzeigen.

Authentifizierungsfehler

Die Kachel **Authentifizierungsfehler** zeigt die wichtigsten API-Endpunkte mit den meisten Authentifizierungsfehlern an. Der Authentifizierungsfehler oder -erfolg hängt von der Richtlinie ab, die einer API-Definition hinzugefügt wurde.

Wenn Sie die Authentifizierungsfehler- und Erfolgsrate in einem API-Endpunkt anzeigen möchten, gehen Sie wie folgt vor:

1. Wählen Sie einen Endpunkt aus **API-Endpunkte**.
2. Wählen Sie die Registerkarte **Sicherheit**. Diese Registerkarte zeigt die Authentifizierungsfehler und -erfolge im ausgewählten Endpunkt an.

Wenn Sie die Authentifizierungsfehler- und Erfolgsrate in den API-Endpunkten einer Instanz anzeigen möchten, gehen Sie wie folgt vor:

1. Wählen Sie eine Instanz aus **API-Instanz**.
2. Wählen Sie die Registerkarte **Sicherheit**. Diese Registerkarte zeigt die Authentifizierungsfehler und -erfolge in den Endpunkten der ausgewählten Instanz an.

Verschiedene API-Einblicke anzeigen

Navigieren Sie durch API Analytics, um spezifische Informationen zu den folgenden Punkten anzuzeigen:

- API-Analysen anzeigen
  - API-Endpunktverteilung
  - API-Instanzen
  - API-Endpunkte
  - Authentifizierungsfehler
  - Verschiedene API-Einblicke anzeigen
    - Top-API-Endpunkte in einer Instanz anzeigen
    - Am häufigsten aufgerufene APIs anzeigen
    - Geo-Standort eines Endpunkts anzeigen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- HTTPS-Antwortstatus anzeigen
- Trend der API-Anfragen anzeigen
- Bandbreitennutzung eines Endpunkts anzeigen
- SSL-Fehler und -Nutzung anzeigen

Top-API-Endpunkte in einer Instanz anzeigen

Die Seite **API Analytics** zeigt die Top-Endpunkte an, die eine hohe Antwortzeit aufweisen. Wenn Sie ähnliche Endpunkte einer Instanz anzeigen möchten, wählen Sie eine Instanz unter **API-Instanzen** aus.

Die Kachel **Top-API-Endpunkte** zeigt die Endpunkte an, die eine hohe Anwendungs- und Server-Antwortzeit aufweisen.

Meistgenutzte APIs anzeigen

Wählen Sie in **API Analytics** eine API-Instanz aus den API-Instanzen aus. Die Kachel **Meistgenutzte APIs** zeigt die Top-Endpunkte an, die mehr Anfragen und Bandbreite haben.

Geostandort eines Endpunkts anzeigen

1. Wählen Sie in **API Analytics** eine der folgenden Optionen aus:
   - Wählen Sie eine Instanz aus **API-Instanzen** aus, um die Standorte anzuzeigen, von denen die Endpunkte der ausgewählten Instanz Anfragen erhalten haben.
   - Wählen Sie einen Endpunkt aus **API-Endpunkten** aus, um die Standorte anzuzeigen, von denen der Endpunkt Anfragen erhalten hat.
2. Unter **Leistung und Nutzung** wird die Kachel **Geostandorte** angezeigt.

   Sie können Standorte nach Antwortzeit, Bandbreite und Anfragen sortieren.

HTTPS-Antwortstatus anzeigen

Die Kachel **HTTPS-Antwortstatus** zeigt den Antwortstatus mit seinen Gründen und Vorkommen an. Sie können den HTTPS-Antwortstatus auf eine der folgenden Arten anzeigen:

- Wählen Sie eine Instanz aus **API-Instanzen** aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wählen Sie einen Endpunkt aus **API-Endpunkten** aus.

Diese Kachel wird auf der Registerkarte **Leistung und Nutzung** angezeigt.

Trend der API-Anfragen anzeigen

Wählen Sie einen Endpunkt unter **API-Endpunkte** aus. Unter **Leistung und Nutzung** zeigt die Kachel **Gesamtanfragen** den Trend der Gesamtzahl der von einem Endpunkt empfangenen Anfragen an.

Wenn Sie den Trend der aufgrund einer Ratenbegrenzung abgebrochenen Anfragen anzeigen möchten, wählen Sie eine Instanz unter **API-Instanzen** aus. Unter **Sicherheit** zeigt die Kachel **Ratenbegrenzung** den Trend der abgebrochenen Anfragen an. Sie zeigt auch den Trend der Gesamtzahl der von einem Endpunkt empfangenen Anfragen an.

Mit diesem Vergleich können Sie feststellen, wie viele Anfragen aufgrund einer Ratenbegrenzung unter den Gesamtanfragen abgebrochen werden.

Bandbreitennutzung eines Endpunkts anzeigen

Um den Trend der Bandbreitennutzung durch einen Endpunkt anzuzeigen, wählen Sie einen Endpunkt aus den API-Endpunkten aus. Die Kachel **Bandbreite** zeigt ein Diagramm der Bandbreitennutzung an.

SSL-Fehler und -Nutzung anzeigen

Wählen Sie eine Instanz unter **API-Instanzen** aus. Unter **Sicherheit** werden die folgenden Kacheln angezeigt:

- **SSL-Fehler** – Zeigt SSL-Fehler an, die auf Clients und Anwendungsservern aufgetreten sind.
- **SSL-Nutzung** – Zeigt SSL-Zertifikate, Protokolle, Chiffren und Schlüsselstärken mit ihren Vorkommen an.

Um die SSL-Nutzung in einem Endpunkt anzuzeigen, wählen Sie einen Endpunkt aus den API-Endpunkten aus. Die Kachel **SSL-Nutzung** wird auf der Registerkarte **Sicherheit** angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

API-Endpunkte ermitteln

Mit API Security können Sie die ermittelten API-Endpunkte in Ihrer Organisation anzeigen. NetScaler Console ermittelt die API-Endpunkte basierend auf dem API-Datenverkehr, der auf NetScaler-Instanzen und API-Bereitstellungen empfangen wird.

In NetScaler Console zeigt die Seite **Security > API Security > API Discovery** die ermittelten API-Endpunkte an.

- **Virtuelle Server** – Die Registerkarte **VServer** zeigt die virtuellen Server Ihrer NetScaler-Instanzen an. Die virtuellen Server werden auf dieser Registerkarte angezeigt, wenn sie API-Anfragen für den angegebenen Zeitraum erhalten.
- **API-Bereitstellungen** – Diese Registerkarte zeigt die API-Bereitstellungen an, die von NetScaler Console mithilfe einer API-Definition bereitgestellt werden. Diese Registerkarte ermittelt die API-Endpunkte, wenn API-Bereitstellungen die API-Anfragen für den angegebenen Zeitraum erhalten. Informationen zum Hinzufügen und Bereitstellen einer API-Definition finden Sie unter API-Definition hinzufügen und API-Definitionen bereitstellen.

HINWEIS:

- Stellen Sie sicher, dass Sie Analysen konfigurieren und Web Insights auf virtuellen Servern aktivieren. Siehe Web Insight auf API-Instanzen aktivieren.
- Sie können Richtlinien nur zu den API-Endpunkten hinzufügen, die unter der Registerkarte **API-Bereitstellungen** ermittelt werden.

API-Endpunkte anzeigen

Wenn Sie in **API Discovery** einen virtuellen Server oder eine API-Bereitstellung auswählen, zeigt die NetScaler Console-GUI die API-Endpunkte und deren Details an, wie zum Beispiel:

- **Methode** – Sie zeigt die in einem API-Endpunkt verwendete Methode an. Zum Beispiel die Methoden `GET` und `POST`.
- **Gesamtanfragen** – Sie zeigt die Anzahl der API-Anfragen am API-Endpunkt an.
- **Antwortstatus** – Sie zeigt die Anzahl für jeden Antwortstatus an. Zum Beispiel `2xx`, `3xx`, `4xx` und `5xx`.
- **In Spezifikation gefunden** – Diese Spalte wird nur für API-Bereitstellungen angezeigt. Manchmal erhalten interne APIs, die nicht Teil der API-Definition sind, möglicherweise

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Datenverkehr von außen. Diese Spalte hilft Ihnen zu erkennen, ob der API-Endpunkt und die beobachtete Methode Teil der API-Definition sind.

Die API-Endpunkte in einem virtuellen Server sind wie folgt verfügbar:

Die API-Endpunkte in API-Bereitstellungen sind wie folgt verfügbar:

Sie können auch den gewünschten API-Endpunkt auswählen, um dessen detaillierten Analysebericht anzuzeigen.

Weitere Informationen zu jedem Abschnitt finden Sie unter API-Analysen anzeigen.

API-Definitionen aus erkannten API-Endpunkten erstellen

So erstellen Sie API-Definitionen aus erkannten API-Endpunkten (API-Ressourcen und -Methoden):

1. Navigieren Sie zu **Security > API Security > API Discovery**, um die Liste der virtuellen Server und API-Bereitstellungen anzuzeigen.
2. Klicken Sie auf einen beliebigen virtuellen Server auf der Registerkarte **VServers**.
3. Die Seite des virtuellen Servers zeigt die Liste der erkannten Endpunkte an. Wählen Sie einen beliebigen Endpunkt aus und klicken Sie auf **Create API Definition**.

HINWEIS:

Wenn Sie keinen Endpunkt auswählen und auf **Create API Definition** klicken, wird ein Pop-up-Fenster angezeigt, in dem Sie bestätigen können, ob Sie eine API-Definition für alle Endpunkte erstellen möchten. Klicken Sie auf **Yes**, um die API-Definition mit allen Endpunkten zu erstellen, andernfalls klicken Sie auf **No**.

1. Geben Sie unter **API-Definition erstellen** Folgendes an:
   - **Name** – Ein Name für die API-Definition.
   - **API-Definition** – Eine Definition muss Titel, Version, Basispfad und Host enthalten. Sie können einen Domänennamen oder eine IP-Adresse im Feld **Host** angeben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **API-Ressourcen** – Fügen Sie Ihrer Definition mehrere API-Ressourcen hinzu. Jede Ressource hat einen Pfad und eine unterstützte Methode.

2. Klicken Sie auf **Definition erstellen**, um die API-Definition zu erstellen.

HINWEIS:

Wenn Sie einen API-Ressourcenpfad bearbeiten möchten, bevor Sie ihn zur API-Definition hinzufügen, verwenden Sie die Sortier- oder Suchfunktion für die API-Ressourcen auf dem Bildschirm der API-Definition.

Betrachten Sie beispielsweise eine API-Ressource namens „/api/products/123-3243-2344334/reviews“, wobei das Pfadsegment „123-3243-2344334“ eine variable Produkt-ID ist. Sie können nun die API-Ressourcen sortieren, den Ressourcenpfad als „/api/products/{id}/reviews“ hinzufügen und alle API-Endpunkte mit IDs wie „/api/products/123-3243-2344334/reviews“ löschen.

Vorhandene API-Definition mit erkannten API-Endpunkten aktualisieren

So aktualisieren Sie eine vorhandene API-Definition mit API-Endpunkten (API-Ressourcen und -Methoden):

1. Navigieren Sie zu **Security > API Security > API Discovery**, um die Liste der virtuellen Server und API-Bereitstellungen anzuzeigen.
2. Klicken Sie auf einen beliebigen virtuellen Server auf der Registerkarte **VServer**.
3. Die Seite des virtuellen Servers zeigt die Liste der erkannten Endpunkte an. Wählen Sie den Endpunkt aus, den Sie einer vorhandenen API-Definition hinzufügen möchten. Klicken Sie auf **Vorhandene API-Definition aktualisieren**.

4. Wählen Sie aus der Dropdown-Liste **Vorhandene API-Definition auswählen** die API-Definition aus, die Sie aktualisieren möchten. Klicken Sie auf **Definition aktualisieren**.
5. Die Seite **Vorhandene API-Definition aktualisieren** wird angezeigt. Der Abschnitt **API-Ressourcen** zeigt die folgenden Tabellen an:

   - **Hinzugefügte Ressourcen** – Die von Ihnen ausgewählten API-Endpunkte
   - **Vorhandene Ressourcen** – Die API-Endpunkte, die bereits in der API-Definition verfügbar sind

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Wenn derselbe API-Endpunkt in **Hinzugefügte Ressourcen** und **Vorhandene Ressourcen** verfügbar ist, wird der Endpunkt nur einmal zur API-Definition hinzugefügt.

6. Klicken Sie auf **Definition aktualisieren**.

Bereitstellung einer API-Instanz aufheben

Sie können die Option zum Aufheben der Bereitstellung verwenden, wenn Sie die API-Instanzkonfiguration von einer NetScaler-Instanz entfernen, aber die API-Instanzobjekte in der NetScaler Console als Entwurf beibehalten möchten. Diese Aktion setzt den Bereitstellungsstatus auf „Als Entwurf“. Sie kann nur auf die bereitgestellten API-Instanzkonfigurationen angewendet werden.

WICHTIG:

- Bevor Sie die Bereitstellung einer API aufheben, stellen Sie sicher, dass alle zugehörigen API-Richtlinien aufgehoben oder gelöscht wurden. Siehe, Bereitstellung einer API-Richtlinie aufheben.
- Bevor Sie die Bereitstellung eines API-Proxys aufheben, stellen Sie sicher, dass alle zugehörigen API-Bereitstellungen aufgehoben oder gelöscht wurden. Siehe, Bereitstellung einer API aufheben.

Bereitstellung einer API-Richtlinie aufheben

Führen Sie die folgenden Schritte aus, um die Bereitstellung einer API-Richtlinie aufzuheben:

1. Wählen Sie unter **Security > API Security > Policies** die Richtlinie aus, deren Bereitstellung Sie aufheben möchten.
2. Klicken Sie auf **Undeploy**.

Diese Aktion setzt den **Richtlinienstatus** auf „Als Entwurf“.

Bereitstellung einer API aufheben

Führen Sie die folgenden Schritte aus, um die Bereitstellung einer API aufzuheben:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Wählen Sie unter **Security > API Security > API Deployments** die API-Bereitstellung aus, deren Bereitstellung Sie aufheben möchten.

   HINWEIS:

   Stellen Sie sicher, dass alle zugehörigen Richtlinien der ausgewählten Bereitstellung aufgehoben oder gelöscht wurden.

2. Klicken Sie auf **Bereitstellung aufheben**.

Diese Aktion setzt den **Bereitstellungsstatus** auf „In Entwurf“.

Bereitstellung eines API-Proxys aufheben

Führen Sie die folgenden Schritte aus, um die Bereitstellung eines API-Proxys aufzuheben:

1. Wählen Sie unter **Security > API Security > API Proxies** den API-Proxy aus, dessen Bereitstellung Sie aufheben möchten.

   HINWEIS:

   Sie können einen API-Proxy mit verschiedenen API-Bereitstellungen teilen. Stellen Sie daher sicher, dass alle zugehörigen Bereitstellungen des ausgewählten Proxys aufgehoben oder gelöscht werden.

2. Klicken Sie auf **Bereitstellung aufheben**.

Diese Aktion setzt den **Proxy-Status** auf „In Entwurf“.

APIs zur Verwaltung der API-Sicherheit verwenden

Sie können auf die APIs zugreifen, um eine API-Sicherheit zu erstellen, zu konfigurieren und bereitzustellen.

HINWEIS:

Um zu verstehen, wie API-Sicherheits-APIs zur Konfiguration der Funktion verwendet werden, siehe die Nitro API-Dokumentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	SCHRITTE	RESSOURCEN-URL
1	Eine API-Definition erstellen	`https://adm.cloud.com/{customerid}/apisec/nitro/v1/config/apidefs`
2	Einen API-Proxy hinzufügen	`https://adm.cloud.com/apiproxies`
3	Eine API-Instanz mithilfe des API-Proxys bereitstellen	`https://adm.cloud.com/apiproxies/{customerid}/deployments`
4	API-Richtlinien hinzufügen	`https://adm.cloud.com/{customerid}/apisec/nitro/v1/config/policies/{id}`

Jede API-Richtlinie hat ein anderes `config_spec`-Objekt. Es ist ein undurchsichtiges Objekt, das ein JSON-Wörterbuch enthält, um ein `policytype` mit spezifischen Werten zu konfigurieren.

In diesem Objekt können Sie eine API-Ressource und ihre Methoden mit den folgenden Optionen auswählen:

- `api-resource-paths` – Geben Sie die API-Ressourcenpfade und -Methoden an, die in einer API-Definition definiert sind.

  Beispiel:

  ```
  {

  "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],

     "get": true,

     "post": false,

     "put": false,

     "delete": false
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

- `custom-rules` – Geben Sie die benutzerdefinierten API-Ressourcenpfade und -Methoden an, die möglicherweise nicht in einer API-Definition vorhanden sind.

  Beispiel:

```
{
"endpoints": ["/pet/categories", "/pet/findByName"],
   "get": true,
   "post": false,
   "put": false,
   "delete": false
}
```

Mit dieser Konfiguration filtert die Richtlinie die eingehenden Datenverkehrsanfragen, die den angegebenen API-Ressourcenpfaden entsprechen.

Informationen zu `config_spec` der einzelnen Richtlinientypen finden Sie unter API-Beispiele für Richtlinientypen.

API-Beispiele für Richtlinientypen

Dieser Abschnitt beschreibt die unterstützten API-Richtlinientypen und deren Konfiguration:

- Ratenbegrenzung
- OAuth
- Basisauthentifizierung
- Keine Authentifizierung
- Bot
- WAF
- Header-Umschreibung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- URI-Pfad-Umschreibung
- Autorisierung
- Verweigern

Ratenbegrenzung

Im Folgenden finden Sie eine Beispielkonfiguration für den `Ratelimit`-Richtlinientyp. Geben Sie die folgende Konfiguration im `config_spec`-Objekt an:

```
{

    "policytype": "Ratelimit",

    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],

            "get": true,

            "post": false,

            "put": false,

            "delete": false

        },

        "custom-rules": {},

        "threshold": "10",

        "timeslice": "20000",

        "limittype": "BURSTY",

        "api-respondertype": "DROP",

        "header_name": "x-api-key",

        "per_client_ip": true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    },
    "order_index": 1,
    "policy_name": "ratelimit_policy"
}
```

Weitere Informationen zu jedem Attribut finden Sie unter Ratenbegrenzungsrichtlinie.

OAuth

Im Folgenden finden Sie eine Beispiel-API-Konfiguration für den `JWT Auth validation`-Richtlinientyp. Geben Sie die folgende Konfiguration im `config_spec`-Objekt an:

```
{
    "policytype": "JWT Auth Validation",
    "config_spec": {
        "api-resource-paths": {
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
        },
        "custom-rules": {},
        "jwks-uri": "https://uri.petstore.com",
        "issuer": "https://issuer.petstore.com",
        "audience": "petstore",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "introspect-uri": "https://introspect.uri.com",
        "clientid": "client",
        "clientsecret": "clientsecret",
        "claims-to-save": ["scope", "scope2"],
        "allowed-algorithms": {
            "hs256": true,
            "rs256": true,
            "rs512": true
        }
    },
    "order_index": 2,
    "policy_name": "Jwt_auth_policy"
}
```

Weitere Informationen zu jedem Attribut finden Sie unter OAuth-Richtlinie

Basisauthentifizierung

Das Folgende ist eine Beispiel-API-Konfiguration für den `BasicAuth` Richtlinientyp:

```
{
    "config_spec": {
        "api-resource-paths": {
            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "get": true,
            "post": true,
            "put": false
        },
        "custom-rules": {}
    },
    "order_index": 3,
    "policy_name": "Auth_BaSIC",
    "policytype": "BasicAuth"
}
```

Weitere Informationen zu jedem Attribut finden Sie unter Basic authentication policy.

Keine Authentifizierung

Das Folgende ist eine Beispiel-API-Konfiguration für den `NoAuth` Richtlinientyp:

```
{
    "config_spec": {
        "api-resource-paths": {
            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": true,
            "post": false,
            "put": false
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        },
        "custom-rules": {}
    },
    "order_index": 4,
    "policy_name": "no_auth_policy",
    "policytype": "NoAuth"
}
```

Bot

Das Folgende ist eine Beispiel-API-Konfiguration für den `Bot` Richtlinientyp:

```
{
    "config_spec": {
        "api-resource-paths": {
            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": false,
            "post": false,
            "put": false
        },
        "bot-prof-name": "apisec_test_profile",
        "custom-rules": {}
    },
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "order_index": 5,

    "policy_name": "bot_policy",

    "policytype": "Bot"

}
```

Weitere Informationen zu jedem Attribut finden Sie unter Bot policy.

WAF

Das Folgende ist eine Beispiel-API-Konfiguration für den WAF-Richtlinientyp:

```
{

    "config_spec": {

        "api-resource-paths": {

            "delete": false,

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],

            "get": false,

            "post": false,

            "put": false

        },

        "waf-prof-name": "apisec_waf_profile",

        "custom-rules": {}

    },

    "order_index": 6,

    "policy_name": "waf_policy",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "policytype": "WAF"

}
```

Weitere Informationen zu jedem Attribut finden Sie unter WAF policy.

Header-Umschreibung

Das Folgende ist eine Beispiel-API-Konfiguration für den Richtlinientyp für Header-Umschreibung. Geben Sie diese Konfiguration im `config_spec` Objekt an:

```
{

    "policytype": "Header Rewrite",

    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],

            "get": true,

            "post": true,

            "put": false,

            "delete": false

        },

        "custom-rules": {},

        "rewrite-policy-header-field-name": "org",

        "rewrite-policy-header-field-val": "Citrix",

        "rewrite-policy-header-field-new-val": "Citrite"

    },

    "order_index": 7,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "policy_name": "header_rewrite_pol"

}
```

Weitere Informationen zu jedem Attribut finden Sie unter Header Rewrite policy.

URI-Pfad-Umschreibung

Das Folgende ist eine Beispiel-API-Konfiguration für den Richtlinientyp für URI-Pfad-Umschreibung:

```
{

    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/store/order", "/store/inventory"],

            "delete": false,

            "get": true,

            "post": true,

            "patch": false,

            "put": false

        },

        "custom-rules": {

            "delete": false,

            "endpoints": [],

            "get": false,

            "post": false,

            "patch": false,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "put": true
        },
        "path-rewrite-params": [
        {
            "insert-segment-position": "beginning",
            "new-path-value": "v3",
            "old-path-value": "v2",
            "action-type": "replace path segment"
        },
        {
            "insert-segment-position": "beginning",
            "new-path-value": "begin",
            "action-type": "insert path segment"
        },
        {
            "insert-segment-position": "end",
            "new-path-value": "end",
            "action-type": "insert path segment"
        },
        {
            "insert-segment-position": "before",
            "new-path-value": "before",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "old-path-value": "store",
            "action-type": "insert path segment"
        },
        {
            "insert-segment-position": "after",
            "new-path-value": "after",
            "old-path-value": "store",
            "action-type": "insert path segment"
        }
        ]
    },
        "order_index": 24,
        "policy_name": "eats_uripathrewrite",
        "policytype": "URI Path Rewrite”
}
```

Weitere Informationen zu jedem Attribut finden Sie unter URI Path Rewrite policy.

Autorisierung

Im Folgenden finden Sie eine Beispiel-API-Konfiguration für den `Authorization` Richtlinientyp. Geben Sie die folgende Konfiguration im `config_spec` Objekt an:

```
{
    "policytype": "Authorization",
    "config_spec": {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "api-resource-paths": {
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
        },
        "custom-rules": {},
        "claims": [{
            "name": "scope",
            "values": ["value1", "value2"]
        }]
    },
    "order_index": 8,
    "policy_name": "authorization"
}
```

Weitere Informationen zu jedem Attribut finden Sie unter Authorization policy.

Verweigern

Im Folgenden finden Sie eine Beispiel-API-Konfiguration für den `Deny` Richtlinientyp. Geben Sie die folgende Konfiguration im `config_spec` Objekt an:

```
{
    "policytype": "Deny",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "config_spec": {
        "api-resource-paths": {
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
        },
        "custom-rules": {},
        "api-denytype": "RESPONDWITH"
    },
    "order_index": 9,
    "policy_name": "deny_policy"
}
```

In `api-denytype` können Sie einen der folgenden Werte angeben:

- RESPONDWITH
- RESET

Weitere Informationen zu jedem Attribut finden Sie unter Deny rule.

WAF- und BOT-Profile mit StyleBooks erstellen

Wenn Sie eine Richtlinie für eine API-Ressource in **API Gateway** auswählen können, können Sie die Kriterien für die Datenverkehrsauswahl definieren, um eine API-Anfrage zu authentifizieren. Außerdem können Sie API-Sicherheitsrichtlinien für den API-Datenverkehr konfigurieren. Weitere Informationen finden Sie unter API-Sicherheit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können WAF- und BOT-Richtlinien für eine API-Ressource konfigurieren. Bevor Sie eine Richtlinie konfigurieren, stellen Sie sicher, dass Sie ihr Profil in NetScaler Console erstellen. Verwenden Sie die folgenden Standard-StyleBooks, um ein Profil zu erstellen:

- API WAF Detection StyleBook
- API BOT Detection StyleBook

Ein WAF-Profil mit StyleBooks erstellen

Führen Sie die folgenden Schritte aus, um ein WAF-Profil zu erstellen:

1. Navigieren Sie in NetScaler Console zu **Applications** > **Configurations** > **StyleBooks**. Suchen Sie nach dem StyleBook, indem Sie den Namen als `api-waf-profile` eingeben. Klicken Sie auf **Create Configuration**.

   Das StyleBook wird als Benutzeroberfläche geöffnet, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
2. Geben Sie Werte für die folgenden Parameter an:

   - **API WAF-Profilname** – Ein Name zur Identifizierung eines WAF-Profils.
   - **Anwendungstyp** – Fügen Sie dem Profil Anwendungstypen hinzu. Das WAF-Profil unterstützt JSON- und XML-Anwendungstypen.
3. Optional können Sie **Security Settings** aktivieren, um HTTP-, JSON- oder XML-Schutzprüfungen anzugeben. Sie können auch eine Fehler-URL für die NetScaler Web App Firewall angeben. Weitere Informationen finden Sie unter Erstellen eines Web App Firewall-Profils.
4. Wählen Sie die Ziel-NetScaler-Instanz oder Instanzgruppe aus, auf der Sie diese Konfiguration bereitstellen möchten.
5. Klicken Sie auf **Create**.

Um eine WAF-Richtlinie zu konfigurieren, siehe Richtlinien zu einer API-Bereitstellung hinzufügen.

BOT-Profil mit dem StyleBook erstellen

Führen Sie die folgenden Schritte aus, um ein BOT-Profil zu erstellen:

1. Navigieren Sie in NetScaler Console zu **Applications** > **Configurations** > **StyleBooks**. Suchen Sie das StyleBook, indem Sie den Namen als `api-bot-profile` eingeben. Klicken Sie auf **Konfiguration erstellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Das StyleBook wird als Benutzeroberflächenseite geöffnet, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

2. Geben Sie unter **BOT Profile Name** einen Namen an, um ein BOT-Profil zu identifizieren.
3. Optional: Aktivieren Sie die folgenden Optionen basierend auf Ihren Anforderungen:

    - **IP-Reputationsprüfung aktivieren** – Diese Option identifiziert die IP-Adresse, die unerwünschte Anfragen sendet. Sie können die IP-Reputationsliste verwenden, um Anfragen präventiv abzulehnen, die von IPs mit schlechter Reputation stammen.
    - **BOT-Signaturen aktivieren** – Geben Sie den Namen der BOT-Signatur an. Es blockiert die Anfragen von der angegebenen Signatur.
    - **Zulassungsliste** – Geben Sie eine IPv4- oder Subnetz- (CIDR-) Adresse an. Diese Option ermöglicht dem BOT-Profil, Anfragen von der angegebenen IPv4- oder Subnetzadresse zu umgehen.
    - **Sperrliste** – Geben Sie eine IPv4- oder Subnetz- (CIDR-) Adresse an. Diese Option ermöglicht dem BOT-Profil, Anfragen von der angegebenen IPv4- oder Subnetzadresse zu blockieren.

4. Wählen Sie die Ziel-NetScaler-Instanz oder Instanzgruppe aus, auf der Sie diese Konfiguration bereitstellen möchten.
5. Klicken Sie auf **Erstellen**.

Um eine BOT-Richtlinie zu konfigurieren, siehe Richtlinien zu einer API-Bereitstellung hinzufügen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Anwendungen

Die Funktion zur Anwendungsanalyse und -verwaltung von NetScaler Console ermöglicht es Ihnen, Anwendungen über einen anwendungszentrierten Ansatz zu überwachen. Dieser Ansatz hilft Ihnen dabei:

- Die Bewertung zu überprüfen und die Gesamtleistung der Anwendungen zu analysieren
- Nach Problemen zu suchen, die beim Server oder Client bestehen
- Anomalien in den Anwendungsverkehrsflüssen zu erkennen und Korrekturmaßnahmen zu ergreifen

> **HINWEIS**
>
> Anwendungen beziehen sich auf einen oder mehrere virtuelle Server, die auf den Instanzen (NetScaler) konfiguriert sind.

Sie können die Anwendungen für Zeiträume wie 1 Stunde, 1 Tag, 1 Woche und 1 Monat überwachen.

Voraussetzungen

- Stellen Sie sicher, dass Sie NetScaler-Instanzen in NetScaler Console hinzugefügt haben.
- Stellen Sie sicher, dass Sie eine gültige Lizenz für Ihre NetScaler-Instanzen besitzen. Weitere Informationen finden Sie unter Lizenzierung.

Anwendungsübersicht

Anwendungen können sein:

- Diskrete Anwendungen
- Benutzerdefinierte Anwendungen
- Microservices-Anwendungen (k8s_discrete)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Diskrete Anwendungen

Alle virtuellen Server, die in NetScaler® Console erkannt werden, werden als diskrete Anwendungen bezeichnet.

Benutzerdefinierte Anwendungen

Die virtuellen Server einer Kategorie werden als benutzerdefinierte Anwendungen bezeichnet. Als Administrator müssen Sie benutzerdefinierte Anwendungen basierend auf einer Kategorie hinzufügen. Sie können die Anwendungen dann über das Dashboard verwalten und überwachen. Dies erleichtert die Überwachung spezifischer Anwendungen, die unter einer Kategorie gruppiert sind.

Sie können beispielsweise eine Kategorie für Ihr Rechenzentrum1 erstellen und dessen NetScaler-Instanzen hinzufügen. Nachdem Sie eine Kategorie definiert und die Instanz für Ihr Rechenzentrum1 hinzugefügt haben, wird das Anwendungs-Dashboard mit einer separaten Kategorie angezeigt, die alle Anwendungen im Zusammenhang mit Ihrem Rechenzentrum1 umfasst.

Hinweise

- Die diskreten Anwendungen, die zu den benutzerdefinierten Anwendungen hinzugefügt werden, werden aus den diskreten Anwendungen entfernt.
- Alle Anwendungen, die keiner Kategorie hinzugefügt wurden, sind als **„Sonstige“** verfügbar.

Microservices-Anwendungen

In einem Kubernetes-Cluster bietet NetScaler einen Ingress Controller für NetScaler MPX (Hardware), NetScaler VPX (virtualisiert) und NetScaler CPX (containerisiert). Weitere Informationen finden Sie unter NetScaler Ingress Controller.

Die diskreten Anwendungen, die mit den NetScaler CPX-Instanzen konfiguriert werden, werden als Microservices-Anwendungen bezeichnet.

Anwendungsverwaltung und Anwendungs-Dashboard

NetScaler Console ermöglicht Ihnen die Verwaltung von Anwendungen und die Anzeige von Anwendungsdetails von der Seite **Dashboard**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Anwendungen verwalten

Vom Anwendungs-Dashboard aus klicken Sie auf **Apps verwalten**, um alle benutzerdefinierten und diskreten Anwendungen anzuzeigen.

Auf der Seite **Anwendungen verwalten** können Sie als Administrator:

- Anwendungen hinzufügen
- Anwendungsdetails anzeigen, wie z. B. App-Name, App-Typ, App-Kategorie, zugeordnete virtuelle Server, zugeordnete Dienste und so weiter.
- Benutzerdefinierte Anwendungen bearbeiten oder löschen

Nachdem Sie Anwendungen hinzugefügt, bearbeitet oder gelöscht haben, werden die Details sofort auf der Seite Anwendungen widergespiegelt.

Weitere Informationen finden Sie unter Anwendungen verwalten.

Anwendungs-Dashboard

Navigieren Sie zu **Anwendungen** > **Dashboard**, um die Liste der Anwendungen entweder in Tabellenansicht oder in grafischer Ansicht anzuzeigen.

Alle Anwendungen werden im Dashboard erst angezeigt, nachdem die Anwendungen begonnen haben, Daten zu erfassen. Klicken Sie im Dashboard auf eine Anwendung, um detaillierte Informationen zur Anwendungsleistung anzuzeigen. Weitere Informationen finden Sie unter Anwendungsdetails.

Wenn die Anwendungsanalyse selbst nach einer Dauer von etwa 10–15 Minuten nicht angezeigt wird, führen Sie die Schritte zur Fehlerbehebung unter Fehlerbehebung App-Dashboard aus.

Daten in Dashboard-Spalten sortieren

Im Anwendungs-Dashboard können Sie in der Tabellenansicht Daten nach den folgenden Spalten sortieren:

- **App-Score**
- **App-Name**
- **Antwortzeit**
- **Gesamtanfragen**
- **Durchsatz**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Datenvolumen**
- **Client-Verbindung**
- **Server-Verbindung**

Wenn Sie eine Sortierung anwenden, wird das Dashboard mit Anwendungen organisiert, die auf allen Seiten verfügbar sind. Wenn das Dashboard beispielsweise 5 Seiten umfasst, erfolgt die Sortierung über alle 5 Seiten hinweg und die Ergebnisse werden entsprechend angezeigt.

Aktualisierungen im neuen Dashboard-Verhalten im Vergleich zum früheren Dashboard

- Nachdem Sie eine benutzerdefinierte Anwendung hinzugefügt oder bearbeitet haben, kann es einige Minuten dauern, bis die Anwendung im Dashboard angezeigt wird.
- Wenn Sie eine benutzerdefinierte Anwendung löschen, zeigt das Dashboard die gelöschte Anwendung weiterhin an, bis NetScaler Console ihre Analysedaten (maximal 1 Monat Dauer) hat.

  Betrachten Sie ein Szenario, in dem Sie am Jan 2, 2020 eine Anwendung erstellt und am Jan 4, 2020 gelöscht haben. In diesem Szenario:

  - Das Dashboard kann die gelöschte Anwendung am Jan 4, 2020 weiterhin anzeigen, wenn Sie die Zeitdauer für den letzten Tag, die letzte Woche und den letzten Monat auswählen.
  - Das Dashboard kann die gelöschte Anwendung am Jan 5, 2020 weiterhin anzeigen, wenn Sie die Zeitdauer für die letzte Woche und den letzten Monat auswählen.
  - Wenn die Dauer das Löschdatum der Anwendung überschreitet, wird die Anwendung nicht im Dashboard angezeigt. Das heißt, das Dashboard wird nicht mit der gelöschten Anwendung am Jan 6, 2020 (für den letzten Tag), Jan 12, 2020 (für die letzte Woche) und nach February 5, 2020 (für den letzten Monat) angezeigt.
  - Wenn Sie im Dashboard auf die gelöschte Anwendung klicken, wird die folgende Meldung angezeigt.

    HINWEIS

    Nachdem Sie eine Anwendung hinzugefügt haben, wenn die zugehörige NetScaler-Instanz ausgefallen, außer Betrieb oder aufgrund einer vorübergehenden Netzwerkstörung nicht erreichbar ist:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

-Die Anwendungen, die der NetScaler-Instanz zugeordnet sind, sind nur auf der Seite **Anwendungen** sichtbar, aber nicht im Dashboard.
-Die Anwendungen werden im Dashboard angezeigt, nachdem die NetScaler-Instanz betriebsbereit ist.

Anwendungen verwalten

Klicken Sie im Dashboard auf **Apps verwalten**, um Anwendungsdetails anzuzeigen und benutzerdefinierte Anwendungen hinzuzufügen, zu bearbeiten oder zu löschen.

Anwendungsdetails anzeigen

- **App-Name** – Bezeichnet den Anwendungsnamen
- **Status** – Bezeichnet den aktuellen Anwendungsstatus, wie z. B. **Up**, **Down**, **Partially Up**, **Out of Service** und **NA**
  - **Up** – Alle mit der Anwendung verbundenen virtuellen Server sind Up.
  - **Down** – Alle mit der Anwendung verbundenen virtuellen Server sind Down.
  - **Partially Up** – Entweder ein mit der Anwendung verbundener virtueller Server ist Down oder außer Betrieb.
  - **Out of Service** – Alle mit den Anwendungen verbundenen virtuellen Server sind außer Betrieb.
  - **NA** – Für die Anwendung sind keine virtuellen Server konfiguriert.
- **Typ** – Gibt an, ob die Anwendung zu Custom oder Discrete gehört.
- **Kategorie** – Bezeichnet die gruppierte Anwendungskategorie.
- **Virtueller Server/Status** – Bezeichnet die insgesamt konfigurierten virtuellen Server und den Status aller virtuellen Server. Fahren Sie mit dem Mauszeiger darüber, um Details wie die Gesamtzahl der virtuellen Server, den Typ des virtuellen Servers und den Status des virtuellen Servers anzuzeigen.

- **Dienste/Status** – Gibt die Gesamtzahl der konfigurierten Dienste und den Status aller Dienste an
- **Dienstgruppen/Status** – Gibt die Gesamtzahl der konfigurierten Dienstgruppen und den Status aller Dienstgruppen an

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Server/Status** – Gibt die Gesamtzahl der für die Anwendung konfigurierten Server und den Status aller Server an
- **Aktionen** – Ermöglicht das Bearbeiten oder Löschen der benutzerdefinierten Anwendungen

Eine Anwendung hinzufügen

1. Klicken Sie auf **Neue Anwendung**, um eine Anwendung zu erstellen

   Die Seite **Anwendung definieren** wird angezeigt

2. Legen Sie die folgenden Parameter fest:

FELD	BESCHREIBUNG
Name	Der Name der benutzerdefinierten Anwendung. Zum Beispiel LB_TEST.
Kategorie	Die Kategorie, in der Sie die Anwendungen gruppieren können. Klicken Sie, um zur Seite Anwendungs-Kategorie zu gelangen. Wählen Sie die Kategorie aus und klicken Sie auf **Auswählen**. So fügen Sie eine Kategorie hinzu:
	1. Klicken Sie auf **Hinzufügen**
	2. Geben Sie einen Namen Ihrer Wahl ein.
	3. Klicken Sie auf **Erstellen**
Vorhandene Anwendungen auswählen	Ermöglicht Ihnen, die vorhandenen Anwendungen auszuwählen, die den NetScaler-Instanzen hinzugefügt wurden.
Anwendung hinzufügen	Zeigt alle virtuellen Server an, die auf den Instanzen konfiguriert sind. Wählen Sie die Anwendungen aus der Liste aus und klicken Sie auf **OK**.
Auswahlkriterien definieren	Option zur Definition der Anwendung nach virtuellem Serverbereich oder nach Ursprungsserver-/Dienst-IP-Adressbereich.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FELD	BESCHREIBUNG
	- **Server.** Geben Sie die Server- oder Dienst-IP-Adresse, den Servernamen oder den Port des Back-End-Servers an, auf dem die Anwendungen ausgeführt werden. Sie können eine IP-Adresse, einen Bereich von IP-Adressen oder eine Kombination aus beidem, durch Kommas getrennt, eingeben. Zum Beispiel können Sie 10.102.29.20, 10.102.43.10-60, 10.216.43.45 eingeben.
	- **Virtuelle Server.** Sie können eine der folgenden Angaben machen: die IP-Adresse des virtuellen Servers, den Namen des virtuellen Servers oder den Port des Back-End-Servers, auf dem die Anwendungen ausgeführt werden. Sie können eine IP-Adresse, einen Bereich von IP-Adressen oder eine Kombination aus beidem, durch Kommas getrennt, eingeben. Zum Beispiel können Sie 10.102.29.20, 10.102.43.10-60, 10.216.43.45 eingeben.
Eine Anwendung aus einem StyleBook erstellen	Ermöglicht Ihnen, eine Anwendung mit dem StyleBook zu erstellen. Weitere Informationen finden Sie unter Eine Anwendung mit dem StyleBook erstellen.

3. Klicken Sie auf **OK**.

HINWEIS:

Derzeit unterstützt das Anwendungs-Dashboard nur Lastausgleichs- und Content-Switching-virtuelle Server.

Das Anwendungs-Dashboard wird nun mit der Kategorie angezeigt, und alle Anwendungen sind darunter gruppiert.

Wenn Sie eine Anwendung mit StyleBooks erstellen, bestätigen Sie den erforderlichen Lizenzverbrauch während der Anwendungsbereitstellung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Klicken Sie bei der Bestätigungsmeldung auf **Ja**. Die NetScaler Console weist einer Anwendung die erforderlichen Lizenzen zu.

Erstellen einer Anwendung mit dem StyleBook

So erstellen Sie eine Anwendung mit dem StyleBook:

1. Navigieren Sie in der NetScaler Console zu **Applications** > **Dashboard** und klicken Sie auf **Manage Apps**.
2. Wählen Sie die Anwendungskategorie im Abschnitt **Category** aus. Mit NetScaler Console können Sie Kategorien definieren, um die benutzerdefinierten Anwendungen zu gruppieren. Sie können bei Bedarf auch weitere Kategorien hinzufügen.
3. Klicken Sie auf **Create a new application from a StyleBook** und dann auf **OK**.

   Die Seite „Choose StyleBook“ wird angezeigt. Diese Seite enthält alle in NetScaler Console verfügbaren Standard-StyleBooks.
4. Wählen Sie das StyleBook aus. Die Seite **Configuration Details** wird angezeigt.
5. Geben Sie die Werte für alle Parameter im StyleBook ein. Sie können auch auf „View Definition“ klicken, um die Struktur des StyleBooks vor der Verwendung anzuzeigen.

   Weitere Informationen finden Sie unter Use Default StyleBooks.
6. Klicken Sie auf **Create**.

   Eine Bestätigungsmeldung wird angezeigt, um die erforderlichen Lizenzen zu verbrauchen und eine Anwendung bereitzustellen.
7. Klicken Sie auf **Ja**.

Sie können auch auf **Dry Run** klicken, um die Konfigurationen zu überprüfen, die NetScaler Console auf der ausgewählten NetScaler-Instanz zu erstellen versucht. Diese Option dient nur zu Testzwecken, um die endgültige Überprüfung der Konfigurationen zu sehen. Selbst wenn die Dry Run-Option erfolgreich ist, kann die tatsächliche Konfiguration auf dem ausgewählten NetScaler aus verschiedenen Gründen (IP-Konflikt, Instanz nicht erreichbar usw.) immer noch fehlschlagen.

Eine Anwendung bearbeiten oder löschen

Auf der Seite **Anwendungen verwalten** können Sie die benutzerdefinierten Anwendungen bearbeiten oder löschen. Klicken Sie auf die Schaltfläche „Bearbeiten“, um eine Anwendung zu bearbeiten, und klicken Sie auf die Schaltfläche „Löschen“, um die Anwendung zu entfernen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Berichte des App-Dashboards und des Sicherheits-Dashboards exportieren

NetScaler Console ermöglicht es Ihnen, einen Snapshot des aktuellen App-Dashboards zu erstellen und diesen als Berichte zu exportieren. In regelmäßigen Abständen müssen die App-Administratoren diese Berichte möglicherweise verwenden, um Informationen zur App-Nutzung und zu Leistungseinbußen zu aktualisieren.

Mit dieser Funktion können die Administratoren diese Daten als .png-, .jpeg- oder .pdf-Berichte extrahieren.

HINWEIS

Im Gegensatz zu anderen Berichts-Exportoptionen in NetScaler Console können Sie die Berichte des App-Dashboards und des Sicherheits-Dashboards nur als .pdf- oder .png-Dateien exportieren. Das .csv-Format wird derzeit nicht unterstützt.

Der Bericht wird auf Ihr System heruntergeladen. Von den Seiten „App-Dashboard“ und „App-Sicherheits-Dashboard“ aus können Sie auch zu Seiten der zweiten Ebene navigieren und diese als Berichte exportieren. Derzeit können Sie Berichte nur für eine Anwendung gleichzeitig herunterladen.

Anwendungen anzeigen

Standardmäßig zeigt das Anwendungs-Dashboard alle Anwendungen an. Je nach Anforderung können Sie die Filteroption verwenden, um Anwendungen anzuzeigen.

HINWEIS:

Ab Build **14.1 20.x** können Sie Metrikdetails für Anwendungen anzeigen, die aus den NetScaler-Administratorpartitionen erstellt wurden.

Das Dashboard zeigt die folgenden Anwendungsdetails an:

- **App-Name** – Bezeichnet den Anwendungsnamen.
- **Instanz** – Bezeichnet die NetScaler-Instanz.
- **App-Score** – Bezeichnet den Anwendungs-Score und den Status wie **Kritisch**, **Gut**, **Mittelmäßig** und **Nicht zutreffend**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Status** – Bezeichnet die aktuelle Verfügbarkeit der Anwendung, z. B. **Aktiv**, **Inaktiv**, **Teilweise aktiv**, **Außer Betrieb** und **N/A**.
  - **Aktiv** – Alle mit der Anwendung verbundenen virtuellen Server sind aktiv.
  - **Inaktiv** – Alle mit der Anwendung verbundenen virtuellen Server sind inaktiv.
  - **Teilweise aktiv** – Entweder ein mit der Anwendung verbundener virtueller Server ist inaktiv oder außer Betrieb.
  - **Außer Betrieb** – Alle mit den Anwendungen verbundenen virtuellen Server sind außer Betrieb.
  - **N/A** – Für die Anwendung sind keine virtuellen Server konfiguriert.
- **App-Typ** – Bezeichnet den Anwendungstyp, wie z. B. **Benutzerdefiniert**, **Diskret** oder **Kubernetes-Dienste**.
- **App-Kategorie** – Bezeichnet die Kategorie, die der Anwendung zugewiesen ist.
- **Hauptproblem** – Bezeichnet das Problem mit der höchsten Fehleranzahl bei der Anwendung.
- **Hauptproblemkategorie** – Bezeichnet die Kategorie des Problems.
- **Problemanzahl** – Bezeichnet die Gesamtzahl der Probleme für die Anwendung.
- **Antwortzeit** – Bezeichnet die durchschnittliche Antwortzeit der Anwendung.
- **Gesamtanfragen** – Bezeichnet die Gesamtzahl der von der Anwendung empfangenen Anfragen.
- **Durchsatz** – Bezeichnet den gesamten Netzwerkdurchsatz für die Anwendung. Der Durchsatz wird berechnet als Req Bytes / Sec + Res Bytes / Sec für die virtuellen Server.
- **Datenvolumen** – Bezeichnet das von der Anwendung verarbeitete Gesamtvolumen an Daten.
- **Client-Verbindungen** – Bezeichnet die durchschnittlichen Client-Verbindungen, die von der Anwendung hergestellt wurden.
- **Server-Verbindungen** – Bezeichnet die durchschnittlichen Server-Verbindungen, die von der Anwendung hergestellt wurden.

Microservices-Anwendungen anzeigen

Um die Microservices-Anwendungen anzuzeigen, wählen Sie die Option **K8s_Discrete** unter dem Filter **App-Typ** aus.

Sie können die Microservice-Anwendungen im **App Dashboard** im folgenden Namensformat anzeigen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`<k8s service>_<k8s namespace>_<k8s cluster_name>`

Zum Beispiel bezieht sich `tea-beverage_sg-demo_adm-cluster` auf einen Dienst namens „tea-beverage“ mit dem Namespace `sg-demo` im Cluster `adm-cluster`.

Die folgenden Metriken werden im Dashboard für den ausgewählten Zeitraum angezeigt:

- **App-Name** – Bezeichnet den Anwendungsnamen.
- **Instanz** – Bezeichnet die IP-Adresse der NetScaler CPX-Instanz.
- **App-Score** – Bezeichnet den App-Score.
  - **Kritisch** – Der App-Score liegt zwischen 0 und < 40
  - **Überprüfung** – Der App-Score liegt zwischen 40 und < 75
  - **Gut** – Der App-Score ist größer als 75
- **Status** – Bezeichnet den aktuellen Anwendungsstatus.
- **App-Kategorie** – Bezeichnet den Clusternamen, auf dem die Anwendung gehostet wird.
- **Hauptproblem** – Bezeichnet die Hauptprobleme, die den aktuellen App-Score beeinflussen.
- **Hauptproblemkategorie** – Bezeichnet die Problemkategorie, die die Anwendung beeinflusst.
- **Anzahl der Probleme** – Bezeichnet die Gesamtzahl der Probleme, die die Anwendung beeinflussen. Fahren Sie mit dem Mauszeiger über die Anzahl der Probleme, um eine Übersicht der Probleme anzuzeigen.

- **Antwortzeit** – Gibt die durchschnittliche Antwortzeit an, die von der Anwendung empfangen wird.
- **Fehlerprozentsatz** – Gibt den durchschnittlichen Fehlerprozentsatz von 5xx-Fehlern für die Anwendung an.
- **Gesamtanfragen** – Gibt die Gesamtzahl der von der Anwendung empfangenen Anfragen an.
- **Durchsatz** – Gibt den gesamten Netzwerkdurchsatz an, der von der Anwendung verarbeitet wird.
- **Datenvolumen** – Gibt die von der Anwendung verarbeiteten Gesamtdaten an. Das Datenvolumen wird als die gesamten Anforderungs- und Antwortbytes für die Anwendung berechnet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Clientverbindungen** – Gibt die durchschnittlichen Clientverbindungen an, die von der Anwendung hergestellt wurden. Dies kann sich auch auf die zugehörigen ausgehenden Dienste beziehen, die mit dem ausgewählten Dienst verbunden sind.
- **Serververbindungen** – Gibt die durchschnittlichen Serververbindungen an, die von der Anwendung hergestellt wurden. Dies kann sich auch auf die zugehörigen eingehenden Dienste beziehen, die mit dem ausgewählten Dienst verbunden sind.

Klicken Sie auf die Option **+**, um die im Dashboard anzuzeigenden Optionen hinzuzufügen oder zu entfernen.

Klicken Sie auf eine Anwendung, um die Anwendungsdetails anzuzeigen. Weitere Informationen finden Sie unter Microservices-Anwendungsdetails

Eine Anwendung konfigurieren und mehreren benutzerdefinierten Anwendungen zuordnen

Im **Anwendungs-Dashboard** können Sie eine Anwendung konfigurieren und mehreren benutzerdefinierten Anwendungen zuordnen. Mit dieser Funktion können Sie dieselbe Anwendung für mehrere benutzerdefinierte Anwendungen wiederverwenden, anstatt für jede benutzerdefinierte App eine separate Anwendung zu erstellen.

Angenommen, Sie verwalten zwei E-Commerce-Portale mit den Namen **ComABC** bzw. **ComCDE**, und Sie möchten einen Payment-Gateway-Server mit dem Namen **PaymentApp** für beide Portale verwenden. In diesem Szenario müssen Sie:

- Erstellen Sie zwei benutzerdefinierte Apps mit den Namen **ComABC** und **ComCDE**.
- Erstellen Sie eine Anwendung mit dem Namen **PaymentApp** und ordnen Sie sie **ComABC** und **ComCDE** zu.

Um dieses Szenario zu implementieren, müssen Sie:

- Erstellen Sie die **benutzerdefinierten Apps (ComABC und ComCDE)**:
  a. Navigieren Sie zu **Applications > Dashboard**, und klicken Sie auf **Manage Apps**.
  b. Klicken Sie auf **New Application**.
  c. Geben Sie einen Namen und eine Kategorie an.
  d. Wählen Sie den Typ für die Auswahl der Anwendung aus. In diesem Beispiel ist die Option **Select Existing Applications** ausgewählt. Weitere Informationen finden Sie unter Anwendung hinzufügen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. Klicken Sie unter **Applications** auf **Add Applications**.

f. Wählen Sie die Anwendungen aus der Liste aus und klicken Sie auf **OK**, um die benutzerdefinierte App zu erstellen.

- Erstellen Sie die **PaymentApp**. Dazu müssen Sie eine diskrete App in eine benutzerdefinierte App konvertieren:

  a. Navigieren Sie zu **Applications > Dashboard**, und klicken Sie auf **Manage Apps**.

  b. Klicken Sie auf **Neue Anwendung**.

  c. Geben Sie einen Namen und eine Kategorie an.

  d. Wählen Sie den Typ für die Auswahl der Anwendung aus. In diesem Beispiel ist die Option „Vorhandene Anwendungen auswählen“ ausgewählt. Weitere Informationen finden Sie unter Anwendung hinzufügen.

  e. Klicken Sie unter **Anwendungen** auf **Anwendungen hinzufügen**.

  f. Wählen Sie die Anwendungen aus der Liste aus und klicken Sie auf **OK**, um die benutzerdefinierte App zu erstellen.

- Als Nächstes können Sie die **PaymentApp** verwenden und sie mit **ComABC** und **ComCDE** verknüpfen.

  a. Navigieren Sie zu **Applications > Dasboard** und **klicken Sie auf Manage Apps**.

  b. Suchen Sie die **ComABC**-App und klicken Sie auf **Bearbeiten**.

  c. Klicken Sie unter **Referenced Applications** auf **Add Custom Applications** und wählen Sie die **PaymentApp** aus.

  d. Die **PaymentApp** ist jetzt unter **Referenced Applications** verfügbar. Klicken Sie auf **OK**, um die **PaymentApp** mit der benutzerdefinierten App **ComABC** zu verknüpfen.

  e. Wiederholen Sie den gleichen Vorgang für die benutzerdefinierte App **ComCDE**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Nachdem die Anwendung der benutzerdefinierten App zugeordnet wurde, wird der endgültige App-Score für die benutzerdefinierte App basierend auf dem niedrigsten Score zwischen der benutzerdefinierten App und der referenzierten App berechnet. Wenn in diesem Beispiel der **ComABC**-App-Score 85 und der **PaymentApp**-Score 69 beträgt, wird der endgültige Score für die **ComABC**-App 69.

Übersicht des Anwendungs-Dashboards

Das Anwendungs-Dashboard zeigt die einzelnen Anwendungen unter **Andere** und die benutzerdefinierten Anwendungen an, die unter ihren jeweiligen Kategorien gruppiert sind.

Navigieren Sie zu **Anwendungen** > **Dashboard**, um das App-Dashboard anzuzeigen.

1 – Zeigt die Anwendungsdetails für den ausgewählten Zeitraum an, z. B. 1 Stunde, 1 Tag, 1 Woche und 1 Monat.

2 – Ermöglicht Ihnen die Verwaltung von Anwendungen und das Hinzufügen neuer Anwendungen

3 – Ermöglicht Ihnen die Anzeige von Anwendungen entweder in der Tabellenansicht oder in der Diagrammansicht

4 – Ermöglicht Ihnen die Suche nach einer Anwendung über die Suchleiste

5 – Ermöglicht Ihnen das Anwenden von Filtern zur Anzeige von Anwendungen. Klicken Sie hier, um Details anzuzeigen.

Der Karussell-Schieberegler ermöglicht Ihnen einen einfachen Zugriff auf alle Optionen.

Sie können:

- Auswählen, um Anwendungen basierend auf den Bewertungen anzuzeigen.
    - **Kritisch** – Der Anwendungs-Score liegt zwischen 0 und < 40
    - **Mittel** – Der Anwendungs-Score liegt zwischen 40 und < 75
    - **Gut** – Anwendungsbewertung ist größer als 75
    - **Nicht zutreffend** – Entweder sind keine virtuellen Server für die Anwendung konfiguriert, oder der Typ des virtuellen Servers ist nicht Lastausgleich oder Inhaltswechsel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die folgende Tabelle beschreibt die Unterschiede zwischen der früheren App-Bewertung und der aktuellen App-Bewertung.

ANWENDUNGSBEWERTUNG (KRITISCH, ÜBERPRÜFUNG, GUT, NICHT ZUTREFFEND)	APP-BEWERTUNG (FRÜHERE ANSICHT MIT FARBLEGENDEN)
Die Bewertung wird berechnet als **100 minus Fehlerpunkte aller aktuellen Anwendungsprobleme**	Die Bewertung wird berechnet als **100 – (App-Server-Ressource + NetScaler-Systemressource)**
Anwendungen werden in Farben wie **Rot (kritisch)**, **Orange (Überprüfung)**, **Grün (gut)** und **Grau (Nicht zutreffend)** angezeigt	Anwendungen werden in Farblegenden angezeigt.

- Auswählen, um Anwendungen basierend auf dem Anwendungsstatus wie „Up“, „Down“ und „Out of Service“ anzuzeigen
- Auswählen, um Anwendungen basierend auf dem Anwendungstyp wie „Diskret“ oder „Benutzerdefiniert“ anzuzeigen
- Auswählen, um Anwendungen basierend auf den darunter gruppierten Kategorien anzuzeigen
- Ziehen Sie das Histogramm, um Filter anzuwenden und Anwendungen anzuzeigen.

  Wenn Sie beispielsweise Anwendungen anzeigen möchten, deren Virtual Server Health zwischen 0 und 20 liegt, ziehen Sie das Histogramm für Virtual Server Health, um die Ergebnisse zu filtern.

  HINWEIS:

  Sie können auch auf das Histogramm klicken, um die relevanten Anwendungen anzuzeigen.

  Klicken Sie auf **Alle löschen**, um den angewendeten Filter zu entfernen.

  Im Folgenden finden Sie die Anwendungsübersicht, für die Sie Filter anwenden können:

  - **Anwendungsbewertung** – Ermöglicht die Anzeige von Anwendungen basierend auf **Kritisch**, **Überprüfung**, **Gut** und **Nicht zutreffend**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Standardmäßig können Sie Anwendungen anzeigen, die den Status Kritisch, Überprüfung und Gut haben. Um Anwendungen anzuzeigen, die den Status N/A haben, müssen Sie die Option **Nicht zutreffend** auswählen.

- **Status** – Ermöglicht die Anzeige von Anwendungen basierend auf dem Anwendungsstatus wie Aktiv, **Inaktiv** und **Außer Betrieb**.
- **Aktuelle Probleme** – Ermöglicht Ihnen, eine Liste der von einem bestimmten Problem betroffenen Anwendungen abzurufen, indem Sie den Problemtyp wie **Leistung**, **Instanzzustand**, **Konfiguration** und **Systemressourcen** auswählen.
- **App-Typ** – Ermöglicht die Anzeige von Anwendungen basierend auf dem Anwendungstyp wie **Benutzerdefiniert**, **Diskret** und **Kubernetes-Dienste**.
- **App-Kategorie** – Ermöglicht die Anzeige der Anwendungen basierend auf der zugewiesenen Kategorie.
- **Antwortzeit** – Ein Histogramm, das die durchschnittliche Antwortzeit anzeigt, die von den Anwendungen empfangen wurde.
- **Gesamtanfragen** – Ein Histogramm, das die Gesamtzahl der von den Anwendungen empfangenen Anfragen anzeigt.
- **Durchsatz** – Ein Histogramm, das den gesamten Netzwerkdurchsatz anzeigt, der von den Anwendungen verarbeitet wurde.
- **Datenvolumen** – Ein Histogramm, das die von den Anwendungen verarbeiteten Gesamtdaten anzeigt. Das Datenvolumen wird anhand der gesamten Anforderungs-Bytes und Antwort-Bytes für die Anwendungen berechnet.
- **Client-Verbindungen** – Ein Histogramm, das die durchschnittlichen Client-Verbindungen anzeigt, die von den Anwendungen hergestellt wurden.
- **Server-Verbindungen** – Ein Histogramm, das die durchschnittlichen Server-Verbindungen anzeigt, die von den Anwendungen hergestellt wurden.
- **Gesendete Pakete** – Ein Histogramm, das die von den Anwendungen gesendeten Gesamtpakete anzeigt.
- **Empfangene Pakete** – Ein Histogramm, das die von den Anwendungen empfangenen Gesamtpakete anzeigt.
- **Integrität des virtuellen Servers** – Ein Histogramm, das die Gesamtzahl der Anwendungen im Bereich von 0 % bis 100 % anzeigt. Die Integrität eines virtuellen Servers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ist der Prozentsatz der aktiven Dienste, die der Anwendung zugeordnet sind. Wenn beispielsweise ein virtueller Server mit 2 Diensten konfiguriert ist und einer davon ausgefallen ist, beträgt der Wert 50 %.

Ergebnisse mithilfe der Suchleiste suchen und filtern

Sie können den Mauszeiger auf die Suchleiste legen und die Kategorie auswählen, um die Suche zu verfeinern.

Filter speichern

Sie können Filter im App-Dashboard anwenden und speichern. Anschließend können Sie den Filternamen aus der Liste auswählen und das angepasste Dashboard bei Bedarf anzeigen.

Angenommen, Sie möchten einen Filter für Anwendungen erstellen, die sich im Status **Up** befinden. Klicken Sie im **App-Dashboard**, nachdem Sie den Filter angewendet haben, auf **Filter speichern**.

Geben Sie einen Namen Ihrer Wahl ein und klicken Sie auf **Speichern**.

Sie können auch **Als Standardfilter festlegen** auswählen, um diesen Filter als Standardansicht im App-Dashboard zu verwenden.

Sie können mehrere Filter speichern und den Filternamen aus der Liste auswählen, um das angepasste Dashboard bei Bedarf anzuzeigen.

Um den Standardfilter oder den Filter zu entfernen, klicken Sie auf das Filtersymbol neben der Filterliste.

Tags für Anwendungen erstellen und anwenden

Wenn Sie eine große Anzahl von Anwendungen haben, können Sie Tags für Anwendungen erstellen und anwenden. Diese Tags verbessern die Suchfunktion.

Beispiel:

Die folgende Prozedur listet die Schritte zum Erstellen von Tags für die Lastausgleichsanwendungen auf:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Wählen Sie im **App-Dashboard** die Lastausgleichsanwendungen aus, für die Sie Tags erstellen möchten, und klicken Sie auf **Tags**.

2. Unter **Tags aktualisieren**:

   - Geben Sie einen Namen Ihrer Wahl an. Zum Beispiel: **Typ**.
   - Geben Sie den Wert an, der es Ihnen ermöglicht, die Tags zuzuweisen. Sie können auch mehrere Werte eingeben. Zum Beispiel: **Lastausgleich**.
   - Klicken Sie auf **Anwenden**.

   Der Tag wurde erstellt.

So wenden Sie Tags an und rufen die Load-Balancing-Anwendungen ab:

1. Klicken Sie in der Suchleiste des App-Dashboards in das Textfeld, um den erstellten Tag anzuzeigen und den Tag-Namen auszuwählen.

2. Wählen Sie den Operator (**IN**) und den erstellten Wert aus, und klicken Sie dann auf **Suchen**.

   Alle Load-Balancing-Anwendungen, die unter **Loadbalance** getaggt sind, werden aufgelistet. Ähnlich können Sie Tags für andere Anwendungen erstellen.

Anwendungsdetails

HINWEIS:

Ab dem Build **14.1 20.x** können Sie Metrikdetails für Anwendungen anzeigen, die aus den NetScaler-Administratorpartitionen erstellt wurden.

Klicken Sie im Dashboard auf eine Anwendung, um weitere detaillierte Informationen anzuzeigen.

Die Seite der ausgewählten Anwendung wird angezeigt.

Auf der Seite mit den Anwendungsdetails:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wählen Sie die Zeitdauer aus der Liste aus, um Details für die spezifische Zeitdauer anzuzeigen.
- Klicken Sie auf **Service Graph**, um den Service-Graphen für die ausgewählte Anwendung anzuzeigen. Weitere Informationen finden Sie unter Service Graph für Anwendungen
- Klicken Sie auf **Transaktionsprotokolle**, um die detaillierten Transaktionen für die ausgewählte Anwendung anzuzeigen.
- Klicken Sie auf **Audit-Protokolle**, um die detaillierten Audit-Protokollinformationen anzuzeigen.
- Klicken Sie auf **Konfigurieren**, um die Dienst- und Dienstgruppenkonfiguration für die ausgewählte Anwendung anzuzeigen oder zu bearbeiten.
- Klicken Sie auf **Dienst**, um die Dienste anzuzeigen, die an die Anwendung gebunden sind.

Nachdem Sie die Zeitdauer ausgewählt haben, werden die folgenden Anwendungsdetails angezeigt:

- **App-Score** – Der Anwendungs-Score für den ausgewählten Zeitraum. Der endgültige Score wird als **100 minus Gesamtstrafe** berechnet.

  Dieses Dashboard ermöglicht es Ihnen auch, die aktuellen Probleme anzuzeigen, die den App-Score beeinflussen. Sie können die Details der Probleme unter „Probleme“ anzeigen.

- **Virtuelle Server** –

  HINWEIS

  Der Abschnitt **Virtuelle Server** wird nur für benutzerdefinierte Anwendungen angezeigt. Klicken Sie bei diskreten Anwendungen auf die **IP-Adresse**, um die Details des virtuellen Servers anzuzeigen.

  Zeigt alle virtuellen Server an, die der benutzerdefinierten Anwendung zugeordnet sind

  Klicken Sie auf **Details anzeigen**, um die Einstellungen des virtuellen Servers anzuzeigen und zu verwalten.

- **Alle Dienste** – Die Dienste, die an die Anwendung gebunden sind

  Klicken Sie hier, um die Dienstdetails anzuzeigen und die Diensteinstellungen zu verwalten

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Probleme** – Die Probleme, die für die ausgewählte Anwendung zutreffen. Sie können die folgenden Probleme zusammen mit ihrer Kategorie anzeigen:

LEISTUNG	INSTANZZUSTAND	KONFIGURATION	SYSTEMRESSOURCEN
Antwortzeit	Durchschnittliche CPU-Auslastung	Instabiler Server	Falscher Persistenztyp
Aktive Dienste	Speicherauslastung	Ungewöhnlich große HTTP-Pakete	NIC-Kartensättigung
Geringe Sitzungswiederverwendung		TCP-Neuordnungs-Warteschlangengrenze erreicht	
App-CPU-Auslastung			
SurgeQueue-Aufbau			
SSL-Echtzeit-Traffic			
Sitzungsaufbau			
Server-Antwortzeit			
Service-Flaps			

Klicken Sie auf jedes Problem, um Details wie die Erkennungsmeldung, den Zeitpunkt des Auftretens des Problems, empfohlene Aktionen und weitere Details anzuzeigen.

Weitere Informationen finden Sie unter Leistungsindikatoren für Anwendungsanalysen.

Die folgende Abbildung zeigt die frühere Ansicht der Seite **App Activity Investigator**:

Sie können jetzt alle Probleme im Abschnitt **Probleme** anzeigen, zusammen mit der Kategorie, die Sie auf der Seite **App Activity Investigator** anzeigen konnten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die Probleme, die auf der Registerkarte **Aktuell** angezeigt werden, beziehen sich auf die Anwendungsprobleme für die ausgewählte Zeitdauer.
- Die Probleme, die auf der Registerkarte **Alle** angezeigt werden, beziehen sich auf alle Anwendungsprobleme.

Das folgende Beispiel zeigt die Anwendungsprobleme für eine Dauer von 1 Tag. Die Registerkarte **Aktuell** zeigt an, dass keine aktuellen Probleme die App-Bewertung beeinflussen.

Aktuell(/en-us/netscaler-console-service/media/issue-current.png)

Die Registerkarte **Alle** zeigt die Gesamtzahl der erkannten Probleme für die Dauer von 1 Tag an.

Alle(/en-us/netscaler-console-service/media/issue-all.png)

Monitorstatus einer Anwendung überprüfen

Sie können das Anwendungs-Dashboard in der NetScaler Console GUI unter **Applications > Dashboard** verwenden, um den Status des Integritätsmonitors einer Anwendung und gegebenenfalls die Fehlermeldung anzuzeigen. Integritätsmonitore können an einen Dienst oder eine Dienstgruppe einer Anwendung gebunden werden, und ein Dienst oder eine Dienstgruppe kann mehrere Monitore gebunden haben. Monitore helfen Ihnen, Ihre Dienste zu überwachen.

Um den Status der Monitore anzuzeigen, führen Sie die folgenden Schritte aus.

1. Navigieren Sie in der NetScaler Console GUI zu **Applications > Dashboard**. Wählen Sie unter **Applications** die Anwendung aus, deren Integrität Sie überprüfen möchten.

   Anwendung auswählen(/en-us/netscaler-console-service/media/monitor-app-step1.png)
2. Klicken Sie auf die Anwendung. Das App-Score-Dashboard wird angezeigt.

   App-Dashboard(/en-us/netscaler-console-service/media/monitor-app-step2.png)
3. Klicken Sie auf die Registerkarte **Services** oben rechts oder auf die Dienstgruppe unter **Group Name**.
4. Wenn Sie auf die Registerkarte **Services** klicken, wählen Sie im nächsten Bildschirm die Dienstgruppe aus.
5. Wenn Sie auf die Dienstgruppe klicken, wird das Fenster **Service Groups** angezeigt. Wählen Sie die Instanz aus und klicken Sie auf **Bound Monitors**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gebundene Monitore überprüfen(/en-us/netscaler-console-service/media/monitor-app-step3.png)

Der Bildschirm für gebundene Monitore wird angezeigt und zeigt den Status des Integritätsmonitors der Anwendung.

App-Score-Komponenten auswählen und Schwellenwerte festlegen

Im **App-Dashboard** können Sie als Administrator entscheiden, die Komponenten auszuwählen und Schwellenwerte für die App-Score-Berechnung zu konfigurieren. Der App Score ist das Bewertungssystem, das Folgendes definiert:

- Wie gut eine Anwendung performt
- Ob die Anwendung hinsichtlich der Reaktionsfähigkeit gut performt

Navigieren Sie zu **Applications > Dashboard** und wählen Sie dann das Einstellungssymbol aus.

App-Score-Einstellung(/en-us/netscaler-console-service/media/app-score-setting.png)

Auf der Seite **App Score konfigurieren** können Sie die Komponenten auswählen und Schwellenwerte konfigurieren, um den endgültigen App Score zu bestimmen.

App-Score-Komponenten(/en-us/netscaler-console-service/media/app-score-components.png)

Die App-Score-Berechnung basiert auf den folgenden Komponenten:

APP-SCORE-KOMPONENTEN	VOM BENUTZER KONFIGURIERTE SCHWELLENWERTE	BESCHREIBUNG
NetScaler-Speichernutzung	Ja	Der niedrige und hohe Schwellenwert für die gesamte Speichernutzung in der NetScaler-Instanz
Aufbau der Surge-Warteschlange	Ja	Der niedrige und hohe Schwellenwert für die gesamten Surge-Anfragen, die sich in der Warteschlange

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APP-SCORE-KOMPONENTEN	VOM BENUTZER KONFIGURIERTE SCHWELLENWERTE	BESCHREIBUNG
		befinden und eine Antwort benötigen.
NetScaler CPU-Auslastung	Ja	Der niedrige und hohe Schwellenwert für die gesamte CPU-Auslastung in der NetScaler-Instanz.
Antwortzeit	Ja	Das Zeitintervall zwischen dem Senden eines Anforderungspakets und dem Empfangen des ersten Antwortpakets vom Dienst, der auf dem virtuellen Server konfiguriert ist.
CPU-Auslastung der Anwendung	Ja	Der niedrige und hohe Schwellenwert für die gesamte CPU-Auslastung durch die Anwendung.
Aktive Dienste	Ja	Der Schwellenwert des Prozentsatzes der Dienste, die aktiv sein müssen und an den virtuellen Server gebunden sind.
Falscher Persistenztyp	Nein	Gibt an, ob die Persistenznutzung auf einem virtuellen Server gering ist.
Serverfehler (5xx)	Nein	Gibt an, ob der Webserver mit 5xx-Fehlern antwortet.
Ungewöhnlich große HTTP-Pakete	Nein	Gibt die Vorkommen an, wenn die HTTP-Nachrichten mit HTTP-Headergröße die konfigurierten Werte in der

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APP-SCORE-KOMPONENTEN	VOM BENUTZER KONFIGURIERTE SCHWELLENWERTE	BESCHREIBUNG
		NetScaler-Instanz überschreiten.
SSL-Echtzeit-Traffic	Nein	Analysiert den SSL-Traffic, um Echtzeit-Traffic zu identifizieren und schlägt optimale Konfigurationseinstellungen zur Verbesserung der Latenz vor.
SSL-Sitzungsaufbau	Nein	Gibt den Sitzungsaufbau über einen bestimmten Zeitraum an, der dazu führen kann, dass eine große Menge an Speicher durch diese Sitzungen in der NetScaler-Instanz belegt wird.
Geringe Sitzungswiederverwendung	Nein	Gibt an, ob die tatsächliche Anzahl der von der NetScaler-Instanz wiederverwendeten Sitzungen geringer ist.
NIC-Kartensättigung	Nein	Gibt die Gesamtzahl der von den Schnittstellen verworfenen Pakete an.
TCP-Wiederzusammensetzungs-Warteschlangengrenze erreicht	Nein	Gibt an, ob die Out-of-Order-Pakete (außerhalb der Reihenfolge) einer TCP-Verbindung die konfigurierte Warteschlangengröße für Out-of-Order-Pakete überschreiten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Standardmäßig sind alle Komponenten aktiviert. Wenn Sie eine Komponente deaktivieren, führt NetScaler Console die endgültige App-Score-Berechnung nur auf der Grundlage der ausgewählten Komponenten durch.

Anwendungsdetails für Microservices-Anwendungen

Klicken Sie im Dashboard auf eine Microservices-Anwendung, um detailliertere Informationen abzurufen.

Die Seite der ausgewählten Anwendung wird angezeigt.

Auf der Seite mit den Anwendungsdetails:

- Wählen Sie die Zeitdauer aus der Liste aus, um Details für die spezifische Zeitdauer anzuzeigen
- Klicken Sie auf **Service Graph**, um den Service Graph für die ausgewählte Anwendung anzuzeigen. Weitere Informationen finden Sie unter Service Graph für Anwendungen
- Klicken Sie auf **Transaktionsprotokolle**, um die detaillierten Transaktionen für die ausgewählte Anwendung anzuzeigen
- Klicken Sie auf **Audit-Protokolle**, um die detaillierten Audit-Protokollinformationen anzuzeigen

Nachdem Sie die Zeitdauer ausgewählt haben, werden die folgenden Anwendungsdetails angezeigt:

- **App-Score** – Der Anwendungs-Score für die ausgewählte Zeitdauer. Sie können auch die aktuellen Anwendungsprobleme anzeigen, die als Strafpunktzahl (Penalty Score) bekannt sind und basierend auf der Problemkategorie angewendet werden. Der endgültige Score wird als **100 minus Gesamtstrafe** berechnet.

  1 – Bezeichnet den aktuellen App-Score

  2 – Bezeichnet die CPX-IP-Adresse, den Anwendungstyp wie Lastenausgleich oder Content Switching sowie den Service-Namespace und den Clusternamen, in dem der Dienst gehostet wird

  3 – Bezeichnet die Probleme, die den aktuellen Anwendungs-Score beeinflussen

  Dieses Dashboard ermöglicht es Ihnen auch, die aktuellen Probleme anzuzeigen, die die App-Bewertung beeinflussen. Die Details zu den Problemen finden Sie unter Probleme.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **K8s-Dienstdetails**

  Sie können die folgenden Details anzeigen:

  - **Dienstname** – Der Dienstname
  - **Clustername** – Der Clustername, auf dem der Dienst gehostet wird
  - **Namespace** – Der dem Dienst zugewiesene Namespace
  - **Dienstbezeichnungen** – Die dem Dienst zugewiesenen Dienstbezeichnungen

- **Pod-Details**

  Ein Pod ist eine Gruppe von Containern, die im Kubernetes-Cluster gehostet werden. Innerhalb eines Pods können Sie mehrere containerisierte Anwendungen bereitstellen. Jeder Pod ist mit einer IP-Adresse verknüpft.

  Klicken Sie auf den Pod-Status, um die Details anzuzeigen

  - **Pod-IP-Adresse** – Bezeichnet die Pod-IP-Adresse
  - **Hostname** – Bezeichnet den dem Pod zugewiesenen Hostnamen
  - **Instanz** – Bezeichnet die IP-Adresse des NetScaler CPX
  - **POD-Status** – Bezeichnet den aktuellen Status des Pods

- **Schlüsselmetriken** – Die Details der Schlüsselmetriken, wie z. B. **Antwortzeit**, **5xx-Fehler**, **Anfragen pro Sekunde**, **Durchsatz**, **Client-Verbindungen**, **Server-Verbindungen** und **Datenvolumen**, werden angezeigt.

  Bei jeder Metrik können Sie den Durchschnittswert und den Differenzwert für die ausgewählte Zeitdauer anzeigen. Der Differenzwert wird als **erster Wert minus letzter Wert** der ausgewählten Zeitdauer berechnet.

  Sie können die folgenden Instanzmetriken für die ausgewählte Zeitdauer in einem Diagrammformat anzeigen:

  Die folgende Abbildung ist ein Beispiel für das **Datenvolumen**, und die ausgewählte Zeitdauer beträgt 1 Monat. Der Wert 202,66 MB ist das gesamte Datenvolumen für die Dauer von 1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monat, und der Wert 8,13 MB ist der Differenzwert. Im Diagramm ist der erste Wert 14,11 und der letzte Wert 5,98. Der Differenzwert beträgt 14,11 – 5,98 = 8,13 MB.

- **Probleme** – Die Probleme, die für die ausgewählte Anwendung zutreffen. Sie können die folgenden Probleme zusammen mit ihrer Kategorie anzeigen:

LEISTUNG	INSTANZZUSTAND	KONFIGURATION	SYSTEMRESSOURCEN
Antwortzeit	Durchschnittliche CPU-Auslastung	Hohe 5xx-Antwort	Falscher Persistenztyp
Geringe Sitzungswiederverwendung	Speichernutzung	Ungewöhnlich große HTTP-Pakete	NIC-Kartensättigung
SurgeQueue-Aufbau		TCP-Neuordnungs-Warteschlangengrenze erreicht	
SSL-Echtzeit-Traffic			

Klicken Sie auf jedes Problem, um die folgenden Informationen anzuzeigen:

  - Gesamtzahl der Vorkommen
  - Empfohlene Maßnahmen zur Behebung des Problems
  - Die Problemdetails wie Zeit, Dienstname, Gesamtzahl der Vorkommen, Schweregrad und Erkennungsmeldung

    - Die Probleme, die auf der Registerkarte **Aktuell** angezeigt werden, beziehen sich auf die Anwendungsprobleme für die ausgewählte Zeitdauer.
    - Die Probleme, die auf der Registerkarte **Alle** angezeigt werden, beziehen sich auf die gesamten Anwendungsprobleme.

Das folgende Beispiel zeigt die Anwendungsprobleme für einen Zeitraum von 1 Tag. Die Registerkarte **Aktuell** zeigt an, dass keine aktuellen Probleme die App-Bewertung beeinflussen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Registerkarte **Alle** zeigt die insgesamt erkannten Probleme für den Zeitraum von 1 Tag an.

Intelligente App-Analysen

Intelligente App-Analysen ermöglichen es Ihnen, Probleme mit der Anwendungsleistung mithilfe von maschinellem Lernen und Regelalgorithmen zu identifizieren. Die Funktion „Intelligente App-Analysen“ von NetScaler Console:

- Bietet eine einfache und skalierbare Lösung zur Überwachung und Fehlerbehebung von Anwendungen, die über NetScaler-Instanzen bereitgestellt werden.
- Überwacht alle Ebenen der Anwendung, um die Bearbeitungszeit für die Fehlerbehebung zu verkürzen und die gesamte Anwendungsverfügbarkeit zu verbessern.

In einer typischen Bereitstellung decken Tausende von Servern den Datenbedarf der Benutzer ab. Der an diese Server gesendete Datenverkehr wird von virtuellen Servern, die auf NetScaler-Appliances konfiguriert sind, lastverteilt und überwacht. Jeder virtuelle Server ist an mehrere Dienste gebunden, die die Back-End-Server darstellen. In solchen Bereitstellungen hilft Ihnen die Funktion „Intelligente App-Analysen“ dabei:

- Überwachen, verwalten und Entscheidungen treffen bei Ausfällen und anderen Ereignissen
- Überwachen der für eine Anwendung konfigurierten virtuellen Server und Dienste
- Anzeigen kritischer Informationen zu virtuellen Servern und Diensten, damit Sie die Konfigurationen bei Bedarf ändern können, um eine optimale Leistung der Anwendungen zu erzielen.

Navigieren Sie zu **Anwendung** > **Dashboard**, und wählen Sie eine Anwendung aus, um die Leistungsindikatoren im Abschnitt **Probleme** anzuzeigen.

Intelligente App-Analysen konfigurieren

HINWEIS:

Ab **14.1-21.x oder späteren Builds** ist der Metrics Collector in den neuen NetScaler-Instanzen, die in NetScaler Console hinzugefügt wurden, standardmäßig deaktiviert. Die Metrics Collector-Konfiguration für die vorhandenen verwalteten Instanzen bleibt unverändert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Funktion Intelligent App Analytics wird nur in **NetScaler 12.1 Build 50.28 oder höher** unterstützt. Der Metrics Collector überträgt die NetScaler-Zählerdaten an NetScaler Console, die zur Erkennung von Anwendungsproblemen verwendet wird. Um die Funktion Intelligent App Analytics nutzen zu können, muss der **Metrics Collector** auf jeder NetScaler-Instanz konfiguriert werden.

Ab Build 14.1-28.x werden Metrics collector und Lean Usage Analytics auf der Ebene des virtuellen Servers anstatt auf Instanzebene aktiviert. Mit dieser Verbesserung bleiben Metrics Collector und Lean Usage Analytics nur auf Ihren aktiven virtuellen Servern mit hohem Datenverkehr aktiviert. Weitere Informationen finden Sie unter Peak- und Lean-Nutzungsanalysen.

Sie können Ihre virtuellen Server überprüfen und Metrics Collector und Lean Usage auf anderen virtuellen Servern aktivieren.

So überprüfen und aktivieren Sie Metrics Collector:

1. Navigieren Sie zu **Einstellungen > Analysekonsfiguration**.
2. Klicken Sie unter **Zusammenfassung der Metriken virtueller Server** auf **Metriken konfigurieren**.

3. Auf der Seite **Alle virtuellen Server** können Sie den Status des Metrik-Collectors auf jedem virtuellen Server anzeigen. Wählen Sie die virtuellen Server aus, die Sie aktivieren möchten, und klicken Sie auf **Metriken aktivieren**.

4. Wählen Sie **Metriken aktivieren**, um den Metrik-Collector zu aktivieren. Sie können auch **Lean Data** auswählen, wenn Sie die Nutzungsanalysen für schlanke Perioden aktivieren und anzeigen möchten. Klicken Sie nach der Auswahl auf **Konfiguration speichern**. Weitere Informationen finden Sie unter Spitzen- und schlanke Nutzungsanalysen.

Alternativ können Sie auch Metrics Collector und Lean Usage für die virtuellen Server über die NetScaler®-Instanzenseite aktivieren:

1. Navigieren Sie zu **Infrastruktur > Instanzen**, wählen Sie den Instanztyp aus und wählen Sie **Metrik-Collector** aus der Liste **Aktion auswählen**.
2. Wählen Sie die virtuellen Server aus, für die Sie den Metrik-Collector aktivieren möchten, und klicken Sie auf **Metriken aktivieren**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Wählen Sie **Metriken aktivieren**, um den Metrik-Collector zu aktivieren. Sie können auch **Lean Data** auswählen, wenn Sie Nutzungsanalysen für schlanke Perioden aktivieren und anzeigen möchten. Klicken Sie nach der Auswahl auf **Konfiguration speichern**.

Sobald die Option **Metrik-Collector** auf dem virtuellen Server aktiviert ist, navigieren Sie zu **Anwendungen** > **Dashboard**. Wählen Sie eine Instanz aus, um Anomalien im Abschnitt **Probleme** anzuzeigen.

Wir empfehlen, auch Analysen zu aktivieren, um Probleme wie detaillierte Webtransaktionen für Serverfehler (5xx) zu visualisieren. Weitere Informationen finden Sie unter Analysen aktivieren.

Leistungsindikatoren für Anwendungsanalysen

Sie können die Leistungsindikatoren zusammen mit ihren Kategorien, die in NetScaler-Webanwendungen vorkommen, anzeigen. Um diese Indikatoren anzuzeigen, müssen Sie sicherstellen, dass Analysen und der Metrik-Collector auf der NetScaler-Instanz aktiviert sind:

Nachdem Sie Analysen und den Metrik-Collector aktiviert haben, können Sie die folgenden Indikatoren anzeigen, indem Sie zu **Anwendungen** > **Dashboard** navigieren, eine Anwendung auswählen und zum Abschnitt **Probleme** scrollen:

Antwortzeit

Dieses Problem wird erkannt, wenn die Anwendungsantwortzeit auf Clientanfragen vom konfigurierten Schwellenwert abweicht. Klicken Sie auf die Registerkarte **Antwortzeit**, um die Problemdetails anzuzeigen.

Klicken Sie unter den **Empfohlenen Aktionen**, um die **Transaktionsprotokolle** anzuzeigen, die die Anwendung mit einer Antwortzeit von > 500 ms zeigen.

Unter **Details** können Sie Folgendes anzeigen:

- Das Diagramm, das die Gesamtereignisse für die ausgewählte Zeit anzeigt. Klicken Sie, um den Filter anzuwenden und Details anzuzeigen
- Wann das Problem aufgetreten ist
- Die Gesamtzahl der Vorkommen für die ausgewählte Zeit
- Der Schweregrad des Problems, z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung, die die gesamte Transaktionsantwortzeit anzeigt, die den konfigurierten Schwellenwert überschreitet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Aktive Dienste

Dieses Problem wird erkannt, wenn der Prozentsatz der aktiven Dienste, die an den virtuellen Server gebunden sind, kleiner ist als der konfigurierte Schwellenwert. Klicken Sie auf die Registerkarte **Aktive Dienste**, um die Problemdetails anzuzeigen.

Unter **Empfohlene Aktionen** klicken Sie, um Details der an den virtuellen Server gebundenen Dienste anzuzeigen.

Unter **Details** können Sie Folgendes anzeigen:

- Das Diagramm, das die Gesamtereignisse für die ausgewählte Zeitdauer anzeigt. Klicken Sie, um den Filter anzuwenden und Details anzuzeigen
- Wann das Problem aufgetreten ist
- Die Gesamtzahl der Vorkommen für die ausgewählte Zeitdauer
- Der Schweregrad des Problems wie niedrig, mittel und hoch
- Die Erkennungsmeldung, die den Prozentsatz der aktiven Dienstsitzungen und den konfigurierten Schwellenwert anzeigt.

Durchschnittliche CPU-Auslastung

Dieses Problem wird erkannt, wenn die NetScaler-CPU-Auslastung für diese Anwendung den konfigurierten Schwellenwert überschreitet. Klicken Sie auf die Registerkarte **Durchschnittliche CPU-Auslastung**, um die Problemdetails anzuzeigen.

Unter **Details** können Sie Folgendes anzeigen:

- Das Diagramm, das die Gesamtereignisse für die ausgewählte Zeitdauer anzeigt. Klicken Sie, um den Filter anzuwenden und Details anzuzeigen
- Wann das Problem aufgetreten ist
- Die Gesamtzahl der Vorkommen für die ausgewählte Zeitdauer
- Der Schweregrad des Problems, wie z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung, die die durchschnittliche CPU-Auslastung in % des NetScaler und den konfigurierten Schwellenwert angibt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Durchschnittliche CPU-Auslastung der Anwendung

Dieses Problem wird erkannt, wenn die CPU-Auslastung der Anwendung den konfigurierten Schwellenwert überschreitet. Klicken Sie auf die Registerkarte **App-CPU-Auslastung**, um die Details des Problems anzuzeigen.

Unter **Details** können Sie Folgendes anzeigen:

Das Diagramm, das die Gesamtzahl der Ereignisse für den ausgewählten Zeitraum anzeigt. Klicken Sie, um den Filter anzuwenden und Details anzuzeigen.

- Wann das Problem aufgetreten ist
- Die Gesamtzahl der Vorkommen für den ausgewählten Zeitraum
- Der Schweregrad des Problems, wie z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung, die die durchschnittliche CPU-Auslastung in % der Anwendung und den konfigurierten Schwellenwert angibt

Speicherauslastung

Dieses Problem wird erkannt, wenn die NetScaler-Speicherauslastung für diese Anwendung den konfigurierten Schwellenwert überschreitet. Klicken Sie auf die Registerkarte **Speicherauslastung**, um die Details des Problems anzuzeigen.

Unter **Details** können Sie Folgendes anzeigen:

- Das Diagramm, das die Gesamtereignisse für den ausgewählten Zeitraum anzeigt. Klicken Sie, um den Filter anzuwenden und Details anzuzeigen.
- Wann das Problem aufgetreten ist
- Die Gesamtzahl der Vorkommen für den ausgewählten Zeitraum
- Der Schweregrad des Problems, wie niedrig, mittel und hoch
- Die Erkennungsmeldung, die die durchschnittliche Speichernutzung in % von NetScaler und den konfigurierten Schwellenwert anzeigt.

NIC-Verwürfe

Ein Paketverwurf kann auftreten, wenn:

- Ein empfangenes Paket Formatfehler aufweist
- Ein empfangendes Gerät nicht genügend Speicherplatz für die Pakete hat

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mithilfe des Indikators **NIC-Verwürfe** können Sie die Gesamtzahl der von der NIC verworfenen Pakete anzeigen. Klicken Sie auf die Registerkarte **NIC-Verwürfe**, um die Details anzuzeigen.

Unter **Details** können Sie Folgendes anzeigen:

- Der Zeitpunkt, zu dem die Anomalie aufgetreten ist
- Die Meldung, die die Gesamtzahl der von der NIC verworfenen Pakete anzeigt

Dienst-Flaps

Als Netzwerkadministrator müssen Sie die optimale Verfügbarkeit der Anwendung sicherstellen. Bei Netzwerkproblemen oder Konfigurationsproblemen kann der Status und die Verfügbarkeit eines Anwendungsservers die Gesamtleistung beeinträchtigen.

Mithilfe der Service-Flap-Ereignisse können Sie die Anwendung identifizieren, die Probleme aufweist. Service-Flap-Ereignisse helfen Ihnen auch dabei:

- Zu verstehen, welcher Dienst für eine bestimmte Dauer den Status „DOWN“ hat
- Zu verstehen, wie viele Dienste für eine bestimmte Dauer den Status „UP“ oder „DOWN“ haben

Klicken Sie auf die Registerkarte **Service Flaps**, um die Details der Service-Flaps anzuzeigen.

Klicken Sie unter **Empfohlene Aktionen**, um die Details der Dienste anzuzeigen, die an den virtuellen Server gebunden sind.

Sie können Details wie die Anzahl der Vorkommen und den Zeitpunkt des letzten Vorkommens anzeigen.

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Service-Flap-Anomalie aufgetreten ist
- Der Dienst-/Dienstgruppenname
- Die Dienst-IP-Adresse
- Der aktuelle Dienststatus

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Geringe Sitzungswiederverwendung

NetScaler-Instanzen verarbeiten SSL-Transaktionen, indem sie den SSL-Handshake-Prozess vom Server auslagern. Nach Erhalt der Antwort vom Server schließt die NetScaler-Instanz die sichere Transaktion mit dem Client ab. Mithilfe der zwischengespeicherten Sitzungsparameter schließt die NetScaler-Instanz den SSL-Handshake-Prozess für die nachfolgenden Anfragen ab.

Werden diese Sitzungen nicht wiederverwendet, stellen sie eine Belastung für die NetScaler-Instanzen dar. Mithilfe des Indikators **Geringe Sitzungswiederverwendung** können Sie feststellen, ob die tatsächliche Anzahl der wiederverwendeten Sitzungen geringer ist.

Klicken Sie auf die Registerkarte **Geringe Sitzungswiederverwendung**, um die Problemdetails anzuzeigen.

Die **empfohlene Aktion** zur Fehlerbehebung besteht darin, entweder die Sitzungswiederverwendung zu deaktivieren oder das Sitzungs-Timeout zu reduzieren. Weitere Informationen finden Sie unter Sitzungswiederverwendung.

Unter **Details** können Sie Folgendes anzeigen:

- Gesamtzahl der Anwendungen mit geringer Sitzungswiederverwendung
- Die Zeit, zu der die Anomalie der geringen Sitzungswiederverwendung aufgetreten ist
- Gesamtzahl der Vorkommen
- Der Schweregrad der Anomalie, z. B. hoch, niedrig und mittel
- Die Erkennungsmeldung, die angibt, dass nur % der konfigurierten Sitzungen wiederverwendet werden

Falscher Persistenztyp

Sie müssen die Persistenz auf einem virtuellen Server konfigurieren, wenn Sie die Zustände von Verbindungen auf den durch diesen virtuellen Server dargestellten Servern (z. B. in E-Commerce verwendeten Verbindungen) aufrechterhalten möchten. Das Gerät verwendet dann die konfigurierte Lastausgleichsmethode für die anfängliche Auswahl eines Servers, leitet aber alle nachfolgenden Anfragen desselben Clients an denselben Server weiter.

Persistenz ist effektiv, wenn vorhandene Sitzungen zur Bearbeitung nachfolgender Anfragen wiederverwendet werden. Ist die Wiederverwendung von Persistenzsitzungen gering, stellen die auf NetScaler erstellten Sitzungen lediglich eine Belastung dar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mithilfe des Indikators **Falscher Persistenztyp** können Sie feststellen, ob die Persistenznutzung auf einem virtuellen Server gering ist. Klicken Sie auf die Registerkarte **Falscher Persistenztyp**, um die Problemdetails anzuzeigen.

Die **empfohlene Aktion** zur Behebung des Problems besteht darin, den Persistenztyp zu überprüfen oder die Persistenz zu deaktivieren. Weitere Informationen finden Sie unter Persistenzeinstellungen.

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Anomalie aufgetreten ist
- Gesamtzahl der Vorkommen
- Der Schweregrad der Anomalie, z. B. hoch, niedrig und mittel
- Die Erkennungsmeldung, die den Prozentsatz der ungenutzten Sitzungen angibt

Instabiler Server

In einigen Szenarien antwortet der Webserver mit Statuscodes, wenn er die Anfragen aus Gründen wie ungültigen Anfragen, temporärer Überlastung oder Serverwartung nicht bearbeiten kann. Diese Fehler werden mit Fehlercodes angezeigt, die verschiedene Fehlerszenarien definieren. Zum Beispiel:

- **502 Bad Gateway** Der Server fungiert als Gateway oder Proxy und hat eine ungültige Antwort vom Upstream-Server erhalten.
- **503 Service Unavailable** Der Server ist nicht verfügbar. Die Server könnten überlastet oder wegen Wartungsarbeiten ausgefallen sein.
- **504 Gateway Time-out** Der Server fungiert als Gateway oder Proxy und hat keine rechtzeitige Antwort vom Upstream-Server erhalten.

Dies können vorübergehende Zustände sein, aber manchmal müssen Sie eine Korrekturmaßnahme auf den Webservern implementieren, um die Webseiten wieder verfügbar zu machen.

Mithilfe des Indikators **Instabiler Server** können Sie diese Fehler anzeigen und Entscheidungen über Korrekturmaßnahmen treffen, um die Probleme zu beheben und sicherzustellen, dass die Client-Anfragen bedient werden und die Webseiten immer verfügbar sind.

Wählen Sie die Registerkarte **Instabiler Server**, um die Problemdetails anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Klicken Sie unter **Empfohlene Aktionen** auf, um die **Transaktionsprotokolle** anzuzeigen, die die Anwendung mit dem Antwortcode 5xx-Fehler zeigen.

Sie können auch die folgenden Fehlerbehebungsmethoden ausprobieren:

- Konfigurieren Sie L7-Monitore mit entsprechenden Parametern für den Server, der mit 5xx-Fehlern antwortet. Ein Monitor ist eine Entität, die den Dienstzustand verfolgt. Das Gerät prüft die Server regelmäßig mithilfe des an jeden Dienst gebundenen Monitors. Wenn ein Server nicht innerhalb eines angegebenen Antwort-Timeouts antwortet und die angegebenen Prüfungen fehlschlagen, wird der Dienst als DOWN markiert. Das Gerät führt dann den Lastausgleich zwischen den verbleibenden Diensten durch. Weitere Informationen zum Konfigurieren eines Monitors finden Sie unter Benutzerdefinierte Monitore
- Fehlerbehebung am Server

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die instabile Serveranomalie aufgetreten ist
- Der Dienst-/Dienstgruppenname
- Gesamtzahl der Vorkommen
- Der Schweregrad der Anomalie, z. B. hoch, niedrig und mittel
- Die Erkennungsmeldung, die den Prozentsatz der Antworten von diesem Dienst angibt, die 5xx-Fehler melden

Detaillierte Informationen zu Webtransaktionen mit Serverfehlern finden Sie unter Webtransaktionsanalyse für Serverfehler

SSL-Echtzeit-Traffic

In der NetScaler-Instanz können Sie ein SSL-Profil zur Verarbeitung des SSL-Traffics verwenden. Das SSL-Profil umfasst bestimmte SSL-Parameter für virtuelle Server, Dienste und Dienstgruppen. Der Indikator **SSL-Echtzeit-Traffic** analysiert den SSL-Traffic, um Echtzeit-Traffic zu identifizieren und optimale Konfigurationseinstellungen zur Verbesserung der Latenz vorzuschlagen.

Klicken Sie auf die Registerkarte **SSL-Echtzeit-Traffic**, um die Details des Problems anzuzeigen.

Die **empfohlene Maßnahme** zur Behebung des Problems besteht darin, die Netzwerklatenz durch Aktualisierung der SSL-Parameter zu verbessern. Weitere Informationen finden Sie unter Globale SSL-Parameter.

Unter **Details** können Sie Folgendes anzeigen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die Zeit, zu der die Anomalie aufgetreten ist
- Der Dienst-/Dienstgruppenname
- Der Schweregrad der Anomalie, wie niedrig, mittel und hoch
- Die Erkennungsmeldung mit der aktuellen Einstellung in der Anwendung

Ungewöhnlich große HTTP-Pakete

Eine HTTP-Transaktion verwendet Anforderungs-Antwort-Nachrichten zwischen Client und Server. In den Anforderungs- und Antwortnachrichten sind HTTP-Header die Werte, die im HTTP-Protokoll angezeigt werden. Sie können die HTTP-Header-Länge in einem virtuellen Server, Dienst oder einer Dienstgruppe konfigurieren, um 4xx-Fehler zu vermeiden.

Wenn eine HTTP-Anforderung/-Antwort die maximale Header-Länge überschreitet, kann dies ein möglicher Angriff sein. Mithilfe des Indikators **Ungewöhnlich große HTTP-Pakete** können Sie die Vorkommen anzeigen, bei denen die HTTP-Nachrichten mit HTTP-Header-Größe die konfigurierten Werte überschreiten.

Klicken Sie auf die Registerkarte **Ungewöhnlich große HTTP-Pakete**, um die Problemdetails anzuzeigen.

Die **empfohlenen Maßnahmen** zur Behebung des Problems sind:

- Überprüfen Sie den Datenverkehr, um festzustellen, ob die Header-Größe echt ist. Wenn die Header-Größe echt ist, aktualisieren Sie den Header-Wert im HTTP-Profil. Weitere Informationen finden Sie unter Pufferüberlaufprüfung.
- Wenn die Header-Größe nicht echt ist, fügen Sie die Quelle der Sperrliste hinzu, um Angriffe zu vermeiden.

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Anomalie aufgetreten ist
- Gesamtzahl der Vorkommen
- Der Schweregrad der Anomalie, z. B. hoch, niedrig und mittel
- Die Erkennungsmeldung, die die aktuelle HTTP-Header-Länge anzeigt, die auf dem virtuellen Server, Server oder der Dienstgruppe konfiguriert ist

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Treffer des TCP-Reassembly-Warteschlangenlimits

TCP verwaltet eine Out-of-Order-Warteschlange, um die OOO-Pakete in der TCP-Kommunikation zu speichern. Diese Einstellung beeinflusst den NetScaler-Speicher, wenn die Warteschlangengröße lang ist, da die Pakete im Laufzeitspeicher gehalten werden müssen.

Dies muss auf einem optimierten Niveau gehalten werden, basierend auf der Art des Netzwerks und den Anwendungseigenschaften.

Mithilfe des Indikators **Treffer des TCP-Reassembly-Warteschlangenlimits** können Sie sehen, ob die Out-of-Order-Pakete einer TCP-Verbindung die konfigurierte Warteschlangengröße für Out-of-Order-Pakete überschreiten.

Klicken Sie auf die Registerkarte **Treffer des TCP-Reassembly-Warteschlangenlimits**, um die Details des Problems anzuzeigen.

Die **empfohlenen Maßnahmen** zur Fehlerbehebung sind:

- Überprüfen Sie den Datenverkehr und fügen Sie die Quelle zur Sperrliste hinzu, wenn es sich um einen Angriff handelt
- Wenn dies ein erwartetes Netzwerkverhalten ist, aktualisieren Sie den Wert für die Größe der Out-of-Order-Pakete im TCP-Profil. Weitere Informationen finden Sie unter TCP-Optimierung
- Wenn es sich nur um eine vorübergehende Netzwerkstörung handelt, sind keine weiteren Maßnahmen erforderlich

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Anomalie aufgetreten ist
- Gesamtzahl der Vorkommen
- Der Schweregrad der Anomalie, z. B. niedrig, mittel und hoch
- Die Erkennungsmeldung, die die aktuellen TCP-Profil- und oooQsize-Einstellungen angibt

Anstieg der Warteschlangenbildung

Wenn ein Server eine Flut von Anfragen erhält, reagiert er nur langsam auf die Clients. Oft führt die Überlastung auch dazu, dass Clients Fehlerseiten erhalten. Ein virtueller Server muss über genügend konfigurierte Backend-Server verfügen, um die eingehenden Anfragen zu bearbeiten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mithilfe des Indikators **Anstieg der Warteschlangenbildung** können Sie die virtuellen Server anzeigen, bei denen ein Anstieg der Warteschlangenbildung vorliegt. Klicken Sie auf die Registerkarte **Anstieg der Warteschlangenbildung**, um die Details des Problems anzuzeigen.

Die **empfohlenen Maßnahmen** zur Behebung des Problems sind:

- Erhöhen Sie das Limit für die Anzahl der Clientverbindungen. Weitere Informationen finden Sie unter Festlegen eines Limits für die Anzahl der Clientverbindungen
- Erhöhen Sie die Anzahl der Backend-Server, um die Anwendungsanfragen zu bearbeiten

Unter **Details** können Sie Folgendes anzeigen:

- Die Zeit, zu der die Anomalie des Anstiegs der Warteschlangenbildung aufgetreten ist
- Gesamtzahl der Vorkommen
- Der Schweregrad der Anomalie, z. B. hoch, niedrig und mittel
- Die Erkennungsmeldung, die den Aufbau der Surge-Warteschlange auf dem virtuellen Server anzeigt

SSL-Bewertung

Wenn eine Anwendung keine A+-SSL-Bewertung hat, wird der App-Score beeinträchtigt. Mithilfe des Indikators **Nicht A+ SSL-Bewertung** können Sie die Gründe analysieren, warum die Anwendung keine A+-SSL-Bewertung hat. Klicken Sie auf die Registerkarte **Nicht A+ SSL-Bewertung**, um die Problemdetails anzuzeigen.

Die **empfohlene Aktion** zur Behebung des Problems ist ein Upgrade auf die A+-SSL-Bewertung. Weitere Informationen finden Sie unter Upgrade auf A+ SSL-Bewertung.

Unter **Details** können Sie die Problemdetails wie Problemkategorie, Problem und Empfehlung anzeigen.

Fehlerbehebung für App-Dashboard

Nachdem Sie eine Anwendung im App-Dashboard hinzugefügt haben, zeigt das Dashboard sofort die grundlegenden Konfigurationsdetails der App an. Die Details der Anwendungsanalyse, wie z. B. App-Score, wichtige Metriken und Probleme, werden innerhalb weniger Minuten (ca. 10 bis 15 Minuten) angezeigt. Weitere Informationen finden Sie unter Anwendungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie müssen sicherstellen, dass es keine Probleme mit dem Metrikdatenfluss (AppFlow-Collector oder Analyseprofil) von der NetScaler-Instanz gibt. Weitere Informationen zum AppFlow-Collector und Analyseprofil finden Sie in diesem Dokument.

Dieses Dokument beschreibt die Schritte zur Fehlerbehebung, die Sie ausführen müssen, wenn:

- Sie auf eine Anwendung klicken und die Analysen für die ausgewählte Anwendung auch nach der angegebenen Dauer (10–15 Minuten) nicht die erforderlichen Daten anzeigen.
- Die CS- oder LB-Anwendung im App-Dashboard immer eine graue Farbe (**Nicht zutreffend** Status) anzeigt.

HINWEIS

Die in diesem Dokument genannten Fehlerbehebungsverfahren gelten nur für virtuelle Server für **Content Switching** und **Load Balancing**.

Fehlerbehebungsszenario

Anwendung ist lizenziert

Sie müssen sicherstellen, dass die Anwendung lizenziert ist.

- **NetScaler Console** – Navigieren Sie zu **Einstellungen > Lizenzierung & Analysekonfiguration** und überprüfen Sie, ob die Anwendung unter **Zusammenfassung der virtuellen Serverlizenzen** lizenziert ist. Wenn die Anwendung nicht lizenziert ist, lesen Sie Lizenzierung verwalten und Analysen auf virtuellen Servern aktivieren, um den virtuellen Server zu lizenzieren.

Metrik-Collector ist aktiviert

Sie müssen sicherstellen, dass der **Metrik-Collector** in der NetScaler-Instanz aktiviert ist.

HINWEIS:

Ab **14.1-21.x oder späteren Builds** ist der Metrics Collector in den neuen NetScaler-Instanzen, die in der NetScaler Console hinzugefügt wurden, standardmäßig deaktiviert. Die Konfiguration des Metrics Collectors für die bestehenden verwalteten Instanzen bleibt unverändert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Um sicherzustellen, dass der Metrics Collector aktiviert ist:

1. Navigieren Sie zu **Einstellungen > Analytics-Konfiguration**.
2. Klicken Sie unter **Zusammenfassung der Metriken des virtuellen Servers** auf **Metriken konfigurieren**.

3. Auf der Seite **Alle virtuellen Server** können Sie den Status des Metrics Collectors auf jedem virtuellen Server anzeigen. Wählen Sie die virtuellen Server aus, die Sie aktivieren möchten, und klicken Sie auf **Metriken aktivieren**.

4. Wählen Sie **Metriken aktivieren**, um den Metrics Collector zu aktivieren. Sie können auch **Lean Data** auswählen, wenn Sie Lean-Perioden-Nutzungsanalysen aktivieren und anzeigen möchten. Klicken Sie nach der Auswahl auf **Konfiguration speichern**.

Alternativ können Sie den Metrics Collector und die Lean-Nutzung für die virtuellen Server auch über die Seite der NetScaler®-Instanzen aktivieren:

1. Navigieren Sie zu **Infrastruktur > Instanzen**, wählen Sie den Instanztyp aus und wählen Sie **Metrics Collector** aus der Liste **Aktion auswählen**.
2. Wählen Sie die virtuellen Server aus, für die Sie den Metrics Collector aktivieren möchten, und klicken Sie auf **Metriken aktivieren**.
3. Wählen Sie **Metriken aktivieren**, um den Metrics Collector zu aktivieren. Sie können auch **Lean Data** auswählen, wenn Sie Lean-Perioden-Nutzungsanalysen aktivieren und anzeigen möchten. Klicken Sie nach der Auswahl auf **Konfiguration speichern**.

Nachdem Sie den Metrics Collector aktiviert haben und die Daten immer noch nicht anzeigen können, überprüfen Sie Folgendes:

- Der AppFlow-Collector in NetScaler-Instanz Version 13.0 **älter als Build 47.x**.
- Das Analyseprofil in NetScaler-Instanz Build **47.x oder höher**.

NetScaler-Instanz älter als Builds 47.x

In NetScaler:

1. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass der Collector auf Port 5563 **UP** und aktiv ist:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`sh appflow collector af_collector_rest_<adm_receiver_ip>`

2. Wenn kein Collector verfügbar ist, führen Sie eine manuelle Instanzabfrage in der NetScaler Console durch.

   a. Navigieren Sie zu **Infrastruktur > Netzwerkfunktion > Jetzt abfragen**

   b. Wählen Sie die Instanz aus und klicken Sie auf **Abfrage starten**.

   Wenn die Abfrage fehlschlägt, entfernen Sie die NetScaler-Instanz aus der NetScaler Console und fügen Sie die NetScaler-Instanz dann erneut hinzu. Wenn Sie die NetScaler-Instanz hinzufügen, wird der Collector auf NetScaler hinzugefügt.

Wenn der Collector den Status **Down** anzeigt:

1. Stellen Sie sicher, dass SNIP konfiguriert ist.

   Wenn SNIP nicht konfiguriert ist, müssen Sie SNIP konfigurieren. Weitere Informationen finden Sie unter SNIP konfigurieren.

2. Stellen Sie sicher, dass die NetScaler-Instanz für NetScaler Console erreichbar ist.

   Sie können dies durch einen Ping-Test überprüfen. Führen Sie `ping -S <SNIP> <adm_receiver_ip>` aus.

NetScaler-Instanz, Builds neuer als 47.x

Stellen Sie in NetScaler Console sicher, dass der Metrik-Collector-Dienst verfügbar ist:

1. Navigieren Sie zu **Infrastructure > Network Function > Load Balancing > Services**.
2. Filtern Sie in der Suchleiste nach **Instance: (IP address)** und **Name: NetScaler Console**.
3. Stellen Sie sicher, dass `adm_metric_collector_svc_<adm_receiver ip>` verfügbar ist. Die IP-Adresse kann entweder die NetScaler Console Management-IP oder die Agent-IP sein.

   Stellen Sie sicher, dass dieser Dienst den Status **UP** hat und auf Port 5563 ausgeführt wird.

Wenn Sie die Daten immer noch nicht anzeigen können, stellen Sie sicher, dass der Collector-Dienst an das Zeitreihen-Analyseprofil in NetScaler gebunden ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Melden Sie sich bei NetScaler an.
2. Führen Sie den folgenden Befehl aus:

   ```
   sh analytics profile ns_analytics_time_series_profile
   ```

Wenn der Kollektor den Status **Down** anzeigt:

1. Stellen Sie sicher, dass SNIP konfiguriert ist.

   Wenn SNIP nicht konfiguriert ist, müssen Sie SNIP konfigurieren. Weitere Informationen finden Sie unter SNIP konfigurieren.
2. Stellen Sie sicher, dass die NetScaler-Instanz für die NetScaler Console erreichbar ist.

   Sie können dies durch einen Ping-Test überprüfen. Führen Sie `ping -S <SNIP> <adm_receiver_ip>` aus

3. Stellen Sie sicher, dass die Datenverkehrskonnektivität über Telnet den Dienst erreichen kann.

   Wenn Telnet den Dienst verbinden kann, ist eine Firewall vorhanden, die den Metrikdatenfluss blockiert. Sie müssen das Problem der Firewall-Blockierung beheben.

Wenn kein Kollektordienst an das Zeitreihen-Analyseprofil in NetScaler gebunden ist, wird der Kollektor als leer angezeigt.

Sie müssen in der NetScaler Console eine manuelle Instanzabfrage durchführen.

1. Navigieren Sie zu **Infrastructure > Network Function > Poll Now**
2. Wählen Sie die Instanz aus und klicken Sie auf **Polling starten**.

   Wenn der Abruf fehlschlägt, fügen Sie den Collector-Dienst direkt auf der NetScaler-Instanz mithilfe der folgenden Befehle hinzu:

   ```
   add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip> HTTP 5563
   ```

   ```
   unset analyticsprofile ns_analytics_time_series_profile -collectors
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set analytics profile ns_analytics_time_series_profile -collectors
adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -events enabled
```

Das Analyse-Zeitreihenprofil wird aktualisiert.

Wenn das Problem auch nach Durchführung aller genannten Schritte zur Fehlerbehebung weiterhin besteht, wenden Sie sich an den **NetScaler-Support**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Anwendungsnutzung und Anomalien

Als Administrator müssen Sie sicherstellen, wie die Anwendung genutzt wird. Die wichtigsten Anwendungsmetriken können Ihnen helfen, die Anwendungsnutzung zu identifizieren. Da der Datenverkehrsbereich zur Anwendung unvorhersehbar ist, können für eine bestimmte Dauer einige ungewöhnliche Abweichungen in der Anwendungsleistung auftreten. In solchen Szenarien möchten Sie als Administrator möglicherweise solche plötzlichen Anomalien anzeigen und analysieren und sicherstellen, ob eine sofortige Fehlerbehebung erforderlich ist.

NetScaler Console erkennt solche Anomalien und liefert die notwendigen Details. Navigieren Sie zu **Applications > Dashboard**, klicken Sie auf eine Anwendung und wählen Sie die Registerkarte **Key Metrics**. NetScaler Console überwacht das Datenverkehrsmuster und analysiert, ob die Schlüsselmetriken im erwarteten Bereich liegen. Wenn es eine Abweichung vom erwarteten Bereich gibt, meldet NetScaler Console diese Abweichungen als Anomalien.

Sie können Anomalien für die folgenden Schlüsselmetriken anzeigen:

- Antwortzeit
- Durchsatz
- Datenvolumen
- Anfragen pro Sekunde

Klicken Sie auf die Registerkarte **Metrics with Anomalies**, um Details anzuzeigen.

In jeder Metrik können Sie auch auf die Option **See more** klicken, um Details anzuzeigen. Das folgende Beispiel gilt für das Anwendungsdatenvolumen:

Sie können Folgendes anzeigen:

- Das Diagramm, das den Maximalwert, den Gesamtwert, den erwarteten Bereich und Anomalien anzeigt
- Die **Empfohlene Aktionen** zur Behebung des Problems
- Die Zeit- und Anomaliedetails unter **Details**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analyse der Spitzen- und Nebennutzung

Eine Webanwendung kann entweder hohen oder niedrigen Datenverkehr empfangen, und der Datenverkehrsbereich für jeden Tag oder jede Stunde ist sicherlich unvorhersehbar. Ebenso benötigt eine Webanwendung auch Ausfallzeiten für eine bestimmte Dauer während einer geplanten Wartung oder eines Upgrades. Als Administrator müssen Sie den Datenverkehr analysieren und den richtigen Zeitpunkt finden, um:

- Die Webanwendung zu skalieren
- Eine Ausfallzeit der Webanwendung zu planen

Die Funktion zur Analyse der Spitzennutzung und der Nebenzeiten in NetScaler Console ermöglicht es Ihnen, die Schlüsselmetriken für eine ausgewählte Zeitdauer zu analysieren. Anhand dieser Metriken können Sie den Datenverkehr analysieren und entscheiden, wann Sie die Webanwendung skalieren oder eine geplante Ausfallzeit planen möchten.

App-Skalierungsgrenzen bewerten

Klicken Sie im **App-Dashboard** auf eine Anwendung und wählen Sie die Registerkarte **Schlüsselmetriken**, um die konsolidierte Ansicht aller Metriken zu visualisieren. Wählen Sie die Zeitdauer aus der Liste aus, um die Metriken zu analysieren.

Für jede Metrik können Sie Folgendes anzeigen:

- **Max.** – Zeigt den Maximalwert für die ausgewählte Dauer an
- **Durchschnitt** – Zeigt den Durchschnittswert für die ausgewählte Dauer an

Gemäß dem Beispiel im Bild beträgt der Maximalwert für die Antwortzeit 1,3 s. Aus dem Diagramm können Sie analysieren, wie oft die hohe Antwortzeit für die ausgewählte Zeitdauer aufgetreten ist. Ebenso können Sie Details für andere Metriken anzeigen, analysieren, ob die Anwendung eine Spitzennutzung erfahren hat, und eine Entscheidung zur Skalierung der Produktionsumgebung treffen.

Die 5 wichtigsten Wartungsfenster für Apps identifizieren

Klicken Sie im **App-Dashboard** auf eine Anwendung und wählen Sie die Registerkarte **Schlüsselmetriken**, um die Nebenzeiten für die Anwendung anzuzeigen. Eine typische Ausfallzeit für eine Anwendung kann je nach Anforderung 1 Stunde, 2 Stunden oder 4 Stunden betragen. Sie können die Zeit aus der Liste (1 Stunde, 2 Stunden oder 4 Stunden) auswählen, die Sie für die Ausfallzeit planen möchten. Nachdem Sie die Zeit aus der Liste ausgewählt haben, können Sie

© 1997–2026 Citrix Systems, Inc. All rights reserved.

den Datenverkehr für Metriken wie Gesamtanfragen, Durchsatz und Datenvolumen analysieren. Sie können den richtigen Zeitpunkt für die Planung einer Ausfallzeit auswählen, wenn die Anwendungsnutzung geringer ist. Das folgende Beispiel dient zur Analyse der Ausfallzeit für die Dauer von 1 Stunde.

Die Heatmap-Ansicht zeigt die Anwendungsnutzung für den ausgewählten Zeitraum an. Je dunkler die Farbe (blau), desto höher ist die Anwendungsnutzung.

Die Heatmap-Ansicht schlägt auch die 5 geringsten Zeiträume (1, 2, 3, 4 und 5) vor, um die Anwendungs-Ausfallzeit zu planen.

1 – Zeigt den ersten Vorschlag für Mittwoch von 16:00 Uhr bis 17:00 Uhr an

2 – Zeigt den zweiten Vorschlag für Donnerstag von 21:00 Uhr bis 22:00 Uhr an

3 – Zeigt den dritten Vorschlag für Sonntag von 7:00 Uhr bis 20:00 Uhr an

4 – Zeigt den vierten Vorschlag für Mittwoch von 12:00 Uhr bis 13:00 Uhr an

5 – Zeigt den fünften Vorschlag für Montag von 7:00 Uhr bis 20:00 Uhr an

Sie können auch jeden anderen Tag und jede andere Uhrzeit auswählen, um eine Ausfallzeit zu planen, nachdem Sie den Traffic für alle anderen Tage analysiert haben.

Klicken Sie auf **Details anzeigen**, um weitere detaillierte Informationen anzuzeigen. Klicken Sie auf die Registerkarte **Gesamtanfragen**, **Durchsatz** oder **Datenvolumen**, um Details für die 5 geringsten Zeiträume und auch für die anderen Tage anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Anwendungsnutzungsanalysen

Anwendungsbesitzer müssen in der Lage sein, die gesamte Anwendung aus Leistungs- und Nutzungsperspektiven zu bewerten und zu visualisieren.

Das verbesserte **App-Dashboard** ermöglicht es Ihnen, alle Anwendungsleistungs- und Nutzungsmetriken zusammen anzuzeigen. Wenn Sie auf eine Anwendung klicken, zeigt die Registerkarte **Web Insight** zusätzlich zu den vorhandenen Anwendungsleistungsmetriken die Metrikdetails an, die Ihnen helfen:

- Ihre Anwendungsnutzung zu verstehen.
- Leistungsabweichungen mit den Nutzungsmetriken zu korrelieren.

HINWEISE:

- Ab der Version **14.1-51.x** sind Web Insight-Analysen für virtuelle Server sichtbar, die mit einer IPv6-Adresse konfiguriert sind.
- Ab der Version **14.1-1.16** oder höher zeigt die Analyseansicht im Zeitreihendiagramm Nullwerte (z. B. 0 ms und 0 Anfragen) für die ausgewählte Dauer an, wenn Sie eine Metrik aufschlüsseln. Zuvor, wenn für die ausgewählte Dauer kein Datenverkehr oder keine Transaktion empfangen wurde, zeigte die Analyseansicht die Diagramme an, indem diese Nullwerte übersprungen wurden.
- Für jede Metrik können Sie Optionen anzeigen, die den Maximalwert und den Gesamtwert angeben. Zum Beispiel:

```
>-  ![Example1](https://docs.netscaler.com/content/dam/netscaler/us/en/
netscaler-console-service/media/wi-sample.png) - The maximum client
network latency for the selected duration. Consider that you have the
network latency for client 1 = 30 ms, client 2 = 15 ms, and client 3 =
3 ms. In this scenario, the **Client Network Latency** displays 30 ms.

>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
>-  ![Example2](https://docs.netscaler.com/content/dam/netscaler/us/en/
netscaler-console-service/media/wi-sample1.png) - The total bandwidth
consumed across all available clients/servers for the selected
duration. Consider that you have the bandwidth consumption for client 1
= 30 MB, Client 2 = 45 MB, Client 3 = 40 MB. In this scenario, the
Bandwidth displays (30 MB + 45 MB + 40 MB) = 115 MB.
```

Die folgenden Metriken können Sie auf der Registerkarte **Web Insight** für die ausgewählte Dauer anzeigen:

- **Anwendungsübersicht** – Zeigt eine Übersicht über die Anwendungsmetriken an.
  - **Anfragen** – Zeigt die Gesamtzahl der von der Anwendung empfangenen Anfragen an. Die Registerkarte **Anfragen** zeigt die Diagrammansicht für die Gesamtzahl der Anfragen und die Top 5 der Client-Anfragen. Sie können die Umschaltoption verwenden, um die Ansicht anzupassen.
  - **Bandbreite** – Zeigt die gesamte von der Anwendung verarbeitete Bandbreite an. Die Registerkarte **Bandbreite** zeigt die Diagrammansicht für die Gesamtbandbreite und die Bandbreite der Top 5 Server. Sie können die Umschaltoption verwenden, um die Ansicht anzupassen.
  - **Antwortzeit** – Zeigt die durchschnittliche Antwortzeit der Anwendung an. Die Registerkarte **Anfragezeit** zeigt die Diagrammansicht der Aufschlüsselung der Antwortzeit und der Client-Latenz, Server-Latenz und Server-Verarbeitungszeit für die ausgewählte Dauer. Sie können die Umschaltoption verwenden, um die Ansicht anzupassen.
  - **Client Network Latency** – Zeigt die durchschnittliche Latenz vom Client an. Die Registerkarte **Client Network Latency** zeigt die grafische Ansicht der Latenzaufschlüsselung für die ausgewählte Dauer.
  - **Server Network Latency** – Zeigt die durchschnittliche Latenz vom Server an. Die Registerkarte **Server Network Latency** zeigt die grafische Ansicht der Latenzaufschlüsselung für die ausgewählte Dauer.
  - **Server Processing Time** – Zeigt die durchschnittliche Verarbeitungszeit vom Server an. Die Registerkarte **Server Processing Time** zeigt die grafische Ansicht der Aufschlüsselung der Verarbeitungszeit für die ausgewählte Dauer.

    Die Registerkarte **Zusammenfassung** ermöglicht es Ihnen, die Korrelation zwischen Anforderungen, Bandbreite und Antwortzeit in der grafischen Ansicht zu visualisieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Clients** – Zeigt die Einblicke für Clients an, die auf die Anwendung zugreifen:

  - **Gesamt-Clients** – Zeigt die Gesamtzahl der Clients an, die auf die Anwendung zugreifen. Klicken Sie auf die Registerkarte **Anforderungen**, um Folgendes anzuzeigen:
    - **Client** – Die IP-Adresse des Clients.
    - **Client-Netzwerklatenz (Durchschnitt)** – Die durchschnittliche Netzwerklatenz vom Client.
    - **Client-Netzwerklatenz (Max)** – Die maximale Netzwerklatenz vom Client.
    - **Anforderungen** – Die Gesamtanforderungen vom Client.
    - **Prozentuale Verteilung nach Anforderungen** – Die prozentuale Verteilung basierend auf den Anforderungen. Wenn beispielsweise die Gesamtzahl der Clients 4 beträgt und jeder Client 100 Anforderungen hat, beträgt die prozentuale Verteilung für jeden Client 25 %.
  - **Client Network Latency** – Zeigt die Netzwerklatenz vom Client zu NetScaler an. Klicken Sie auf die Registerkarte **Client Network Latency**, um Folgendes anzuzeigen:
    - **Client** – Die IP-Adresse des Clients.
    - **Client-Netzwerklatenz (Durchschnitt)** – Die durchschnittliche Netzwerklatenz vom Client.
    - **Client-Netzwerklatenz (Maximum)** – Die maximale Netzwerklatenz vom Client.
    - **Anfragen** – Die gesamten Anfragen vom Client.
    - **Prozentuale Verteilung nach Anfragen** – Die prozentuale Verteilung basierend auf den Anfragen.
  - **Renderzeit** – Zeigt die Zeit an, die zum Rendern der Serverantwort benötigt wird. Klicken Sie auf die Registerkarte **Renderzeit**, um Folgendes anzuzeigen:
    - **Client** – Die IP-Adresse des Clients.
    - **Renderzeit (Durchschnitt)** – Die durchschnittliche Renderzeit vom Client.
    - **Anfragen** – Die gesamten Anfragen vom Client.
    - **Prozentuale Verteilung nach Anfragen** – Die prozentuale Verteilung basierend auf den Anfragen.
- **Server** – Zeigt die Einblicke für Server an, die auf die Anwendung zugreifen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Bei integrierten Cache-Anfragen können Sie die IP-Adresse des virtuellen NetScaler-Servers mit einer IC-Benachrichtigung anzeigen. Weitere Informationen finden Sie unter Integrierte Cache-Anfragen.

- **Gesamtzahl der Server** – Zeigt die Gesamtzahl der Server an, die auf die Anwendung zugreifen. Klicken Sie auf die Registerkarte **Anfragen**, um Folgendes anzuzeigen:
  - **Server** – Die IP-Adresse des Servers.
  - **Server-Netzwerklatenz (Durchschnitt)** – Die durchschnittliche Netzwerklatenz vom Server.
  - **Server-Netzwerklatenz (Max.)** – Die maximale Netzwerklatenz vom Server.
  - **Anfragen** – Die gesamten Anfragen vom Server.
  - **Prozentuale Verteilung nach Anfragen** – Die prozentuale Verteilung basierend auf den Anfragen. Wenn beispielsweise die Gesamtzahl der Server 10 beträgt und jeder Server 1000 Anfragen hat, beträgt die prozentuale Verteilung für jeden Server 10 %.
- **Server-Netzwerklatenz (Max.)** – Zeigt die maximale Netzwerklatenz vom Server zu NetScaler an. Klicken Sie auf die Registerkarte **Server-Netzwerklatenz**, um Folgendes anzuzeigen:
  - **Server** – Die IP-Adresse des Servers.
  - **Server-Netzwerklatenz (Durchschnitt)** – Die durchschnittliche Netzwerklatenz vom Server.
  - **Server-Netzwerklatenz (Max.)** – Die maximale Netzwerklatenz vom Server.
  - **Anfragen** – Die gesamten Anfragen vom Server.
  - **Prozentuale Verteilung nach Anfragen** – Die prozentuale Verteilung basierend auf den gesamten Anfragen.
- **Server-Antwortzeit (Max.)** – Zeigt die maximale Zeit an, die der Server für die Beantwortung von Anfragen benötigt. Klicken Sie auf die Registerkarte **Server-Antwortzeit**, um Folgendes anzuzeigen:
  - **Server** – Die IP-Adresse des Servers.
  - **Server-Antwortzeit (Durchschnitt)** – Die durchschnittliche Antwortzeit vom Server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **Server-Antwortzeit (Max.)** – Die maximale Antwortzeit vom Server.
    - **Anfragen** – Die gesamten Anfragen vom Server.
    - **Prozentuale Verteilung nach Anfragen** – Die prozentuale Verteilung basierend auf den gesamten Anfragen.
  - **Bandbreite** – Zeigt die von den Servern verbrauchte Gesamtbandbreite an. Klicken Sie auf die Registerkarte **Bandbreite**, um Folgendes anzuzeigen:
    - **Server** – Die IP-Adresse des Servers.
    - **Bandbreite** – Die vom Server verbrauchte Gesamtbandbreite.
    - **Anfragen** – Die gesamten Anfragen vom Server.
    - **Prozentuale Verteilung nach Anfragen** – Die prozentuale Verteilung basierend auf den gesamten Anfragen.
- **Geostandorte** – Zeigt die Erkenntnisse für Clients an, die von einem bestimmten Standort aus auf die Anwendung zugreifen:

  - **Gesamtstandorte** – Zeigt die gesamten Client-Standorte an, die auf die Anwendung zugreifen.
  - **Antwortzeit** – Zeigt die Antwortzeit vom Client-Standort an.
  - **Bandbreite** – Zeigt die von Clients an allen Standorten verbrauchte Gesamtbandbreite an.
  - **Anfragen** – Zeigt die gesamten Anfragen von allen Client-Standorten an.

    Klicken Sie auf jede Registerkarte zum Anzeigen:
    - **Land** – Der Standortname.
    - **Antwortzeit** – Die durchschnittliche Antwortzeit vom Client-Standort.
    - **Bandbreite** – Die von der Client-Position verbrauchte Bandbreite.
    - **Anfragen** – Die gesamten Anfragen von der Client-Position.
    - **Prozentuale Verteilung nach Anfragen** – Die prozentuale Verteilung basierend auf den gesamten Anfragen. Wenn beispielsweise die Gesamtzahl der Standorte 10 beträgt, die gesamten Anfragen 1 Million sind und Land A allein 0,9 Millionen erhält, dann beträgt die prozentuale Verteilung für Land A 90 %. Die anderen Länder erhalten die verbleibende prozentuale Verteilung basierend auf den in jedem Land erhaltenen Anfragen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **URLs** – Zeigt die Erkenntnisse für URLs mit hoher Lade- und Renderzeit an:

  - **Gesamt-URLs** – Zeigt die Gesamt-URLs an. Klicken Sie auf die Registerkarte **Anfragen**, um Folgendes anzuzeigen:
    - **URL** – Der URL-Name.
    - **Ladezeit (Durchschnitt)** – Die durchschnittliche Zeit, die zum Laden der URL benötigt wird.
    - **Anfragen** – Die gesamten Anfragen von der URL.
    - **Prozentuale Verteilung nach Anfragen** – Die prozentuale Verteilung basierend auf den gesamten Anfragen und in jeder URL.
  - **Ladezeit** – Zeigt die Zeit an, die zum Laden der URL benötigt wird. Klicken Sie auf die Registerkarte **Ladezeit**, um Folgendes anzuzeigen:
    - **URL** – Der URL-Name.
    - **Ladezeit (Durchschnitt)** – Die durchschnittliche Zeit, die zum Laden der URL benötigt wird.
    - **Anfragen** – Die gesamten Anfragen von der URL.
    - **Prozentuale Verteilung nach Anfragen** – Die prozentuale Verteilung basierend auf den gesamten Anfragen.
  - **Renderzeit** – Zeigt die Zeit an, die zum Rendern und Anzeigen der URL benötigt wird. Klicken Sie auf die Registerkarte **Renderzeit**, um Folgendes anzuzeigen:
    - **URL** – Der URL-Name.
    - **Renderzeit (Durchschnitt)** – Die durchschnittliche Zeit, die zum Rendern der URL benötigt wird.
    - **Anfragen** – Die Gesamtzahl der Anfragen von der URL.
    - **Prozentuale Verteilung nach Anfragen** – Die prozentuale Verteilung basierend auf der Gesamtzahl der Anfragen.

- **HTTP-Antwortstatus** – Zeigt die Einblicke für eine bestimmte abgeschlossene HTTP-Anfrage an.

  - **Antwortstatus** – Zeigt den Antwortcode an, z. B. 2xx, 4xx, 5xx usw.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Antwortstatusgrund** – Zeigt den Antwortgrund an, z. B. interner Serverfehler, Nicht gefunden usw.
- **Anzahl der Vorkommen** – Zeigt die Gesamtzahl der Vorkommen an.

- **Betriebssystem** – Zeigt die Einblicke für das Betriebssystem an, das auf die Anwendung zugreift.

  - **Anfragen** – Zeigt die Gesamtzahl der Anfragen von jedem Betriebssystem an.
  - **Bandbreite** – Zeigt die von jedem Betriebssystem verbrauchte Gesamtbandbreite an.
  - **Ladezeit** – Zeigt die Gesamtzeit an, die jedes Betriebssystem zum Laden vom Server benötigt.

- **Browser** – Zeigt die Erkenntnisse zu den Browsertypen an, die von den Clients zum Zugriff auf die Anwendung verwendet werden.

  - **Anfragen** – Zeigt die Gesamtzahl der Anfragen von jedem Browser an.
  - **Bandbreite** – Zeigt die von jedem Browser verbrauchte Gesamtbandbreite an.
  - **Ladezeit** – Zeigt die Gesamtzeit an, die ein Browser zum Laden vom Server benötigt.

- **SSL-Fehler** – Zeigt die Erkenntnisse zu den SSL-Fehlern vom Frontend-Server und Backend-Server an.

  - **Gesamtfehler** – Zeigt die Gesamtzahl der SSL-Fehlerereignisse an.
  - **Frontend** – Zeigt die gesamten SSL-Fehler vom Frontend-Server an. Klicken Sie auf die Registerkarte **Frontend**, um den SSL-Fehlertyp und die Gesamtzahl der Vorkommen anzuzeigen.
  - **Backend** – Zeigt die gesamten SSL-Fehler vom Backend-Server an. Klicken Sie auf die Registerkarte **Backend**, um den SSL-Fehlertyp und die Gesamtzahl der Vorkommen anzuzeigen.

- **SSL-Nutzung** – Zeigt die Erkenntnisse zur SSL-Nutzung an, wie SSL-Zertifikate, Protokolle, Chiffren und Schlüssellänge.

  - **Zertifikate** – Zeigt die gesamten SSL-Zertifikate an. Klicken Sie auf die Registerkarte **Zertifikate**, um den Zertifikatsnamen und die Gesamtzahl der Treffer anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Protokolle** – Zeigt die gesamten SSL-Protokolle an. Klicken Sie auf die Registerkarte **Protokolle**, um Details zum SSL/TSL-Protokoll und die Gesamtzahl der Treffer anzuzeigen.
- **Chiffren** – Zeigt die gesamten Chiffren an. Klicken Sie auf die Registerkarte **Chiffren**, um Details zu jedem Chiffre-Suite-Namen und die Gesamtzahl der Treffer anzuzeigen.
- **Schlüsselstärke** – Zeigt die gesamte Schlüsselstärke an, die in SSL-Zertifikaten verwendet wird. Klicken Sie auf die Registerkarte **Schlüsselstärke**, um Details für jede Schlüsselstärke und die Gesamtzahl der Treffer anzuzeigen.

Metrikdetails im grafischen Format anzeigen

Für jede Metrik können Sie weitere Details in einem grafischen Format anzeigen, indem Sie auf die Option **Mehr anzeigen** klicken. Klicken Sie auf **>** , um Details in einem grafischen Format anzuzeigen.

Grafisches Format(/en-us/netscaler-console-service/media/web-insight-1.gif)

Im Folgenden sind die Details aufgeführt, die Sie für jede Metrik anzeigen können, nachdem Sie auf die Option **Mehr anzeigen** geklickt haben:

INSIGHT-NAME	METRIKEN	BESCHREIBUNG
Clients	Clients	Bezeichnet die Client-Liste
	Client-Netzwerklatenz (MAX)	Bezeichnet die maximale Netzwerklatenz vom Client zur NetScaler-Instanz
	Client-Netzwerklatenz (AVG)	Bezeichnet die durchschnittliche Netzwerklatenz vom Client zur NetScaler-Instanz
	Renderzeit (AVG)	Bezeichnet die durchschnittliche Zeit, die der Client benötigt, um die Serverantwort zu rendern.
	Anfragen	Bezeichnet die Gesamtzahl der Anfragen vom Client.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHT-NAME	METRIKEN	BESCHREIBUNG
Server	Server	Bezeichnet die Serverliste und den virtuellen NetScaler-Server (im Falle von integrierten Cache-Anfragen).
	Server-Netzwerklatenz (AVG)	Bezeichnet die durchschnittliche Netzwerklatenz vom Server zur NetScaler-Instanz.
	Server-Netzwerklatenz (MAX)	Bezeichnet die maximale Netzwerklatenz vom Server zur NetScaler-Instanz.
	Server-Antwortzeit (AVG)	Bezeichnet die durchschnittliche Zeit, die der Server benötigt, um die Anfragen zu verarbeiten.
	Server-Antwortzeit (MAX)	Bezeichnet die maximale Zeit, die der Server benötigt, um die Anfragen zu verarbeiten.
	Anfragen	Bezeichnet die Gesamtzahl der vom Server empfangenen Treffer
	Integrierte Cache-Treffer	Bezeichnet die Gesamtzahl der Antworten, die die NetScaler-Appliance aus dem Cache bereitstellt
	Integrierte Cache-Fehlzugriffe	Bezeichnet die Gesamtzahl der Antworten, die die NetScaler-Appliance vom Ursprungsserver bereitstellt
Geostandorte	Land	Bezeichnet die Client-Standorte

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHT-NAME	METRIKEN	BESCHREIBUNG
	Antwortzeit (Durchschnitt)	Bezeichnet die durchschnittliche Antwortzeit vom Client-Standort
	Bandbreite	Bezeichnet die gesamte Bandbreite, die vom Standort verbraucht wird
	Anfragen	Bezeichnet die Gesamtzahl der Anfragen vom Standort
URL	Renderzeit (Durchschn.)	Gibt die durchschnittliche Zeit an, die zum Laden der Seite vom Server benötigt wird.
	Ladezeit (Durchschn.)	Gibt die durchschnittliche Zeit an, die die URL zum Rendern und Anzeigen benötigt.
	Anfragen	Gibt die Gesamtzugriffe von der URL an.
HTTP-Antwortstatus	Antwortstatus	Bezeichnet den Namen des Antwortstatus, wie z. B. OK, Nicht gefunden, Interner Serverfehler usw.
	Grund des Antwortstatus	Gibt den vom Server empfangenen Antwortstatuscode an, wie z. B. 200, 400, 500 usw.
	Anzahl der Vorkommen	Gibt die Gesamtzugriffe vom Antwortcode an.
Betriebssystem	Betriebssystem	Bezeichnet den Namen des Betriebssystems, z. B. Windows, MAC

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHT-NAME	METRIKEN	BESCHREIBUNG
	Renderzeit	Bezeichnet die Gesamtzeit, die das Betriebssystem zum Rendern vom Server benötigt
	Bandbreite	Bezeichnet die vom Betriebssystem verbrauchte Gesamtbandbreite
	Anfragen	Bezeichnet die Gesamtzahl der Anfragen vom Betriebssystem
Browser	Browser	Bezeichnet den Browsernamen, z. B. Mozilla Firefox, Chrome usw.
	Renderzeit	Bezeichnet die Gesamtzeit, die ein Browser zum Rendern vom Server benötigt
	Bandbreite	Bezeichnet die vom Browser verbrauchte Gesamtbandbreite
	Anfragen	Bezeichnet die Gesamtzahl der Anfragen vom Browser
SSL-Fehler	SSL-Fehlertyp	Bezeichnet den Fehlernamen, z. B. CLIENTAUTH FAILURE
	Anzahl der Vorkommen	Bezeichnet die Gesamtzahl der Vorkommen für den SSL-Fehler
SSL-Nutzung	Bezeichnet den Protokollnamen und die Versionen wie TLS, SSL	
	Anzahl der Vorkommen	Bezeichnet die Gesamtzahl der Zugriffe vom Protokoll

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Automatisieren Sie die Verwaltung von SSL-Zertifikaten

Um die digitale Sicherheit zu gewährleisten, müssen Sie die Verwaltung von SSL-Zertifikaten in Ihrer Umgebung automatisieren. Sie benötigen Möglichkeiten, alle Zertifikate proaktiv zu verwalten und zu überwachen, Sie über ablaufende Zertifikate zu benachrichtigen und die Zertifikate automatisch zu erneuern, bevor sie ablaufen. Abgelaufene SSL-Zertifikate führen zu Sicherheitsrisiken. Sie können Venafi Trust Protection Platform-Server mit NetScaler Console konfigurieren, um die Verwaltung von auf NetScaler-Instanzen installierten SSL-Zertifikaten zu automatisieren.

Durch die Verwendung von Venafi mit NetScaler Console können Sie die SSL-Zertifikate über ihren gesamten Lebenszyklus hinweg verwalten. Sie können die folgenden Aufgaben im NetScaler Console **Anwendungs**-Dashboard ausführen:

- SSL-Probleme und Anwendungsbewertungen überprüfen.
- SSL-Probleme beheben und vorgeschlagene Abhilfemaßnahmen anwenden.
- An eine Anwendung gebundene Zertifikate überprüfen.
- Zertifikate schnell erstellen, installieren und erneuern.
- Erneuerung von Zertifikaten automatisieren.
- Anwendungen sichern, indem generierte Zertifikate an virtuelle NetScaler-Server gebunden werden.
- Alle SSL-aufgabenbezogenen Protokolle für eine bestimmte Anwendung überprüfen.

Einen Venafi-Server auf NetScaler Console konfigurieren

Das Konfigurieren eines Venafi-Servers ist ein zweistufiger Prozess. Zuerst fügen Sie den Venafi-Server in NetScaler Console hinzu. Als Nächstes konfigurieren Sie die Richtlinien auf dem Venafi-Server. Um den Venafi-Server in NetScaler Console hinzuzufügen, navigieren Sie in der NetScaler Console GUI zu **Infrastructure > SSL Dashboard > Third party CA**. Klicken Sie auf **Add**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Geben Sie die Details in die dafür vorgesehenen Felder ein. Aktivieren Sie die Option **Auto-Renew**, wenn die Zertifikate automatisch erneuert werden sollen. Für Details zu jedem Feld fahren Sie mit der Maus über das Feld und klicken Sie auf das `i` Symbol.

HINWEIS

Der Richtlinienordner muss Unterordner enthalten.

Beispiel:

`"policy_folder": "\\VED\\Policy\\TLS`

`TLS Certificates`

`NetScaler Console"`

Nachdem Sie den Venafi-Server konfiguriert haben, können Sie das NetScaler Console-Dashboard verwenden, um Ihre SSL-Zertifikate zu verwalten.

Verwalten des Lebenszyklus von SSL-Zertifikaten

Das Anwendungs-Dashboard ist eine zentrale Anlaufstelle für die End-to-End-Verwaltung Ihrer SSL-Zertifikate. Navigieren Sie in der NetScaler Console-GUI zu **Applications > App Dashboard**. Wählen Sie unter **Issue Categories** die Option **SSL Config**. Unter **Current Issues** können Sie die SSL-bezogenen Probleme Ihrer Anwendungen sehen. Um den SSL-Bericht anzuzeigen, bewegen Sie den Mauszeiger unter **Applications** über die App. Um Details des Berichts anzuzeigen, klicken Sie auf die App. In diesem Beispiel haben wir eine Anwendung mit einem Score von 27.

Darüber hinaus können Sie Ihre Probleme mithilfe von **Application Scores** wie „kritisch“ oder „Überprüfung“ filtern. Die SSL-Anwendungsscores basieren auf SSL-Parametern, die standardmäßig unter den Einstellungen **Manage Apps** in der oberen rechten Ecke des Dashboards aktiviert sind.

Um einen der SSL-Parameter zu deaktivieren, deaktivieren Sie das Kontrollkästchen und klicken Sie auf **OK**. Um die Details des SSL-Berichts anzuzeigen, klicken Sie unter **Applications** auf die App, für die Sie den Bericht anzeigen möchten.

Sie können den Performance-Score überprüfen und auf der Seite nach unten scrollen, um Details wie die virtuellen Server der App und die an die virtuellen Server gebundenen Zertifikate sowie die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Probleme mit den Zertifikaten anzuzeigen. Um Details des Zertifikats anzuzeigen, klicken Sie auf den Link unter **Certificate Name**. Für ein abgelaufenes Zertifikat können Sie es erneuern.

Die Erneuerung des Zertifikats umfasst das Erstellen des Zertifikats, dessen Installation und die Bindung an den virtuellen Server.

HINWEIS

Wenn Sie einen Venafi-Server in der NetScaler Console hinzufügen und die Option zur automatischen Verlängerung aktivieren, werden Zertifikate automatisch vor Ablauf erneuert.

Durch Klicken auf **SSL-Zertifikat erneuern** gelangen Sie zur Registerkarte **SSL**, die alle Zertifikate auflistet, die an die virtuellen Server der Anwendung gebunden sind. Über diese Registerkarte können Sie Zertifikate erstellen und installieren sowie an die virtuellen Server binden. Außerdem können Sie alle SSL-aufgabenbezogenen Protokolle einer bestimmten Anwendung auf der Registerkarte für SSL-aufgabenbezogene Protokolle einer bestimmten Anwendung überprüfen.

Um ein Zertifikat zu erstellen, klicken Sie auf **Zertifikat erstellen** und geben Sie die Details ein. Geben Sie ein Passwort ein, da heruntergeladene Zertifikate verschlüsselt sind, und klicken Sie auf **Erstellen**. Die NetScaler Console kontaktiert den Venafi-Server, um das Zertifikat zu erstellen. Klicken Sie auf **Schließen**, wenn das Zertifikat heruntergeladen wurde.

Klicken Sie anschließend auf der Registerkarte **SSL** auf **Zertifikat installieren**. Wählen Sie das heruntergeladene Zertifikat aus und klicken Sie auf **Installieren**. Weitere Informationen zur Installation eines SSL-Zertifikats auf NetScaler mithilfe der NetScaler Console finden Sie im Abschnitt zur Installation eines SSL-Zertifikats von der NetScaler Console im Thema Installieren von SSL-Zertifikaten auf einer NetScaler-Instanz.

Klicken Sie anschließend auf **Zertifikat binden**. Bei Bedarf können Sie ein Zertifikat auch entbinden. Nach der nächsten SSL-Abfrage wird das Anwendungs-Dashboard mit den neuen Daten aktualisiert. Wenn Sie alle SSL-Aufgabenprotokolle einer bestimmten Anwendung überprüfen möchten, klicken Sie auf **Zertifikatsaufgabenprotokoll**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A+ SSL-Bewertungsanalysen

HINWEIS:

Für die Massenaktualisierung nicht konformer SSL-Zertifikate können Sie die **SSL A+ rating upgrade** unter **Tasks** verwenden.

Eine Anwendung muss sichere Chiffren und Protokolle für SSL-Transaktionen verwenden. Andernfalls kann dies die Privatsphäre, die Datenintegrität und die Sicherheit der Benutzer beeinträchtigen, die auf die Anwendung zugreifen. NetScaler Console überprüft die SSL-Einstellungen des virtuellen Servers der Anwendung mit dem sicheren NetScaler-Front-End-Profil. Die für eine A+-Bewertung erforderlichen Einstellungen sind im sicheren Front-End-Profil vorinstalliert.

Als Anwendungsbesitzer können Sie beurteilen, ob Ihre Anwendung eine **A+**-Bewertung hat. Sie können auch die Protokoll- und Cipher-Suite-Scores einer Anwendung anzeigen. Wenn Ihre Anwendung keine **A+**-Bewertung hat, können Sie auf **A+**-Bewertung aktualisieren.

So zeigen Sie die SSL-Bewertung der Anwendung an:

1. Gehen Sie zu **Applications > Dashboard**.
2. Filtern Sie Anwendungen basierend auf ihren SSL-Bewertungen.

   Wenn eine Anwendung keine Bewertung hat, wird sie unter **NA** kategorisiert.
3. Wählen Sie das gewünschte Anwendungsraster aus der GUI aus.
4. Wählen Sie die Registerkarte **SSL** aus. Diese Registerkarte zeigt die SSL-Bewertung der Anwendung an.

Die Registerkarte **SSL** bietet eine der folgenden Optionen, um die Bewertung Ihrer Anwendung zu ändern oder zu aktualisieren:

- Auf A+ SSL-Bewertung aktualisieren
- SSL-Bewertung zurücksetzen

Upgrade auf A+ SSL-Bewertung

Wenn Sie eine Anwendung auf die A+ SSL-Bewertung aktualisieren, treten die folgenden Änderungen auf, abhängig vom Status eines Standard-SSL-Profils auf einer NetScaler-Instanz:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wenn das Standard-SSL-Profil deaktiviert ist, ändert NetScaler Console die empfohlenen SSL-Einstellungen auf dem virtuellen SSL-Server.
- Wenn das Standard-SSL-Profil aktiviert ist, erstellt NetScaler Console ein neues SSL-Profil mit den empfohlenen A+-Einstellungen, basierend auf einem sicheren Profil.

Die Anwendung ohne **A+**-Bewertung zeigt die Details der betroffenen virtuellen Server auf der Registerkarte **SSL** an.

Unter **App-Details** können Sie die Details der virtuellen Server überprüfen, deren Konfiguration nicht mit dem sicheren Front-End-Profil übereinstimmt. Außerdem werden die Abhilfemaßnahmen in der Spalte **Empfehlung** angezeigt. Diese Maßnahmen dienen dazu, Ihre Anwendung mit dem sicheren Front-End-Profil konform zu machen.

In diesem Beispiel weist der virtuelle Server einige Sicherheitsprobleme auf. **Protokoll TLSv1.0 aktiviert** ist eines dieser Probleme. Der Abschnitt **App-Details** empfiehlt eine geeignete Maßnahme zur Behebung dieses Problems. Um alle derartigen Probleme mit den entsprechenden Empfehlungen zu beheben, gehen Sie wie folgt vor:

1. Klicken Sie auf **Upgrade auf A+-Bewertung**.

   Die Bestätigungsmeldung zeigt die Befehle an, die auf einem virtuellen Server ausgeführt werden. Diese Befehle können Ihren Anwendungsverkehr beeinträchtigen.
2. Überprüfen Sie die Befehle und klicken Sie auf **Bestätigen**.

SSL-Bewertung zurücksetzen

HINWEIS:

Wenn Sie eine Anwendung auf die SSL-Bewertung A+ aktualisieren, können Sie nur innerhalb von 7 Tagen nach dem Upgrade zur ursprünglichen Bewertung zurückkehren.

Nachdem Sie die Anwendung auf die Bewertung A+ aktualisiert haben, können Sie den eingehenden Datenverkehr in SSL insight analysieren. Diese Seite zeigt die Chiffren und Protokolle an, über die SSL-Transaktionen ausgehandelt werden.

Wenn Sie jedoch feststellen, dass legitimer Datenverkehr verworfen wird, können Sie das auf Ihrer Anwendung konfigurierte sichere Front-End-Profil zurücksetzen. Diese Aktion ändert die SSL-Bewertung auf die frühere Bewertung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Um eine SSL-Bewertung zurückzusetzen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Rollback**.

   Die Bestätigungsmeldung zeigt die Befehle an, die auf einem virtuellen Server ausgeführt werden.
2. Überprüfen Sie die Befehle und klicken Sie auf **Confirm**.

Auswirkungen der SSL-Bewertung auf den Anwendungsdatenverkehr bestimmen

Der Anwendungsdatenverkehr kann beeinträchtigt werden, wenn Sie die SSL-Bewertung aktualisieren. In den **SSL-Metriken** können Sie beobachten, ob nach dem Upgrade Verbindungen unterbrochen werden. Mit diesen Informationen können Sie entscheiden, ob Sie die SSL-Bewertung beibehalten oder zurücksetzen möchten.

Im folgenden Beispielgrafen werden einige Verbindungen nach dem Upgrade der SSL-Bewertung auf **A+** unterbrochen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web Insight-Dashboard

HINWEIS:

Ab der Version **14.1-51.x** sind Web Insight-Analysen für virtuelle Server sichtbar, die mit einer IPv6-Adresse konfiguriert sind.

Die verbesserte Web Insight-Funktion wurde erweitert und bietet Einblick in detaillierte Metriken für Webanwendungen, Clients und NetScaler-Instanzen. Dieses verbesserte Web Insight ermöglicht es Ihnen, die gesamte Anwendung sowohl aus Leistungs- als auch aus Nutzungsperspektive zu bewerten und zu visualisieren. Als Administrator können Sie Web Insight anzeigen für:

- Eine Anwendung. Navigieren Sie zu **Applications > Dashboard**, klicken Sie auf eine Anwendung und wählen Sie die Registerkarte **Web Insight**, um die detaillierten Metriken anzuzeigen. Weitere Informationen finden Sie unter Application Usage Analytics.
- Alle Anwendungen. Navigieren Sie zu **Applications > Web Insight** und klicken Sie auf jede Registerkarte (Applications, Clients, Instances), um die folgenden Metriken anzuzeigen:

ANWENDUNGEN	CLIENTS	URLS	INSTANZEN
Anwendung mit Antwortzeitanomalien	Clients	URLs	Instanzmetriken
Anwendungen	Geostandorte		Anwendungen
Server	HTTP-Anforderungsmethoden		Domänen
Domänen	HTTP-Antwortstatus		URLs
Geostandorte	URLs		HTTP-Anforderungsmethoden
URLs	Betriebssystem		HTTP-Antwortstatus

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ANWENDUNGEN	CLIENTS	URLS	INSTANZEN
HTTP-Anforderungsmethoden	Browser		Clients
HTTP-Antwortstatus	SSL-Fehler		Server
SSL-Fehler	SSL-Nutzung		Betriebssystem
SSL-Nutzung			Browser

In jeder Metrik können Sie die Top-5-Ergebnisse anzeigen. Sie können klicken, um tiefer zu gehen, das Problem zu analysieren und Fehlerbehebungsmaßnahmen schneller zu ergreifen.

HINWEIS

- Ab Version **14.1-1.16** oder einer späteren Version zeigt die Analyseansicht im Zeitreihendiagramm Nullwerte (z. B. 0 ms und 0 Anfragen) für die ausgewählte Dauer an, wenn Sie eine Metrik detailliert untersuchen. Zuvor, wenn für die ausgewählte Dauer kein Datenverkehr oder keine Transaktion empfangen wurde, zeigte die Analyseansicht die Diagramme an, indem diese Nullwerte übersprungen wurden.
- In einigen Szenarien ist NetScaler möglicherweise nicht in der Lage, die RTT-Werte für bestimmte Transaktionen zu berechnen. Für solche Transaktionen zeigt NetScaler Console die RTT-Werte wie folgt an:
  - **NA** – Wird angezeigt, wenn die NetScaler-Instanz die RTT nicht berechnen kann.
  - **< 1ms** – Wird angezeigt, wenn die NetScaler-Instanz die RTT in Dezimalwerten zwischen 0 ms und 1 ms berechnet. Zum Beispiel 0,22 ms.

Details zu Chiffre-bezogenen Problemen anzeigen

Unter **SSL-Fehler** können Sie Details zu den folgenden SSL-Parametern anzeigen:

- Chiffre-Nichtübereinstimmung
- Nicht unterstützte Chiffren

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Klicken Sie unter **SSL-Fehler** auf einen SSL-Parameter (Chiffre-Nichtübereinstimmung oder Nicht unterstützte Chiffren), um Details wie den SSL-Chiffrenamen, die empfohlenen Aktionen und die Details der betroffenen Anwendungen und Clients anzuzeigen.

Die Detailseite für den ausgewählten SSL-Parameter wird angezeigt. Sie können:

- Überprüfen Sie die Vorschläge unter **Empfohlene Aktionen**.
- Zeigen Sie die Chiffrenamen und die Anzahl der Vorkommen unter **SSL-Chiffre** an.
- Zeigen Sie die Gesamtzahl der betroffenen Anwendungen und Clients an.

Klicken Sie auf den **SSL-Chiffrenamen**, um die Anwendungen und Clients anzuzeigen, die von der ausgewählten SSL-Chiffre betroffen sind.

Integrierte Cache-Anfragen

Der integrierte Cache bietet In-Memory-Speicher auf der NetScaler-Appliance und stellt Benutzern Webinhalte bereit, ohne dass ein Roundtrip zu einem Ursprungsserver erforderlich ist.

Die Integrations-Cache-Anfragen sind derzeit unter **Server** mit einer IC-Benachrichtigung neben der IP-Adresse des virtuellen NetScaler-Servers sichtbar. Alle anderen Anfragen sind mit der IP-Adresse des Ursprungsservers sichtbar.

Wenn Sie einen Server aufrufen, um weitere Details anzuzeigen, zeigen die **Server-Metriken** Registerkarten für integrierte Cache-Treffer und -Fehler an.

Die Diagrammansicht in:

- Die Registerkarte **Integrierte Cache-Treffer** ermöglicht es Ihnen, die Gesamtzahl der Antworten anzuzeigen, die die NetScaler Appliance aus dem Cache bereitstellt.

- Die Registerkarte **Integrierte Cache-Fehler** ermöglicht es Ihnen, die Gesamtzahl der Antworten anzuzeigen, die die NetScaler Appliance vom Ursprungsserver bereitstellt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Anderer Anwendungsfall

Angenommen, Sie möchten die Server-Netzwerklatenz für einen Zeitraum von 1 Monat analysieren und eine Entscheidung treffen, ob die Produktionsumgebung hoch- oder herunterskaliert werden soll. Um dies zu analysieren:

1. Wählen Sie Letzter 1 Monat aus der Liste und scrollen Sie auf der Registerkarte **Anwendungen** nach unten zu **Server**, und klicken Sie auf einen Server.

   Die Metrikdetails für den ausgewählten Server werden angezeigt.
2. Wählen Sie die Registerkarte **Server-Netzwerklatenz**, um die Latenz zu analysieren.

   Die durchschnittliche Latenz beträgt 10,01 s, und anhand des Diagramms können Sie erkennen, dass die Server-Netzwerklatenz im letzten Monat hoch zu sein scheint. Als Administrator können Sie die Entscheidung treffen, die Produktionsumgebung zu skalieren.

Grundursache für Anwendungsverlangsamung analysieren

Anwendungsverlangsamung ist ein großes Problem für jedes Unternehmen, da sie sich auf das Geschäft oder die Produktivität auswirkt. Als Administrator müssen Sie sicherstellen, dass alle Anwendungen optimal funktionieren, um geschäftliche Auswirkungen zu vermeiden. Wenn Ihre Benutzer eine Verlangsamung beim Zugriff auf die Anwendung feststellen, müssen Sie sicherstellen, ob das Problem bei Folgendem liegt:

- Client-Netzwerklatenz
- Server-Netzwerklatenz
- Server-Verarbeitungszeit

NetScaler Console führt stündlich Anomalieprüfungen durch und meldet Anomalien für den Datenverkehr der letzten Stunde, basierend auf bestimmten Voraussetzungen. Um beispielsweise falsch positive Ergebnisse zu vermeiden, werden die Anomalieprüfungen für Ergebnisse übersprungen, wenn die Antwortzeit < 1 ms beträgt.

Die Seite **Anwendungen > Web Insight** ermöglicht es Ihnen, die Anwendungen mit Antwortzeitanomalien für den ausgewählten Zeitraum anzuzeigen. Die Metrik **Anwendungen mit Antwortzeitanomalien** zeigt die fünf wichtigsten Anwendungen basierend auf den gesamten Anomalien an. Klicken Sie auf **Mehr anzeigen**, um alle Anwendungen anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Anwendung** – Bezeichnet den Anwendungsnamen.
- **Gesamtanomalien und Verursacher** – Bezeichnet die Gesamtanomalien der Anwendung. Wenn Sie den Mauszeiger darüber bewegen, können Sie die Gesamtanomalien anzeigen, die jeweils von der Client-Netzwerklatenz, der Server-Netzwerklatenz und der Server-Verarbeitungszeit stammen.
- **Antwortzeitbereich** – Bezeichnet den erwarteten Antwortzeitbereich der Anwendung.
- **Maximale anomale Antwortzeit** – Bezeichnet die höchste Antwortzeit der Anwendung.
- **Maximaler Anomalie-Verursacher** – Bezeichnet, ob die maximale Anzahl von Anomalien für die Anwendung von der Client-Netzwerklatenz, der Server-Netzwerklatenz oder der Server-Verarbeitungszeit stammt.

Anwendungs-Drilldown

Klicken Sie auf eine Anwendung, um die Details der **Anwendungsmetriken** für den ausgewählten Zeitraum anzuzeigen.

Die **Anwendungsmetriken** ermöglichen Ihnen die Anzeige von:

- **Zusammenfassung** – Eine Übersicht zur Visualisierung der Anwendungsleistung wie Antwortzeit, Anfragen und Bandbreite
- **Anfragen** – Die Gesamtzahl der von der Anwendung empfangenen Anfragen. Sie können auch Anfragen der Top 5 Clients basierend auf der Gesamtzahl der Anfragen anzeigen
- **Bandbreite** – Die gesamte von der Anwendung verarbeitete Bandbreite. Sie können auch den Bandbreitenverbrauch der Top 5 Server basierend auf dem gesamten Bandbreitenverbrauch anzeigen
- **Antwortzeit** – Eine Übersicht zur Visualisierung von Client-Netzwerklatenz, Server-Netzwerklatenz und Server-Verarbeitungszeit im selben Diagramm
- **Client-Netzwerklatenz** – Die durchschnittliche Client-Netzwerklatenz (vom Client zu NetScaler)
- **Server-Netzwerklatenz** – Die durchschnittliche Server-Netzwerklatenz (von NetScaler zum Server)
- **Server-Verarbeitungszeit** – Die durchschnittliche Server-Verarbeitungszeit (vom Server zu NetScaler)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn die Anwendung Anomalien aufweist, können Sie sehen, ob die Anomalien von der Client-Netzwerklatenz, der Server-Netzwerklatenz oder der Server-Verarbeitungszeit herrühren. Klicken Sie auf jede Registerkarte, um Details anzuzeigen.

Auf den Registerkarten **Client-Netzwerklatenz** und **Server-Netzwerklatenz** können Sie Folgendes anzeigen:

- **Eine Suchleiste** – Klicken Sie auf die Suchleiste, um die IP-Adresse aller Clients (in Client-Netzwerklatenz) und Server (in Server-Netzwerklatenz) anzuzeigen. Sie können die IP-Adresse auswählen, um die Ergebnisse zu filtern.
- **Eine Exportoption** – Klicken Sie auf **CSV herunterladen**, um die Details im CSV-Format zu exportieren.

Antwortzeit

Klicken Sie unter **Anomaliedetails**, um Details zu den Ursachen der Antwortzeit (vom Client zum Server) anzuzeigen. Das folgende Beispiel weist eine Anomalie für Client-Netzwerklatenz, Server-Netzwerklatenz und Server-Verarbeitungszeit auf. Sie können auch die erwarteten Bereiche und die Überschreitung, die über den erwarteten Bereich hinausgegangen ist, anzeigen.

Die **Empfohlenen Aktionen** schlagen Ihnen die möglichen Lösungen für die Anomalien vor.

Ähnlich können Sie auf die Registerkarten **Client-Netzwerklatenz**, **Server-Netzwerklatenz** und **Server-Verarbeitungszeit** klicken, um Folgendes anzuzeigen:

- Anomalie, die den erwarteten Bereich überschritten hat.
- Empfohlene Aktionen, die Ihnen die möglichen Lösungen vorschlagen.

Wenn die Anwendung gut funktioniert, können Sie Anwendungsmetriken ohne Anomalien anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service-Graph

Die Service-Graph-Funktion in NetScaler Console ermöglicht es Ihnen, alle Kubernetes-Dienste in einer grafischen Darstellung zu überwachen. Diese Funktion ermöglicht es Ihnen auch, eine detaillierte Analyse und umsetzbare Metriken der Dienste anzuzeigen. Navigieren Sie zu **Applications > Service Graph**, um den Service-Graph für Folgendes anzuzeigen:

- Anwendungen, die über alle NetScaler-Instanzen hinweg konfiguriert sind
- Kubernetes-Anwendungen
- 3-Tier-Webanwendungen

Service-Graph für Anwendungen über alle NetScaler-Instanzen hinweg

Die globale Service-Graph-Funktion ermöglicht Ihnen eine ganzheitliche Visualisierung der `clients to infrastructure to application`-Ansicht. Von dieser Service-Graph-Ansicht mit einer einzigen Oberfläche aus können Sie als Administrator:

- Verstehen, aus welcher Region die Benutzer auf die spezifischen Anwendungen (3-Tier-Web-Apps und Microservices-App) zugreifen
- Die Infrastrukturansicht (NetScaler-Instanz) visualisieren, in der die Client-Anfrage verarbeitet wird
- Verstehen, ob die Probleme vom Client, der Infrastruktur oder der Anwendung ausgehen
- Weiter ins Detail gehen, um das Problem zu beheben

Navigieren Sie zu **Applications > Service Graph** und klicken Sie auf die Registerkarte **Global**, um Folgendes anzuzeigen:

- End-to-End-Details aller Anwendungen, die vom Client mit den Back-End-Servern verbunden sind
- Alle NetScaler-Instanzen, die mit ihren jeweiligen Rechenzentren verbunden sind

HINWEIS

Sie können Rechenzentren nur anzeigen, wenn Sie GSLB-Anwendungen haben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die Client-Metrikinformationen
- Die NetScaler-Metrikinformationen
- Alle NetScaler-Instanzen, die diskrete Anwendungen, benutzerdefinierte Anwendungen und diskrete Microservice-Anwendungen haben
- Die Top 4 der Anwendungen mit niedriger Bewertung, die zu benutzerdefinierten Anwendungen, diskreten Anwendungen und Microservice-Anwendungen gehören
- Die Metrikinformationen für die Top 4 der virtuellen Server mit niedriger Bewertung
- Der Status der Anwendungen (diskrete Anwendungen, benutzerdefinierte Anwendungen und Microservice-Anwendungen) wie **Kritisch**, **Überprüfung**, **Gut** und **Nicht zutreffend**.

Weitere Informationen finden Sie unter Ganzheitliche Ansicht von Anwendungen im Service-Graph.

Service-Graph für Kubernetes-Anwendungen

Navigieren Sie zu **Applications > Service Graph** und klicken Sie auf die Registerkarte **Microservices**, um:

- Die End-to-End-Gesamtleistung der Anwendung sicherzustellen
- Engpässe zu identifizieren, die durch die gegenseitige Abhängigkeit verschiedener Komponenten Ihrer Anwendungen entstehen
- Einblicke in die Abhängigkeiten verschiedener Komponenten Ihrer Anwendungen zu gewinnen
- Dienste innerhalb des Kubernetes-Clusters zu überwachen
- Zu überwachen, welcher Dienst Probleme hat
- Überprüfen Sie die Faktoren, die zu Leistungsproblemen beitragen
- Detaillierte Sichtbarkeit von HTTP-Transaktionen des Dienstes anzeigen
- Analysieren Sie die HTTP-, TCP- und SSL-Metriken
- Client-Metriken und Details zur Client-Transaktionszusammenfassung anzeigen

Durch die Visualisierung dieser Metriken in NetScaler Console können Sie die Grundursache von Problemen analysieren und notwendige Fehlerbehebungsmaßnahmen schneller ergreifen. Der Service-Graph zeigt Ihre Anwendungen in verschiedenen Komponentendiensten an. Diese Dienste, die innerhalb des Kubernetes-Clusters ausgeführt werden, können mit verschiedenen Komponenten innerhalb und außerhalb der Anwendung kommunizieren. Um zu beginnen, siehe Einrichten des Service-Graphen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service-Graph für 3-Tier-Webanwendungen

Navigieren Sie zu **Anwendungen > Service-Graph** und klicken Sie auf die Registerkarte **Web-Apps**, um Folgendes anzuzeigen:

- Details zur Konfiguration der Anwendung (mit Content Switching Virtual Server und Load Balancing Virtual Server)

  Für GSLB-Anwendungen können Sie Rechenzentrum, NetScaler-Instanz, CS- und LB-Virtual Server anzeigen.
- End-to-End-Transaktionen vom Client zum Dienst
- Der Speicherort, von dem aus der Client auf die Anwendung zugreift
- Der Name des Rechenzentrums, in dem die Client-Anfragen verarbeitet werden, und die zugehörigen NetScaler-Metriken des Rechenzentrums (nur für GSLB-Anwendungen)
- Metrikdetails für Client, Dienst und Virtual Server
- Ob die Fehler vom Client oder vom Dienst stammen
- Der Dienststatus wie **Kritisch**, **Überprüfung** und **Gut**. NetScaler Console zeigt den Dienststatus basierend auf der Dienstantwortzeit und der Fehleranzahl an.
  - **Kritisch (rot)** – Zeigt an, wenn die durchschnittliche Dienstantwortzeit > 200 ms UND die Fehleranzahl > 0 ist
  - **Überprüfung (orange)** – Zeigt an, wenn die durchschnittliche Dienstantwortzeit > 200 ms ODER die Fehleranzahl > 0 ist
  - **Gut (grün)** – Zeigt keinen Fehler an und die durchschnittliche Dienstantwortzeit < 200 ms
- Der Client-Status wie **Kritisch**, **Überprüfung** und **Gut**. NetScaler Console zeigt den Client-Status basierend auf der Client-Netzwerklatenz und der Fehleranzahl an.
  - **Kritisch (rot)** – Zeigt an, wenn die durchschnittliche Client-Netzwerklatenz > 200 ms UND die Fehleranzahl > 0 ist
  - **Überprüfung (orange)** – Zeigt an, wenn die durchschnittliche Client-Netzwerklatenz > 200 ms ODER die Fehleranzahl > 0 ist
  - **Gut (grün)** – Zeigt keinen Fehler an und die durchschnittliche Client-Netzwerklatenz < 200 ms
- Der Status des virtuellen Servers wie **Kritisch**, **Überprüfung** und **Gut**. NetScaler Console zeigt den Status des virtuellen Servers basierend auf dem App-Score an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Kritisch (rot)** – Zeigt an, wenn der App-Score < 40 ist
- **Überprüfung (orange)** – Zeigt an, wenn der App-Score zwischen 40 und 75 liegt
- **Gut (grün)** – Zeigt an, wenn der App-Score > 75 ist

Hinweise:

- Nur virtuelle Load Balancing-, Content Switching- und GSLB-Server werden im Service-Graph angezeigt.
- Wenn kein virtueller Server an eine benutzerdefinierte Anwendung gebunden ist, sind die Details im Service-Graph für die Anwendung nicht sichtbar.
- Sie können Metriken für Clients und Dienste im Service-Graph nur anzeigen, wenn aktive Transaktionen zwischen virtuellen Servern und der Webanwendung stattfinden.
- Wenn keine aktiven Transaktionen zwischen virtuellen Servern und der Webanwendung verfügbar sind, können Sie Details im Service-Graph nur basierend auf den Konfigurationsdaten wie Lastausgleich, Content Switching, GSLB-virtuellen Servern und Diensten anzeigen.
- Wenn Änderungen an der Anwendungskonfiguration vorgenommen werden, kann es 10 Minuten dauern, bis diese im Service-Graph widergespiegelt werden.

Weitere Informationen finden Sie unter Service-Graph für Anwendungen.

Service-Graph für Kubernetes-Apps

Die Service-Graph-Funktion in NetScaler Console ermöglicht es Ihnen, Ihre Kubernetes-Anwendungen in einer grafischen Darstellung zu überwachen. Sie können den Service-Graph einrichten und konfigurieren, Service- und Ingress-Details anzeigen, Schwellenwerte konfigurieren, Anfragen verfolgen und Probleme in Ihren Microservices beheben.

Die folgenden Themen helfen Ihnen beim Einrichten und Verwenden des Service-Graphs für Kubernetes-Apps:

- Vereinfachtes Onboarding des Service-Graphs
- Einrichten des Service-Graphs
- Details im Service-Graph anzeigen
- Schwellenwerte im Service-Graph konfigurieren
- Servicedetails anzeigen
- Ingress-Details zur Fehlerbehebung anzeigen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Verteiltes Tracing
- Diagnose anzeigen

Service Graph – Vereinfachtes Onboarding

Der Onboarding-Prozess des Service Graph ist vereinfacht, und Sie können den Service Graph onboarden, indem Sie:

- Einen Agenten automatisch als Kubernetes-Job bereitstellen.
- Service Graph manuell konfigurieren.

Einen Agenten automatisch als Kubernetes-Job bereitstellen

Sie können den Onboarding-Prozess des Service Graph automatisieren, und dieser Prozess führt automatisch Folgendes aus:

- Lädt die für den Agenten erforderliche YAML-Datei herunter.
- Konfiguriert den Agenten.
- Registriert den Kubernetes-Cluster in der NetScaler Console.
- Führt die erforderlichen Einstellungen aus, um den Service Graph in der NetScaler Console zu füllen.

Voraussetzungen

Stellen Sie sicher, dass Sie Folgendes haben:

- Ein Citrix Cloud-Konto.
- Kubernetes Version 1.19 oder höher installiert haben.
- HELM Version 3.x installiert haben.
- Die erforderlichen Ports geöffnet.
- Die Konnektivität durch Konfigurieren der statischen Routen hergestellt. Um NetScaler MPX oder VPX in NetScaler Console mithilfe des Agenten zu registrieren, müssen Sie sicherstellen, dass die Verbindung zwischen den Clusterknoten und NetScaler MPX oder VPX hergestellt ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Falls Sie die statischen Routen nicht konfigurieren möchten, können Sie den Node-Controller konfigurieren. Weitere Informationen finden Sie unter `https://github.com/citrix/citrix-k8s-node-controller` und `https://github.com/citrix/citrix-helm-charts/tree/master/citrix-node-controller`.

Client- und Secret-CSV-Datei von Citrix Cloud™ abrufen

Nachdem Sie den Agenten konfiguriert haben, rufen Sie die Client- und Secret-CSV-Datei von der Citrix Cloud-Seite ab:

1. Melden Sie sich bei citrix.cloud.com an
2. Klicken Sie auf das **Home**-Symbol und wählen Sie **Identity and Access Management** aus.

3. Geben Sie auf der Registerkarte **API Access** einen sicheren Clientnamen ein und klicken Sie auf **Create Client**.

4. ID und Secret werden generiert. Klicken Sie auf **Download** und speichern Sie die CSV-Datei.

5. Führen Sie auf dem Kubernetes-Hauptknoten den folgenden Befehl aus, um ein Autorisierungstoken mit der ID und dem Secret zu erstellen: `wget https://raw.githubusercontent.com/citrix/citrix-helm-charts/master/generate_token.py`

   `python3 generate_token.py --accessID=<accessID> --accessSecret=<accessSecret>`

   Hinweis

   Das Autorisierungstoken ist nur 1 Stunde lang gültig.

Sie können Folgendes konfigurieren:

- NetScaler-Agent durch Erstellen eines automatischen Secrets

Oder

- NetScaler-Agent durch Erstellen eines manuellen Secrets

© 1997–2026 Citrix Systems, Inc. All rights reserved.

KONFIGURIEREN SIE DIE NETSCALER CONSOLE DURCH ERSTELLEN EINES AUTOMATISCHEN SECRETS

Stellen Sie einen Agenten mit dem Helm-Chart bereit
Führen Sie die folgenden Befehle im Kubernetes-Hauptknoten aus, um den Agenten bereitzustellen:

```
helm repo add citrix https://citrix.github.io/citrix-helm-charts
```

```
helm install citrix-adm citrix/adm-agent-onboarding --namespace <namespace> --set token=<Token>
```

Der Agent wird bereitgestellt, und der Cluster wird bei der NetScaler Console registriert. Wenn Sie den Agenten mit dem automatischen Secret erstellen, können Sie auch `adm-agent-helper` zusammen mit dem Agenten bereitstellen, der das Kubernetes-Secret mit den Agenten-Anmeldeinformationen erstellen kann.

Dieser Prozess erfolgt automatisch, wenn der Namespace als `citrix-cpx=enabled` gekennzeichnet ist. Führen Sie den folgenden Befehl auf dem Kubernetes-Hauptknoten aus:

```
kubectl label namespace <namespace> citrix-cpx=enabled
```

Hinweis

> Wenn Sie `adm-agent-helper` nicht bereitstellen möchten, können Sie das Anmeldegeheimnis manuell für den Agenten erstellen.

NetScaler VPX/MPX bei NetScaler Console registrieren
Hinweis

> Sie können NetScaler VPX/MPX in NetScaler Console nur für zusätzliche Vorteile registrieren.

Um NetScaler VPX/MPX bei NetScaler Console zu registrieren, müssen Sie die Konnektivität zwischen NetScaler VPX oder MPX und Cluster-Knoten durch Konfigurieren der statischen Routen herstellen. Sie können diesen Prozess ignorieren, wenn Sie den Citrix-Node-Controller konfiguriert haben.

Sie müssen ein Kubernetes-Geheimnis erstellen, das die NetScaler VPX/MPX-Anmeldeinformationen im Namespace enthält. Nach diesem Prozess wird das Agent-Onboarding gestartet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
kubectl create secret generic nslogin --from-literal=username=<username> --from-literal=password=<adc-password> -n <namespace>
```

Sie müssen die Management-IP-Adresse von NetScaler VPX/MPX als Umgebungsvariable festlegen: `adc.IP`.

```
helm repo add citrix https://citrix.github.io/citrix-helm-charts
```

```
helm install citrix-adm citrix/adm-agent-onboarding --namespace <namespace> --set adc.IP=<ADC ManagementIP>,adc.loginSecret=nslogin --set token=<Token>
```

Hinweis

> Stellen Sie sicher, dass die Management-HTTP-Port adc.mgmtHTTPPort und HTTPS-Port adc.mgmtHTTPSPort als 80 und 443 geöffnet sind.

AGENT DURCH ERSTELLEN EINES MANUELLEN GEHEIMNISSES KONFIGURIEREN

NetScaler CPX benötigt die Anmeldeinformationen des Agenten, um sich bei NetScaler Console zu registrieren. Sie können den Namespace manuell festlegen, um NetScaler CPX bereitzustellen.

```
kubectl create secret generic admlogin --from-literal=username=nsroot --from-literal=password=<adm-agent-password> -n <namespace>
```

Nachdem Sie das Secret erstellt haben, können Sie den folgenden Befehl verwenden, um den Agenten zu konfigurieren.

```
helm install citrix-adm citrix/adm-agent-onboarding --namespace <namespace> --set admAgent.loginSecret=admlogin --set token=<Token>
```

NetScaler VPX/MPX bei NetScaler Console registrieren

Um NetScaler VPX/MPX bei NetScaler Console zu registrieren, müssen Sie die Konnektivität zwischen NetScaler VPX oder MPX und Cluster-Knoten durch Konfigurieren der statischen Routen herstellen. Sie können diesen Vorgang ignorieren, wenn Sie `Citrix-node-controller` konfiguriert haben.

Nach dem Konfigurieren der statischen Routen müssen Sie ein Kubernetes-Secret erstellen, das die Anmeldeinformationen für NetScaler VPX/MPX im Namespace enthält. Nach diesem Vorgang wird das Agent-Onboarding gestartet.

```
kubectl create secret generic nslogin --from-literal=username=<username> --from-literal=password=<adc-password> -n <namespace>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie müssen die Verwaltungs-IP-Adresse von NetScaler VPX/MPX als Umgebungsvariable festlegen: `adc.IP`.

```
helm repo add citrix https://citrix.github.io/citrix-helm-charts
```

```
helm install citrix-adm citrix/adm-agent-onboarding --namespace <namespace> --set adc.IP=<ADC ManagementIP>,adc.loginSecret=nslogin --set token=<Token>
```

Hinweis

Stellen Sie sicher, dass der Verwaltungs-HTTP-Port adc.mgmtHTTPPort und der HTTPS-Port adc.mgmtHTTPSPort als 80 und 443 geöffnet sind.

Nachdem Sie die genannten Schritte konfiguriert haben, beginnt der Service Graph innerhalb von 15 Minuten, sich zu füllen. Navigieren Sie in NetScaler Console zu **Applications > Service Graph** und klicken Sie dann auf **Microservices**, um den Service Graph anzuzeigen.

Beispiele:

- Um einen Service Graph mit Service Mesh Lite zu generieren, siehe Service Graph Beispiel.
- Um einen Service Graph der Citrix-Integration mit Istio Service Mesh zu generieren, siehe Service Graph mit NetScaler Observability und NetScaler Console.

Service Graph manuell konfigurieren

Sie können den Service Graph manuell füllen durch:

- Konfigurieren des Agenten als Microservice im Kubernetes-Cluster.
- Abschließen der anderen Workflows, wie das Registrieren des Clusters, Hinzufügen von Instanzen und Aktivieren der Lizenzierung sowie detaillierter TCP- und Web-Transaktionen.

HINWEIS

Wenn Sie einen vorhandenen Agenten verwenden oder einen lokalen NetScaler-Agenten mithilfe eines Hypervisors konfigurieren möchten, befolgen Sie die Anweisungen unter Einrichten des Service Graph, um den Service Graph zu füllen.

1. Navigieren Sie zu **Applications > Service Graph** und wählen Sie die Registerkarte **Microservices**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können sehen, dass der Microservices-Cluster nicht konfiguriert ist. Klicken Sie auf die Option zum Konfigurieren.

2. Wählen Sie **Benutzerdefinierte Bereitstellung**.
3. Wählen Sie den Bereitstellungstyp aus.
4. Wählen Sie **Microservices** als Anwendungstyp.
5. Klicken Sie auf **Weiter**, um den Agenten einzurichten.
6. Geben Sie auf der Seite **Agent Microservice herunterladen** die folgenden Parameter an:
   a. **Anwendungs-ID** – Eine Zeichenfolgen-ID zur Definition des Dienstes für den Agenten im Kubernetes-Cluster und zur Unterscheidung dieses Agenten von anderen Agenten im selben Cluster.
   b. **Passwort** – Geben Sie ein Passwort an, damit CPX dieses Passwort verwenden kann, um CPX über den Agenten in die NetScaler Console aufzunehmen.
   c. **Passwort bestätigen** – Geben Sie zur Bestätigung dasselbe Passwort ein.

      Hinweis

      Sie dürfen das Standardpasswort (`nsroot`) nicht verwenden.

   d. Klicken Sie auf **Senden**.
7. Klicken Sie auf **YAML-Datei herunterladen** oder **Helm-Chart herunterladen**.
8. Im Kubernetes-Hauptmodus speichern Sie die heruntergeladene YAML-Datei und führen den folgenden Befehl aus, um den Agenten zu registrieren:

   `kubectl create -f <yaml file>`

   Zum Beispiel: `kubectl create -f testing.yaml`

   Der Agent wurde erfolgreich erstellt.
9. Klicken Sie auf **Agent registrieren**.

   Die Seite wird für einige Sekunden geladen und zeigt den registrierten Agenten an.
10. Stellen Sie sicher, dass der Agent in der Liste vorhanden ist, und klicken Sie auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. Sie müssen den Cluster registrieren. Klicken Sie auf **Weitere Cluster hinzufügen** und geben Sie die folgenden Parameter an:

    a. **Name** – Geben Sie einen Namen Ihrer Wahl an.

    b. **API-Server-URL** – Die Details der API-Server-URL erhalten Sie vom Kubernetes-Hauptknoten.

        i. Führen Sie auf dem Kubernetes-Hauptknoten den Befehl `kubectl cluster-info` aus.

        ii. Geben Sie die URL ein, die für **„Kubernetes main is running at.“** angezeigt wird.

    c. **Authentifizierungstoken** – Geben Sie das Authentifizierungstoken an. Das Authentifizierungstoken ist erforderlich, um den Zugriff für die Kommunikation zwischen dem Kubernetes-Cluster und der NetScaler Console zu validieren. So generieren Sie ein Authentifizierungstoken:

        Auf dem Kubernetes-Hauptknoten:

        i. Verwenden Sie die folgende YAML-Datei, um ein Dienstkonto zu erstellen:

        ```
        apiVersion: v1

        kind: ServiceAccount

        metadata:

          name: <name>

          namespace: <namespace>
        ```

        ii. Führen Sie `kubectl create -f <yaml file>` aus.

        Das Dienstkonto wird erstellt.

        iii. Führen Sie `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` aus, um die Clusterrolle an das Dienstkonto zu binden.

        Das Dienstkonto hat nun den clusterweiten Zugriff.

        Beim Erstellen des Dienstkontos wird automatisch ein Token generiert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iv. Führen Sie `kubectl describe sa <name>` aus, um das Token anzuzeigen.

v. Führen Sie `kubectl describe secret <token-name>` aus, um die geheime Zeichenfolge abzurufen.

12. Wählen Sie den Agenten aus der Liste aus.
13. Klicken Sie auf **Erstellen**.
14. Auf der Seite **Cluster** werden die Clusterinformationen angezeigt. Klicken Sie auf **Weiter**.

15. Konfigurieren Sie die CPX- und VPX-Instanzen, und klicken Sie auf **Weiter**.

16. Klicken Sie auf **Weiter**, um detaillierte Web- und TCP-Transaktionen zu aktivieren.

17. Die Konfigurationen sind abgeschlossen. Wählen Sie **Service Graph** aus und klicken Sie auf **Fertig**.

Der Service Graph wird in etwa 15 Minuten gefüllt. Navigieren Sie zu **Applications > Service Graph** und wählen Sie die Registerkarte **Microservices** aus, um den Service Graph anzuzeigen.

Einrichten des Service-Graphen

Softwareanforderungen

KUBERNETES-DISTRIBUTION	KUBERNETES-VERSION	CONTAINER-NETZWERKSCHNITTSTELLEN (CNI)	CPX-VERSION	CIC-VERSION	AGENTEN-VERSION	
Open Source	v1.16.3	Flannel, Calico oder Canal	13.0–47.103 oder höher	1.6.1 oder höher	13.0–49.x oder höher	

Sie können den Kubernetes-Cluster mit verschiedenen Bereitstellungstopologien konfigurieren, und die folgende Tabelle zeigt die Topologien, die im Service-Graphen unterstützt werden:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TOPOLOGIE	IM SERVICE-GRAPH UNTERSTÜTZT
Single-Tier oder Unified Ingress	Ja
Dual-Tier	Ja
Cloud	Ja, aber der Cloud-Lastenausgleich wird im Graph nicht angezeigt
Service Mesh Lite	Ja
Service Mesh	Ja
Dienste vom Typ LoadBalancer	Nein
Dienste vom Typ NodePort	Nein

Um die Einrichtung des Service-Graphen in NetScaler Console abzuschließen, klicken Sie auf den Topologie-Typ, den Sie für Ihren Kubernetes-Cluster konfiguriert haben, und führen Sie die genannten Verfahren aus:

- Einzelschicht- oder Unified-Ingress-Topologie
- Zweischicht- oder Service Mesh Lite-Topologie
- Service-Mesh-Topologie

HINWEIS

Das Verfahren zur Einrichtung des Service-Graphen für Zweischicht- und Service Mesh Lite-Topologien bleibt dasselbe.

Einzelschicht- oder Unified-Ingress-Topologie

Stellen Sie sicher, dass Sie die folgenden Schritte ausführen, um die Einzelschicht- oder Unified-Ingress-Topologie einzurichten. Weitere Informationen finden Sie unter Detaillierte Verfahren zur Einrichtung der Einzelschicht- oder Unified-Ingress-Topologie.

- Konfigurierter Kubernetes-Cluster mit Einzelschicht- oder Unified-Ingress-Topologie.
- Hinzugefügte VPX-, MPX-, SDX-, BLX-Instanz in NetScaler Console und **Web Insight** aktiviert.
- Hinzugefügter Kubernetes-Cluster in NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zweischicht- oder Service Mesh Lite-Topologie

Stellen Sie sicher, dass Sie die folgenden Schritte ausführen, um die Zweischicht- oder Service Mesh Lite-Topologie einzurichten. Weitere Informationen finden Sie unter Detaillierte Verfahren zur Einrichtung der Zweischicht- oder Service Mesh Lite-Topologie.

- Konfigurierter Kubernetes-Cluster mit einer der unterstützten Topologien.
- Einen Agenten installiert und konfiguriert, um die Kommunikation zwischen NetScaler Console und Kubernetes-Cluster oder verwalteten Instanzen in Ihrem Rechenzentrum oder in der Cloud zu ermöglichen.

  Sie können einen Agenten auch als Microservice bereitstellen. Weitere Informationen finden Sie im Abschnitt **Installieren eines NetScaler-Agenten** in Erste Schritte.
- Statische Routen auf dem Agenten konfiguriert, um die Kommunikation zwischen NetScaler Console und NetScaler CPX zu ermöglichen.

  HINWEIS

  Sie können diesen Vorgang ignorieren, wenn Sie einen Agenten als Microservice im selben Cluster bereitgestellt haben.
- Die Beispiel-Bereitstellungsdateien aus dem GitHub-Repository heruntergeladen.
- Erforderliche Parameter in der CPX-YAML-Datei hinzugefügt, um eine erfolgreiche CPX-Registrierung bei NetScaler Console sicherzustellen.
- Eine VPX-, MPX-, SDX- oder BLX-Instanz in NetScaler Console hinzugefügt.
- Den Kubernetes-Cluster in NetScaler Console hinzugefügt.
- Eine Beispiel-Microservice-Anwendung bereitgestellt.
- NetScaler CPX bereitgestellt und CPX bei NetScaler Console registriert (nur für zweistufige Architekturen anwendbar).
- Webtransaktions- und TCP-Transaktionseinstellungen auf **Alle** gesetzt, damit der Agent HTTP- und TCP-Transaktionen erhält.
- Datenverkehr an Microservices gesendet.

Service-Mesh-Topologie

Stellen Sie sicher, dass Sie die folgenden Schritte ausführen, um die Service-Mesh-Topologie einzurichten. Weitere Informationen finden Sie unter Detaillierte Verfahren zur Einrichtung der Service-Mesh-Topologie.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Konfigurierte Kubernetes-Cluster-Version `1.14.0` mit einer der folgenden Service-Mesh-Topologien:
  - NetScaler CPX als Sidecar-Proxy für Istio
  - NetScaler als Ingress-Gateway für Istio
- Aktivierte `admissionregistration.k8s.io/v1beta1` API. Sie können die API überprüfen, indem Sie Folgendes verwenden:

  ```
  kubectl api-versions | grep admissionregistration.k8s.io/v1beta1
  ```

  Die folgende Ausgabe zeigt an, dass die API aktiviert ist:

  ```
  admissionregistration.k8s.io/v1beta1
  ```
- Istio `istio v.1.3.0` installiert.
- Helm Version 3.x installiert.
- Einen Agent installiert und konfiguriert, um die Kommunikation zwischen NetScaler Console und dem Kubernetes-Cluster oder verwalteten Instanzen in Ihrem Rechenzentrum oder Ihrer Cloud zu ermöglichen.

  Sie können einen Agent auch als Microservice bereitstellen. Weitere Informationen finden Sie im Abschnitt **Installieren eines NetScaler-Agenten** unter Erste Schritte.
- Statische Routen auf dem Agenten konfiguriert, um die Kommunikation zwischen NetScaler Console und NetScaler CPX zu ermöglichen.

  HINWEIS

  Sie können diesen Vorgang ignorieren, wenn Sie den NetScaler-Agenten als Microservice im selben Cluster bereitgestellt haben.
- Die erforderlichen Parameter konfiguriert, um die Service-Mesh-Topologiedaten zu füllen.
- Eine Beispielanwendung bereitgestellt.
- Den Kubernetes-Cluster in NetScaler Console hinzugefügt.
- Webtransaktions- und TCP-Transaktionseinstellungen für den Agenten auf **Alle** gesetzt, um HTTP- und TCP-Transaktionen abzurufen.
- Datenverkehr an Microservices gesendet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nachdem Sie die erforderlichen Einrichtungsprozeduren abgeschlossen haben, können Sie den Service-Graph unter **Applications** > **Service Graph** und auf der Registerkarte **Microservices** anzeigen. Weitere Informationen finden Sie unter Service-Graph-Details.

Details im Service-Graph anzeigen

Nachdem Sie den Kubernetes-Cluster in NetScaler Console hinzugefügt haben, dauert es etwa 10 Minuten, bis die Daten im Service-Graph gefüllt sind. Navigieren Sie zu **Anwendungen** > **Service-Graph** und klicken Sie auf die Registerkarte **Microservices**, um die Details des Service-Graphs anzuzeigen.

ZWEISCHICHT-/SERVICE MESH LITE-TOPOLOGIE	EINSCHICHT-/UNIFIED INGRESS-TOPOLOGIE

- **Tier-1-Ingress** – Der NetScaler Ingress Controller innerhalb des Kubernetes-Clusters konfiguriert eine NetScaler-Instanz (VPX/MPX/SDX/BLX) außerhalb des Kubernetes-Clusters.
- **Tier-2-Ingress** – Der NetScaler Ingress Controller läuft als Sidecar zusammen mit der NetScaler CPX-Instanz innerhalb des Kubernetes-Clusters.
- **Ingress** – Wird für alle anderen Bereitstellungstopologien angezeigt.

Service-Graph-Dashboard

1 – End-to-End-Netzwerkkarte Ihrer Anwendung, die zeigt, wie Ihre Komponentendienste kommunizieren

2 – Diagramm, das Treffer und Fehler für eine bestimmte Zeitdauer anzeigt

3 – Suchleiste zum Suchen von Diensten

4 – Zeitliste zur Auswahl der Zeitdauer

5 - Filter anwenden, um Dienste anzuzeigen

6 – Einstellungssymbol

7 – Ansicht vergrößern und verkleinern

8 – Diagrammansicht oder Tabellenansicht

Basierend auf der ausgewählten Zeitdauer können Sie das Dienstdiagramm anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DIENSTSYMBOL	BESCHREIBUNG
	Die Kantenbreite gibt die Anzahl der Treffer an. Je größer die Kantenbreite, desto höher ist die Anzahl der Treffer.
	Ein Dienst mit einem Warnsymbol weist darauf hin, dass der Dienst Fehler aufweist.
	Ein Dienst mit einem Stoppuhrsymbol weist darauf hin, dass der Dienst Latenz- oder Antwortzeitprobleme aufweist.
	Ein Dienst mit sowohl Stoppuhr- als auch Warnsymbolen weist darauf hin, dass der Dienst sowohl Fehler als auch Latenz-/ Antwortzeitprobleme aufweist.

HINWEIS

Wenn ein Dienst kein Warn- oder Stoppuhrsymbol hat, bedeutet dies, dass der Dienst Anomalien oder eine Schwellenwertüberschreitung für Treffer aufweist.

Wählen Sie den Zeitraum aus dem Diagramm, der Treffer anzeigt, um weitere Informationen abzurufen.

HINWEIS

Wenn keine aktiven Transaktionen von NetScaler Console empfangen werden, können Sie nur die Dienste anzeigen, die von der NetScaler-Instanz lastverteilt werden. Wenn Sie den Mauszeiger über einen Dienst bewegen, werden alle Metriken als 0 angezeigt.

Der Dienstgraph wird nun mit dem von den Diensten verwendeten Protokoll angezeigt. Angenommen, Sie haben die folgenden Dienste in Ihrem Kubernetes-Cluster ausgeführt, wie im Bild gezeigt:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Wenn Sie mehrere Cluster unter **Infrastructure > Orchestration > Kubernetes > Clusters** hinzugefügt haben, können Sie die mit jedem Cluster verbundenen Dienste anzeigen.

Sie können den folgenden Status für Ihre Dienste anzeigen:

- **Kritisch (rot)** – Der Dienst weist Anomalien oder Schwellenwertüberschreitungen bei mehreren Metriken auf. Bei den Standardschwellenwerten bedeutet der Status „Kritisch“, dass die durchschnittliche Dienstantwortzeit > 200 ms UND die Fehleranzahl > 0 ist.
- **Überprüfung (orange)** – Der Dienst weist Anomalien oder Schwellenwertüberschreitungen bei einer der Metriken auf. Bei den Standardschwellenwerten bedeutet der Status „Überprüfung“, dass die durchschnittliche Dienstantwortzeit > 200 ms ODER die Fehleranzahl > 0 ist.
- **Gut (grün)** – Dienst ohne Anomalien oder Schwellenwertüberschreitungen. Bei den Standardschwellenwerten bedeutet der Status „Gut“ keinen Fehler und eine durchschnittliche Dienstantwortzeit von < 200 ms.

  Weitere Informationen zu Anomalien finden Sie unter Dienste mithilfe der Golden-Signal-Metriken überwachen.

  Weitere Informationen zu Schwellenwerten finden Sie unter Schwellenwerte im Service-Graph konfigurieren.

Im Folgenden sind Protokolle aufgeführt, mit denen Sie das von einem Dienst verwendete Protokoll identifizieren können:

- **TCP** – Zeigt an, dass der Dienst das TCP-Protokoll verwendet.
- **SSL, HTTP** – Zeigt an, dass der Dienst das SSL-über-HTTP-Protokoll verwendet.
- **SSL, TCP** – Zeigt an, dass der Dienst das SSL-über-TCP-Protokoll verwendet.

  HINWEIS

  Der Dienst ohne Protokoll zeigt an, dass der Dienst das HTTP-Protokoll verwendet.

Wichtige Metrik-Trends in der Tabellenansicht anzeigen

In der Tabellenansicht können Sie Folgendes sehen:

- Wichtige Metriken für den Dienst

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wichtige Metriken zwischen einem Quelldienst und einem Zieldienst

Als Administrator können Sie mithilfe dieser Schlüsselmetriken die Trends der Golden Signals für die ausgewählte Zeitdauer analysieren. Weitere Informationen finden Sie unter Dienstdetails anzeigen.

Pxx-Wert für die Dienstantwortzeit anzeigen

Bewegen Sie den Mauszeiger über einen Dienst, um den Pxx-Wert für die Antwortzeit anzuzeigen.

Antwortzeit (P99) – Bedeutet, dass 99 % der Anfragen für die ausgewählte Dauer unter dem P99-Wert liegen.

Wenn Sie die Dienstdetails aufrufen, können Sie auch das 99. Perzentil und das 99,9. Perzentil der Antwortzeit für die ausgewählte Dauer anzeigen.

Als Administrator können Sie mithilfe des Pxx-Werts die Dienstantwortzeit besser verstehen. Weitere Informationen finden Sie unter Dienstdetails anzeigen.

Dienstdetails anzeigen

Klicken Sie auf einen Dienst, um die folgenden Optionen anzuzeigen:

- **Details anzeigen** – Ermöglicht die Anzeige von Dienstdetails wie Namespace, Labels, Cluster, in dem der Dienst gehostet wird, und so weiter. Weitere Informationen finden Sie unter Dienstdetails anzeigen.
- **Im App-Dashboard anzeigen** – Ermöglicht die Anzeige der ausgewählten Anwendungsdetails wie App-Score, Kubernetes-Dienstdetails, Pod-Details und so weiter. Weitere Informationen finden Sie unter Kubernetes-Anwendungsdetails
- **Transaktionsprotokolle** – Ermöglicht die Anzeige der HTTP- und SSL-über-HTTP-Transaktionsdetails. Weitere Informationen finden Sie unter Analysen für Webtransaktionen anzeigen.
- **Trace-Informationen** – Ermöglicht die Anzeige des verteilten Dienst-Tracings. Weitere Informationen finden Sie unter Verteiltes Tracing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Client-Metriken anzeigen

Sie können sehen, von welchem Standort aus der Client auf den Dienst zugreift. Als Administrator können Sie die Client-Metriken visualisieren und die Probleme analysieren, die vom Client ausgehen.

Bewegen Sie den Mauszeiger über eine Client-Region, um die Metriken anzuzeigen.

- **Treffer** – Zeigt die Gesamtzahl der vom Client empfangenen Treffer an.
- **Client-Netzwerklatenz** – Zeigt die durchschnittliche Client-Netzwerklatenz an.
- **Client-4xx-Fehler** – Zeigt die Gesamtzahl der Client-4xx-Fehler an.
- **Client-SSL-Fehler** – Zeigt die Gesamtzahl der Client-SSL-Fehler an.

IP-Blöcke in NetScaler Console – NetScaler Console kann den Client-Standort erkennen, wenn der Client eine öffentliche IP-Adresse verwendet. NetScaler Console verfügt über eine integrierte Standort-CSV-Datei, die den Standort basierend auf dem IP-Adressbereich des Clients abgleicht.

NetScaler Console kann den Client-Standort mit einer privaten IP-Adresse nur erkennen, wenn die IP-Adresse zum NetScaler Console-Server hinzugefügt wurde. Wenn beispielsweise die Client-IP-Adresse in einen privaten IP-Adressbereich fällt, der mit Stadt A verbunden ist, erkennt NetScaler Console, dass der Datenverkehr für diesen Client aus Stadt A stammt.

Client-Transaktionsübersicht anzeigen

Die detaillierte Client-Transaktionsübersicht ermöglicht Ihnen die Anzeige von:

- Antwortzeit > 500 ms
- 5xx-Fehler

Klicken Sie auf einen Client-Standort und wählen Sie **Transaktionsprotokolle**.

Weitere Informationen finden Sie unter Webtransaktionsanalyse.

Ingress-Metriken anzeigen

Sie können den Typ des Ingress anzeigen, der im Kubernetes-Cluster verwendet wird.

- NetScaler-IP-Adresse und deren Score
- **Aktueller Status** – Zeigt an, ob die NetScaler-Instanz „Up“, „Down“ oder „Out of Status“ ist.
- **Max. Beitrag** – Zeigt das Problem an, das den Instanz-Score beeinflusst.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Für die einstufige Topologie können Sie nur einen einzigen **Ingress** anzeigen.

Klicken Sie auf den **Ingress**, um weitere Details anzuzeigen. Weitere Informationen finden Sie unter Ingress-Details zur Fehlerbehebung anzeigen.

TCP- und SSL-Metriken anzeigen

Mithilfe der TCP- und SSL-Metriken können Sie:

- TCP-Verbindungsdetails zwischen Diensten anzeigen
- Feststellen, ob TCP-bezogene Probleme vom Quell- oder Zieldienst stammen
- Anzeigen, ob der SSL-Fehler vom Quell- oder Zieldienst stammt
- Die von SSL-Diensten verwendete SSL-Protokollversion anzeigen

TCP-Metriken

Fahren Sie mit dem Mauszeiger über einen TCP-Dienst oder den zugehörigen eingehenden Dienst, um die TCP-Metriken anzuzeigen.

- **TCP-Verbindungen** – Gesamtzahl der zwischen den Diensten hergestellten Verbindungen
- **Datenvolumen** – Gesamte vom Dienst verarbeitete Datenmenge
- **TCP-Server-Reset** – Gesamtzahl der vom Server initiierten TCP-Resets

SSL-Metriken

Fahren Sie mit dem Mauszeiger über einen Dienst, der das SSL-Protokoll verwendet, um die SSL-Metriken anzuzeigen.

- **SSL-Serverfehler** – Zeigt die Gesamtzahl der SSL-Fehler vom Server an. (Zum Beispiel: SSL-Zertifikat unbekannt)
- **SSL-Protokoll** – Zeigt die vom Dienst verwendete SSL-Protokollversion an
- **SSL-Clientfehler** – Zeigt die Gesamtzahl der SSL-Fehler vom Client an. (Zum Beispiel: SSL-Clientauthentifizierungsfehler)

Filter anwenden

Sie können Filter anwenden, um spezifische Dienstinformationen anzuzeigen. Klicken Sie auf die Liste **Keine Filter**, um die Filteroptionen zu erhalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Sie beispielsweise Dienste anzeigen möchten, deren Latenz weniger als 150 ms beträgt, klicken Sie auf das Balkendiagramm unter **Dienstantwortzeit**, um die Ergebnisse anzuzeigen.

Klicken Sie auf **Service Info**, um Filter auszuwählen und anzuwenden für:

- **Cluster** – Zeigt alle Dienste an, die für den ausgewählten Cluster oder die ausgewählten Cluster anwendbar sind.
- **Namespace** – Zeigt alle Dienste an, die für den ausgewählten Namespace anwendbar sind.

  Hinweis

  Abhängig von den für den Dienst in der Kubernetes-Dienstdefinitions-YAML konfigurierten Bezeichnungen können Sie auch weitere Filteroptionen anzeigen.

Klicken Sie auf **Alle löschen**, um alle Filter zu löschen.

Alternativ können Sie auch das Suchtextfeld verwenden und einen Dienstnamen eingeben, um die Ergebnisse im Dienstgraphen anzuzeigen.

Einstellungsoption

1 – Einstellungen-Symbol

2 – Optionen zur Anzeige des Dienstgraphen als Standard-, Ebenenbasierte oder Kraftgesteuerte Ansichten

3 – Wählen Sie die Optionen aus der Liste, um die Dienste nach Kategorien anzuzeigen. Nachdem Sie eine Kategorie aus der Liste ausgewählt haben, klicken Sie auf **+** im Diagramm, um alle Dienste anzuzeigen.

4 – Ermöglicht Ihnen die Auswahl der Option, wie Sie die Dienste anzeigen möchten.

5 – Wählen Sie die Option **Inaktive Dienste ausblenden**, um nur die aktiven Dienste anzuzeigen.

6 – Ermöglicht Ihnen das Ändern der **Dienstinfo**-Beschriftungen. Die Registerkarte **Filter** ermöglicht Ihnen die Auswahl der Beschriftungen (basierend auf der ausgewählten Dauer und den aktiven Transaktionen der Dienste).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nachdem Sie die Beschriftungen ausgewählt haben, ermöglicht Ihnen die Registerkarte **Dienstinfo** im Abschnitt **Filter**, Filter auf die ausgewählten Beschriftungen anzuwenden, um die Ergebnisse zu filtern.

Fehler analysieren

Fahren Sie mit dem Mauszeiger über einen Dienst, der Fehler anzeigt.

FEHLER	BESCHREIBUNG
	Der **TCP-Server-Reset** zeigt die Gesamtzahl der vom Server initiierten TCP-Resets an.
	Der **TCP-Client-Reset** zeigt die Gesamtzahl der vom Client initiierten TCP-Resets an.
	Die SSL-Clientfehler geben die gesamten SSL-Fehler vom Client an. (Zum Beispiel SSL-Clientauthentifizierungsfehler).
	Die SSL-Serverfehler geben die gesamten SSL-Fehler vom Server an. (Zum Beispiel SSL-Zertifikat unbekannt)

HINWEIS

- Die Clientfehleranzahl (unabhängig vom Protokolltyp) wird in jedem Dienst angezeigt, wenn die Clientfehleranzahl **1 oder höher** ist.
- Die für einen Dienst angezeigte Clientfehleranzahl weist darauf hin, dass die Fehler vom Client stammen.

HTTP-Transaktionsdetails anzeigen

HINWEIS

Sie können die Fehler anzeigen, indem Sie den Mauszeiger über einen fehlerhaften Dienst bewegen und auf die Anzahl der Probleme klicken.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gemäß dem im Bild gezeigten Beispiel können Sie eine End-to-End-Netzwerkkarte Ihrer Anwendung anzeigen, die zeigt, wie Ihre Komponentendienste kommunizieren.

Wenn Sie den Mauszeiger über den **Ecommerce-Service** bewegen, können Sie Metrikdetails für den **Ecommerce-Service** anzeigen.

- NetScaler Console ermöglicht Ihnen auch, Transaktionsdetails zwischen Ingress und Diensten anzuzeigen. Bewegen Sie den Mauszeiger, um Details wie Gesamtfehler, durchschnittliche Dienstantwortzeit usw. zwischen Ingress und Dienst anzuzeigen.

- **Treffer** – Gibt die Gesamtzahl der vom Dienst empfangenen Treffer an.

Dienst-Antwortzeit – Gibt die durchschnittliche Antwortzeit an, die der Dienst benötigt, um auf Time To First Byte (TTFB) zu antworten.

Fehler – Gibt die Gesamtanzahl der Fehler an, z. B. 4xx, 5xx usw.

Datenvolumen – Gibt das gesamte vom Dienst verarbeitete Datenvolumen an.

SSL-Protokoll – Gibt die SSL-Protokollversion an.

Klicken Sie auf den Pfeil zwischen **Ingress** und **Dienst**, um die detaillierten Transaktionen anzuzeigen.

Weitere Informationen finden Sie unter Analysen für Webtransaktionen anzeigen.

Schwellenwerte im Service-Graph konfigurieren

Als Administrator können Sie Schwellenwerte für Kubernetes-Dienste konfigurieren. NetScaler Console zeigt den Dienststatus (Kritisch, Überprüfung und Gut) basierend auf der Dienstantwortzeit und der Fehleranzahl an. Standardmäßig können Sie den auf alle Dienste angewendeten **Standardschwellenwert** (Dienstantwortzeit = 200 ms und Fehleranzahl = 0) anzeigen.

HINWEIS

Sie können den Standardschwellenwert nicht löschen.

So konfigurieren Sie einen neuen Schwellenwert:

1. Klicken Sie unter **Applications > Service Graph** auf die Registerkarte **Microservices**:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Klicken Sie auf das Einstellungssymbol und wählen Sie die Registerkarte **Thresholds** aus.
3. Klicken Sie auf **New Threshold**, um einen neuen Schwellenwert zu konfigurieren.

   Die Seite **New Threshold** wird angezeigt.
4. Konfigurieren Sie die folgenden Parameter:

   a. **Name** – Geben Sie einen Namen für den Schwellenwert an.

   b. Wählen Sie unter **Microservices** die Dienste aus, auf die Sie den Schwellenwert anwenden möchten.

   c. Wählen Sie unter **Thresholds Single** oder **Double** für:

      - Hohe Antwortzeit (Durchschnitt, P99, P99.9)
      - Hohe Fehler
      - Hohe Treffer

   d. Geben Sie die Schwellenwerte an.

      HINWEIS

      Wenn Sie einen doppelten Schwellenwert auswählen, stellen Sie sicher:

      - Der Wert von Schwellenwert 1 ist kleiner als der Wert von Schwellenwert 2. Wenn Sie beispielsweise Schwellenwert 1 als 250 ms konfigurieren, muss Schwellenwert 2 251 ms oder höher sein.
      - Der Wert von Schwellenwert 1 darf nicht gleich dem Wert von Schwellenwert 2 sein.
5. Klicken Sie auf **Speichern**.

   Der Schwellenwert wurde erfolgreich erstellt. Sie können die Schwellenwertdetails auf der Seite **Schwellenwerte** anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

NetScaler Console berechnet die endgültige Dienstbewertung und den Status basierend auf den ausgewählten Metriken. Wenn Sie beispielsweise nur **Hohe Treffer** für die Schwellenwertkonfiguration auswählen, verwendet NetScaler Console den Standardschwellenwert (Antwortzeit = 200 ms und Fehleranzahl = 0) und hohe Treffer, um die Dienstbewertung und den Status zu berechnen.

Einzelner Schwellenwert

Wenn Sie einen einzelnen Schwellenwert für alle Metriken oder ausgewählte Metriken konfigurieren, führt NetScaler Console Folgendes aus:

- Vergleicht die aktuellen Werte in jeder Metrik mit den konfigurierten Schwellenwerten in jeder Metrik
- Berechnet die Gesamtstrafe basierend auf den überschrittenen Schwellenwerten in jeder Metrik

  Hinweis

  Wenn eine Metrik den Schwellenwert nicht überschritten hat, wird die Strafe entsprechend berechnet.

- Zeigt den Service-Score und den Service-Status basierend auf der Strafberechnung an

Doppelter Schwellenwert

Wenn Sie einen doppelten Schwellenwert für alle Metriken oder ausgewählte Metriken konfigurieren, führt NetScaler Console Folgendes aus:

- Vergleicht die aktuellen Werte in jeder Metrik mit den konfigurierten Schwellenwerten in jeder Metrik
- Prüft, ob die aktuellen Werte sind:
  - Kleiner als Schwellenwert 1
  - Zwischen Schwellenwert 1 und Schwellenwert 2
  - Größer als Schwellenwert 2
- Berechnet die Gesamtstrafe basierend auf den überschrittenen Schwellenwerten in jeder Metrik

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hinweis

Wenn eine Metrik den Schwellenwert nicht überschritten hat, wird die Strafe entsprechend berechnet.

- Zeigt den Service-Score und den Service-Status basierend auf der Strafberechnung an

Servicedetails anzeigen

Klicken Sie auf einen Dienst und wählen Sie **Details anzeigen**.

Auf der Seite mit den Servicedetails können Sie Folgendes anzeigen:

- Der Clustername, auf dem der Dienst gehostet wird (1)
- Die Namespace- und Dienstbezeichnungen des Dienstes (2) (4)
- Alle zugehörigen eingehenden und ausgehenden Dienste, die mit dem ausgewählten Dienst verbunden sind (3)
- Wichtige Dienstmetriken in einem Diagrammformat, wie z. B. Treffer, Antwortzeit, Fehler, Datenvolumen, SSL-Frontend-Fehler und TCP-Frontend-Fehler. Die Registerkarte **Metriken mit Anomalien** ermöglicht es Ihnen, die Anomalien für einen bestimmten Zeitraum anzuzeigen (5).

  Weitere Informationen finden Sie unter Dienste mithilfe der Golden-Signal-Metriken überwachen.
- Die dem Dienst zugeordneten Backend-Pods (6).

Mithilfe dieser wichtigen Metriktrends können Sie analysieren, wie der Dienst über einen bestimmten Zeitraum hinweg funktioniert.

Angenommen, ein Dienst zeigt für alle Anfragen eine Dienstantwortzeit von > 700 ms an. Als Administrator können Sie:

- Den Metriktrend der Dienstantwortzeit für einen bestimmten Zeitraum analysieren
- Das Problem beheben
- Überprüfen Sie die Metrik der Dienstantwortzeit erneut, um zu analysieren, ob sich die Antwortzeit verbessert hat.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Metrikdetails

METRIKEN	BESCHREIBUNG
Treffer	Die Gesamtzahl der vom Dienst empfangenen Anfragen
Fehler	Die gesamten HTTP-Fehler vom Dienst
Dienstantwortzeit	Die durchschnittliche Antwortzeit, die der Dienst für die Reaktion auf Time To First Byte (TTFB) benötigt.
Datenvolumen	Das gesamte vom Dienst verarbeitete Datenvolumen
SSL-Frontend-Fehler	Die gesamten SSL-Frontend-Fehler vom Dienst. Zum Beispiel: SSL CLIENTAUTH FAILURE
SSL-Backend-Fehler	Die gesamten SSL-Back-End-Fehler des Dienstes. Zum Beispiel: SSL-Clientfehler
TCP-Back-End-Fehler	Die gesamten TCP-Back-End-Fehler des Dienstes. Zum Beispiel: TCP-Server-Reset
TCP-Front-End-Fehler	Die gesamten TCP-Front-End-Fehler des Dienstes. Zum Beispiel: TCP-Client-Reset

Backend-Pod-Details anzeigen

Klicken Sie auf die Registerkarte **Pods**, um die dem Dienst zugeordneten Backend-Pods anzuzeigen.

- **Pod-Name** – Bezeichnet den Pod-Namen
- **Status** – Gibt an, ob der Pod ausgeführt wird (UP) oder nicht (DOWN).
- **IP-Adresse** – Bezeichnet die Pod-IP-Adresse

Verwenden Sie die Option Poll Now, um den Pod-Status abzurufen

Die Option **Jetzt abfragen** ruft den neuesten Pod-Status vom Cluster ab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dienste mithilfe der Golden-Signal-Metriken überwachen

Die Golden-Signal-Metriken in Diensten, die in Kubernetes-Clustern ausgeführt werden, beziehen sich auf eine Reihe von Metriken, mit denen Sie potenzielle Anomalien für eine bestimmte Dauer erkennen können. Wenn Sie Hunderte von Mikroservices im Kubernetes-Cluster haben, kann es schwierig sein, einen Dienst zu identifizieren, der häufig Probleme aufweist. Die folgenden drei Schlüsselmetriken sind die Golden-Signal-Metriken, mit denen der NetScaler Console-Graph Ihnen helfen kann, potenzielle Anomalien für einen Kubernetes-Dienst zu identifizieren:

- Treffer
- Antwortzeit (Durchschnitt) und Antwortzeit (P99)
- Fehler

Als Administrator können Sie mit diesen Metriken Folgendes tun:

- Den Dienststatus identifizieren
    - **Kritisch** – Der Dienst weist Anomalien oder Schwellenwertüberschreitungen bei mehreren Metriken auf
    - **Überprüfen** – Der Dienst weist Anomalien oder Schwellenwertüberschreitungen bei einer der Metriken auf
    - **Gut** – Dienst ohne Anomalien oder Schwellenwertüberschreitungen
- Analysieren, wie viele Anomalien in jeder Metrik identifiziert werden
- Das Problem beheben und größere Auswirkungen vermeiden

Anomalien identifizieren

Wenn Sie auf einen Dienst klicken und **Details anzeigen** auswählen, zeigt die Dienstdetailseite die Übersicht aller Metriken an. Klicken Sie auf die Registerkarte **Metriken mit Anomalien**, um die Anomaliedetails anzuzeigen.

Für jede Metrik ermöglicht Ihnen das Diagramm, die erkannten Anomalien anzuzeigen, wann immer der erwartete Bereich überschritten wird. Sie können auf die Optionen klicken, um die Ansichten im Diagramm zu filtern.

Angenommen, Sie möchten die Anomalien für die Dienst-Antwortzeit (P99) analysieren.

Unter **Antwortzeit** können Sie die folgenden Details für den ausgewählten Zeitraum anzeigen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **99. Perzentil** – Gibt an, dass 99 % der Anfragen für den ausgewählten Zeitraum weniger als 60 ms betragen
- **Durchschnitt** – Gibt die durchschnittliche Antwortzeit des Dienstes an
- **99,9. Perzentil** – Gibt die höchste Antwortzeit des Dienstes an
- **Anomalien** – Gibt die insgesamt erkannten Anomalien an

Das Diagramm ermöglicht es Ihnen auch, den erwarteten Bereich für den ausgewählten Zeitraum anzuzeigen. Gemäß dem Beispiel können Sie Folgendes anzeigen:

- Der erwartete Bereich der Antwortzeit liegt zwischen 1 ms und 9 ms.
- Zwei Anomalien für den Dienst erkannt (eine für 60 ms und eine weitere für 25 ms), da die Dienst-Antwortzeit den erwarteten Bereich (zwischen 1 ms und 9 ms) überschritten hat.

Ingress-Details zur Fehlerbehebung anzeigen

Klicken Sie im Service-Graph auf den Ingress und wählen Sie **Details anzeigen**, um die Details der NetScaler-Instanz anzuzeigen, die für den Kubernetes-Cluster konfiguriert ist.

Ingress-Details(/en-us/netscaler-console-service/media/ingress-details.png)

Klicken Sie auf **Instanzdetails**, um die Details anzuzeigen.

Instanzdetails(/en-us/netscaler-console-service/media/instanceinfo-ingress.png)

Die folgenden Details werden angezeigt:

- **Informationen** – Instanzdetails wie Instanztyp, Bereitstellungstyp, Version, Modell usw.

  Informationen(/en-us/netscaler-console-service/media/infra-analytics-instanceinfo.png)
- **Funktionen** – Standardmäßig werden die nicht lizenzierten Funktionen angezeigt. Klicken Sie auf **Lizenzierte Funktionen**, um die lizenzierten Funktionen anzuzeigen.

  Funktionen(/en-us/netscaler-console-service/media/infra-analytics-instancefeature.png)
- **Modi** – Standardmäßig werden alle auf der Instanz deaktivierten Modi angezeigt. Klicken Sie auf **Aktivierte Modi anzeigen**, um die aktivierten Modi auf der Instanz anzuzeigen.

  Modi(/en-us/netscaler-console-service/media/infra-analytics-instancemodes.png)

Das Instanz-Dashboard bietet eine Instanzübersicht, in der Sie die folgenden Details sehen können:

- **Instanz-Score**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instanz-Score(/en-us/netscaler-console-service/media/infra-analytics-instancescore.png)

1 – Zeigt den aktuellen NetScaler-Instanz-Score für die ausgewählte Zeitdauer an. Der End-Score wird berechnet als **100 minus Gesamtstrafen**. Das Diagramm zeigt die Score-Bereiche für die ausgewählte Zeitdauer.

2 – Zeigt den aktuellen Status der NetScaler-Instanz an, z. B. **Aktiv**, **Inaktiv** und **Außer Betrieb**.

3 – Zeigt die Dauer an, während der die NetScaler-Instanz aktiv und betriebsbereit ist.

4 – Zeigt die Gesamtzahl der aktivierten und deaktivierten Netzwerkschnittstellen für die Instanz an. Klicken Sie hier, um Details wie den Namen der Netzwerkschnittstelle und den Status (aktiviert oder deaktiviert) anzuzeigen.

5 – Wählen Sie die Zeitdauer aus der Liste aus, um die Instanzdetails anzuzeigen.

6 – Zeigt die Gesamtanzahl der Probleme und die Problemkategorie der NetScaler-Instanz an.

- **Wichtige Metriken**

  Klicken Sie auf jede Registerkarte, um die Details anzuzeigen. Bei jeder Metrik können Sie den Durchschnittswert und den Differenzwert für die ausgewählte Zeit anzeigen.

  Die folgende Abbildung ist ein Beispiel für HTTPS-Anfragen/Sek. und die ausgewählte Zeitdauer beträgt den letzten Monat. Der Wert **692** ist der durchschnittliche HTTPS-Anfragen/Sek.-Wert für den letzten Monat und der Wert **20** ist der Differenzwert. Im Diagramm ist der erste Wert **139** und der letzte Wert **119**. Der Differenzwert ist **139 – 119 = 20**.

  Sie können die folgenden Instanzmetriken für die ausgewählte Zeitdauer in einem Diagrammformat anzeigen:

  - **CPU-Auslastung** – Die durchschnittliche CPU-Auslastung in % der Instanz für die ausgewählte Dauer (wird sowohl für die Paket-CPU als auch für die Management-CPU angezeigt).
  - **Speichernutzung** – Die durchschnittliche Speichernutzung in % der Instanz für die ausgewählte Dauer.
  - **Festplattennutzung** – Der durchschnittliche Festplattenspeicher in % der Instanz für die ausgewählte Dauer.
  - **Durchsatz** – Der durchschnittliche Netzwerkdurchsatz, der von der Instanz für die ausgewählte Dauer verarbeitet wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **HTTPS-Anfragen/Sek.** – Die durchschnittliche Anzahl der vom Instanz empfangenen HTTPS-Anfragen für den ausgewählten Zeitraum.
- **TCP-Verbindungen** – Die durchschnittliche Anzahl der vom Client und Server hergestellten TCP-Verbindungen für den ausgewählten Zeitraum.
- **SSL-Transaktionen** – Die durchschnittliche Anzahl der von der Instanz verarbeiteten SSL-Transaktionen für den ausgewählten Zeitraum.

- **Probleme**

  Sie können die folgenden Probleme anzeigen, die in der NetScaler-Instanz auftreten:

PROBLEMKATEGORIE	BESCHREIBUNG	PROBLEME
Systemressourcen	Zeigt alle Probleme im Zusammenhang mit NetScaler-Systemressourcen wie CPU, Arbeitsspeicher, Festplattennutzung usw. an.	- Hohe CPU-Auslastung
		- Hohe Speicherauslastung
		- Hohe Festplattenauslastung
		- SSL-Kartenfehler
		- Stromausfall
		- Festplattenfehler
		- Flash-Fehler
		- NIC-Verwürfe
SSL-Konfiguration	Zeigt alle Probleme im Zusammenhang mit der SSL-Konfiguration auf der NetScaler-Instanz an.	- SSL-Zertifikate abgelaufen
		- Nicht empfohlener Aussteller

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PROBLEMKATEGORIE	BESCHREIBUNG	PROBLEME
		- Nicht empfohlener Algorithmus
		- Nicht empfohlene Schlüsselstärke
Konfigurationsabweichung	Zeigt alle Probleme im Zusammenhang mit den auf der NetScaler-Instanz angewendeten Konfigurationsaufträgen an.	- Konfigurationsdrift
		- Laufend vs. Vorlage
Kapazitätsprobleme	Zeigt NetScaler-Kapazitätsprobleme an. Die NetScaler Console fragt diese Ereignisse alle fünf Minuten von der NetScaler-Instanz ab und zeigt Paketverluste oder Erhöhungen des Ratenbegrenzungszählers an, falls vorhanden. Die Probleme werden nach den folgenden Kapazitätsparametern kategorisiert.	- Durchsatzgrenze erreicht
		- PE CPU-Grenze erreicht
		- PPS-Grenze erreicht
		- SSL-Durchsatzratenbegrenzung
		- SSL-TPS-Ratenbegrenzung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PROBLEMKATEGORIE	BESCHREIBUNG	PROBLEME
Netzwerk	Zeigt die betrieblichen Probleme an, die in den Instanzen auftreten.	Weitere Informationen finden Sie unter Erweiterte Infrastrukturanalysen mit neuen Indikatoren.

Klicken Sie auf jede Registerkarte, um das Problem zu analysieren und zu beheben. Betrachten Sie beispielsweise, dass eine Instanz die folgenden Fehler für die ausgewählte Zeitdauer aufweist:

- Die Registerkarte **Aktuell** zeigt die aktuellen betrieblichen NetScaler-Probleme an, die die Instanzbewertung beeinflussen.
- Die Registerkarte **Alle** zeigt alle erkannten Infrastrukturprobleme für die ausgewählte Dauer an.

Verteiltes Tracing

Im Service-Graph können Sie die Ansicht für verteiltes Tracing verwenden, um:

- Die Gesamtleistung des Dienstes zu analysieren.
- Den Kommunikationsfluss zwischen dem ausgewählten Dienst und seinen voneinander abhängigen Diensten zu visualisieren.
- Zu identifizieren, welcher Dienst Fehler anzeigt, und den fehlerhaften Dienst zu beheben.
- Transaktionsdetails zwischen dem ausgewählten Dienst und jedem seiner voneinander abhängigen Dienste anzuzeigen.

Voraussetzungen

Um die Trace-Informationen für den Dienst anzuzeigen, müssen Sie:

- Sicherstellen, dass eine Anwendung die folgenden Trace-Header beibehält, während sie Ost-West-Verkehr sendet:
- Für **CIC-Builds vor 1.7.23** aktualisieren Sie die CPX-YAML-Datei mit `NS_DISTRIBUTED_TRACING` und dem Wert `yes`
- Für **CIC-Builds nach 1.7.23** müssen Sie eine ConfigMap verwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ConfigMaps ermöglichen es Ihnen, Ihre Konfigurationen von Ihren Pods zu trennen und Ihre Workloads portabel zu machen. Mit ConfigMaps können Sie Ihre Workload-Konfigurationen einfach ändern und verwalten und die Notwendigkeit reduzieren, Konfigurationsdaten in Pod-Spezifikationen fest zu codieren.

Mit ConfigMap-Unterstützung können Sie die Konfiguration automatisch aktualisieren, während der NetScaler Ingress Controller Pod läuft. Sie müssen den Pod nach dem Update nicht neu starten. Weitere Informationen finden Sie unter ConfigMap-Unterstützung für den Ingress-Controller.

Mithilfe der ConfigMap können Sie verteiltes Tracing, Ereignisse, Audit-Protokolle usw. aktivieren oder deaktivieren. So verwenden Sie die ConfigMap:

a. Erstellen Sie eine YAML-Datei mit den erforderlichen Parametern.

   Die folgende YAML-Beispieldatei hat das verteilte Tracing aktiviert und andere Variablen wie Audit-Protokolle, Ereignisse und Transaktionen deaktiviert:

```
apiVersion: v1

kind: ConfigMap

metadata:

  name: cic-configmap

  namespace: default

data:

  LOGLEVEL: 'debug'

  NS_PROTOCOL: 'http'

  NS_PORT: '80'

  NS_HTTP2_SERVER_SIDE: 'ON'

  NS_ANALYTICS_CONFIG: |

    distributed_tracing:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <AgentIP> / <AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'false'
      events:
        enable: 'false'
    transactions:
      enable: 'false'
      port: 5557
```

Hinweis

Sie können die Werte für `Samplingrate` zwischen 0 und 100 angeben. NetScaler Console zeigt die angegebene Anzahl von Trace-Transaktionen an.

b. Stellen Sie die ConfigMap bereit, indem Sie Folgendes verwenden:

`kubectl create -f <configmap-yaml>.yaml`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Bearbeiten Sie die CPX-YAML-Datei und verwenden Sie entweder `envFrom` oder `args`, um die folgenden Argumente anzugeben:

```
envFrom:

 - configMapRef:

     name: cic-configmap
```

ODER

☐ Die ConfigMap-YAML-Konfiguration wird in CIC bereitgestellt.

d. Wenn Sie den Wert für eine Variable ändern möchten, bearbeiten Sie die Werte in der ConfigMap. In diesem Beispiel werden alle anderen Variablen von `false` in `true` geändert.

```
apiVersion: v1

kind: ConfigMap

metadata:

  name: cic-configmap

  namespace: default

data:

  LOGLEVEL: 'debug'

  NS_PROTOCOL: 'http'

  NS_PORT: '80'

  NS_HTTP2_SERVER_SIDE: 'ON'

  NS_ANALYTICS_CONFIG: |

    distributed_tracing:

      enable: 'true'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      samplingrate: 100
    endpoint:
      server: <AgentIP> / <AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'true'
      events:
        enable: 'true'
    transactions:
      enable: 'true'
      port: 5557
```

e. Wenden Sie die ConfigMap mit dem folgenden Befehl erneut an:

```
kubectl apply -f <yaml-file>.yaml
```

Details zur Dienstverfolgung anzeigen

Klicken Sie im Service-Graph auf einen Dienst und wählen Sie **Trace-Info** aus.

Die Seite „Trace-Zusammenfassung“ wird für den ausgewählten Dienst angezeigt.

Die **Trace-Zusammenfassung** zeigt an:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Eine erweiterte Suche, mit der Sie Transaktionen mit Vorschlägen und Operatoren durchsuchen können (1). Weitere Informationen finden Sie unter Erweiterte Suche.
- Die Liste der Zeitdauern, mit der Sie die Zeitdauer auswählen können, z. B. 1 Stunde, 12 Stunden, 1 Tag, 1 Woche, 1 Monat und benutzerdefinierte Zeit (2).
- Das Diagramm „Zeitachsen-Details“, mit dem Sie Ergebnisse für eine bestimmte Zeitdauer per Drag & Drop auswählen und anzeigen können (3).
- Das Filterfenster, mit dem Sie Optionen aus jeder Metrik auswählen können (4).
- Die Transaktionsdetails für den ausgewählten Dienst (5).

Transaktionsdetails anzeigen

Klicken Sie auf eine Transaktion, um detaillierte Informationen anzuzeigen. Sie können Transaktionsdetails für den ausgewählten Dienst anzeigen, z. B.:

- Startzeit
- Endzeit
- SSL-Metriken
- Kommunikation mit voneinander abhängigen Diensten (zusammen mit Fehlern und Antwortzeit bei jedem Dienst).

Das folgende Beispiel zeigt einen Fehler von `catalogue-store-service`. Klicken Sie auf **Trace-Details anzeigen**, um weitere Informationen zu erhalten.

Die Seite „Trace-Details“ wird angezeigt.

1 – Zeigt die Startzeit, Antwortzeit, die Gesamtzahl der Dienste und die Gesamtzahl der Spans für die Transaktion an.

2 – Zeigt die Details für den ausgewählten Dienst an, der mit seinen voneinander abhängigen Diensten kommuniziert hat. Sie können auf jede Transaktion klicken, um Details anzuzeigen.

3 – Zeigt die Transaktionsdetails für jeden Dienst an.

Gemäß dem Beispielbild zeigte `catalogue-store-service` einen Fehler an. Klicken Sie auf die für `catalogue-store-service` verfügbare Transaktion.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Transaktionsdetails zwischen `product-catalogue-service` und `catalogue-store-service` zeigen eine HTTP-Antwort von 500 an. Mit diesen Details können Sie als Administrator den fehlerhaften Dienst analysieren und `product-catalogue-service` als Lösung beheben.

Sie können Ergebnisse auch filtern, indem Sie Optionen aus jeder Metrik unter dem Bereich **Filter** auswählen. Wenn Sie beispielsweise alle 5xx-Transaktionen anzeigen möchten, klicken Sie auf **Antwortcode** und wählen Sie **500** aus.

- **Client-RTT**: Die Zeitdauer, die ein Paket benötigt, um vom Client zu gelangen.
- **Server-RTT**: Die Zeitdauer, die ein Paket benötigt, um vom Server zu gelangen.
- **App-Antwortzeit**: Die durchschnittliche Antwortzeit der Anwendung
- **Datenübertragungszeit**: Die Größe der Datenübertragung und die Rate, mit der die Übertragung von/zu einem Dienst erfolgen kann.
- **Standort**: Der Client-Standort
- **Browser**: Die von den Clients verwendeten Browsertypen. Zum Beispiel: Chrome, Firefox.
- **Client-Betriebssystem**: Das Client-Betriebssystem basierend auf den User-Agent-Details des Browsers.
- **Gerät**: Die Geräte basierend auf den User-Agent-Details des Browsers. Zum Beispiel: Tablet, Mobiltelefon.
- **Anfragetyp**: Der Transaktionsanfragetyp. Zum Beispiel: GET.
- **Antwortcode**: Der vom Server empfangene Antwortcode. Zum Beispiel: 501, 404, 200.
- **Antwort-Inhaltstyp**: Der Transaktions-Inhaltstyp. Wenn die Client-Anfrage für text/html ist, muss die Antwort vom Server text/html sein.
- **SSL-Protokoll**: Die von den Clients verwendete SSL-Protokollversion. Zum Beispiel: SSLv3.
- **SSL-Chiffrierstärke**: Die Chiffrierstärke basierend auf der Schlüsselgröße des SSL-Zertifikats, wie hoch, mittel und niedrig.
- **SSL-Schlüsselstärke**: Die SSL-Chiffrierstärke wird aus der Schlüsselgröße des SSL-Zertifikats berechnet. Die Schlüssellänge definiert die Sicherheit des SSL-Algorithmus. Zum Beispiel: 2048
- **SSL-Frontend-Fehlerursache**: Die Fehlermeldung des Frontend-SSL-Handshakes. Zum Beispiel: SSL CLIENTAUTH FAILURE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Diagnosedetails für teilweise oder keine Daten im Service-Graph anzeigen

Nachdem Sie die erforderliche Service-Graph-Konfiguration abgeschlossen und den Kubernetes-Cluster in NetScaler Console hinzugefügt haben, beginnt der Service-Graph, Daten zu befüllen. In einigen Szenarien stellen Sie möglicherweise fest, dass der Service-Graph entweder teilweise Daten oder gar keine Daten anzeigt. Einige der möglichen Gründe für teilweise oder keine Daten im Service-Graph sind:

- Statische Route ist nicht konfiguriert
- Status des Kubernetes-Clusters ist ausgefallen
- CPX-Registrierung ist fehlgeschlagen
- CPX-virtuelle Server sind nicht lizenziert
- Die erforderliche Analysekonfiguration ist nicht festgelegt, was verhindert, dass der Service-Graph alle Daten lädt

Als Administrator kann es schwierig sein, die Gründe zu analysieren, wenn der Service-Graph teilweise oder keine Daten anzeigt. Die Diagnoseinformationen auf der Service-Graph-Seite ermöglichen es Ihnen, die möglichen Gründe und erforderlichen Maßnahmen zur Behebung des Problems mit teilweisen oder fehlenden Daten zu sehen.

Navigieren Sie in NetScaler Console zu **Anwendungen** > **Service-Graph** und klicken Sie auf die Registerkarte **Microservices**.

Diagnose bei fehlenden Daten

Wenn der Service-Graph keine Daten anzeigt, wird die folgende Diagnosemeldung angezeigt.

Klicken Sie auf **>** um Details anzuzeigen. Sie können die möglichen Gründe dafür anzeigen, dass der Service-Graph keine Daten anzeigt. Die folgende Abbildung ist ein Beispiel für fehlende Daten im Service-Graph.

Klicken Sie auf **Mehr anzeigen**, um Details zu den Problemen anzuzeigen.

- **Problemtyp** – Gibt an, ob die Probleme aufgrund von Konfiguration, Analyseeinstellungen oder Lizenzierung auftreten.
- **Meldung** – Gibt an, was das Problem verursacht hat.
- **Aktion** – Gibt an, welche Aktion zur Behebung des Problems durchgeführt werden muss.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Diagnose für Teildaten

Wenn der Service-Graph nur Teildaten anzeigt, klicken Sie auf die Schaltfläche **Diagnose anzeigen**, um die Diagnoseinformationen anzuzeigen.

Das folgende Beispiel zeigt an, dass die TCP-Transaktionen deaktiviert sind.

Für dieses Beispiel müssen Sie die **TCP-Transaktionseinstellungen** auf **Alle** aktivieren, indem Sie zu **Einstellungen > Analyseeinstellungen** navigieren.

Fehlerbehebung

Als Administrator können Sie diese Diagnosemeldungen verwenden, um diese Probleme zu überprüfen und zu beheben. Nach der Fehlerbehebung führt NetScaler Console automatisch in regelmäßigen Abständen eine periodische Diagnoseprüfung durch. Nach Abschluss der Diagnoseprüfung wird das Problem mit Teildaten oder fehlenden Daten im Service-Graph behoben.

Sie können auch auf **Diagnose ausführen** klicken, die **CPX-Instanzen** auswählen und erneut auf **Diagnose ausführen** klicken.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service-Graph für 3-Schicht-Webanwendungen

So zeigen Sie den Service-Graph für eine Anwendung an:

1. Navigieren Sie zu **Anwendungen** > **Dashboard**.
2. Wählen Sie eine Anwendung aus.

   Die Seite mit den Anwendungsdetails wird angezeigt.
3. Wählen Sie die Zeitdauer aus und klicken Sie auf **Service-Graph**.

   Die Service-Graph-Seite wird für die ausgewählte Anwendung angezeigt.

Sie können den Service-Graph in der **Anwendungsansicht** oder in der **Netzwerkfunktionsansicht** anzeigen.

Anwendungsansicht

Zeigt die Übersicht der Anwendungskonfiguration an. In dieser Ansicht können Sie die Kommunikation zwischen Client, NetScaler und Webanwendungen visualisieren.

Für eine GSLB-Anwendung können Sie die Kommunikation zwischen Client, Rechenzentrum, NetScaler und Diensten visualisieren.

Ansicht der Netzwerkfunktionen

Zeigt die virtuellen Server an, die der Anwendung zugeordnet sind. In dieser Ansicht können Sie visualisieren, ob der NetScaler kommuniziert mit:

- Virtueller Content Switching-Server für den Zugriff auf die Anwendung
- Virtueller Load Balancing-Server für den Zugriff auf die Anwendung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Sowohl virtuelle Content Switching- als auch Load Balancing-Server für den Zugriff auf die Anwendung

Für GSLB-Anwendungen werden die Details zusammen mit dem Rechenzentrum und dem NetScaler angezeigt.

Service-Graph-Ansicht für keine aktiven Transaktionen

Wenn keine aktiven Transaktionen zwischen NetScaler und der Webanwendung stattfinden, zeigt der Service-Graph nur die Basiskonfiguration der Anwendung an (ohne Client und NetScaler).

Wenn Sie den Mauszeiger über einen Dienst oder virtuellen Server bewegen, werden die Details für alle Metriken als 0 angezeigt, da keine Transaktionen stattfinden.

Metriken analysieren

Bewegen Sie den Mauszeiger über jeden Dienst, um Metrikdetails entweder in der **Anwendungsansicht** oder in der **Netzwerkfunktionsansicht** anzuzeigen.

Client-Metriken

Fahren Sie mit dem Mauszeiger über den Client, um die Client-Metriken anzuzeigen.

- **Treffer** – Gesamtzahl der vom Client empfangenen Anfragen.
- **Client-Netzwerklatenz** – Zeigt die Netzwerklatenz vom Client an.
- **Datenvolumen** – Zeigt die vom Client verarbeiteten Gesamtdaten an.

Metriken der Netzwerkfunktion

Fahren Sie mit dem Mauszeiger über einen Lastausgleichs- oder Content-Switching-Dienst, um die Metrikdetails anzuzeigen.

- **Aktueller Status** – Zeigt den aktuellen Status des virtuellen Servers an
- **Treffer** – Zeigt die Gesamtzahl der vom virtuellen Server empfangenen Treffer an

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Datenvolumen** – Zeigt das vom virtuellen Server verarbeitete Gesamtdatenvolumen an

Dienstmetriken

Fahren Sie mit dem Mauszeiger über einen Dienst (Webanwendung), um die Metriken anzuzeigen

- **Treffer** – Gibt die Gesamtzahl der vom Dienst empfangenen Treffer an
- **Dienstantwortzeit** – Gibt die durchschnittliche Antwortzeit des Dienstes an
- **Fehler** – Gibt die Gesamtzahl der vom Dienst aufgetretenen Fehler an
- **Datenvolumen** – Gibt die vom Dienst verarbeitete Gesamtmenge an Daten an

NetScaler-Metriken (nur für GSLB-Anwendungen)

Fahren Sie mit dem Mauszeiger über den NetScaler, um die Metriken anzuzeigen.

- Zeigt den Hostnamen und den aktuellen NetScaler-Score an. Der Score wird basierend auf den verschiedenen potenziellen NetScaler-Problemen berechnet. Weitere Informationen finden Sie unter Instanz-Score.
- **IP-Adresse** – Bezeichnet die NetScaler-IP-Adresse
- **Aktueller Status** – Bezeichnet den NetScaler-Status wie Up, Down oder Außer Betrieb
- **NetScaler-Verarbeitungszeit** – Bezeichnet die durchschnittliche Verarbeitungszeit der NetScaler-Instanz

HINWEIS

Wenn dem NetScaler kein Hostname zugewiesen ist:

- Die NetScaler-IP-Adresse wird anstelle des Hostnamens angezeigt.
- In den Metriken werden die Informationen zur NetScaler-IP-Adresse nicht angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ganzheitliche Ansicht aller Anwendungen im Service-Graph

Navigieren Sie zu **Applications** > **Service Graph** und klicken Sie dann auf **Global**.

Der Service-Graph zeigt Folgendes für den ausgewählten Zeitraum an:

- Die Region, von der aus die Benutzer auf die spezifische Anwendung zugreifen
- Rechenzentren, in denen die NetScaler-Instanzen gehostet werden
- Die gesamten diskreten Anwendungen von allen NetScaler-Instanzen

  HINWEIS

  Wenn eine NetScaler-Instanz keine diskreten Anwendungen hat, ist die Pfeilkante von der NetScaler-Instanz zum diskreten virtuellen Server nicht sichtbar.

- Die gesamten benutzerdefinierten Anwendungen von allen NetScaler-Instanzen
- Die gesamten Microservice-Anwendungen von der NetScaler CPX-Instanz

Client-Metriken anzeigen

Fahren Sie mit dem Mauszeiger über eine Client-Region, um die Metriken anzuzeigen.

- **Treffer** – Gesamtzahl der vom Client empfangenen Anfragen.
- **Client-Netzwerklatenz** – Zeigt die Netzwerklatenz vom Client an.
- **Datenvolumen** – Zeigt die vom Client verarbeitete Gesamtmenge an Daten an.

NetScaler-Details anzeigen

Der Service Graph ermöglicht Ihnen die Anzeige von:

- Das Rechenzentrum, gruppiert nach seinen gesamten NetScaler-Instanzen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Nur die Top 4 der NetScaler-Instanzen mit der niedrigsten Bewertung aus jedem Rechenzentrum

Klicken Sie auf **Weitere NetScaler-Instanzen**, um alle NetScaler-Instanzen anzuzeigen, indem Sie die entsprechenden Status-Registerkarten (Kritisch, Überprüfung, Gut und Nicht zutreffend) auswählen.

Bewegen Sie den Mauszeiger über eine NetScaler-Instanz, um die Metriken anzuzeigen.

Sie können Folgendes anzeigen:

- IP-Adresse und Bewertung der NetScaler-Instanz
- **Hostname** – Zeigt den Hostnamen an, der der NetScaler-Instanz zugewiesen ist
- **Aktueller Status** – Zeigt den aktuellen Status der NetScaler-Instanz an, z. B. Up, Down, Out-of-Service.
- **Maximaler Beitrag** – Gibt das Hauptproblem an, das den aktuellen NetScaler-Score beeinflusst.
- **SSL-Probleme** – Gibt die Gesamtzahl der SSL-Probleme der NetScaler-Instanz an. Klicken Sie auf die Fehleranzahl, um Details zu den SSL-Fehlern anzuzeigen.

Klicken Sie auf die **NetScaler-Instanz**, um die Instanzdetails wie Instanz-Score, Schlüsselmetriken und Probleme, die mit der NetScaler-Instanz verbunden sind, anzuzeigen. Weitere Informationen finden Sie unter Instanzdetails in Infrastructure Analytics anzeigen.

Diskrete Anwendungen anzeigen

Der Service-Graph zeigt die 4 diskreten Anwendungen mit den niedrigsten Scores an.

Angenommen, Sie haben die folgenden diskreten Anwendungen:

APP-NAME	NETSCALER	APP-SCORE	APP-STATUS
App1	10.102.29.50	35 (Kritisch)	Aktiv
App2	10.102.29.90	100 (Gut)	Inaktiv
App 3	10.102.32.40	49 (Überprüfung)	Aktiv

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APP-NAME	NETSCALER	APP-SCORE	APP-STATUS
App4	10.102.113.208	92 (Gut)	Inaktiv
App5	10.102.25.25	86 (Gut)	Hoch
App6	10.102.29.41	77 (Gut)	Hoch
App7	10.102.29.102	41 (Überprüfung)	Hoch

In diesem Szenario können Sie App1, App3, App6 und App7 als die 4 Anwendungen mit der niedrigsten Bewertung im Service-Graph anzeigen.

Ebenso können Sie die 4 Anwendungen mit der niedrigsten Bewertung für **benutzerdefinierte** und **Microservices**-Anwendungen anzeigen.

Fahren Sie mit dem Mauszeiger über einen Dienst, um die Metrikinformationen anzuzeigen.

Sie können Folgendes anzeigen:

- Der Anwendungsname und die Bewertung
- **Aktueller Status** – Zeigt den aktuellen Status der Anwendung an, z. B. „Up“ oder „Down“
- **Probleme** – Zeigt die Gesamtzahl der für die Anwendung zutreffenden Probleme an
- **Top-Problem** – Zeigt das Hauptproblem an, das die Gesamtbewertung der Anwendung beeinflusst

Klicken Sie auf **Mehr**, um alle diskreten Anwendungen anzuzeigen. Die Seite „Diskreter virtueller Server“ wird wie in der folgenden Abbildung gezeigt angezeigt:

Die virtuellen Server werden entsprechend dem Status angezeigt.

- **Gesamt** – Gesamtzahl der diskreten Anwendungen
- **Kritisch** – App-Score liegt zwischen 0 und < 40
- **Überprüfen** – App-Score liegt zwischen 40 und < 75
- **Gut** – App-Score ist > 75
- **Nicht zutreffend** – App ist keinem virtuellen Server zugeordnet

Sie können auf jede Registerkarte klicken, um die virtuellen Server anzuzeigen. Wenn Sie auf eine Anwendung klicken, wird der Service Graph für die ausgewählte Anwendung angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen finden Sie unter Service Graph für Anwendungen.

Microservice-Anwendungen anzeigen

Der Dienstgraph zeigt auch alle Microservice-Anwendungen an, die zu den Kubernetes-Clustern gehören. Fahren Sie mit dem Mauszeiger über einen Dienst, um die Metrikdetails anzuzeigen.

Sie können Folgendes anzeigen:

- Der Dienstname
- Das vom Dienst verwendete Protokoll, z. B. SSL, HTTP, TCP, SSL über HTTP
- **Treffer** – Die Gesamtzahl der vom Dienst empfangenen Treffer
- **Dienst-Antwortzeit** – Die durchschnittliche Antwortzeit des Dienstes.

  (Antwortzeit = Client-RTT + letztes Byte der Anforderung – erstes Byte der Anforderung)
- **Fehler** – Die Gesamtfehler, z. B. 4xx, 5xx usw.
- **Datenvolumen** – Das vom Dienst verarbeitete Gesamtvolumen der Daten
- **Namespace** – Der Namespace des Dienstes
- **Clustername** – Der Clustername, auf dem der Dienst gehostet wird
- **SSL-Serverfehler** – Die gesamten SSL-Fehler vom Dienst

Wenn Sie auf einen Dienst klicken, wird der Kubernetes-Dienstgraph für den ausgewählten Dienst zusammen mit den angewendeten Filtern für Dienst-Namespace und Clusternamen angezeigt.

Klicken Sie auf **Mehr**, um den Kubernetes-Dienstgraph mit allen Diensten anzuzeigen. Weitere Informationen zum Kubernetes-Dienstgraph finden Sie unter Dienstgraph für Cloud-native Anwendungen.

Suchleiste zum Filtern von Ergebnissen

Sie können die Suchleiste verwenden, um Ergebnisse zu filtern. Als Administrator können Sie mit dieser Suchleiste schnell eine bestimmte Instanz/einen bestimmten Client/eine bestimmte Anwendung/ein bestimmtes Rechenzentrum eingrenzen, wenn Sie Folgendes haben:

- Ein großes Unternehmen mit vielen Rechenzentren

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Viele NetScaler-Instanzen für jedes Rechenzentrum konfiguriert
- Viele Anwendungen konfiguriert, die über jede NetScaler-Instanz bereitgestellt oder darauf zugegriffen werden
- Clients, die von verschiedenen Standorten aus auf die Anwendung zugreifen

Platzieren Sie den Mauszeiger auf der Suchleiste und wählen Sie die Kategorie aus, für die Sie den Filter erstellen möchten.

Wenn Sie beispielsweise eine bestimmte NetScaler-Instanz anzeigen möchten, wählen Sie **Instanz** aus der Suchleiste und wählen Sie die IP-Adresse der Instanz aus. Der globale Service-Graph zeigt die ausgewählte Instanz und ihre zugehörigen Anwendungen, Rechenzentren und Client-Standorte an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

StyleBooks vereinfachen die Verwaltung komplexer NetScaler-Konfigurationen für Ihre Anwendungen. Ein StyleBook ist eine Vorlage, die Sie zum Erstellen und Verwalten von NetScaler-Konfigurationen verwenden können.

Mit einem StyleBook können Sie:

- Eine bestimmte Funktion von NetScaler konfigurieren.
- Konfigurationen für eine Unternehmensanwendungsbereitstellung wie Microsoft Exchange oder Lync erstellen.

StyleBooks passen gut zu den Prinzipien von Infrastructure-as-Code, die von DevOps-Teams praktiziert werden, wo Konfigurationen deklarativ und versionskontrolliert sind. Die Konfigurationen werden auch wiederholt und als Ganzes bereitgestellt. StyleBooks bieten die folgenden Vorteile:

- **Deklarativ**: StyleBooks sind in einer deklarativen statt einer imperativen Syntax geschrieben. StyleBooks ermöglichen es Ihnen, sich auf die Beschreibung des Ergebnisses oder des „gewünschten Zustands“ der Konfiguration zu konzentrieren, anstatt auf die Schritt-für-Schritt-Anweisungen, wie dies auf einer bestimmten NetScaler-Instanz erreicht werden kann. NetScaler Console berechnet die Differenz zwischen dem vorhandenen Zustand auf einem NetScaler und dem von Ihnen angegebenen gewünschten Zustand und nimmt die notwendigen Änderungen an der Infrastruktur vor. Da StyleBooks eine deklarative Syntax verwenden, die in YAML geschrieben ist, können Komponenten eines StyleBooks in beliebiger Reihenfolge angegeben werden, und NetScaler Console bestimmt die korrekte Reihenfolge basierend auf ihren berechneten Abhängigkeiten.
- **Atomar**: Wenn Sie StyleBooks zur Bereitstellung von Konfigurationen verwenden, wird entweder die vollständige Konfiguration bereitgestellt oder gar keine, und dies stellt sicher, dass die Infrastruktur immer in einem konsistenten Zustand bleibt.
- **Versioniert**: Ein StyleBook hat einen Namen, einen Namespace und eine Versionsnummer, die es eindeutig von jedem anderen StyleBook im System unterscheidet. Jede Änderung an einem StyleBook erfordert eine Aktualisierung seiner Versionsnummer (oder seines Namens oder Namespaces), um diesen einzigartigen Charakter zu erhalten. Die Versionsaktualisierung ermöglicht es Ihnen auch, mehrere Versionen desselben StyleBooks zu verwalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Komponierbar**: Nachdem ein StyleBook definiert wurde, kann es als Einheit verwendet werden, um andere StyleBooks zu erstellen. Sie können die Wiederholung gängiger Konfigurationsmuster vermeiden. Es ermöglicht Ihnen auch, Standardbausteine in Ihrer Organisation zu etablieren. Da StyleBooks versioniert sind, führen Änderungen an bestehenden StyleBooks zu neuen StyleBooks, wodurch sichergestellt wird, dass abhängige StyleBooks niemals unbeabsichtigt beschädigt werden.
- **Anwendungszentriert**: StyleBooks können verwendet werden, um die NetScaler-Konfiguration einer vollständigen Anwendung zu definieren. Die Konfiguration der Anwendung kann durch die Verwendung von Parametern abstrahiert werden. Daher können Benutzer, die Konfigurationen aus einem StyleBook erstellen, mit einer einfachen Oberfläche interagieren, die darin besteht, einige Parameter auszufüllen, um eine potenziell komplexe NetScaler-Konfiguration zu erstellen. Konfigurationen, die aus StyleBooks erstellt werden, sind nicht an die Infrastruktur gebunden. Eine einzelne Konfiguration kann somit auf einer oder mehreren NetScaler-Instanzen bereitgestellt und auch zwischen Instanzen verschoben werden.
- **Automatisch generierte Benutzeroberfläche**: NetScaler Console generiert automatisch UI-Formulare, die zum Ausfüllen der Parameter des StyleBooks verwendet werden, wenn die Konfiguration über die NetScaler Console GUI erfolgt. StyleBook-Autoren müssen keine neue GUI-Sprache lernen oder separate UI-Seiten und -Formulare erstellen.
- **API-gesteuert**: Alle Konfigurationsvorgänge werden über die NetScaler Console GUI oder über REST-APIs unterstützt. Die APIs können im synchronen oder asynchronen Modus verwendet werden. Zusätzlich zu den Konfigurationsaufgaben ermöglichen die StyleBooks-APIs auch die Entdeckung des Schemas (Parameterbeschreibung) jedes StyleBooks zur Laufzeit.

Sie können ein StyleBook verwenden, um mehrere Konfigurationen zu erstellen. Jede Konfiguration wird als Konfigurationspaket gespeichert. Angenommen, Sie haben ein StyleBook, das eine typische HTTP-Lastverteilungsanwendungskonfiguration definiert. Sie können eine Konfiguration mit Werten für die Lastverteilungsentitäten erstellen und diese auf einer NetScaler-Instanz ausführen. Diese Konfiguration wird als Konfigurationspaket gespeichert. Sie können dasselbe StyleBook verwenden, um eine weitere Konfiguration mit anderen Werten zu erstellen und diese auf derselben oder einer anderen Instanz auszuführen. Für diese Konfiguration wird ein neues Konfigurationspaket erstellt. Ein Konfigurationspaket wird sowohl auf der NetScaler Console als auch auf der NetScaler-Instanz gespeichert, auf der die Konfiguration ausgeführt wird.

Sie können entweder Standard-StyleBooks, die mit NetScaler Console geliefert werden, verwenden, um Konfigurationen für Ihre Bereitstellung zu erstellen, oder Ihre eigenen StyleBooks entwerfen und in NetScaler Console importieren. Sie können die StyleBooks verwenden, um Konfigurationen entweder über die NetScaler Console GUI oder über APIs zu erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dieses Dokument enthält die folgenden Abschnitte:

- Anzeigen von StyleBooks
- Standard-StyleBooks
- Für Geschäftsanwendungen entwickelte StyleBooks
- Benutzerdefinierte StyleBooks
- APIs in StyleBooks
- StyleBooks-Grammatik

StyleBook-Kategorien

In NetScaler Console gibt es zwei StyleBook-Kategorien: Standard und Benutzerdefiniert, die entweder öffentlich oder privat sein können. NetScaler Console ermöglicht es Ihnen, alle im System vorhandenen StyleBooks anzuzeigen und zu sehen, wie sie miteinander verbunden sind.

Dieses Dokument erläutert die verschiedenen Arten von StyleBooks und die folgenden Aktionen, die Sie mit den StyleBooks von NetScaler Console ausführen können:

- Ein benutzerdefiniertes StyleBook herunterladen und Änderungen vornehmen oder ein StyleBook basierend auf einem vorhandenen erstellen.
- Standard-StyleBooks von NetScaler Console ausblenden.
- Ein benutzerdefiniertes StyleBook aus NetScaler Console löschen.
- Tags zu den StyleBooks hinzufügen.

Standard- und benutzerdefinierte StyleBooks

- **Standard-StyleBooks** sind die mit NetScaler Console ausgelieferten StyleBooks, mit denen Sie Konfigurationen erstellen können, die Sie auf Ihren NetScaler-Instanzen bereitstellen können. Sie können Standard-StyleBooks nicht löschen, aber Sie können sie in der NetScaler Console-GUI ausblenden.
- **Benutzerdefinierte StyleBooks** sind Ihre eigenen StyleBooks, die Sie in NetScaler Console importiert haben.

Sowohl Standard- als auch benutzerdefinierte StyleBooks können entweder öffentlich oder privat sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Öffentliche und private StyleBooks

StyleBooks, aus denen Sie Konfigurationspakete erstellen können, werden als **öffentliche** StyleBooks kategorisiert. Das heißt, sie stehen Ihnen alle zur direkten Verwendung zur Verfügung, um Konfigurationen über die NetScaler Console-GUI und APIs zu erstellen.

Einige StyleBooks werden jedoch als Bausteine für andere StyleBooks verwendet. Solche StyleBooks sind als **privat** gekennzeichnet. Die privaten StyleBooks können nicht direkt verwendet werden, um Konfigurationspakete über die NetScaler Console-GUI zu erstellen. Sie können diese StyleBooks jedoch weiterhin in NetScaler Console anzeigen und einsehen. Um eines Ihrer benutzerdefinierten StyleBooks als **privat** zu kennzeichnen, setzen Sie das private Attribut im StyleBook auf **true**. Sie können private StyleBooks weiterhin verwenden, um Konfigurationspakete mithilfe der NetScaler Console-APIs zu erstellen.

Beispiel eines als privat gekennzeichneten StyleBooks

```
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Configuration

description: |

    This StyleBook defines a simple load balancing configuration and is a
building block to build other load balancing configurations.

schema-version: "1.0"

private: true
```

StyleBooks anzeigen

Die Anzahl der StyleBooks – sowohl Standard- als auch private – nimmt in NetScaler Console zu. Möglicherweise möchten Sie nach dem bestimmten StyleBook suchen, auf das Sie zugreifen möchten. Sie möchten möglicherweise auch beide Arten von StyleBooks separat anzeigen.

In NetScaler Console können Sie, wenn Sie zu **Applications > Configuration > StyleBooks** navigieren, eine Liste der im System vorhandenen StyleBooks anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ein öffentliches Standard-StyleBook hat das folgende Symbol auf seinem Panel:

Ein privates Standard-StyleBook hingegen hat ein Symbol, das es als privates StyleBook kennzeichnet:

Obwohl Sie die Definition und Abhängigkeiten eines privaten StyleBooks anzeigen können, können Sie über die GUI kein Konfigurationspaket aus einem privaten StyleBook erstellen. Der Hauptzweck eines privaten StyleBooks besteht darin, es als Baustein für ein anderes StyleBook zu verwenden. Die Verwendung von Baustein-StyleBooks fördert die Wiederverwendung gängiger Konfigurationsmuster.

Ein benutzerdefiniertes öffentliches StyleBook hat ein anderes Symbol, wie in der folgenden Abbildung gezeigt:

Ein benutzerdefiniertes privates StyleBook erscheint mit diesem Symbol:

Oben rechts auf der Seite sehen Sie eine Option zur Auswahl des anzuzeigenden StyleBook-Typs. Es gibt drei Optionen: alle, öffentliche oder private StyleBooks. Klicken Sie auf eine der Optionen.

Sie können auch nach einem bestimmten StyleBook suchen, indem Sie auf das Suchsymbol klicken. Sie können nach Namen, Namensräumen und Versionsattributen oder einer Kombination dieser Optionen suchen. Die Suchoperation ist nicht zwischen Groß- und Kleinschreibung zu unterscheiden.

Benutzerdefinierte StyleBooks herunterladen

Um die benutzerdefinierten StyleBooks von NetScaler Console herunterzuladen, navigieren Sie zu **Applications > Configuration > Confg Packs**. Aktivieren Sie in der Liste der StyleBooks, die im rechten Bereich angezeigt werden, die Option zum Herunterladen der benutzerdefinierten StyleBooks. Klicken Sie auf **Download**. Wenn das StyleBook abhängige benutzerdefinierte StyleBooks enthält, können Sie die abhängigen StyleBooks in das heruntergeladene Bundle aufnehmen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Sie können benutzerdefinierte StyleBooks herunterladen, die entweder als öffentlich oder privat gekennzeichnet sind.

HINWEIS

Sie können die Standard-StyleBooks der NetScaler Console nicht herunterladen. Sie können deren Definitionen und Abhängigkeiten anzeigen. Klicken Sie dazu auf die Links **View Definition** und **View Dependencies** im StyleBook-Bereich.

Benutzerdefiniertes StyleBook aktualisieren

Sie können die Definitionen der benutzerdefinierten StyleBooks direkt über die NetScaler Console GUI aktualisieren. So können Sie das StyleBook ändern, ohne dessen Version zu ändern. Sie können auch die Definitionen aktualisieren, die aus einem StyleBook-Bundle importiert wurden.

WICHTIG

Bevor Sie die StyleBook-Definition über die NetScaler Console GUI aktualisieren, stellen Sie sicher, dass die StyleBook-Definition keine abhängigen StyleBooks hat.

Sie können eine StyleBook-Definition aktualisieren, die Konfigurationspakete enthält. Stellen Sie sicher, dass die StyleBook-Definition abwärtskompatibel ist. So bleiben alle Parameter im aktualisierten StyleBook erhalten und die neu hinzugefügten Parameter erscheinen als optional.

1. Navigieren Sie zu **Applications > Configuration > StyleBooks**.
2. Wählen Sie die Registerkarte **Custom StyleBooks** aus.
3. Wählen Sie **Definition aktualisieren** für das StyleBook, das Sie aktualisieren möchten.
4. Aktualisieren Sie die Definition nach Bedarf und klicken Sie auf **Aktualisieren**.
5. Aktualisieren Sie die Seite, um die neuesten Änderungen anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benutzerdefinierte StyleBooks löschen

Sie können ein benutzerdefiniertes StyleBook auch löschen, indem Sie auf die Schaltfläche **Löschen** klicken. Ein Pop-up-Fenster fordert Sie auf, zu bestätigen, ob Sie das StyleBook aus der NetScaler Console entfernen möchten. Wenn das StyleBook andere benutzerdefinierte StyleBooks verwendet, können Sie diese StyleBooks durch Aktivieren des Kontrollkästchens entfernen.

HINWEIS:

Löschen Sie kein benutzerdefiniertes StyleBook, wenn es abhängige StyleBooks in der NetScaler Console hat. Diese Aktion kann die vorhandenen StyleBooks beschädigen.

StyleBook-Abhängigkeiten anzeigen

Ein wichtiges und leistungsstarkes Merkmal von StyleBooks ist, dass sie als Bausteine für andere StyleBooks verwendet werden können.

Sie können:

- **Ein StyleBook in ein anderes StyleBook importieren** — Ein importiertes StyleBook wird als Typ deklariert und von den Komponenten oder Parametern des zweiten StyleBooks verwendet. Zeigen Sie die vorhandenen Standard-StyleBooks in der NetScaler Console an, um zu erfahren, wie ein StyleBook auf einem anderen StyleBook aufgebaut werden kann.
- **Eine grafische Darstellung der Verbindung von StyleBooks untereinander anzeigen** — Diese Darstellung ist nützlich für komplexe StyleBooks, die unter Verwendung anderer StyleBooks als Bausteine erstellt werden. Der Abhängigkeitsgraph ermöglicht es Ihnen, die Beziehungen und Abhängigkeiten zwischen den StyleBooks zu sehen.

HINWEIS:

Sie können ein StyleBook, das von anderen StyleBooks verwendet wird, nicht löschen, da diese Aktion die vorhandenen StyleBooks beschädigen kann. Verwenden Sie die Abhängigkeitsgrafik, um zu ermitteln, welche StyleBooks das Entfernen eines StyleBooks verhindern.

So zeigen Sie StyleBook-Abhängigkeiten an

Navigieren Sie in NetScaler Console zu **Applications > Configuration > StyleBooks**. Die Seite „StyleBooks“ zeigt alle StyleBooks an, die Ihnen in NetScaler Console zur Verfügung stehen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scrollen Sie nach unten und suchen Sie Ihr StyleBook. Klicken Sie auf **View Dependencies**, um die abhängigen StyleBooks anzuzeigen.

Vorwärtsabhängigkeiten

Auf der Registerkarte **Forward Dependencies** können Sie die verschiedenen Standard-StyleBooks anzeigen, die Ihr StyleBook verwendet. Folgen Sie den Pfeilen, um das StyleBook zu finden, das ein StyleBook verwendet. Wenn Sie mit der Maus auf einen der Pfeile zeigen, werden der Pfeil und die miteinander verbundenen StyleBooks hervorgehoben. Sie können auch auf ein StyleBook klicken, um die Definition dieses StyleBooks anzuzeigen.

Rückwärtsabhängigkeiten

Auf der Registerkarte **Reverse Dependencies** können Sie die StyleBooks grafisch anzeigen, die Ihr StyleBook verwenden. Wenn Sie den Pfeilen folgen, können Sie sehen, dass alle StyleBooks in der Anzeige auf Ihr StyleBook zeigen. Einige StyleBooks verwenden das StyleBook möglicherweise direkt, und einige StyleBooks verwenden das StyleBook möglicherweise über ein anderes StyleBook.

NetScaler-Konfiguration anhand von Konfigurationspaketen prüfen

Sie können die Änderungen, die ein StyleBook-Konfigurationspaket vorgenommen hat, mit der aktuellen NetScaler-Konfiguration vergleichen. Mit diesem Vergleich können Sie Folgendes tun:

- Erkennen Sie die Konfigurationsabweichung zwischen StyleBook-Konfigurationspaket und NetScaler-Konfiguration.
- Identifizieren Sie alle geänderten und gelöschten Objekte auf dem NetScaler, die die vom Konfigurationspaket vorgenommenen Änderungen nicht anzeigen.

Um die Änderungen des Konfigurationspakets mit der NetScaler-Instanzkonfiguration zu vergleichen, gehen Sie wie folgt vor:

1. Navigieren Sie zu **Applications > Configuration > Config Packs**.
2. Klicken Sie auf **Konfigurationsprüfung**.

   Die Seite „Konfigurationsprüfung“ zeigt die erstellten und geprüften Objekte an.

   NetScaler-Konfiguration anhand des Konfigurationspakets prüfen(/en-us/netscaler-console-service/media/configuration-audit-configpack.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Beim Aktualisieren eines StyleBook-Konfigurationspakets, das auf einer NetScaler-Instanz bereitgestellt ist, kann es Unterschiede zu seinem bereitgestellten Zustand aufweisen. Und die Aktualisierung des Konfigurationspakets schlägt fehl. Die StyleBook-Engine gleicht diese Unterschiede automatisch ab und aktualisiert das Konfigurationspaket.

Support-Bundle eines Konfigurationspakets herunterladen

Das Support-Bundle eines Konfigurationspakets hilft dem technischen Supportteam von Citrix, Probleme mit Konfigurationspaketen anzuzeigen, zu analysieren und zu beheben. Führen Sie die folgenden Schritte aus, um das Support-Bundle herunterzuladen:

1. Gehen Sie zu **Anwendungen > Konfiguration > Konfigurationspakete**.
2. Wählen Sie das Konfigurationspaket aus, für das Sie das Support-Bundle herunterladen möchten.
3. Klicken Sie unter **Aktion auswählen** auf **Support-Bundle**.

   Sie können das Bundle im Zip- oder TGZ-Dateiformat komprimieren.
4. Optional können Sie die Passphrase zum Verschlüsseln der Bundle-Datei angeben.
5. Klicken Sie auf **Herunterladen**.

Support-Bundle(/en-us/netscaler-console-service/media/support-bundle-configpack.png)

Ein Tag für das StyleBook erstellen

Sie können jedem StyleBook in NetScaler Console Tags hinzufügen. Tags sind Schlüssel-Wert-Paare, mit denen Sie StyleBooks nach verschiedenen Kriterien gruppieren können. Sie können diese Tags beim Suchen oder Filtern von StyleBooks in NetScaler Console verwenden.

So fügen Sie dem StyleBook einen Tag hinzu:

1. Navigieren Sie zu **Applications > Configuration > StyleBooks**.
2. Wählen Sie **Tags** für das StyleBook aus, dem Sie Tags hinzufügen möchten.

   Sie können Tags zu allen Arten von StyleBooks hinzufügen.
3. Geben Sie die erforderlichen Informationen für **Key** und **Value** an, die Ihnen beim Filtern des StyleBooks helfen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zum Beispiel: Key=team und Value=bizdata

Um weitere Tags hinzuzufügen, klicken Sie auf **+**.

4. Klicken Sie auf **Create**.

Um StyleBooks mithilfe von Tags zu filtern, klicken Sie in der Suchleiste auf **Tags** und wählen Sie einen Schlüssel und einen Wert aus der Liste aus. Die StyleBooks, die dem angegebenen Tag entsprechen, werden angezeigt.

Das Folgende ist eine Beispielsuche für StyleBooks, die einen Tag haben, bei dem `key=team` und `value=bizdata`:

Sie können die StyleBook-Tags mit dem zugehörigen Konfigurationspaket verknüpfen. So können Sie die Konfigurationspakete mithilfe der StyleBook-Tags selbst durchsuchen.

Wenn Sie ein Konfigurationspaket erstellen, verwenden Sie eine der folgenden Optionen im Abschnitt **Tag-Zuordnung**:

- **Alle vorhandenen und zukünftigen StyleBook-Tags der Konfiguration zuordnen** – Diese Option ordnet alle StyleBook-Tags einem Konfigurationspaket zu. Sie stellt auch sicher, dass neue Tags zugeordnet werden, die Sie möglicherweise zukünftig zu den StyleBooks hinzufügen.
- **Tags auswählen** – Diese Option zeigt die Tags des ausgewählten StyleBooks an. Sie können die erforderlichen StyleBook-Tags auswählen und einem Konfigurationspaket zuordnen.

Ein StyleBook klonen

Als Administratoren können Sie ein Duplikat eines StyleBooks zusammen mit seinen abhängigen StyleBooks erstellen. Sie können dieses Bundle dann zur Anpassung verwenden, z. B. zum Aktualisieren der Abschnitte `parameters` und `components`.

So klonen Sie ein StyleBook:

1. Navigieren Sie zu **Applications > Configuration > StyleBooks**.
2. Wählen Sie **Klonen** für das Standard- oder benutzerdefinierte StyleBook, das Sie duplizieren möchten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Geben Sie auf der Seite **StyleBook klonen** einen Namespace und eine Version für das StyleBook und die abhängigen StyleBooks ein. Sie können auch die vorgeschlagenen Namespaces und Versionen auswählen.

   HINWEIS:

   Das geklonte StyleBook und seine abhängigen StyleBooks müssen unterschiedliche Namespaces und Versionen haben, um sie von den vorhandenen StyleBooks zu unterscheiden. Sie können keine reservierten NetScaler Console-Namespaces für die geklonten StyleBooks verwenden.

4. Klicken Sie auf **Klonen**. Das geklonte StyleBook-Paket wird in NetScaler Console importiert und erscheint auf der Seite **StyleBooks**.

StyleBooks aus einem externen Repository importieren und synchronisieren

Stellen Sie sich ein Szenario vor, in dem Sie CI/CD-Prozesse für Ihre Entwicklung verwenden. Oder ein Szenario, in dem Sie den gesamten Anwendungsquellcode und die Bereitstellungsartefakte in GitHub/GitLab verwalten.

Im GitHub/GitLab-Repository pflegen Sie möglicherweise mehrere StyleBooks für die Bereitstellung der NetScaler-Konfigurationen und die Verwaltung dieser StyleBooks. Sie müssen diese StyleBooks in die NetScaler Console hochladen. Mit dieser Funktion können Sie Ihre in GitHub/GitLab vorhandenen StyleBooks direkt in die NetScaler Console importieren. Sie müssen sie nicht manuell von GitHub/GitLab kopieren und dann in die NetScaler Console hochladen. Oder die Dateien in NetScaler Console und GitHub/GitLab manuell synchronisieren. Außerdem können Sie Konfigurationspakete von GitHub/GitLab importieren und synchronisieren.

Um StyleBooks und Konfigurationspakete zu importieren, definieren Sie ein Repository in der NetScaler Console, das ein GitHub/GitLab-Repository darstellt. Geben Sie die GitHub/GitLab-Repository-URL sowie Ihren Benutzernamen und das in GitHub/GitLab erstellte API- oder Personal Access (PA)-Token an. Das bedeutet, dass nur autorisierte Benutzer mit einem gültigen Konto in GitHub/GitLab StyleBooks importieren und synchronisieren können.

Sie können die folgenden Repository-Typen importieren und synchronisieren:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Öffentlich zugängliche Repositorys** – Die Repositorys, die öffentlich zugänglich sind und über das Internet erreicht werden können.
- **On-Premise- oder private GitLab/GitHub-Repositorys** – Die Repositorys, die privat gehostet werden und typischerweise nur innerhalb des Intranets eines Unternehmens zugänglich sind. Für diese Repositorys müssen Sie während des Registrierungsprozesses einen NetScaler-Agenten auswählen. Der NetScaler-Agent fungiert als Proxy für den Zugriff auf die Repositorys innerhalb des Intranets des Unternehmens.

Nachdem Sie das Repository erstellt haben, können Sie Ihr GitHub/GitLab-Repository mit der NetScaler Console synchronisieren. Die NetScaler Console stellt eine Verbindung zu GitHub/GitLab her und importiert StyleBooks und Konfigurationspakete, die in diesem Repository gefunden werden. Die NetScaler Console validiert dann die StyleBooks und fügt sie der Liste der StyleBooks in der NetScaler Console hinzu. StyleBooks werden der NetScaler Console nicht hinzugefügt, wenn sie die Validierung nicht bestehen. Sie können die Fehler in Ihren StyleBooks identifizieren und korrigieren. Committen Sie dann die aktualisierten Versionen in Ihr GitHub/GitLab-Repository. Später können Sie versuchen, sie erneut in die NetScaler Console zu importieren oder zu synchronisieren.

Wenn Sie beim Erstellen eines Repositorys den folgenden Fehler erhalten, bedeutet dies, dass die NetScaler Console das SSL-Zertifikat für das Repository aufgrund eines fehlenden oder nicht erkannten Zertifizierungsstellen-Zertifikats (CA-Zertifikat) nicht überprüfen kann:

```
certificate verify failed: unable to get local issuer certificate
```

Um dieses Problem zu beheben, können Sie das erforderliche CA-Zertifikat manuell zum NetScaler Console-Agenten hinzufügen, der für den Zugriff auf das Repository verwendet wird. Das Hinzufügen des erforderlichen CA-Zertifikats stellt sicher, dass sichere Verbindungen zum externen Repository ordnungsgemäß validiert werden.

Melden Sie sich beim NetScaler Console-Agenten an, der für den Zugriff auf das Repository verwendet wird, und fügen Sie Ihr CA-Zertifikat zum vertrauenswürdigen Zertifikatsbündel `/var/mps/ca_certs/cacert.pem` hinzu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG

- StyleBook-Dateien können von jedem Branch eines GitHub/GitLab-Repositorys importiert und synchronisiert werden.
- Sie können auch StyleBooks importieren und synchronisieren, die abhängige StyleBooks enthalten. Diese abhängigen StyleBooks können sich im GitHub/GitLab-Repository befinden oder bereits in der NetScaler Console vorhanden sein.
- Die Synchronisierung von StyleBooks aus einem GitHub-/GitLab-Repository muss manuell über die NetScaler Console GUI oder API initiiert werden. Das heißt, das Importieren und Synchronisieren von StyleBooks erfolgt derzeit nicht automatisch basierend auf Ihrer GitHub-/GitLab-Commit-Aktivität.
- Die Konfigurationspaketdatei, die Sie importieren möchten, muss im JSON-Format vorliegen. Außerdem müssen die Inhalte der Konfigurationsdatei dem exportierten Konfigurationsformat entsprechen. In Ihrem GitHub-/GitLab-Repository müssen sich die mit dem Konfigurationspaket verbundenen Dateien im Ordner `configpacks` befinden.

Sie können StyleBook-Dateien aus jedem Ordner im GitHub-/GitLab-Repository in NetScaler Console importieren. Um Konfigurationspakete zu importieren, gehen Sie wie folgt vor:

1. Erstellen Sie einen Ordner mit dem Namen `configpacks` im Stammverzeichnis. Stellen Sie sicher, dass sich alle mit Konfigurationen verbundenen Dateien in diesem Ordner befinden.
2. Erstellen Sie im Ordner `configpacks` eine JSON-Datei, die die Nutzlast für das Konfigurationspaket enthält. Diese Nutzlast wird zur Synchronisierung von Konfigurationspaketen verwendet. Das Folgende ist eine Beispielnutzlast:

```
{

    "config_key": "unique-key-for-configpack",



    "parameters": {

        "param-name1": "param-value1",

        "param-name": "param-value2",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "param-namen": "param-valuen"
    },
    "stylebook": {
        "namespace": "some namespace",
        "name": "somename",
        "version": "spme-version"
    }
}
```

- `config_key` – Eine eindeutige ID oder ein Name zur Identifizierung eines Konfigurationspakets in NetScaler Console. Wenn Sie config_key nicht angeben, generiert NetScaler Console die ID automatisch beim Erstellen des Konfigurationspakets.

  Wenn die angegebene ID in der NetScaler Console GUI gefunden wird, aktualisiert die Synchronisierungsaktion das Konfigurationspaket in der NetScaler Console GUI. Andernfalls wird ein Konfigurationspaket mit der angegebenen ID erstellt.
- `parameters` – Es enthält alle notwendigen Parameter zum Erstellen oder Aktualisieren des Konfigurationspakets.
- `stylebook` – Dies ist eine obligatorische Eigenschaft in einer JSON-Datei. Sie enthält einen Namespace, eine Version und den StyleBook-Namen, mit dem Sie das Konfigurationspaket verknüpfen möchten.

3. Bewahren Sie im Ordner `configpacks` alle Dateien auf, die mit dem Konfigurationspaket verbunden sind, wie z. B. Zertifikate, Signaturdateien und XML-Dateien.

Repository hinzufügen

1. Gehen Sie in NetScaler Console zu **Applications > Configuration > Repositories**. Klicken Sie auf **Add**.
2. Geben Sie im Fenster **Add Repository** die folgenden Parameter ein:

   - **Name** – Geben Sie den Namen des Repositorys ein. Dieser Name kann derselbe sein wie der Repository-Name in GitHub/GitLab oder ein anderer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Repository URL** – Geben Sie die GitHub-/GitLab-Repository-URL ein.

  Sie können eine GitHub/GitLab Enterprise-URL angeben. Dies hilft Ihnen, StyleBooks und Konfigurationspakete von GitHub/GitLab Enterprise-Konten zu importieren oder zu synchronisieren.
- **Ist es eine private URL?** – Wenn das Repository ein lokales oder privates GitLab/GitHub-Repository ist, aktivieren Sie dieses Kontrollkästchen und wählen Sie dann einen **Agenten** aus.
- **Benutzername** – Geben Sie den Benutzernamen ein, den Sie für den Zugriff auf das GitHub/GitLab-Konto oder das Enterprise-Konto verwenden.
- **API/PA-Token** – Dieses Token wird für den Zugriff auf Ihr GitHub/GitLab-Repository verwendet. Informationen zum Erstellen von API/PA-Tokens für Ihr GitHub/GitLab-Repository finden Sie in der GitHub/GitLab-Dokumentation unter Erstellen persönlicher Zugriffstoken.

3. Klicken Sie auf **Erstellen**.

   Das Repository wird in NetScaler Console erstellt.

Repository-Optionen

Im Folgenden sind die zusätzlichen Optionen für Ihre Repositorys aufgeführt:

- **Bearbeiten** – Sie können die Repository-URL, den Benutzernamen und das API-Token bearbeiten.
- **Löschen** – Sie können das Repository zusammen mit allen in NetScaler Console vorhandenen StyleBooks löschen, die zuvor aus diesem GitHub/GitLab-Repository importiert wurden.

  HINWEIS

  Sie können ein Repository nicht aus NetScaler Console löschen, wenn es StyleBooks enthält, denen Konfigurationspakete zugeordnet sind. Löschen Sie zuerst alle Konfigurationspakete dieser StyleBooks. Sie können das Repository später aus NetScaler Console entfernen, um die StyleBooks aus diesem Repository zu bereinigen.
- **Zurücksetzen** – Sie können alle in NetScaler Console synchronisierten StyleBooks aus diesem Repository entfernen, ohne den Repository-Eintrag tatsächlich zu löschen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Dateien auflisten** – Sie können eine Liste aller in NetScaler Console vorhandenen StyleBooks sehen, die aus dem GitHub/GitLab-Repository stammen.

Schritte zum Importieren von StyleBooks und Konfigurationspaketen aus GitHub/GitLab

Nachdem Sie die Voraussetzungen erfüllt haben, führen Sie die folgenden Schritte aus, um StyleBooks und Konfigurationspakete aus einem GitHub/GitLab-Repository zu importieren:

1. Optional, ein Repository hinzufügen, falls Sie noch keines hinzugefügt haben.
2. Wählen Sie das Repository auf der Seite **Repositories** aus.
3. Klicken Sie auf **Synchronisieren**.

Standard-StyleBooks verwenden

Ein Satz von Standard-StyleBooks wird zusammen mit NetScaler Console bereitgestellt. Wenn Sie ein Standard-StyleBook verwenden, müssen Sie Werte für die Parameter im StyleBook angeben und die IP-Adressen der NetScaler-Instanzen auswählen, auf denen Sie die Konfiguration ausführen möchten. Nachdem Sie die Konfiguration übermittelt haben, validiert NetScaler Console die von Ihnen angegebenen Parameterwerte, erstellt ein Diagramm der Konfiguration, stellt eine Verbindung zu den NetScaler-Instanzen her und führt die Konfiguration auf den Instanzen aus.

NetScaler-Funktionen

Diese Tabelle listet die StyleBooks auf, die Ihnen helfen, virtuelle Server für Lastenausgleich, Inhaltswechsel und GSLB zu konfigurieren:

STYLEBOOK-NAME	BESCHREIBUNG	VERSIONEN
`lb`	Konfigurieren Sie einen einfachen virtuellen Lastenausgleichsserver. Siehe Lastenausgleich.	1.1, 2.0
`lb-mon`	Konfigurieren Sie einen virtuellen Lastenausgleichsserver mit Monitoren. Siehe Monitore in einer Lastenausgleichseinrichtung konfigurieren.	1.0, 2.0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STYLEBOOK-NAME	BESCHREIBUNG	VERSIONEN
`cs-lb-mon`	Konfigurieren Sie einen virtuellen Content-Switching-Server mit Monitoren. Weitere Informationen finden Sie unter Content Switching.	1.0, 1.1
`lb-mon-full`	Konfigurieren Sie einen Lastausgleichs-Virtual-Server mit Monitoren auf Ihren NetScaler-Instanzen. Konfigurieren Sie außerdem die NetScaler-Funktionen wie Rewrite, Responder, Compression und SSL-Chiffren.	1.0
`cs-lb-mon-full`	Konfigurieren Sie einen Content-Switching-Virtual-Server mit Monitoren auf Ihren NetScaler-Instanzen. Konfigurieren Sie außerdem die NetScaler-Funktionen wie Rewrite, Responder und Compression.	1.0
`gslb`	Konfigurieren Sie eine oder mehrere NetScaler-Instanzen verschiedener Sites im GSLB-Setup. Bevor Sie beginnen, konfigurieren Sie die SNIP-IP-Adresse auf den NetScaler-Instanzen. Dieses StyleBook verwendet die SNIP-IP-Adresse als Site-IP-Adresse.	1.0
`multicloud-glb`	Konfigurieren Sie GLB für NetScaler-Instanzen. Diese Instanzen werden als GLB-Knoten in öffentlichen Clouds und lokalen Rechenzentren	1.1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STYLEBOOK-NAME	BESCHREIBUNG	VERSIONEN
	bereitgestellt. Sie können dieses StyleBook verwenden, um GLB-Knoten in einer hierarchischen Bereitstellung zu konfigurieren.	

Funktionen der Web Application Firewall

Diese Tabelle listet die Standard-StyleBooks für Web Application Firewall (WAF)-Funktionen auf:

STYLEBOOK-NAME	BESCHREIBUNG	VERSIONEN
`waf-basic`	Konfigurieren Sie eine einfache Webanwendung mit Anwendungs-Firewall-Richtlinien.	1.2
`waf-adv`	Konfigurieren Sie eine erweiterte Webanwendung mit Anwendungs-Firewall-Richtlinien.	1.2
`waf-default-130` und `waf-default-131`	Konfigurieren Sie WAF- und IP-Reputation-Richtlinien für Ihre NetScaler-Instanzen.	1.2
`lb-appfw`	Stellen Sie eine Lastenausgleichskonfiguration zusammen mit der Anwendungs-Firewall- und IP-Reputationsrichtlinie auf NetScaler-Instanzen bereit.	1.0
`appfw-import-object`	Erstellen oder laden Sie ein Anwendung-Firewall-Objekt hoch.	1.1
`appfw-general-settings`	Konfigurieren Sie globale Einstellungen für Ihre Anwendungs-Firewall. Diese Einstellungen gelten für alle	1.0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STYLEBOOK-NAME	BESCHREIBUNG	VERSIONEN
	Anwendungen innerhalb der NetScaler-Instanz.	
`apic-http-lb`	Erstellen Sie eine HTTP-Lastenausgleichsanwendung über Cisco APIC.	1.0
`api-waf-profile`	Erstellen Sie ein WAF-Profil in NetScaler Console. Mit diesem Profil können Sie WAF-Richtlinien für eine API-Ressource konfigurieren.	1.0

Funktionen der Anwendungssicherheit

Diese Tabelle listet die Standard-StyleBooks für Anwendungssicherheitsfunktionen auf:

STYLEBOOK-NAME	BESCHREIBUNG	VERSIONEN
`api-proxy`	Erstellen Sie einen API-Proxy in Ihrer NetScaler-Instanz. Sie können mehrere Proxys mit demselben Richtlinientyp erstellen.	1.1
`appsec-for-gateway`	Bevor Sie beginnen, erstellen Sie eine benutzerdefinierte Bot-Signatur. Konfigurieren Sie eine Authentifizierungsrichtlinie mit WAF und Bot, um Ihre Gateway-Anmeldeseite zu schützen. Binden Sie diese Authentifizierungsrichtlinie an Ihren virtuellen Authentifizierungsserver.	1.0
`appsec-for-gateway-with-insights`	Bevor Sie beginnen, erstellen Sie eine benutzerdefinierte Bot-Signatur. Konfigurieren Sie eine	1.0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STYLEBOOK-NAME	BESCHREIBUNG	VERSIONEN
	Authentifizierungsrichtlinie mit WAF und Bot, um Ihre Gateway-Anmeldeseite mit Sicherheitserkenntnissen zu schützen. Binden Sie diese Authentifizierungsrichtlinie an Ihren virtuellen Authentifizierungsserver.	
`appvserver-contentrule-networkfunction-bind`	Wenden Sie Ihre eigene `contentRule` Konfiguration auf den Anwendungsverkehr von Ihrer NetScaler-Instanz an.	1.0
`appsec-owasptop10-protection`	Erstellen Sie eine Schutzkonfiguration mithilfe von WAF- und Bot-Richtlinien. Dieses StyleBook ordnet die NetScaler-Konfigurationen den Top-10-OWASP-Schwachstellen zu.	1.0

Bot-Verwaltungsfunktionen

Diese Tabelle listet die Standard-StyleBooks für Bot-Verwaltungsfunktionen auf:

STYLEBOOK-NAME	BESCHREIBUNG	VERSIONEN
`api-bot-profile`	Erstellen Sie ein Bot-Profil in NetScaler Console. Mit diesem Profil können Sie Bot-Richtlinien für eine API-Ressource konfigurieren.	1.0
`bot-signature`	Erstellen Sie eine Bot-Signatur für Ihre NetScaler-Instanzen.	1.2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STYLEBOOK-NAME	BESCHREIBUNG	VERSIONEN
`bot-management`	Definieren Sie eine Webanwendungskonfiguration mit Bot-Richtlinien.	1.2
`bot-general-settings`	Konfigurieren Sie globale Einstellungen für Bot-Management-Prüfungen auf Ihren NetScaler-Instanzen. Weitere Informationen finden Sie unter Bot-Management.	1.2

NetScaler-Netzwerkkonfigurationen

Diese Tabelle listet die Standard-StyleBooks für NetScaler-Netzwerkkonfigurationen auf:

STYLEBOOK-NAME	BESCHREIBUNG	VERSIONEN
`adc_globalparam_configuration`	Legen Sie globale Parameter für Ihre NetScaler-Instanzen fest.	1.0
`snmp_configuration`	Stellen Sie SNMP-Konfigurationen auf einer NetScaler-Instanz bereit. Eine SNMP-Anwendung (Simple Network Management Protocol) hilft Ihnen, NetScaler-Ereignisse in NetScaler Console zu protokollieren. Weitere Informationen finden Sie unter SNMP-Konfiguration.	1.0
`adv_network_configuration`	Stellen Sie erweiterte Netzwerkkonfigurationen wie VXLAN, Cluster und mehr bereit. Weitere Informationen finden Sie unter Netzwerk.	1.0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STYLEBOOK-NAME	BESCHREIBUNG	VERSIONEN
`storefront`	Konfigurieren Sie Ihre NetScaler-Instanzen für Citrix StoreFront.	1.0
`ntp_configuration`	Konfigurieren Sie Network Time Protocol (NTP)-Ressourcen in Ihren NetScaler-Instanzen.	1.0
`network_param_configuration`	Konfigurieren Sie Netzwerkparameter wie AppAlg, ARP, Inbound NAT usw.	1.0
`network_configuration`	Stellen Sie grundlegende Netzwerkkomponenten bereit. Weitere Informationen finden Sie unter Netzwerk.	1.0
`cs-netfunc`	Konfigurieren Sie die erweiterten Netzwerkfunktionen eines virtuellen Content-Switching-Servers für Ihre NetScaler-Instanzen.	1.0

Was kommt als Nächstes?

Um ein Konfigurationspaket aus Standard-StyleBooks zu erstellen, führen Sie die Schritte unter Konfigurationspaket erstellen aus.

StyleBook für Web Application Firewall

NetScaler Web App Firewall ist eine Web Application Firewall (WAF), die Webanwendungen und Websites vor bekannten und unbekannten Angriffen schützt, einschließlich aller Anwendungs-Layer- und Zero-Day-Bedrohungen.

NetScaler Console bietet jetzt ein Standard-StyleBook, mit dem Sie bequemer eine Application Firewall-Konfiguration auf NetScaler-Instanzen erstellen können.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bereitstellen von Application Firewall-Konfigurationen

Die folgende Aufgabe unterstützt Sie bei der Bereitstellung einer Lastausgleichskonfiguration zusammen mit der Application Firewall und der IP-Reputationsrichtlinie auf NetScaler-Instanzen in Ihrem Unternehmensnetzwerk.

So erstellen Sie eine LB-Konfiguration mit Application Firewall-Einstellungen:

1. Navigieren Sie in NetScaler Console zu **Applications** > **Configurations** > **StyleBooks**. Die Seite StyleBooks zeigt alle StyleBooks an, die Ihnen in NetScaler Console zur Verfügung stehen. Scrollen Sie nach unten und suchen Sie das HTTP/SSL Load Balancing StyleBook mit Application Firewall-Richtlinie und IP-Reputationsrichtlinie. Sie können auch nach dem StyleBook suchen, indem Sie den Namen als `lb-appfw` eingeben. Klicken Sie auf **Create Configuration**.

   Das StyleBook wird als Benutzeroberfläche geöffnet, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
2. Geben Sie Werte für die folgenden Parameter ein:

   - **Load Balanced Application Name**. Name der Lastausgleichskonfiguration mit Application Firewall, die in Ihrem Netzwerk bereitgestellt werden soll.
   - **Load balanced App Virtual IP address**. Virtuelle IP-Adresse, unter der die NetScaler-Instanz Clientanfragen empfängt.
   - **Load Balanced App Virtual Port**. Der TCP-Port, der von den Benutzern für den Zugriff auf die Lastausgleichsanwendung verwendet werden soll.
   - **Load Balanced App Protocol**. Wählen Sie das Frontend-Protokoll aus der Liste aus.
   - **Application Server Protocol**. Wählen Sie das Protokoll des Anwendungsservers aus.

   ☐
3. Optional können Sie die **Erweiterten Load Balancer-Einstellungen** aktivieren und konfigurieren.

   ☐
4. Optional können Sie auch einen Authentifizierungsserver für die Authentifizierung des Datenverkehrs für den virtuellen Lastausgleichsserver einrichten.

   ☐
5. Klicken Sie im Abschnitt „Server-IPs und Ports“ auf „+“, um Anwendungsserver und die Ports zu erstellen, über die auf sie zugegriffen werden kann.

   ☐

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Sie können auch FQDN-Namen für Anwendungsserver erstellen.

7. Sie können auch die Details des SSL-Zertifikats angeben.

8. Sie können auch Monitore in der Ziel-NetScaler-Instanz erstellen.

9. Um eine Anwendungs-Firewall auf dem virtuellen Server zu konfigurieren, aktivieren Sie die WAF-Einstellungen.

   Stellen Sie sicher, dass die Richtlinienregel der Anwendungs-Firewall „true“ ist, wenn Sie die Anwendungs-Firewall-Einstellungen auf den gesamten Datenverkehr dieser VIP anwenden möchten. Andernfalls geben Sie die NetScaler-Richtlinienregel an, um eine Untergruppe von Anforderungen auszuwählen, auf die die Anwendungs-Firewall-Einstellungen angewendet werden sollen. Wählen Sie anschließend den anzuwendenden Profiltyp aus – HTML oder XML.

10. Optional können Sie detaillierte Anwendungssicherheits-Profil-Einstellungen konfigurieren, indem Sie das Kontrollkästchen „Anwendungssicherheits-Profileinstellungen“ aktivieren.
11. Optional, wenn Sie Anwendungssicherheits-Signaturen konfigurieren möchten, geben Sie den Namen des Signaturobjekts ein, das auf der NetScaler-Instanz erstellt wurde, auf der der virtuelle Server bereitgestellt werden soll.

    HINWEIS

    Sie können mit diesem StyleBook kein Signaturobjekt erstellen.

12. Als Nächstes können Sie auch andere Anwendungssicherheits-Profileinstellungen konfigurieren, wie z. B. StartURL-Einstellungen, DenyURL-Einstellungen und andere.

    Weitere Informationen zur Anwendungssicherheit und den Konfigurationseinstellungen finden Sie unter Anwendungssicherheit.

13. Wählen Sie im Abschnitt **Zielinstanzen** die NetScaler-Instanz aus, auf der der Lastausgleichs-Virtual-Server mit der Anwendungssicherheit bereitgestellt werden soll.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich entdeckte NetScaler-Instanzen in NetScaler Console zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

14. Sie können auch die **IP-Reputationsprüfung** aktivieren, um die IP-Adresse zu identifizieren, die unerwünschte Anfragen sendet. Sie können die IP-Reputationsliste verwenden, um Anfragen, die von einer IP mit schlechter Reputation kommen, präventiv abzulehnen.
15. Klicken Sie auf **Erstellen**, um die Konfiguration auf den ausgewählten NetScaler-Instanzen zu erstellen.

TIPP

Wir empfehlen Ihnen, **Testlauf** auszuwählen, um die Konfigurationsobjekte zu überprüfen, die auf der Zielinstanz erstellt werden müssen, bevor Sie die eigentliche Konfiguration auf der Instanz ausführen.

Wenn die Konfiguration erfolgreich erstellt wurde, erstellt das StyleBook den erforderlichen Lastausgleichs-Virtual-Server, Anwendungsserver, Dienste, Dienstgruppen, Anwendungssicherheits-Labels, Anwendungssicherheits-Richtlinien und bindet diese an den Lastausgleichs-Virtual-Server.

Die folgende Abbildung zeigt die auf jedem Server erstellten Objekte:

16. Um das auf NetScaler Console erstellte ConfigPack anzuzeigen, navigieren Sie zu **Applications** > **Configurations**.

StyleBook für SNMP-Konfiguration

Eine Anwendung für das Simple Network Management Protocol (SNMP) hilft Ihnen, NetScaler-Ereignisse in der NetScaler Console zu protokollieren. Diese Anwendung wird auf der NetScaler Console ausgeführt und fragt den SNMP-Agenten auf einer NetScaler-Instanz ab. Der Agent durchsucht die Management Information Base (MIB) nach Daten, die von der Netzwerkverwaltungsanwendung angefordert wurden, und sendet die Daten an die Anwendung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn eine Konfigurationsänderung auf einer Instanz auftritt, wird eine SNMP-Trap generiert. Die Traps werden dann an ein Remote-Gerät gesendet, das als Trap-Zielserver oder SNMP-Trap-Ziel bezeichnet wird. NetScaler Console ist als Trap-Ziel konfiguriert. Sie können den SNMP-Agenten von einem Remote-Gerät, das als SNMP-Manager bezeichnet wird, nach systemspezifischen Informationen abfragen. Der Agent durchsucht dann die Management Information Base (MIB) nach den angeforderten Daten und sendet die Daten an den SNMP-Manager.

Führen Sie die folgenden Schritte aus, um SNMP-Konfigurationen auf einer NetScaler-Instanz mithilfe von StyleBook bereitzustellen:

1. Gehen Sie in der NetScaler Console zu **Applications > Configuration > StyleBooks**. Suchen Sie das StyleBook, indem Sie den Namen als `snmp_configuration` eingeben. Klicken Sie auf **Konfiguration erstellen**.

   Das StyleBook wird als Benutzeroberflächenseite geöffnet, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
2. Geben Sie die folgenden Parameter an:

   - **SNMP-MIB-Konfiguration** – Geben Sie die folgenden Instanzinformationen an:
     - **Administrator-Kontakt**: Die E-Mail-Adresse eines Administrators.
     - **NetScaler-Name**: Name einer NetScaler-Instanz.
     - **NetScaler-Standort**: Der physische Standort einer Instanz.
     - **Benutzerdefinierte Identifikationsnummer**: Benutzerdefinierte Identifikationsnummer für den NetScaler. Diese Nummer hilft, eine Instanz zu identifizieren.
     - **Ownernode**: Die Clusterknoten-ID, auf der Sie diese MIB festlegen. Dieses Feld ist obligatorisch, um SNMP-MIB auf CLIP festzulegen.

   - **SNMP-Community-Konfiguration** – Eine SNMP-Community-Konfiguration authentifiziert SNMP-Abfragen von SNMP-Managern. Sie können diese Zeichenfolge mit beliebigen SNMP-Abfragetypen wie GET, GET NEXT, ALL, GET BULK verknüpfen.

   - **SNMP-Engine-ID-Konfiguration** – Die SNMPv3-Engine verfügt über eine eindeutige Identifikation (ID). Diese ID wird in der Kommunikation zwischen SNMPv3-Benutzer und SNMPv3-Engine verwendet. Diese ID ist ein hexadezimaler Wert von mindestens 10 Zeichen. Geben Sie in dieser Konfiguration die `Ownernode` an, die Sie bei der MIB-Konfiguration erwähnen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Konfiguration der SNMP-Optionen** – Sie können SNMP-Optionen für einen SNMP-Manager aktivieren oder deaktivieren.
  - **SNMP-Set-Anfragen**: Aktivieren Sie diese Option, die es SNMP-Managern ermöglicht, Werte in MIB-Objekte zu schreiben.
  - **SNMP-Trap-Protokollierung**: Diese Option protokolliert SNMP-Trap-Ereignisse.
  - **SNMP-Trap-Protokollierungsstufe**: Diese Option sendet eine Überwachungsprotokollstufe von SNMP-Trap-Protokollen.
  - **Partitionsnamen senden**: Diese Option sendet den Partitionsnamen.

- **SNMP-Manager-Konfiguration** – Ein SNMP-Manager zum Abfragen einer NetScaler-Instanz. Der Manager ist kompatibel mit SNMP V1, V2 und V3. Wenn Sie einen oder mehrere SNMP-Manager angeben, akzeptiert die Instanz keine SNMP-Abfragen von anderen Hosts als den angegebenen SNMP-Managern.
  - **IP-Adresse**: Eine IP-Adresse des SNMP-Managers.
  - **Netzmaske**: Subnetzmaske, die einer IPv4-Netzwerkadresse zugeordnet ist.
  - **Wiederholung der Domänenauflösung**: Wenn die letzte DNS-Abfrage den Hostnamen des SNMP-Managers nicht auflösen kann, wartet die NetScaler-Instanz das angegebene Intervall ab, bevor sie eine weitere DNS-Abfrage sendet.

- **SNMP-Alarmkonfiguration** – Fügen Sie SNMP-Alarme hinzu, um unternehmensspezifische Trap-Nachrichten zu generieren. Eine NetScaler-Instanz sendet die Trap-Nachrichten nur an Trap-Listener vom Typ (Klasse) SPECIFIC. Die SNMP-Alarme sind entweder ereignisbasiert oder schwellenwertbasiert.
  - **Trap-Name**: Name des SNMP-Alarms.
  - **Status**: Eine NetScaler-Instanz generiert Trap-Nachrichten nur für SNMP-Alarme, die aktiviert sind.
  - **Protokollierung**: Wenn Sie die Protokollierung aktivieren, protokolliert die NetScaler-Instanz jede Trap-Nachricht, die für diesen Alarm generiert wird.
  - **Oberer Schwellenwert**: Dieser Wert ist die maximale Grenze eines Attributs, das mit diesem Alarm verknüpft ist. Wenn das Attribut diesen Wert erreicht oder überschreitet, generiert eine NetScaler-Instanz eine SNMP-Trap-Nachricht.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Normaler Schwellenwert**: Dieser Wert ist die minimale Grenze eines Attributs, das mit diesem Alarm verknüpft ist. Wenn das Attribut diesen Wert erreicht oder unterschreitet, generiert eine NetScaler-Instanz eine SNMP-Trap-Nachricht.
- **Zeit (Sek.)**: Ein Intervall, in dem die NetScaler-Instanz SNMP-Trap-Nachrichten generiert, wenn die angegebenen Bedingungen erfüllt sind.
- **Schweregrad**: Der Schweregrad für die von diesem Alarm generierten Trap-Nachrichten. Dieses Feld ist hilfreich, wenn Sie möchten, dass eine Instanz Trap-Nachrichten basierend auf dem Schweregrad sendet.

- **SNMP-Trap-Konfiguration** – Diese Konfiguration fügt SNMP-Trap-Listener hinzu. Eine NetScaler-Instanz generiert Trap-Nachrichten, um anormale Bedingungen zu melden. Die Trap-Nachrichten werden an einen Trap-Listener gesendet, um Administratoren bei der Überwachung der Instanz und der schnellen Reaktion auf Probleme zu unterstützen.
  - **Trap-Klasse**: Typ der Trap-Nachrichten, die eine Instanz an einen Trap-Listener sendet.
  - **Trap-Ziel**: Die IPv4- oder IPv6-Adresse des Trap-Listeners. Eine Instanz sendet SNMP-Trap-Nachrichten an diese IP-Adresse.
  - **Version**: Eine SNMP-Version. Diese Version muss mit der Version auf dem Trap-Listener übereinstimmen. Andernfalls verwirft der Listener die Trap-Nachrichten.
  - **UDP-Zielport**: UDP-Port, an dem der Trap-Listener Trap-Nachrichten empfängt. Dieser Wert muss mit dem Wert auf dem Trap-Listener übereinstimmen. Andernfalls verwirft der Listener die Trap-Nachrichten.
  - **Community-Name**: Eine Zeichenfolge wird mit den Trap-Nachrichten gesendet. Der Trap-Listener verwendet diese Zeichenfolge zur Authentifizierung.
  - **Quell-IP**: Quell-IP-Adresse. Die IPv4- oder IPv6-Adresse einer NetScaler-Instanz.
  - **Schweregrad**: Der Schweregrad für die Trap-Nachrichten. Eine NetScaler-Instanz sendet die Trap-Nachrichten für die angegebenen und höheren Schweregrade.
  - **Traffic-Domäne**: Ein ganzzahliger Wert, der die Traffic-Domäne eindeutig identifiziert.
  - **Alle Partitionen**: Wenn diese Option aktiviert ist, sendet eine Instanz die Trap-Nachrichten aller Partitionen an die Ziel-IP-Adresse.

- **SNMP-Ansichtskonfiguration** – SNMP-Ansichten werden verwendet, um die Zugriffssteuerung für einen SNMPv3-Benutzer zu implementieren. Die SNMP-Ansichten beschränken den Benutzerzugriff auf bestimmte Teile der MIB.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Ansichtsname**: Ein Name für die SNMPv3-Ansicht.

  Eine Instanz kann mehrere SNMPv3-Ansichten mit demselben Namen haben, die sich durch die Einstellungen der Unterbaumparameter unterscheiden. Sie können maximal 1000 SNMPv3-Ansichten hinzufügen.
- **Unterbaum**: Ein bestimmter Zweig (Unterbaum) des MIB-Baums, den Sie dieser SNMPv3-Ansicht zuordnen möchten. Sie müssen den Unterbaum als SNMP-OID angeben.
- **Typ**: Dieses Feld ermöglicht es Ihnen, Unterbäume in eine Ansicht einzuschließen oder auszuschließen.

- **SNMP-Gruppenkonfiguration** – Die SNMPv3-Benutzergruppen auf einer Instanz. Diese Gruppen sind logische Aggregationen von SNMPv3-Benutzern. SNMPv3-Gruppen werden verwendet, um die Zugriffssteuerung zu implementieren und die Sicherheitsstufen für die Benutzer zu definieren. Sie können maximal 1000 SNMPv3-Gruppen zu einer NetScaler-Instanz hinzufügen.

- **SNMP-Benutzerkonfiguration** – Fügen Sie SNMPv3-Benutzer hinzu, die SNMP-Abfragen an eine NetScaler-Instanz senden können. Sie können maximal 1000 SNMPv3-Benutzer hinzufügen.

  - **Name**: Name des SNMPv3-Benutzers.
  - **Gruppe**: Name der konfigurierten SNMPv3-Gruppe, die Sie mit dem SNMPv3-Benutzer verbinden möchten. Die Zugriffsrechte (gebundene SNMPv3-Ansichten) und die für diese Gruppe festgelegte Sicherheitsstufe werden diesem Benutzer zugewiesen.
  - **Authype**: Ein Algorithmus, der zur Authentifizierung des SNMPv3-Benutzers für den Zugriff auf die NetScaler-Instanz verwendet wird. Sie müssen denselben Authentifizierungsalgorithmus angeben, wenn Sie den SNMPv3-Benutzer im SNMP-Manager konfigurieren.
  - **Authpassword**: Ein Passwort zur Authentifizierung. Dieses Passwort verwendet den angegebenen Authentifizierungsalgorithmustyp.
  - **Privtype**: Ein Algorithmus, der die Kommunikation zwischen einem SNMPv3-Benutzer und der NetScaler-Instanz verschlüsselt.
  - **privpasswd**: Ein Verschlüsselungsschlüssel für den in **Privtype** angegebenen Verschlüsselungsalgorithmus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **SNMP-Benutzer-Trap-Bindungskonfiguration** – SNMPv3 bietet Sicherheitsfunktionen wie Authentifizierung und Verschlüsselung unter Verwendung der Anmeldeinformationen von SNMP-Benutzern. Ein SNMP-Manager kann SNMPv3-Trap-Nachrichten nur empfangen, wenn seine Konfiguration das dem SNMP-Benutzer zugewiesene Passwort enthält.

3. Wählen Sie unter **Zielinstanzen** Instanzen oder Instanzgruppen aus, in denen Sie die Konfiguration ausführen möchten.

   HINWEIS:

   Sie können die Konfiguration auf mehr als einem NetScaler bereitstellen, indem Sie so viele Zielinstanzen wie nötig angeben.

4. Ordnen Sie unter **Tag-Zuordnung** alle vorhandenen und zukünftigen StyleBook-Tags der Konfiguration zu.

   Diese Option ordnet alle StyleBook-Tags einem Konfigurationspaket zu. Sie stellt auch sicher, dass neue Tags, die Sie in Zukunft zu den StyleBooks hinzufügen könnten, zugeordnet werden.

5. Klicken Sie auf **Probelauf**.

   Die Seite „Objekte“ zeigt die Objekte an, die in den NetScaler-Instanzen erstellt, geändert oder entfernt werden.

6. Klicken Sie auf **Erstellen**.

   Das Konfigurationspaket wird auf der Seite **StyleBook > Konfigurationen** angezeigt.

NetScaler Netzwerkkonfigurationen StyleBook

Wenn Sie verschiedene Netzwerkkomponenten auf einer NetScaler-Instanz bereitstellen möchten, können Sie NetScaler Console StyleBooks verwenden. Verwenden Sie die folgenden StyleBooks, um NetScaler-Netzwerkkomponenten zu erstellen:

- `network_configuration`: Für grundlegende Netzwerkkomponenten.
- `adv_network_configuration`: Für erweiterte Konfigurationen wie VXLAN, Cluster und mehr.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen zu NetScaler-Netzwerkkomponenten finden Sie unter Netzwerk.

Grundlegende Netzwerkkomponenten bereitstellen

Die grundlegenden Netzwerkkomponenten können Schnittstellen-, Kanal-, VLAN-, NSIP-, Address Resolution Protocol (ARP)- oder Bridge-Gruppenkonfigurationen sein. Führen Sie die folgenden Schritte aus, um eine dieser Komponenten bereitzustellen:

1. Navigieren Sie in NetScaler Console zu **Anwendungen > Konfiguration > StyleBooks**. Suchen Sie das StyleBook, indem Sie den Namen als `network_configuration` eingeben.
2. Klicken Sie auf **Konfiguration erstellen**.
3. Fügen Sie die folgenden Konfigurationen nach Bedarf hinzu:

   HINWEIS

   Klicken Sie auf das (+) Symbol in jedem Abschnitt, um Konfigurationen hinzuzufügen.

   - **Schnittstellenkonfigurationen** – Die Anzahl der Schnittstellen in Ihrer Konfiguration unterscheidet sich je nach Modell der NetScaler-Instanz. Weitere Informationen zu Schnittstellen finden Sie unter Schnittstellen. Geben Sie die Felder an, die zum Konfigurieren einer Schnittstelle erforderlich sind.
   - **Kanalkonfigurationen** – Das Konfigurieren der Link-Aggregation erhöht die Kapazität und Verfügbarkeit des Kommunikationskanals zwischen der NetScaler-Instanz und anderen verbundenen Geräten. Ein aggregierter Link wird auch als „Kanal“ bezeichnet. Die Link-Aggregation kombiniert Daten von mehreren Ports zu einem einzigen Hochgeschwindigkeits-Link. Weitere Informationen finden Sie unter Link-Aggregation konfigurieren.
   - **Kanal-Schnittstellen-Bindungskonfigurationen** – Geben Sie die Schnittstellen- und Kanal-IDs an, um die Konfigurationen zu binden.
   - **VLAN-Konfigurationen** – Sie können VLANs konfigurieren und an IP-Subnetze binden. Der NetScaler führt dann die IP-Weiterleitung zwischen diesen VLANs durch (wenn er als Standard-Router für die Hosts in diesen Subnetzen konfiguriert ist). Weitere Informationen finden Sie unter VLANs verstehen. Geben Sie die Details zur Konfiguration eines VLANs an.
   - **NS-IP-Konfigurationen** – Die NSIP-Adresse ist die IP-Adresse, über die Sie zu Verwaltungszwecken auf die NetScaler-Instanz zugreifen. Die Instanz kann nur eine NSIP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

haben, die auch als Management-IP-Adresse bezeichnet wird. Weitere Informationen finden Sie unter Konfigurieren der NSIP-Adresse.

- **NS-IP6-Konfigurationen** – Sie können auch eine IPv6-Adresse für eine NetScaler-Instanz als NSIP konfigurieren.
- **Konfigurationen für die VLAN-Schnittstellenbindung** – Wenn Sie eine Netzwerkschnittstelle an ein VLAN binden, wird die Netzwerkschnittstelle aus dem Standard-VLAN entfernt. Wenn die Netzwerkschnittstellen Teil mehrerer VLANs sein müssen, können Sie die Netzwerkschnittstellen als getaggte Mitglieder an die VLANs binden.
- **Konfigurationen für die VLAN-NS-IP-Bindung** – Sie können die NetScaler-IP-Adresse (NSIP) an ein VLAN binden. Wenn eine IP-Adresse einem VLAN zugeordnet ist, werden alle IP-Adressen in diesem Subnetz automatisch dem VLAN zugeordnet.
- **Routenkonfigurationen für IPv4** – Fügen Sie eine Netzwerk-IP-Adresse (IPv4) hinzu, für die Sie einen Routeneintrag in der Routingtabelle der NetScaler-Instanz hinzufügen möchten.
- **Routenkonfigurationen für IPv6** – Fügen Sie eine Netzwerk-IP-Adresse (IPv6) hinzu, für die Sie einen Routeneintrag in der Routingtabelle der NetScaler-Instanz hinzufügen möchten.
- **ARP-Konfigurationen** – Sie können statische ARP-Einträge zur ARP-Tabelle hinzufügen und daraus entfernen. Weitere Informationen finden Sie unter Statisches ARP.
- **ND6-Variablenkonfigurationen** – Die Neighbor Discovery (ND) ist eines der wichtigsten Protokolle von IPv6. Es ist ein nachrichtenbasiertes Protokoll, das die Funktionalität des Address Resolution Protocol (ARP), des Internet Control Message Protocol (ICMP) und der Router Discovery kombiniert. ND ermöglicht es Knoten, ihre Link-Layer-Adressen bekannt zu geben und die MAC-Adressen oder Link-Layer-Adressen der benachbarten Knoten zu erhalten. Weitere Informationen finden Sie unter Neighbor Discovery.

  Sie können die ND6-Variablen für eine NetScaler-Instanz konfigurieren.
- **Neighbor Discovery-Konfigurationen für IPv6** – Sie können ND für eine IPv6-Adresse konfigurieren.
- **Bridge-Gruppen-Konfigurationen** – Die Bridge-Gruppen-Funktion funktioniert auf die gleiche Weise wie ein VLAN. Mehrere VLANs können an eine einzelne Bridge-Gruppe gebunden werden, und alle VLANs, die an dieselbe Bridge-Gruppe gebunden sind, bilden eine einzige Broadcast-Domäne. Weitere Informationen finden Sie unter Bridge-Gruppen konfigurieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Bridge-Gruppe NS IPv46-Bindungskonfigurationen** – Binden Sie eine NetScaler-IP-Adresse (NSIP) an eine Bridge-Gruppe.
- **Bridge-Gruppe VLAN-Bindungskonfigurationen** – Binden Sie ein VLAN an eine Bridge-Gruppe.

4. Wählen Sie unter **Zielinstanzen** die NetScaler-Instanzen oder Instanzgruppen aus.
5. Ordnen Sie unter **Tag-Zuordnung** alle vorhandenen und zukünftigen StyleBook-Tags der Konfiguration zu.

   Diese Option ordnet alle StyleBook-Tags einem Konfigurationspaket zu. Sie stellt auch sicher, dass neue Tags, die Sie möglicherweise in Zukunft zu den StyleBooks hinzufügen, zugeordnet werden.
6. Klicken Sie auf **Probelauf**.

   Auf der Seite „Objekte“ werden die Objekte angezeigt, die in den NetScaler-Instanzen erstellt, geändert oder entfernt werden.
7. Klicken Sie auf **Erstellen**.

Das Konfigurationspaket wird auf der Seite **StyleBook > Konfigurationen** angezeigt.

Erweiterte Netzwerkkomponenten bereitstellen

Die erweiterten Netzwerkkomponenten können VXLAN, VRID, Bridge Table, Failover Interface Set (FIS), INAT, RNAT-Konfigurationen und mehr sein. Führen Sie die folgenden Schritte aus, um solche erweiterten Netzwerkkomponenten bereitzustellen:

1. Navigieren Sie in NetScaler Console zu **Anwendungen > Konfiguration > StyleBooks**. Suchen Sie das StyleBook, indem Sie den Namen als `adv_network_configuration` eingeben.
2. Klicken Sie auf **Konfiguration erstellen**.
3. Fügen Sie die folgenden Konfigurationen nach Bedarf hinzu:

   HINWEIS

   Klicken Sie auf das (+) Symbol in jedem Abschnitt, um Konfigurationen hinzuzufügen.

   - **VXLAN-Konfigurationen** – VXLANs bieten eine höhere Skalierbarkeit und Flexibilität als VLANs. Weitere Informationen finden Sie unter VXLAN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **VXLAN VLAN MAP-Konfigurationen** – Erstellen Sie eine Zuordnungstabelle auf der NetScaler-Instanz. Diese Tabelle ordnet eine VXLAN-ID einer entsprechenden VLAN-ID zu.
- **VRID-Konfigurationen** – Fügen Sie eine IPv4-Adresse hinzu, die eine virtuelle MAC (VMAC) identifiziert. Sie können auch andere VRID-Optionen und Bindungsinformationen konfigurieren.
- **VRID6-Konfigurationen** – Fügen Sie eine IPv6-Adresse hinzu, die eine virtuelle MAC (VMAC) identifiziert. Sie können auch andere VRID6-Optionen und Bindungsinformationen konfigurieren.
- **BridgeTable-Konfigurationen** – Eine NetScaler-Instanz überbrückt die Frames basierend auf einer Bridge-Tabellen-Suche der Ziel-MAC-Adresse und der VLAN-ID. Geben Sie die erforderlichen Details an, um die Bridge-Tabelle zu überwachen.
- **FIS-Konfigurationen** – Ein FIS ist eine logische Gruppe von Schnittstellen. In einer NetScaler HA-Konfiguration ist die Verwendung eines FIS eine Möglichkeit, ein Failover zu verhindern, indem Schnittstellen gruppiert werden, sodass bei Ausfall einer Schnittstelle andere funktionierende Schnittstellen weiterhin verfügbar sind. Ein FIS kann auch für die Knoten eines NetScaler-Clusters konfiguriert werden. Weitere Informationen finden Sie unter Konfigurieren eines Failover-Schnittstellensatzes.
- **Konfigurationen für ForwardingSession** – Eine Weiterleitungssitzungsregel erstellt Weiterleitungssitzungseinträge für Datenverkehr, der von einem bestimmten Netzwerk stammt oder für dieses bestimmt ist und von der NetScaler-Instanz weitergeleitet wird. Sie können Weiterleitungssitzungsregeln sowohl für IPv4- als auch für IPv6-Datenverkehr erstellen. Siehe, Konfigurieren von Weiterleitungssitzungsregeln.
- **INAT-Konfigurationen** – Wenn ein Client ein Paket an eine NetScaler-Instanz sendet, die für Inbound Network Address Translation (INAT) konfiguriert ist, übersetzt die Instanz die öffentliche Ziel-IP-Adresse des Pakets in eine private Ziel-IP-Adresse. Und die Instanz leitet das Paket an den Server unter dieser Adresse weiter. Siehe, Inbound Network Address Translation.
- **NAT64-Konfigurationen** – Das Stateful NAT64 ermöglicht die Kommunikation zwischen IPv6-Clients und IPv4-Servern durch IPv6-zu-IPv4-Paketübersetzung und umgekehrt, während die Sitzungsinformationen auf der NetScaler-Appliance beibehalten werden. Siehe, Stateful NAT64 Translation.
- **RNAT-Konfigurationen** – Bei der Reverse Network Address Translation (RNAT) ersetzt die NetScaler-Appliance die Quell-IP-Adressen in den von den Servern generierten Paketen durch öffentliche NAT-IP-Adressen. Siehe, RNAT.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **RNAT6-Konfigurationen** – Regeln für die Reverse Network Address Translation (RNAT) für IPv6-Pakete werden als RNAT6s bezeichnet. Siehe, RNAT6 konfigurieren.
- **IPSet-Konfigurationen** – Ein IP-Set ist eine Menge von IP-Adressen, die auf der NetScaler-Instanz als Subnetz-IP-Adressen (SNIPs) oder virtuelle IP-Adressen (VIPs) konfiguriert sind. Geben Sie die erforderlichen Details an, um ein IP-Set zu erstellen.
- **IPTunnel-Konfigurationen** – Geben Sie die Details an, um einen IP-Tunnel und seine Bindungen zu erstellen. Siehe, IP-Tunnel.
- **IP6-Tunnel-Konfigurationen** – Geben Sie für IPv6-Adressen die Details an, um einen IP-Tunnel und seine Bindungen zu erstellen.
- **Linkset-Konfigurationen** – Ein Linkset ist eine Gruppe von Schnittstellen von Clusterknoten, die zur selben Broadcast-Domäne gehören. Siehe, Konfigurieren von Linksets.
- **MAP-T-Basiskonfigurationen für Zuordnungsregeln** – Mapping Address and Port using Translation (MAP-T). Es ist ein Mechanismus, der eine doppelte Übersetzung (IPv4 zu IPv6 und umgekehrt) auf Customer Edge (CE)-Geräten und Border-Routern (im ISP-Kernnetzwerk) durchführt. Geben Sie die Details an, um eine grundlegende Zuordnungsregel hinzuzufügen. Siehe, Mapping Address and Port using Translation.
- **MAP-T-Standardkonfigurationen für Zuordnungsregeln** – Geben Sie die Details an, um eine Standard-Zuordnungsregel hinzuzufügen.
- **MAP-T Map-Domänenkonfigurationen** – Geben Sie die Details an, um eine Map-Domäne hinzuzufügen.
- **NetProfile-Konfigurationen** – Fügen Sie ein Netzprofil hinzu und konfigurieren Sie die Überschreibung `lsn`.
- **NetBridge-Konfigurationen** – Binden Sie eine VXLAN-VLAN-Zuordnung an eine Netzwerkbrücke.
- **On-link IPv6 globale Präfixe für Router-Advertisement-Konfigurationen** – Konfigurieren Sie für die IPv6-Clusterkonfiguration globale Präfixe und Router-Advertisements. Siehe, Unterstützung des IPv6-Ready-Logos für Cluster.

4. Unter **Zielinstanzen** wählen Sie die NetScaler-Instanzen oder Instanzgruppen aus.
5. Unter **Tag Assosiation** ordnen Sie alle aktuellen und zukünftigen StyleBook-Tags der Konfiguration zu.

   Diese Option ordnet alle StyleBook-Tags einem Konfigurationspaket zu. Sie stellt auch sicher, dass neue Tags, die Sie zukünftig zu den StyleBooks hinzufügen könnten, zugeordnet werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Klicken Sie auf **Probelauf**.

   Die Seite „Objekte“ zeigt die Objekte an, die auf den NetScaler-Instanzen erstellt, geändert oder entfernt werden.

7. Klicken Sie auf **Erstellen**.

Das Konfigurationspaket wird auf der Seite **StyleBook > Konfigurationen** angezeigt.

Prometheus Analytics StyleBook

Sie können Metriken von NetScaler nach Prometheus exportieren, indem Sie ein Analyseprofil in NetScaler erstellen und die Schemadatei angeben. In StyleBooks können Sie das `Prometheus TimeSeries Analytics Configuration` StyleBook verwenden und die Konfiguration auf alle verwalteten Instanzen anwenden.

Voraussetzung

Stellen Sie sicher, dass die verwalteten NetScaler-Instanzen **13.1 Build 39-27 oder höher** sind.

So konfigurieren Sie mit dem `Prometheus TimeSeries Analytics Configuration` StyleBook:

1. Navigieren Sie zu **Applications** > **Configurations** > **StyleBooks**, suchen Sie nach dem StyleBook, indem Sie den Namen als `Prometheus TimeSeries Analytics Configuration` eingeben, und klicken Sie auf **Create Configuration**.
2. Unter **Configpack Details**:
   a. Geben Sie den Namen des Analyseprofils an. Weitere Informationen finden Sie unter Metrik-Collector konfigurieren.
   b. **Zählerschema-Datei**:
      - Wenn Sie das Standardschema verwenden möchten, können Sie diesen Schritt überspringen.
      - Wenn Sie das benutzerdefinierte Schema verwenden möchten, laden Sie die Schemadatei hoch, die Sie mit den Parametern geändert haben. In NetScaler ist eine Referenzdatei `reference_schema.json` mit allen unterstützten Zählern unter dem Pfad `/var/metrics_conf/` verfügbar. Sie können einen FTP-Client verwenden, um die Datei auf Ihr lokales System zu kopieren.
3. Unter **Target Instances** wählen Sie die Instanzen oder Instanzgruppe aus, auf denen Sie die Konfiguration ausführen möchten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Unter **Tag Assosiation** ordnen Sie alle aktuellen und zukünftigen StyleBook-Tags der Konfiguration zu.

   Diese Option ordnet alle StyleBook-Tags einem Konfigurationspaket zu. Sie stellt auch sicher, dass neue Tags, die Sie möglicherweise zukünftig zu den StyleBooks hinzufügen, zugeordnet werden.

   HINWEIS:

   Klicken Sie auf **Dry Run**, um die Ergebnisse anzuzeigen, die von den NetScaler®-Instanzen erstellt, geändert oder entfernt werden.

5. Klicken Sie auf **Create**, um die Konfiguration auszuführen.

Migration der NetScaler-Anwendungskonfiguration mit dem StyleBooks Configuration Builder

Der StyleBooks Configuration Builder wird verwendet, um eine vorhandene NetScaler-Konfiguration zu StyleBooks zu migrieren. Diese Funktion automatisiert auch die Migration der Anwendungskonfiguration von einer NetScaler-Instanz zu einer anderen Instanz oder einer Autoscale-Gruppe.

Der Configuration Builder bietet ein strukturiertes Anwendungs-StyleBook, das für alle Varianten der NetScaler-Konfiguration verwendet werden kann. Diese Funktion hilft Ihnen, mit StyleBooks zu beginnen, ohne detaillierte Kenntnisse der StyleBooks-Grammatik und -Konstrukte zu besitzen. Andernfalls sind Kenntnisse der StyleBooks-Grammatik und -Konstrukte erforderlich, um ein StyleBook zu erstellen.

Der Configuration Builder erstellt auch ein Konfigurationspaket, das dieselbe NetScaler-Konfiguration auf einer neuen NetScaler-Instanz widerspiegelt. Mit diesem Konfigurationspaket kann die ursprüngliche NetScaler-Konfiguration von einer NetScaler-Instanz auf eine andere NetScaler-Instanz dupliziert werden. Die ursprüngliche Konfigurationsquelle kann eine der folgenden sein:

- **Eine NetScaler-Instanz:** Geben Sie die Instanz an, auf der die Anwendungskonfiguration, die Sie duplizieren möchten, gehostet wird.

  Der Configuration Builder konvertiert die NetScaler-Konfiguration in ein StyleBook und ein Konfigurationspaket, auch wenn Sie die Zielinstanz nicht angeben. Sie können dieses

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfigurationspaket später verwenden, um die NetScaler-Konfiguration auf andere NetScaler-Instanzen zu migrieren.

Wenn die Zielinstanz eine Autoscale™-Gruppe ist, wird das Konfigurationspaket auf der Seite **Network > AutoScale Group** angezeigt. Unter der Registerkarte **Configuration**.

- **Ein Satz von CLI-Befehlen:** Fügen Sie die Konfiguration aus `ns.conf` oder `Application config` ein.

Der Configuration Builder identifiziert die Liste der unterschiedlichen Anwendungen, die in der Quellkonfiguration eingebettet sind. Wenn Sie die Anwendungskonfiguration auswählen, die Sie interessiert, extrahiert der Configuration Builder den Satz von CLI-Befehlen für die ausgewählte Anwendung. Diese CLI-Befehle werden aus der Quellkonfiguration extrahiert. Außerdem identifiziert er die Bereitstellungs- und Konfigurationsattribute, die Ihre Eingabe erfordern könnten.

- **IP-Adresse/Ports** – Sie können die IP-Adresse und den Port der virtuellen Server, Dienste und Dienstgruppenmitglieder aus der ursprünglichen Konfiguration anzeigen und bearbeiten.
- **Konfigurationsdateien/Geheimnisse** – Diese Attribute können Passwörter oder Zertifikate sein, die in der Quellkonfiguration angegeben sind.

Nachdem Sie die erforderlichen Informationen angegeben haben, beginnen Sie mit der Migration oder Duplizierung der Anwendungskonfiguration auf einer Ziel-NetScaler-Instanz.

Nach der Erstellung und Migration der Anwendung wird in NetScaler Console ein Konfigurationspaket mithilfe des `adc_nitro_application` StyleBook erstellt. Dieses StyleBook wird basierend auf den NetScaler NITRO-Ressourcen erstellt. Dieses Konfigurationspaket stellt die Anwendungskonfiguration auf der Ziel-NetScaler-Instanz dar. Um das erstellte Konfigurationspaket anzuzeigen, navigieren Sie zu **Applications > Configuration > Confg Packs**.

Freigabe von Konfigurationsentitäten zwischen migrierten Konfigurationen

Sie können Konfigurationsentitäten bei der Migration von Konfigurationen mit dem Konfigurationsmigrationsdienstprogramm wiederverwenden. Nachfolgende Migrationen verwenden vorhandene Konfigurationsentitäten erfolgreich wieder. Zuvor schlug die Migration von Konfigurationen mit dem Fehler **Ressource existiert bereits** fehl, wenn zwei Konfigurationen migriert wurden, die einige Konfigurationsentitäten gemeinsam nutzten. Diese Option optimiert den Migrations-Workflow, indem sie die Wiederverwendung von Konfigurationsentitäten in Szenarien ermöglicht, in denen sie über mehrere Konfigurationen hinweg verwendet werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unterstützte NetScaler-Funktionen

Der StyleBook Configuration Builder erkennt und unterstützt die folgenden NetScaler-Funktionen in der Quellkonfiguration:

- Inhaltswechsel
- Lastenausgleich
- Überwachung
- SSL-Offloading
- Ratenbegrenzung
- Rewrite
- Responder
- Web Application Firewall (WAF)
- Bot-Verwaltung
- Komprimierungssteuerung

Erstellen Sie ein StyleBook, um die NetScaler-Anwendungskonfiguration zu migrieren

Das folgende Verfahren dient der Erstellung eines StyleBooks, das die NetScaler-Anwendungsmigration in NetScaler Console migriert:

1. Navigieren Sie zu **Applications > Configuration > Confg Packs**.
2. Klicken Sie auf **Migrate NetScaler Configuration**.
3. Klicken Sie auf **Get Started**.
4. Wählen Sie unter **Specify Configuration** die Konfigurationsquelle aus:
    - **Import from a NetScaler**: Diese Option erkennt die aktiven Anwendungen auf der ausgewählten NetScaler-Instanz.
    - **Import using CLI Commands**: Diese Option analysiert die CLI-Befehle und extrahiert die Anwendungen aus den CLI-Befehlen.
5. Geben Sie die **Source NetScaler Instance** an, von der Sie die Anwendungskonfiguration migrieren oder duplizieren möchten.

    Um die Anwendungskonfiguration in eine Autoscale-Gruppe zu migrieren, stellen Sie sicher, dass die folgenden Informationen nicht in der Quellkonfiguration enthalten sind:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `IPset`
- Geräteprofil
- Protokoll
- Port

6. Geben Sie die **Target NetScaler Instance** an, zu der Sie die Anwendungskonfiguration migrieren oder duplizieren möchten.

   Um eine Anwendungskonfiguration in eine Autoscale-Gruppe zu migrieren, wählen Sie die Autoscale-Gruppe aus der Liste aus.

7. Unter **Define Application**,

   a. Geben Sie unter **Anwendungsname** den Namen der Anwendung an.

      Wenn die Zielinstanz eine Autoscale-Gruppe ist, geben Sie die folgenden Autoscale-Parameter an:

      - **Zugriffstyp** – Sie können die NetScaler Console Autoscaling-Lösung sowohl für externe als auch für interne Anwendungen verwenden. Wählen Sie den erforderlichen Anwendungszugriffstyp aus.
      - **Domänenname** – Geben Sie den Domänennamen einer Anwendung an. Diese Option ist nur anwendbar, wenn Sie den Typ Benutzerdefinierter FQDN auswählen.
      - **Zone der Domäne** – Wählen Sie den Zonennamen einer Anwendung aus der Liste aus. Diese Option ist nur anwendbar, wenn Sie den Typ Benutzerdefinierter FQDN auswählen.

        Dieser Domänen- und Zonenname leitet zu den virtuellen Servern in Azure um. Wenn Sie beispielsweise eine Anwendung in `app.example.com` hosten, ist `app` der Domänenname und `example.com` der Zonenname.

   b. Wählen Sie die virtuellen Server aus, die Sie migrieren möchten.

   c. Klicken Sie auf **Weiter**.

8. Überprüfen Sie unter **Äquivalente CLI-Befehle** die Befehle und klicken Sie auf **Weiter**.

   Diese Befehle sind spezifisch für die ausgewählte Anwendungskonfiguration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Sie können die Konfiguration bei Bedarf auch hinzufügen oder bearbeiten.

9. Unter **Bereitstellungsattribute** können Sie die IP-Adresse und den Port der virtuellen Server, Dienste und Dienstgruppenmitglieder anzeigen und bearbeiten.

   Um die IP-Adresse und den Port zu bearbeiten, klicken Sie auf das Bearbeitungssymbol auf dem virtuellen Server, Dienst oder Dienstgruppenmitglied im Flussdiagramm.

   HINWEIS:

   Wenn die Zielinstanz eine Autoscale-Gruppe ist, ist die Bearbeitung der Frontend-IP-Adresse deaktiviert.

   Diese Registerkarte wird nur in den folgenden Fällen angezeigt:

   - Die Quell- und Zielinstanzen sind unterschiedlich.
   - Konfigurationen mithilfe von CLI-Befehlen importieren.

10. Geben Sie unter **Konfigurationsattribute** die erforderlichen Details an und klicken Sie auf **Weiter**.

    Diese Registerkarte listet die Geheimnisse auf, wie z. B. Schlüssel zum Entschlüsseln von Passwörtern und Zertifikaten.

    HINWEIS:

    Bevor Sie die Migration starten, werden die fehlenden oder nicht unterstützten Konfigurationen in einer der folgenden Registerkarten angezeigt:

    - **Nicht unterstützte Konfigurationen**
    - **Nicht unterstützte globale Konfigurationen**

    Um diese Konfigurationen erfolgreich zu migrieren, müssen Sie die fehlenden oder nicht unterstützten Konfigurationen separat auf der Zielinstanz anwenden. Klicken Sie anschließend auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. Klicken Sie unter **Migrieren** auf **Migrieren**.

Einschränkungen

- Die in der Quellinstanz erwähnten benannten Ausdrücke und `responderhtmlpages` werden nicht identifiziert. Stellen Sie sicher, dass Sie die benannten Ausdrücke und `responderhtmlpages` vor der Migration auf der Zielinstanz konfigurieren.
- Wenn die Quelle eine Konfiguration für `servicegroup` und Monitorbindung wie folgt hat:

  `bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>`

  Der folgende Fehler wird angezeigt:

  ```
  CLI Command conversion failed: 100 - No such command [{ "errorcode":
  1090, "message": "No such argument [XXX]", "severity": "ERROR" }]
  ```

  Dieser Fehler tritt auf, weil NetScaler die Bindung zwischen Dienstgruppe und Monitor in einem ungültigen Format speichert. Dieses Problem ist ab NetScaler Build 12.1.52.15 behoben.

StyleBooks für Geschäftsanwendungen

NetScaler Console bietet die StyleBooks, die Ihnen helfen, eine NetScaler-Konfiguration für bestimmte Geschäftsanwendungen bereitzustellen. Weitere Informationen zu solchen StyleBooks finden Sie in den folgenden Themen:

- SSO Google Apps StyleBook
- SSO Office 365 StyleBook
- StyleBook für Microsoft Skype for Business
- Microsoft Exchange StyleBook
- Microsoft SharePoint StyleBook
- Microsoft ADFS-Proxy StyleBook
- Oracle E-Business StyleBook

SSO Google Apps StyleBook

Google Apps ist eine Sammlung von Cloud-Computing-, Produktivitäts- und Kollaborationstools, Software und Produkten, die von Google entwickelt wurden. Single Sign-On (SSO) ermöglicht Benutzern den Zugriff auf alle ihre Unternehmens-Cloud-Anwendungen – einschließlich

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Administratoren, die sich bei der Administratorkonsole anmelden – indem sie sich einmalig für alle Dienste mit ihren Unternehmensanmeldeinformationen anmelden.

Das NetScaler Console SSO Google Apps StyleBook ermöglicht Ihnen, SSO für Google Apps über NetScaler-Instanzen zu aktivieren. Das StyleBook konfiguriert die NetScaler-Instanz als SAML-Identitätsanbieter zur Authentifizierung von Benutzern für den Zugriff auf Google Apps.

Die Aktivierung von SSO für Google Apps in einer NetScaler-Instanz mithilfe dieses StyleBooks umfasst die folgenden Schritte:

1. Konfigurieren des virtuellen Authentifizierungsservers
2. Konfigurieren einer SAML-IdP-Richtlinie und eines Profils
3. Binden der Richtlinie und des Profils an den virtuellen Authentifizierungsserver
4. Konfigurieren eines LDAP-Authentifizierungsservers und einer Richtlinie auf der Instanz
5. Binden des LDAP-Authentifizierungsservers und der Richtlinie an Ihren auf der Instanz konfigurierten virtuellen Authentifizierungsserver

Konfigurationsdetails:

Die folgende Tabelle listet die mindestens erforderlichen Softwareversionen auf, damit diese Integration erfolgreich funktioniert. Der Integrationsprozess unterstützt auch höhere Versionen davon.

PRODUKT	MINDESTENS ERFORDERLICHE VERSION
NetScaler	Version 11.0, Advanced-/Premium-Lizenz

Die folgenden Anweisungen gehen davon aus, dass Sie bereits die entsprechenden externen und internen DNS-Einträge erstellt haben, um Authentifizierungsanfragen an eine von NetScaler überwachte IP-Adresse weiterzuleiten.

Bereitstellen von SSO Google Apps StyleBook-Konfigurationen:

Die folgende Aufgabe unterstützt Sie bei der Bereitstellung des Microsoft SSO Google Apps StyleBook in Ihrem Unternehmensnetzwerk.

So stellen Sie das SSO Google Apps StyleBook bereit

1. Navigieren Sie in NetScaler Console zu **Applications** > **Configurations** > **StyleBooks**. Die Seite StyleBooks zeigt alle StyleBooks an, die Ihnen in NetScaler Console zur Verfügung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

stehen. Scrollen Sie nach unten und suchen Sie **SSO Google Apps StyleBook**. Klicken Sie auf **Create Configuration**.

2. Das StyleBook wird als Benutzeroberfläche geöffnet, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
3. Geben Sie Werte für die folgenden Parameter ein:

    a. **Application Name**. Name der SSO Google Apps-Konfiguration, die in Ihrem Netzwerk bereitgestellt werden soll.

    b. **Authentication Virtual IP address**. Virtuelle IP-Adresse, die vom virtuellen NetScaler AAA-Server verwendet wird, an den die Google Apps SAML IdP-Richtlinie gebunden ist.

    c. **SAML Rule Expression**. Standardmäßig wird der folgende NetScaler Policy (PI)-Ausdruck verwendet: HTTP.REQ.HEADER("Referrer").CONTAINS("google"). Aktualisieren Sie dieses Feld mit einem anderen Ausdruck, wenn Ihre Anforderung anders ist. Dieser Richtlinienausdruck gleicht den Datenverkehr ab, auf den diese SAML-SSO-Einstellungen angewendet werden, und stellt sicher, dass der Referrer-Header von einer Google-Domain stammt.

4. Der Abschnitt SAML IdP Settings ermöglicht es Ihnen, Ihre NetScaler-Instanz als SAML-Identitätsanbieter zu konfigurieren, indem Sie das SAML IdP-Profil und die Richtlinie erstellen, die vom in Schritt 3 erstellten virtuellen NetScaler AAA-Server verwendet werden.

    a. **SAML Issuer Name**. Geben Sie in diesem Feld den öffentlichen FQDN Ihres virtuellen Authentifizierungsservers ein. Beispiel: `https://<Citrix_ADC_VIP>/saml/login`

    b. **SAML Service Provider (SP) ID**. (optional) Der NetScaler-Identitätsanbieter akzeptiert SAML-Authentifizierungsanfragen von einem Ausstellernamen, der mit dieser ID übereinstimmt.

    c. **Assertion Consumer Service URL**. Geben Sie die URL des Dienstanbieters ein, an die der NetScaler-Identitätsanbieter die SAML-Assertions nach erfolgreicher Benutzerauthentifizierung senden muss. Die Assertion Consumer Service URL kann auf der Seite des Identitätsanbieters oder auf der Seite des Dienstanbieters initiiert werden.

    d. Es gibt weitere optionale Felder, die Sie in diesem Abschnitt eingeben können. Sie können beispielsweise die folgenden Optionen festlegen:

        i. SAML-Bindungsprofil (Standard ist das „POST“-Profil).

        ii. Signaturalgorithmus zum Überprüfen/Signieren von SAML-Anfragen/-Antworten (Standard ist „RSA-SHA1“).

        iii. Methode zum Hashen für SAML-Anfragen/-Antworten (Standard ist „SHA-1“).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iv. Verschlüsselungsalgorithmus (Standard ist AES256) und andere Einstellungen.

HINWEIS

Citrix empfiehlt, die Standardeinstellungen beizubehalten, da diese Einstellungen zur Unterstützung von Google Apps getestet wurden.

e. Sie können auch das Kontrollkästchen „Benutzerattribute“ aktivieren, um die Benutzerdetails einzugeben, wie z. B.:

i. Name des Benutzerattributs

ii. NetScaler PI-Ausdruck, der ausgewertet wird, um den Wert des Attributs zu extrahieren

iii. Benutzerfreundlicher Name des Attributs

iv. Wählen Sie das Format des Benutzerattributs aus.

Diese Werte sind in der ausgestellten SAML-Assertion enthalten. Sie können bis zu fünf Sätze von Benutzerattributen in eine von NetScaler mit diesem StyleBook ausgestellte Assertion aufnehmen.

5. Geben Sie im Abschnitt „LDAP-Einstellungen“ die folgenden Details ein, um Google Apps-Benutzer zu authentifizieren. Damit Domänenbenutzer sich mit ihren geschäftlichen E-Mail-Adressen bei der NetScaler-Instanz anmelden können, müssen Sie Folgendes konfigurieren:

a. **LDAP (Active Directory) Basis**. Geben Sie den Basisdomänennamen für die Domäne ein, in der sich die Benutzerkonten innerhalb des Active Directory (AD) befinden, für das Sie die Authentifizierung zulassen möchten. Zum Beispiel: `dc=netscaler,dc=com`

b. **LDAP (Active Directory) Bind DN**. Fügen Sie ein Domänenkonto hinzu (verwenden Sie eine E-Mail-Adresse zur Vereinfachung der Konfiguration), das über Rechte zum Durchsuchen des AD-Baums verfügt. Zum Beispiel: `cn=Manager,dc=netscaler,dc=com`

c. **LDAP (Active Directory) Bind DN-Passwort**. Geben Sie das Passwort des Domänenkontos für die Authentifizierung ein.

d. Einige weitere Felder, die Sie in diesem Abschnitt eingeben müssen, sind die folgenden:

i. IP-Adresse des LDAP-Servers, mit dem NetScaler zur Authentifizierung von Benutzern eine Verbindung herstellt

ii. FQDN-Name des LDAP-Servers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Sie müssen mindestens eine der beiden oben genannten Angaben machen – die IP-Adresse des LDAP-Servers oder den FQDN-Namen.

iii. LDAP-Server-Port, mit dem NetScaler zur Authentifizierung von Benutzern eine Verbindung herstellt (Standard ist 389).

iv. LDAP-Hostname. Dieser wird zur Validierung des LDAP-Zertifikats verwendet, wenn die Validierung aktiviert ist (standardmäßig ist sie deaktiviert).

v. LDAP-Anmeldenamenattribut. Das Standardattribut zum Extrahieren von Anmeldenamen ist `samAccountname`.

vi. Weitere optionale sonstige LDAP-Einstellungen

6. Im Abschnitt SAML IdP SSL-Zertifikat können Sie die Details des SSL-Zertifikats angeben:

   a. **Zertifikatsname**. Geben Sie den Namen des SSL-Zertifikats ein.

   b. **Zertifikatsdatei**. Wählen Sie die SSL-Zertifikatsdatei aus dem Verzeichnis auf Ihrem lokalen System oder in der NetScaler Console aus.

   c. **Zertifikatsschlüsselformat**. Wählen Sie das Format der Zertifikats- und Private-Key-Dateien aus der Dropdown-Liste aus. Die unterstützten Formate sind `.pem`- und `.der`-Erweiterungen.

   d. **Zertifikatsschlüsselname**. Geben Sie den Namen des privaten Zertifikatsschlüssels ein.

   e. **Zertifikatsschlüsseldatei**. Wählen Sie die Datei mit dem privaten Schlüssel des Zertifikats von Ihrem lokalen System oder von NetScaler Console aus.

   f. **Passwort für den privaten Schlüssel**. Wenn Ihre private Schlüsseldatei durch eine Passphrase geschützt ist, geben Sie diese in dieses Feld ein.

   g. Sie können auch das Kontrollkästchen „Erweiterte Zertifikatseinstellungen“ aktivieren, um Details wie den Benachrichtigungszeitraum für den Zertifikatsablauf einzugeben, den Zertifikatsablaufmonitor zu aktivieren oder zu deaktivieren.

7. Optional können Sie das IdP-SSL-CA-Zertifikat auswählen, wenn das oben eingegebene SAML-IdP-Zertifikat ein öffentliches CA-Zertifikat erfordert, das auf NetScaler installiert werden muss. Stellen Sie sicher, dass Sie in den erweiterten Einstellungen „Ist ein CA-Zertifikat“ auswählen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Optional können Sie das SAML-SP-SSL-Zertifikat auswählen, um das Google-SSL-Zertifikat (öffentlicher Schlüssel) anzugeben, das zur Validierung von Authentifizierungsanfragen von Google Apps (SAML SP) verwendet wird.
9. Klicken Sie auf **Zielinstanzen** und wählen Sie die NetScaler-Instanz(en) aus, auf der/denen diese Google Apps SSO-Konfiguration bereitgestellt werden soll. Klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und auf der/den ausgewählten NetScaler-Instanz(en) bereitzustellen.

   HINWEIS

   Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich entdeckte NetScaler-Instanzen in NetScaler Console zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

Außerdem,

TIPP

SSO Office 365 StyleBook

Microsoft Office 365 ist eine Suite von cloudbasierten Produktivitäts- und Kollaborationsanwendungen, die von Microsoft auf Abonnementbasis bereitgestellt werden. Sie umfasst die beliebten serverbasierten Anwendungen von Microsoft wie Exchange, SharePoint, Office und Skype for Business. Single Sign-On (SSO) ermöglicht Benutzern den Zugriff auf alle ihre Cloud-Anwendungen des Unternehmens:

- Einschließlich Administratoren, die sich bei der Admin-Konsole anmelden
- Einmalige Anmeldung für alle Microsoft Office 365-Dienste unter Verwendung ihrer Unternehmensanmeldeinformationen.

Das SSO Office 365 StyleBook ermöglicht Ihnen die Aktivierung von SSO für Microsoft Office 365 über NetScaler-Instanzen. Sie können jetzt die SAML-Authentifizierung konfigurieren, wobei NetScaler als SAML Identity Provider (IdP) und Microsoft Office 365 als SAML-Dienstanbieter fungiert.

Die Aktivierung von SSO für Microsoft Office 365 in einer NetScaler-Instanz mithilfe dieses StyleBooks umfasst die folgenden Schritte:

1. Konfigurieren des virtuellen Authentifizierungsservers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Konfigurieren einer SAML IdP-Richtlinie und eines Profils
3. Binden der Richtlinie und des Profils an den virtuellen Authentifizierungsserver
4. Konfigurieren eines LDAP-Authentifizierungsservers und einer Richtlinie auf der Instanz
5. Binden des LDAP-Authentifizierungsservers und der Richtlinie an Ihren auf der Instanz konfigurierten virtuellen Authentifizierungsserver.

Die Tabelle listet die mindestens erforderlichen Softwareversionen auf, damit diese Integration erfolgreich funktioniert. Der Integrationsprozess unterstützt auch höhere Versionen davon.

PRODUKT	MINDESTENS ERFORDERLICHE VERSION
NetScaler	11.0, Advanced/Premium-Lizenz

Die folgenden Anweisungen gehen davon aus, dass Sie die entsprechenden externen und internen DNS-Einträge bereits erstellt haben. Diese Einträge sind unerlässlich, um Authentifizierungsanfragen an eine von NetScaler überwachte IP-Adresse weiterzuleiten.

Die folgenden Anweisungen helfen Ihnen bei der Implementierung des SSO Office 365 StyleBook in Ihrem Unternehmensnetzwerk.

So stellen Sie das SSO Microsoft Office 365 StyleBook bereit

1. Navigieren Sie in NetScaler Console zu **Applications > Configuration > StyleBooks**. Die Seite **StyleBooks** zeigt alle StyleBooks an, die Ihnen in NetScaler Console zur Verfügung stehen. Scrollen Sie nach unten und suchen Sie **SSO Office 365 StyleBook**. Klicken Sie auf **Create Configuration**.
2. Das StyleBook wird als Benutzeroberflächenseite geöffnet, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
3. Geben Sie Werte für die folgenden Parameter ein:

    a. **Application Name**. Name der SSO Microsoft Office 365-Konfiguration, die in Ihrem Netzwerk bereitgestellt werden soll.

    b. **Authentication Virtual IP address**. Virtuelle IP-Adresse, die vom virtuellen NetScaler AAA-Server verwendet wird, an den die Microsoft Office 365 SAML IdP-Richtlinie gebunden ist.

4. Geben Sie im Abschnitt **SSL Certificates Settings** die Namen des SSL-Zertifikats und des Zertifikatsschlüssels ein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Dies ist nicht das Office 365-Dienstanbieterzertifikat. Dieses SSL-Zertifikat ist an den virtuellen Authentifizierungsserver auf der NetScaler-Instanz gebunden.

5. Wählen Sie die entsprechenden Dateien aus Ihrem lokalen Speicherordner aus. Sie können auch das Kennwort für den privaten Schlüssel eingeben, um verschlüsselte private Schlüssel im PEM-Format zu laden.

6. Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie den Benachrichtigungszeitraum für den Zertifikatsablauf eingeben, den Zertifikatsablaufmonitor aktivieren oder deaktivieren.
7. Optional können Sie das Kontrollkästchen **SSL-CA-Zertifikat für die virtuelle Authentifizierung** IP auswählen, wenn das SSL-Zertifikat ein öffentliches CA-Zertifikat erfordert, das auf NetScaler installiert werden muss. Stellen Sie sicher, dass Sie im obigen Abschnitt **Erweiterte Zertifikateinstellungen** die Option „Ist ein CA-Zertifikat“ auswählen.
8. Geben Sie im Abschnitt **LDAP-Einstellungen für SSO Office 365** die folgenden Details ein, um Office 365-Benutzer zu authentifizieren. Um Domänenbenutzern die Anmeldung bei der NetScaler-Instanz mit ihren geschäftlichen E-Mail-Adressen zu ermöglichen, konfigurieren Sie Folgendes:

   a. **LDAP (Active Directory) Basis**. Geben Sie den Basisdomänennamen für die Domäne ein, in der sich die Benutzerkonten innerhalb des Active Directory (AD) befinden, um die Authentifizierung zu ermöglichen. Zum Beispiel: `dc=netscaler,dc=com`

   b. **LDAP (Active Directory) Bind-DN**. Fügen Sie ein Domänenkonto hinzu (verwenden Sie zur Vereinfachung der Konfiguration eine E-Mail-Adresse), das über Rechte zum Durchsuchen des AD-Baums verfügt. Zum Beispiel: `cn=Manager,dc=netscaler,dc=com`

   c. **LDAP (Active Directory) Bind-DN-Passwort**. Geben Sie das Passwort des Domänenkontos für die Authentifizierung ein.

   d. Einige weitere Felder, die Sie in diesem Abschnitt eingeben müssen, sind die folgenden:

      i. LDAP-Server-IP-Adresse, mit der NetScaler zur Authentifizierung von Benutzern eine Verbindung herstellt.

      ii. FQDN-Name des LDAP-Servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Sie müssen mindestens eine der beiden oben genannten Angaben machen – die IP-Adresse des LDAP-Servers oder den FQDN-Namen.

iii. LDAP-Server-Port, mit dem NetScaler zur Authentifizierung von Benutzern eine Verbindung herstellt (Standard ist 389). LDAPS verwendet 636.

iv. LDAP-Hostname. Der Hostname wird zur Validierung des LDAP-Zertifikats verwendet, wenn die Validierung aktiviert ist (standardmäßig ist sie deaktiviert).

v. LDAP-Anmeldenamenattribut. Das Standardattribut zum Extrahieren von Anmeldenamen ist „sAMAccountName“.

vi. Weitere optionale sonstige LDAP-Einstellungen.

9. Im Abschnitt **SAML IdP-Zertifikat** können Sie die Details der für die SAML-Assertion verwendeten SSL-Zertifikate angeben.

   a. **Zertifikatsname**. Geben Sie den Namen des SSL-Zertifikats ein.

   b. **Zertifikatsdatei**. Wählen Sie die SSL-Zertifikatsdatei aus dem Verzeichnis auf Ihrem lokalen System aus.

   c. **Zertifikatsschlüsselformat**. Wählen Sie das Format des Zertifikats und der privaten Schlüsseldateien aus der Dropdown-Liste aus. Die unterstützten Formate sind die Erweiterungen .pem und .der.

   d. **Zertifikatsschlüsselname**. Geben Sie den Namen des privaten Zertifikatsschlüssels ein.

   e. **Zertifikatsschlüsseldatei**. Wählen Sie die Datei mit dem privaten Schlüssel des Zertifikats von Ihrem lokalen System aus.

   f. **Passwort für privaten Schlüssel**: Geben Sie die Passphrase ein, die Ihre private Schlüsseldatei schützt.

   Sie können auch das Kontrollkästchen **Erweiterte Zertifikatseinstellungen** aktivieren. Hier können Sie Details wie den Benachrichtigungszeitraum für den Zertifikatsablauf eingeben, den Zertifikatsablaufmonitor aktivieren oder deaktivieren.

10. Optional können Sie **SAML IdP CA-Zertifikat** auswählen, wenn das oben eingegebene SAML IdP-Zertifikat ein öffentliches CA-Zertifikat erfordert, das auf NetScaler installiert werden muss.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Stellen Sie sicher, dass Sie im obigen Abschnitt **Erweiterte Zertifikatseinstellungen** die Option „Ist ein CA-Zertifikat“ auswählen.

11. Geben Sie im Abschnitt **SAML SP-Zertifikat** die folgenden Details für das öffentliche Office 365 SSL-Zertifikat ein. Dieses Zertifikat wird von der NetScaler-Instanz verwendet, um eingehende SAML-Authentifizierungsanfragen zu überprüfen.

    a. **Zertifikatsname**. Geben Sie den Namen des SSL-Zertifikats ein.

    b. **Zertifikatsdatei**. Wählen Sie die SSL-Zertifikatsdatei aus dem Verzeichnis auf Ihrem lokalen System aus.

    c. **Zertifikatsschlüsselformat**. Wählen Sie das Format des Zertifikats und der privaten Schlüsseldateien aus der Dropdown-Liste aus. Die unterstützten Formate sind die Erweiterungen .pem und .der.

    Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie den Benachrichtigungszeitraum für den Zertifikatsablauf eingeben und den Zertifikatsablaufmonitor aktivieren oder deaktivieren.

12. Der Abschnitt **SAML Idp-Einstellungen** ermöglicht es Ihnen, Ihre NetScaler-Instanz als SAML-Identitätsanbieter zu konfigurieren, indem Sie das SAML IdP-Profil und die Richtlinie erstellen, die vom in Schritt 3 erstellten NetScaler AAA Virtual Server verwendet werden.

    a. **SAML-Ausstellername**. Geben Sie in diesem Feld den öffentlichen FQDN Ihres Authentifizierungs-Virtual-Servers ein. Beispiel: `https://<NetScaler_VIP_Address\>/saml/login`

    b. **Name Identifier Expression**. Geben Sie den NetScaler-Ausdruck ein, der ausgewertet wird, um den im SAML-Assertion gesendeten SAML NameIdentifier zu extrahieren. Beispiel: `"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`

    c. **Signaturalgorithmus**: Wählen Sie den Algorithmus zum Überprüfen/Signieren von SAML-Anfragen/Antworten (Standard ist „RSA-SHA256“).

    d. **Digest-Methode**. Wählen Sie die Methode zum Hashen für SAML-Anfragen/Antworten (Standard ist „SHA256“).

    e. **Zielgruppenname**. Geben Sie den Entitätsnamen oder die URL ein, die den Dienstanbieter (Microsoft Office 365) darstellt.

    f. **SAML Service Provider (SP) ID**. (optional) Der NetScaler-Identitätsanbieter akzeptiert SAML-Authentifizierungsanfragen von einem Ausstellernamen, der dieser ID entspricht.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

g. **Assertion Consumer Service URL**. Geben Sie die URL des Dienstanbieters ein, an die der NetScaler-Identitätsanbieter die SAML-Assertions nach erfolgreicher Benutzerauthentifizierung senden muss. Die Assertion Consumer Service URL kann auf der Seite des Identitätsanbieterservers oder auf der Seite des Dienstanbieters initiiert werden.

h. Es gibt weitere optionale Felder, die Sie in diesem Abschnitt eingeben können. Sie können beispielsweise die folgenden Optionen festlegen:

   i. **SAML-Attributname**. Name des in der SAML-Assertion gesendeten Benutzerattributs.

   ii. **SAML-Attribut-Anzeigename**. Anzeigename des in der SAML-Assertion gesendeten Benutzerattributs.

   iii. **PI-Ausdruck für SAML-Attribut**. Standardmäßig wird der folgende NetScaler Policy (PI)-Ausdruck verwendet: HTTP.REQ.USER.ATTRIBUTE(1). Dieses Feld gibt das erste vom LDAP-Server gesendete Benutzerattribut (Mail) als SAML-Authentifizierungsattribut an.

   iv. Wählen Sie das Format des Benutzerattributs aus.

   Diese Werte sind in der ausgestellten SAML-Assertion enthalten.

   TIPP

   Citrix empfiehlt, die Standardeinstellungen beizubehalten, da diese Einstellungen getestet wurden, um Microsoft Office 365-Apps zu unterstützen.

13. Klicken Sie auf **Zielinstanzen**, und wählen Sie die NetScaler-Instanz(en) aus, auf der/denen diese Microsoft Office 365 SSO-Konfiguration bereitgestellt werden soll. Klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und auf der/den ausgewählten NetScaler-Instanz(en) bereitzustellen.

TIPP

Citrix empfiehlt, dass Sie vor dem Ausführen der eigentlichen Konfiguration die Option **Testlauf** auswählen, um die Konfigurationsobjekte anzuzeigen, die vom StyleBook auf den Ziel-NetScaler-Instanzen erstellt werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBook für Microsoft Skype for Business

Die Anwendung Skype for Business 2015 ist für ihre Funktion auf mehrere externe Komponenten angewiesen. Das Skype for Business-Netzwerk besteht aus verschiedenen Systemen, wie Servern und deren Betriebssystemen, Datenbanken, Authentifizierungs- und Autorisierungssystemen, Netzwerksystemen und -infrastruktur sowie Telefon-PBX-Systemen. Skype for Business Server 2015 ist in zwei Versionen erhältlich: Standard Edition und Advanced Edition. Der Hauptunterschied liegt in der Unterstützung von Hochverfügbarkeitsfunktionen, die nur in der Advanced Edition enthalten sind. Um Hochverfügbarkeit zu implementieren, müssen mehrere Front-End-Server in einem Pool bereitgestellt und SQL-Server gespiegelt werden.

Eine Bereitstellung der Advanced Edition ermöglicht die Erstellung mehrerer Server mit unterschiedlichen Rollen.

Die primären Komponenten der Skype for Business 2015-Anwendung sind:

- Front-End-Server
- Edge-Server
- Director-Server
- Datenbank-(SQL-)Server

Front-End-Server:

In der Skype for Business-Anwendung ist der Front-End-Server der Kernserver in Ihrem Netzwerk. Er stellt die Links und Dienste für Benutzerauthentifizierung, Registrierung, Präsenz, Adressbuch, A/V-Konferenzen, Anwendungsfreigabe, Instant Messaging und Webkonferenzen bereit. Wenn Sie Skype for Business 2015 Enterprise Edition bereitstellen, besteht die Topologie typischerweise aus mindestens zwei Front-End-Servern, die in einem Front-End-Pool lastverteilt sind, mit einem Datenbankserver, der die SQL Server-Instanz hostet, die die Skype for Business-Datenbank enthält.

Edge-Server:

Die Bereitstellung von Edge-Servern für Skype for Business ist notwendig, wenn externe Benutzer, die nicht in Ihrem

internen Netzwerk der Organisation angemeldet sind, mit internen Benutzern interagieren können müssen. Diese externen Benutzer können authentifizierte und anonyme Remote-Benutzer, Verbundpartner oder andere mobile Clients sein.

Es gibt vier Arten von Rollen im Skype for Business Edge-Server:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Access Edge, der SIP-Verkehr verarbeitet und externe Verbindungen authentifiziert, Remote-Verbindungen und Verbundverbindungen ermöglicht
- Webkonferenzen, die Datenkonferenzpakete verarbeiten und externen Benutzern den Zugriff auf Skype for Business ermöglichen
- A/V-Konferenzen, die A/V-Konferenzpakete verarbeiten und Audio und Video, App-Sharing und Dateitransfer für externe Benutzer erweitern
- XMPP-Proxy, der XMPP-Pakete verarbeitet und XMPP-basierte Server oder Clients die Verbindung zu Skype for Business ermöglicht.

Director-Server:

Die Hauptfunktion des Director-Servers in Skype for Business 2015 besteht darin, Endpunkte zu authentifizieren und die Benutzer zu dem Pool zu „leiten“, der ihr Konto enthält. In Skype for Business 2015 ist der Director zwar eine vollständig dedizierte und spezifische Rolle auf einem eigenständigen Server, aber ein optionaler Server. Dies erleichtert die Sicherheit, indem es die Bereitstellung oder Entfernung der Konfigurationen vereinfacht.

Direktoren sind am nützlichsten, wenn mehrere Pools vorhanden sind, da sie einen einzigen Kontaktpunkt für die Authentifizierung von Endpunkten bieten. Auch für Remote-Benutzer dient ein Director als zusätzlicher Hop zwischen dem Edge-Pool und dem Front-End-Pool und bietet eine zusätzliche Schutzschicht gegen Angriffe.

Die folgende Abbildung stellt die Bereitstellung von Skype-Servern im Netzwerk schematisch dar:

Konfigurieren von NetScaler-Instanzen in einem Unternehmen

Die folgende Tabelle listet die IP-Adressen auf, die in der Beispielkonfiguration in den folgenden Anweisungen verwendet werden:

SKYPE FOR BUSINESS SERVER	VIRTUELLE IP-ADRESSE	SERVER-IP-ADRESSEN	NETSCALER-INSTANZ
Edge-Server	Externe VIP – 192.20.20.20	192.20.20.21; 192.20.20.22	10.102.29.141
	Interne VIP – 10.10.10.20	10.10.10.21; 10.10.10.22	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SKYPE FOR BUSINESS SERVER	VIRTUELLE IP-ADRESSE	SERVER-IP-ADRESSEN	NETSCALER-INSTANZ
Front-End-Server	10.10.10.10	10.10.10.11; 10.10.10.12	10.102.29.60
Director-Server	10.10.10.30	10.10.10.31; 10.10.10.32	10.102.29.93

So konfigurieren Sie Front-End-Server:

1. Navigieren Sie in NetScaler Console zu **Applications** > **Configuration**, und klicken Sie auf **Create New**. Die Seite **Choose StyleBook** zeigt alle StyleBooks an, die Ihnen in NetScaler Console zur Verfügung stehen. Scrollen Sie nach unten und wählen Sie **Microsoft Skype for Business 2015 StyleBook**. Das StyleBook wird als Benutzeroberflächenseite geöffnet, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
2. Geben Sie im Abschnitt **Edge Server** die folgenden virtuellen IP-Adressen (VIP) und IP-Adressen aller Edge-Server im Netzwerk ein.
    a. Externe VIP-Adresse und IP-Adressen für die Edge-Server, die für Access Edge, Webkonferenz-Edge und A/V-Edge verwendet werden.
    b. Interne VIP-Adresse und IP-Adressen für die Edge-Server, die mit dem internen Netzwerk verbunden werden.
    c. Zwei externe und zwei interne Edge-Server in Ihrem Netzwerk.
3. Geben Sie im Abschnitt **Front-End Server** die IP-Adresse des virtuellen Front-End-Servers (VIP) ein, der für die Skype for Business Front-End-Server erstellt werden soll. Geben Sie außerdem die IP-Adressen aller Skype for Business Front-End-Server im Netzwerk ein.
4. Geben Sie im Abschnitt **Director Server** die virtuelle IP-Adresse (VIP) für die Director-Server ein, die für die Skype for Business-Anwendung erstellt werden soll. Geben Sie außerdem die IP-Adressen aller Skype for Business Director-Server im Netzwerk ein. Erstellen Sie mindestens zwei Director-Server für Hochverfügbarkeit.
5. Der Abschnitt **Advanced Settings** listet alle Standardports auf, die auf den NetScaler-Instanzen für die drei Skype-Server konfiguriert sind.

Die folgende Tabelle enthält eine Liste aller Standardports und -protokolle:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BEZEICHNUNG	PORT	PROTOKOLL	BESCHREIBUNG
HTTP-Port	80	HTTP	Wird für die Kommunikation von Front-End-Servern zu den FQDNs der Webfarm verwendet, wenn HTTPS nicht verwendet wird.
HTTPS-Port	443	HTTPS	Wird für die Kommunikation von Front-End-Servern zu den FQDNs der Webfarm verwendet.
Auto Discover Interner Port	4443	HTTPS	HTTPS (vom Reverse Proxy) und HTTPS Front-End Inter-Pool-Kommunikation für die Auto Discover-Anmeldung.
RPC-Port	135	DCOM und Remote Procedure Call (RPC)	Wird für DCOM-basierte Operationen wie das Verschieben von Benutzern, die Benutzerreplikator-Synchronisierung und die Adressbuch-Synchronisierung verwendet.
SIP-Port	5061	TCP (TLS)	Wird von Front-End-Servern für die gesamte interne SIP-Kommunikation verwendet.
SIP-Fokus-Port	444	HTTPS, TCP	Wird für die HTTPS-Kommunikation zwischen dem Fokus

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BEZEICHNUNG	PORT	PROTOKOLL	BESCHREIBUNG
			(der Komponente, die den Skype-Konferenzstatus verwaltet) und den einzelnen Servern verwendet.
SIP-Gruppen-Port	5071	TCP	Wird für eingehende SIP-Anfragen für die Antwortgruppenanwendung verwendet.
SIP-AppSharing-Port	5065	TCP	Wird für eingehende SIP-Listening-Anfragen für die Anwendungsfreigabe verwendet.
SIP-Attendant-Port	5072	TCP	Wird für eingehende SIP-Anfragen für den Vermittler verwendet (d.h. für Einwahlkonferenzen).
`SIP Conf Announcement Port`	5073	TCP	Wird für eingehende SIP-Anfragen für den Konferenzansagedienst des Skype for Business-Servers verwendet (d.h. für Einwahlkonferenzen).
SIP CallPark-Port	5075	TCP	Wird für eingehende SIP-Anfragen für die CallPark-Anwendung verwendet.
SIP Call Admission-Port	448	TCP	Wird für die Anrufzulassungssteuerung durch den

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BEZEICHNUNG	PORT	PROTOKOLL	BESCHREIBUNG
			Bandbreitenrichtliniendienst des Skype for Business-Servers verwendet.
SIP-Anrufzulassung TURN-Port	5080	TCP	Wird für die Anrufzulassungssteuerung durch den Bandbreitenrichtliniendienst für Audio-/Video-Edge-TURN-Verkehr verwendet.
SIP-Audio-Testport	5076	TCP	Wird für eingehende SIP-Anfragen für den Audio-Testdienst verwendet.
HTTPS externer Port	443	HTTPS	Wird für externe Ports für die SIP-/TLS-Kommunikation für den Fernzugriff von Benutzern, den Zugriff auf interne Webkonferenzen und STUN/TCP-Ein- und Ausgangsmedienkommunikation für den Zugriff auf interne Medien- und A/V-Sitzungen verwendet.
HTTPS interner Port	443	HTTPS	Wird für interne Ports für SIP/TLS-Kommunikation für den Fernzugriff von Benutzern, den Zugriff auf interne Webkonferenzen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BEZEICHNUNG	PORT	PROTOKOLL	BESCHREIBUNG
			und STUN/TCP-Ein- und Ausgangsmedienkommunikation für den Zugriff auf interne Medien- und A/V-Sitzungen verwendet.
SIP Externer Remotezugriffsport	5061	TCP	Wird für externe Ports für SIP/MTLS-Kommunikation für den Fernzugriff von Benutzern oder die Föderation verwendet.
SIP Interner Remotezugriffsport	5061	TCP	Wird für interne Ports für SIP/MTLS-Kommunikation für den Fernzugriff von Benutzern oder die Föderation verwendet.
SIP Externer STUN UDP Port	3478	UDP	Wird für externe Ports für STUN/UDP-Ein- und Ausgangsmedienkommunikation verwendet.
SIP Interner STUN UDP Port	3478	UDP	Wird für interne Ports für STUN/UDP-Medienkommunikation (eingehend und ausgehend) verwendet.
SIP Interner IM-Port	5062		Wird für interne Ports zur SIP/MTLS-Authentifizierung von

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BEZEICHNUNG	PORT	PROTOKOLL	BESCHREIBUNG
			IM-Kommunikationen verwendet, die über die interne Firewall nach außen fließen.
HTTP-Port	80	TCP	Wird für die anfängliche Kommunikation von Direktoren zu den FQDNs der Webfarm verwendet.
HTTPS-Port	443	HTTPS	Wird für die Kommunikation von Direktoren zu den FQDNs der Webfarm verwendet.
Interner Auto-Discover-Port	4443	HTTPS	Wird für HTTPS (vom Reverse Proxy) und die Inter-Pool-Kommunikation des HTTPS Director für die Auto Discover-Anmeldung verwendet.
SIP Interner Port	5061	TCP	Wird für die interne Kommunikation zwischen Servern und für Client-Verbindungen verwendet.

1. Wählen Sie im Abschnitt **Zielinstanzen** die drei verschiedenen NetScaler-Instanzen aus, auf denen die drei Skype for Business-Server bereitgestellt werden sollen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich entdeckte NetScaler-Instanzen in NetScaler Console zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

2. Klicken Sie auf **Erstellen**, um die Konfiguration auf den ausgewählten NetScaler-Instanzen zu erstellen.

TIPP

Citrix empfiehlt, **Testlauf** auszuwählen, um die Konfigurationsobjekte zu überprüfen, die auf der Zielinstanz erstellt werden müssen, bevor Sie die eigentliche Konfiguration auf der Instanz ausführen.

Wenn die Konfiguration erfolgreich erstellt wurde, erstellt das StyleBook 25 virtuelle Lastausgleichsserver. Das heißt, für jeden Port wird ein virtueller Lastausgleichsserver zusammen mit einer Dienstgruppe definiert, und die Dienstgruppe wird an den virtuellen Lastausgleichsserver gebunden. Die Konfiguration fügt auch die Front-End-Server als Dienstgruppenmitglieder hinzu und bindet sie an die Dienstgruppe. Die Anzahl der erstellten Dienstgruppenmitglieder entspricht der Anzahl der erstellten Front-End-Server.

Die folgende Abbildung zeigt die auf jedem Server erstellten Objekte:

Microsoft Exchange StyleBook

Sie können das Microsoft Exchange 2016 StyleBook verwenden, um eine NetScaler-Konfiguration bereitzustellen, die eine Microsoft Exchange 2016 Unternehmensanwendung in Ihrem Netzwerk optimiert und sichert. Microsoft Exchange 2016 ist eine wichtige Unternehmensanwendung zur Bereitstellung von E-Mail-, persönlichen Informationsmanagement- und Messaging-Diensten für Ihre Mitarbeiter und andere Stakeholder.

NetScaler-Funktionen, die mit Microsoft Exchange StyleBook konfiguriert werden

Das Microsoft Exchange 2016 StyleBook aktiviert und konfiguriert die folgenden NetScaler-Funktionen für Microsoft Exchange 2016-Server:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Lastausgleich – Grundlegender Lastausgleich, der den Lastausgleich mehrerer Exchange-Server ermöglicht
- Content Switching – Content Switching, das den Zugriff über eine einzige IP-Adresse und die Umleitung von Abfragen an die richtigen virtuellen Lastausgleichsserver ermöglicht
- Rewrite – Leitet Benutzer auf sichere Seiten um
- SSL-Offload – Entlastet den NetScaler von der SSL-Verarbeitung, wodurch die Last auf dem Exchange-Server reduziert wird

Die folgende Abbildung stellt die Bereitstellung von Exchange-Servern im Netzwerk schematisch dar:

Voraussetzungen

- Für die zertifikatbasierte Authentifizierung müssen alle adressierbaren Hosts, die Teil der Netzwerkkonfiguration sind, auflösbare Domänennamen und nicht nur IP-Adressen haben.
- Stellen Sie sicher, dass die SIP-Ports auf dem Microsoft Exchange 2016-Server zugänglich sind.

Konfigurieren des Microsoft Exchange StyleBook

Konfigurieren Sie das Microsoft Exchange StyleBook in Ihrem Unternehmen, um die NetScaler-Konfiguration bereitzustellen.

So konfigurieren Sie die Microsoft Exchange-Anwendung

1. Navigieren Sie in NetScaler Console zu **Anwendungen > Konfiguration > StyleBooks**.
2. Suchen Sie nach **Microsoft Exchange 2016 StyleBook** und klicken Sie auf **Konfiguration erstellen**.

   Das StyleBook wird als Benutzeroberflächenformular angezeigt, in das Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

3. Geben Sie die Details für die folgenden Parameter ein:

   - **Exchange Application Name** – Name der Microsoft Exchange-Anwendung in Ihrem Netzwerk
   - **Exchange VIP** – Virtuelle IP-Adresse auf NetScaler, die Clientanfragen für die Microsoft Exchange-Anwendung empfängt

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Exchange Server IPs** – IP-Adressen aller Exchange-Server im Netzwerk.

  Wenn Sie weitere IP-Adressen hinzufügen möchten, klicken Sie auf das Pluszeichen (**+**). Normalerweise sind zwei Exchange-Server im Netzwerk konfiguriert.

4. Laden Sie im Abschnitt **Exchange-Zertifikate** Exchange-Zertifikate in NetScaler Console hoch. Geben Sie die Namen der Zertifikats- und Schlüsseldateien ein und laden Sie sie vom lokalen Speicher hoch. Sie können auch ein Kennwort für den privaten Schlüssel angeben, um die Schlüsseldatei zu verschlüsseln.

   HINWEIS

   Stellen Sie sicher, dass die Zertifikatsdateien im Format „.pem“ oder „.der“ vorliegen. NetScaler Console lehnt Dateien anderer Formate ab.

   Wenn Sie Details zum Ablauf des Zertifikats angeben oder erweiterte Einstellungen vornehmen möchten, wählen Sie **Erweiterte Zertifikatseinstellungen** aus.

5. Konfigurieren Sie im Abschnitt **Exchange Active Directory-Authentifizierungskonfiguration** die AD-Einstellungen durch Eingabe der Daten.

   - **Active Directory Authentifizierungs-VIP** – Die virtuelle IP-Adresse, die zum Erstellen und Konfigurieren des virtuellen AD (LDAP)-Servers auf einer NetScaler Appliance verwendet wird.
   - **Active Directory Server-IP** – Die IP-Adresse Ihres Active Directory-Domänencontrollers.
   - **Active Directory Basiszeichenfolge** – Die LDAP-Basiszeichenfolge in Active Directory. Zum Beispiel: CN=Users,DC=CTXNSSFB,DC=COM.
   - **Active Directory LDAP Bind Distinguished Name (DN)** – LDAP Bind Distinguished Name (DN) wird verwendet, um dieses Objekt an den LDAP-Server (AD) zu binden. Zum Beispiel: „cn=Administrator,cn=Users,dc=acme,dc=com“
   - **Active Directory LDAP Bind Distinguished Name (DN) Kennwort** – LDAP Bind Distinguished Name (DN) ist das Kennwort für die AD-Authentifizierung.
   - **Active Directory Benutzername-Attribut** – AD-Attribut für den Benutzernamen. Der NetScaler verwendet das LDAP-Attribut, um externe Active Directory-Server abzufragen. Zum Beispiel: „sAMAccountName“
   - **Active Directory Gruppenattributname** – Die auf dem LDAP-Server konfigurierten LDAP-Gruppenattributnamen. Zum Beispiel: „memberOf“ für das Gruppenattribut in LDAP.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Active Directory Unterattributname** – Die auf dem LDAP-Server konfigurierten LDAP-Unterattributnamen. Zum Beispiel: „cn“ für das Unterattribut in LDAP.
- **Active Directory Authentifizierungsdomäne** – Der für die Authentifizierung verwendete AD/LDAP-Domänenname. Zum Beispiel: ctxnssfb.com.

6. Wählen Sie im Abschnitt **Zielinstanzen** die NetScaler-Instanz aus, auf der diese Exchange-Konfiguration bereitgestellt werden soll.

   HINWEIS

   Wenn Sie die kürzlich erkannten NetScaler-Instanzen anzeigen möchten, klicken Sie auf das Aktualisierungssymbol.

7. Klicken Sie auf **Erstellen**, um die Konfigurationsdatei zu erstellen und die Konfiguration auf der ausgewählten NetScaler-Instanz auszuführen.

   Citrix empfiehlt, zuerst **Testlauf** auszuwählen, um die Konfigurationsobjekte zu überprüfen, die auf der Zielinstanz erstellt werden, bevor die eigentliche Konfiguration auf der Instanz ausgeführt wird.

Nachdem die Konfiguration erfolgreich erstellt wurde, hat das StyleBook einen Content Switching Virtual Server, fünf Load Balancing Virtual Server und eine LDAP-Richtlinie erstellt, die an einen LDAP-Authentifizierungs-Virtual Server gebunden ist. Außerdem wurden die entsprechenden Dienstgruppen erstellt und an die Load Balancing Virtual Server gebunden.

Microsoft SharePoint StyleBook

Microsoft SharePoint 2016 ist eine wichtige Unternehmensanwendung, die primär ein Dokumentenmanagement- und Speichersystem bereitstellt, das hochgradig konfigurierbar ist und von allen gängigen Browsern unterstützt wird.

Sie können das Microsoft SharePoint 2016 StyleBook verwenden, um eine NetScaler-Konfiguration bereitzustellen, die die Microsoft SharePoint 2016 Unternehmensanwendung in Ihrem Netzwerk optimiert und sichert.

Voraussetzungen

- Microsoft SharePoint 2016
- NetScaler Console, Version 12.0 und höher
- NetScaler, Version 10.5 und höher

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler-Funktionen, die vom Microsoft SharePoint 2016 StyleBook konfiguriert werden

Sie können das Microsoft SharePoint 2016 StyleBook verwenden, um die folgenden NetScaler-Funktionen für Microsoft SharePoint 2016 zu aktivieren und zu konfigurieren:

- Lastausgleich
- Content Switching
- Responder
- Rewrite
- Komprimierung
- Integriertes Caching

LASTAUSGLEICH

Der NetScaler-Lastausgleich verteilt Anfragen gleichmäßig auf die Backend-SharePoint-Server. Eine intelligente Überwachung der Backend-Server verhindert, dass Anfragen an fehlerhafte Server gesendet werden.

Das SharePoint StyleBook konfiguriert 12 virtuelle Lastausgleichsserver, die jeweils dem Lastausgleich von Anfragen für einen bestimmten Inhaltstyp gewidmet sind, z. B. Dokumente, Bilder, Audio, Video und andere Dateitypen.

NetScaler Console unterstützt jetzt den SSL-Modus der SharePoint-Anwendung durch die Konfiguration von SSL-basierten virtuellen LB-Servern. Stellen Sie sicher, dass Sie SSL als Frontend-Protokoll auswählen. Beachten Sie, dass der virtuelle Port standardmäßig auf 443 eingestellt ist.

INHALTSUMSCHALTUNG

Die Inhaltsumschaltungsfunktion wird verwendet, um Client-Anfragen basierend auf bestimmten Typen von angeforderten SharePoint-Inhalten (z. B. Dokumente, Bilder sowie Audio- oder Videodateien) auf mehrere virtuelle Lastausgleichsserver zu verteilen. Das Inhaltsumschaltungsmodul leitet eingehenden Datenverkehr an einen optimal passenden virtuellen Lastausgleichsserver weiter, der diesen Inhaltstyp verarbeiten kann. Sie können daher unterschiedliche Optimierungsrichtlinien auf verschiedene Arten von Datenverkehr anwenden. Beispielsweise möchten Sie möglicherweise andere Komprimierungs- oder Caching-Richtlinien für Videos als für Textdokumente verwenden.

RESPONDER

Die Responder-Funktionalität einer NetScaler-Instanz kann verwendet werden, um Benutzer nahtlos von HTTP zu HTTPS umzuleiten. Responder kann auch so konfiguriert werden, dass

© 1997–2026 Citrix Systems, Inc. All rights reserved.

angepasste Fehlerseiten bereitgestellt werden. Die Responder-Richtlinie bestimmt die Anfragen (Datenverkehr), auf die eine Aktion angewendet werden muss, und bindet jede Richtlinie an einen virtuellen Lastausgleichsserver. Das SharePoint StyleBook enthält eine Konfiguration, die Benutzer von HTTP- zu HTTPS-URLs umleitet.

REWRITE

Das Rewrite-Modul wird verwendet, um Anforderungs-/Antwort-Header, URLs oder Inhalte spontan zu ändern. Dieses Modul arbeitet inline mit der Datenverkehrsverarbeitung und kann daher den Datenverkehrsfluss je nach Anwendungsfall anpassen. Beispielsweise kann das Umschreiben den Zugriff auf den angeforderten Inhalt ermöglichen, ohne unnötige Details über den Server der Website preiszugeben.

Im SharePoint StyleBook wird die Rewrite-Funktion verwendet, um unnötige Header aus Benutzeranfragen zu entfernen.

KOMPRIMIERUNG

Die NetScaler-Komprimierungs-Engine identifiziert und komprimiert komprimierbare Inhalte. Dieser Prozess verbessert die Datenübertragungszeit und reduziert die Netzwerkanforderungen für Clients, während CPU-Zyklen auf SharePoint-Content-Servern eingespart werden. Eine NetScaler-Instanz kann sowohl statische als auch dynamisch generierte Daten komprimieren. Sie wendet den GZIP- oder den DEFLATE-Komprimierungsalgorithmus an, um überflüssige und sich wiederholende Informationen aus den Serverantworten zu entfernen und die ursprünglichen Informationen in einem kompakteren und effizienteren Format darzustellen. Die Fähigkeit des Client-Browsers, die Daten zu dekomprimieren, hängt davon ab, welchen Algorithmus oder welche Algorithmen er unterstützt: GZIP, DEFLATE oder beide.

Eine NetScaler-Instanz ist so konfiguriert, dass sie Text in HTML-, XML-, Reintext-, Cascading Style Sheet (CSS)- und Microsoft Office-Dokumenten komprimiert, jedoch keine Bilder im GIF- oder JPG-Format. Die Hauptvorteile von komprimiertem Datenverkehr sind reduzierte Bandbreitenkosten, eine Verringerung der WAN-Latenz und eine bessere Serverleistung.

INTEGRIERTES CACHING

Der NetScaler In-Memory-Cache kann SharePoint-Objekte speichern, um häufig angeforderte Inhalte schnell an Benutzer zu liefern. Zwischengespeicherte Inhalte umfassen heruntergeladene Dokumente sowie Audio-, Video- und Bilddateien.

Die folgende Abbildung stellt schematisch die Bereitstellung von SharePoint-Servern in einem Netzwerk dar, das von einer NetScaler-Instanz vorgelagert ist, auf der NetScaler Console verwendet wird, um eine SharePoint StyleBook-Konfiguration bereitzustellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bereitstellung von SharePoint StyleBook-Konfigurationen

Die folgende Aufgabe hilft Ihnen bei der Bereitstellung des Microsoft SharePoint 2016 StyleBook in Ihrem Unternehmensnetzwerk.

So stellen Sie das Microsoft SharePoint 2016 StyleBook bereit:

1. Navigieren Sie in NetScaler Console zu **Applications** > **Administration** > **Configuration**, und klicken Sie auf **Create New**.

   Die Seite **Choose StyleBook** zeigt alle StyleBooks an, die Ihnen in NetScaler Console zur Verfügung stehen.
2. Scrollen Sie nach unten und wählen Sie **Microsoft SharePoint 2016 StyleBook** aus.

   HINWEIS

   Navigieren Sie in NetScaler Console zu **Applications** > **Configurations** > **StyleBooks**. Scrollen Sie nach unten, um das **Microsoft SharePoint 2016 StyleBook** zu finden. Klicken Sie im Bereich **Microsoft SharePoint 2016 StyleBook** auf **Create Configuration**.

   Das StyleBook wird als Benutzeroberflächenformular geöffnet, in dem Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

   Geben Sie Werte für die folgenden Parameter ein:

   a. **SharePoint Application Name**. Name der SharePoint-Konfiguration, die in Ihrem Netzwerk bereitgestellt werden soll.
   b. **SharePoint Virtual IP**. Virtuelle IP-Adresse, unter der die NetScaler-Instanz Clientanfragen für die Microsoft SharePoint-Anwendung empfängt.
   c. **SharePoint virtueller Port**. Der TCP-Port, der von den Benutzern für den Zugriff auf die SharePoint-Anwendung verwendet werden soll
   d. **SharePoint Frontend-Protokoll**. Wählen Sie das SharePoint-Frontend-Protokoll aus der Dropdown-Liste aus. Die verfügbaren Optionen sind HTTP oder SSL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Wenn Sie SSL auswählen, stellen Sie sicher, dass der Parameter „Rewrite Configuration“ im Abschnitt „SharePoint Advanced Settings“ in diesem StyleBook aktiviert ist.

e. **SharePoint Server-IPs**. IP-Adressen aller SharePoint-Server im Netzwerk.

f. **SharePoint Server-Port**. TCP-Portnummer, die von den SharePoint-Servern verwendet wird. Standardmäßig ist dies 80. Sie können diesen Wert bei Bedarf bearbeiten, stellen Sie jedoch sicher, dass dieser Port auf Microsoft SharePoint 2016-Servern zugänglich ist.

3. Im Abschnitt **SSL-Zertifikateinstellungen** klicken Sie auf +, um den Namen des SSL-Zertifikats und den Zertifikatsschlüssel einzugeben und die entsprechenden Dateien aus Ihrem lokalen Speicherordner auszuwählen.

4. Klicken Sie optional auf **Erweiterte Zertifikateinstellungen**, um die Überwachung des Ablaufs von SSL-Zertifikaten zu aktivieren oder zu deaktivieren. Wenn Sie die Überwachung des Zertifikatsablaufs aktivieren, legen Sie die Anzahl der Tage fest, nach denen NetScaler Console einen Alarm ausgibt, wenn das Zertifikat abläuft. Sie haben auch die Möglichkeit, die OCSP-Prüfung als optionale oder obligatorische Funktion festzulegen.

5. Der Abschnitt **Erweiterte Einstellungen** von SharePoint ermöglicht es Ihnen, die NetScaler-Funktionen zu aktivieren, die auf den NetScaler-Instanzen konfiguriert werden. Während die Funktionen für Lastenausgleich und Inhaltsumschaltung standardmäßig auf den Instanzen konfiguriert sind, können Sie die anderen Funktionen, d. h. Responder-Konfiguration, Rewrite-Konfiguration, Komprimierungskonfiguration und integrierte Caching-Konfiguration, auswählen, die auf der Instanz konfiguriert werden sollen.

6. Klicken Sie auf **Zielinstanzen** und wählen Sie die NetScaler-Instanz aus, auf der diese SharePoint-Konfiguration bereitgestellt werden soll. Klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und auf der ausgewählten NetScaler-Instanz bereitzustellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich entdeckte NetScaler-Instanzen in NetScaler Console zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

HINWEIS

Citrix empfiehlt, dass Sie vor dem Ausführen der eigentlichen Konfiguration **Probelauf** auswählen, um die Konfigurationsobjekte zu überprüfen, die auf der Zielinstanz erstellt werden.

Wenn die Konfiguration erstellt und erfolgreich bereitgestellt wird, erstellt das SharePoint StyleBook einen virtuellen Content-Switching-Server und 12 virtuelle Lastausgleichsserver. Es erstellt auch Richtlinien und Dienstgruppen und bindet diese an die virtuellen Lastausgleichsserver. Welche Richtlinien erstellt werden, hängt von den im StyleBook ausgewählten Funktionen während der Erstellung des Konfigurationspakets ab.

Anzeigen der auf der NetScaler-Instanz definierten Objekte

Nachdem das Konfigurationspaket in der NetScaler Console erstellt wurde, können Sie alle auf der NetScaler-Instanz für das SharePoint StyleBook erstellten Objekte anzeigen. Navigieren Sie zu **Anwendungen** > **Administration** > **Konfiguration**, und klicken Sie auf **Erstellte Objekte anzeigen**. Die folgende Abbildung zeigt einige der erstellten Objekte mit den im Beispiel unter „Bereitstellen von SharePoint StyleBook-Konfigurationen aus der NetScaler Console“ angegebenen IP-Adressen.

Microsoft ADFS-Proxy-StyleBook

Der Microsoft ADFS-Proxy spielt eine wichtige Rolle, indem er Single Sign-On-Zugriff sowohl für interne föderationsfähige Ressourcen als auch für Cloud-Ressourcen ermöglicht. Ein solches Beispiel für Cloud-Ressourcen ist Office 365. Der Zweck des ADFS-Proxyservers besteht darin, Anfragen an ADFS-Server zu empfangen und weiterzuleiten, die nicht über das Internet zugänglich sind. Der ADFS-Proxy ist ein Reverse-Proxy und befindet sich typischerweise im Umkreisnetzwerk (DMZ) Ihrer Organisation. Der ADFS-Proxy spielt eine entscheidende Rolle bei der Konnektivität entfernter Benutzer und dem Anwendungszugriff.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler verfügt über die präzise Technologie, um sichere Konnektivität, Authentifizierung und die Handhabung föderierter Identitäten zu ermöglichen. Die Verwendung von NetScaler als ADFS-Proxy vermeidet die Notwendigkeit, eine zusätzliche Komponente in der DMZ bereitzustellen.

Das Microsoft ADFS-Proxy-StyleBook in NetScaler Console ermöglicht Ihnen die Konfiguration eines ADFS-Proxyservers auf einer NetScaler-Instanz.

Die folgende Abbildung zeigt die Bereitstellung einer NetScaler-Instanz als ADFS-Proxyserver in der Unternehmens-DMZ.

Vorteile der Verwendung von NetScaler als ADFS-Proxy

1. Erfüllt sowohl die Anforderungen an den Lastausgleich als auch an den ADFS-Proxy
2. Unterstützt sowohl interne als auch externe Benutzerzugriffsszenarien
3. Unterstützt umfangreiche Methoden zur Vorauthentifizierung
4. Bietet ein Single Sign-On-Erlebnis für Benutzer
5. Unterstützt sowohl aktive als auch passive Protokolle
    a. Beispiele für aktive Protokoll-Apps sind – Microsoft Outlook, Microsoft Skype for Business
    b. Beispiele für passive Protokoll-Apps sind – Microsoft Outlook Web App, Webbrowser
6. Gehärtetes Gerät für DMZ-basierte Bereitstellung
7. Bietet Mehrwert durch die Nutzung zusätzlicher NetScaler-Kernfunktionen
    a. Content Switching
    b. SSL-Offload
    c. Rewrite
    d. Sicherheit (NetScaler AAA)

Für aktive protokollbasierte Szenarien können Sie sich mit Office 365 verbinden und Ihre Anmeldeinformationen angeben. Das Microsoft Federation Gateway kontaktiert den ADFS-Dienst (über ADFS Proxy) im Namen des aktiven Protokollclients. Das Gateway übermittelt dann die Anmeldeinformationen mithilfe der Basisauthentifizierung (401). NetScaler übernimmt die Clientauthentifizierung vor dem Zugriff auf den ADFS-Dienst. Nach der Authentifizierung stellt der ADFS-Dienst dem Federation Gateway ein SAML-Token zur Verfügung. Das Federation Gateway wiederum übermittelt das Token an Office 365, um den Clientzugriff zu ermöglichen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Für passive Clients erstellt das ADFS Proxy StyleBook ein Benutzerkonto für die Kerberos Constrained Delegation (KCD). Das KCD-Konto ist für die Kerberos-SSO-Authentifizierung erforderlich, um eine Verbindung zu den ADFS-Servern herzustellen. Das StyleBook generiert außerdem eine LDAP-Richtlinie und eine Sitzungsrichtlinie. Diese Richtlinien werden später an den virtuellen NetScaler AAA-Server gebunden, der die Authentifizierung für passive Clients übernimmt.

Das StyleBook kann auch sicherstellen, dass die DNS-Server auf dem NetScaler für ADFS konfiguriert sind.

Der folgende Konfigurationsabschnitt beschreibt, wie NetScaler für die Handhabung sowohl aktiver als auch passiver protokollbasierter Clientauthentifizierung eingerichtet wird.

Konfigurationsdetails

Die folgende Tabelle listet die mindestens erforderlichen Softwareversionen auf, damit diese Integration erfolgreich bereitgestellt werden kann.

PRODUKT	MINDESTENS ERFORDERLICHE VERSION
NetScaler	11.0, Advanced/Premium-Lizenz

Die folgenden Anweisungen setzen voraus, dass Sie die entsprechenden externen und internen DNS-Einträge bereits erstellt haben.

Bereitstellen von Microsoft ADFS-Proxy-StyleBook-Konfigurationen über NetScaler Console

Die folgenden Anweisungen unterstützen Sie bei der Implementierung des Microsoft ADFS-Proxy-StyleBooks in Ihrem Unternehmensnetzwerk.

So stellen Sie das Microsoft ADFS-Proxy-StyleBook bereit

1. Navigieren Sie in NetScaler Console zu **Applications > Configuration > StyleBooks**. Die Seite **StyleBooks** zeigt alle StyleBooks an, die Ihnen in NetScaler Console zur Verfügung stehen.
2. Scrollen Sie nach unten und suchen Sie das **Microsoft ADFS-Proxy-StyleBook**. Klicken Sie auf **Create Configuration**. Das StyleBook wird als Benutzeroberfläche geöffnet, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
3. Geben Sie Werte für die folgenden Parameter ein:

    a. **ADFS Proxy Deployment Name**. Wählen Sie einen Namen für die in Ihrem Netzwerk bereitgestellte ADFS-Proxy-Konfiguration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **ADFS Servers FQDNs or IPs**. Geben Sie die IP-Adressen oder FQDNs (Domänennamen) aller ADFS-Server im Netzwerk ein.

c. **ADFS Proxy Public VIP IP**. Geben Sie die öffentliche virtuelle IP-Adresse auf dem NetScaler ein, der als ADFS-Proxyserver fungiert.

4. Geben Sie im Abschnitt **ADFS Proxy Certificates** die Details des SSL-Zertifikats und des Zertifikatsschlüssels ein.

   Dieses SSL-Zertifikat ist an alle auf der NetScaler-Instanz erstellten virtuellen Server gebunden.

   Wählen Sie die entsprechenden Dateien aus Ihrem lokalen Speicherordner aus. Sie können auch das Kennwort für den privaten Schlüssel eingeben, um verschlüsselte private Schlüssel im .pem-Format zu laden.

   Sie können auch das Kontrollkästchen **Erweiterte Zertifikateinstellungen** aktivieren. Hier können Sie Details wie den Benachrichtigungszeitraum für den Zertifikatsablauf eingeben und den Zertifikatsablaufmonitor aktivieren oder deaktivieren.

5. Optional können Sie das Kontrollkästchen **SSL-CA-Zertifikat** auswählen, wenn das SSL-Zertifikat ein öffentliches CA-Zertifikat erfordert, das auf NetScaler installiert werden muss. Stellen Sie sicher, dass Sie im Abschnitt **Erweiterte Zertifikateinstellungen** die Option „Ist ein CA-Zertifikat“ auswählen.

6. Aktivieren Sie die Authentifizierung für aktive und passive Clients. Geben Sie den DNS-Domänennamen ein, der in Active Directory für die Benutzerauthentifizierung verwendet wird. Sie können die Authentifizierung dann entweder für aktive oder passive Clients oder für beide konfigurieren.

7. Geben Sie die folgenden Details ein, um die Authentifizierung für aktive Clients zu aktivieren:

   HINWEIS

   Die Konfiguration der Unterstützung für aktive Clients ist optional.

   a. **ADFS Proxy Aktive Authentifizierungs-VIP**. Geben Sie die virtuelle IP-Adresse des virtuellen Authentifizierungsservers auf der NetScaler-Instanz ein, an die die aktiven Clients zur Authentifizierung umgeleitet werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **Dienstkontobenutzername**. Geben Sie den Dienstkontobenutzernamen ein, der von NetScaler verwendet wird, um Ihre Benutzer gegenüber dem Active Directory zu authentifizieren.

c. **Dienstkontopasswort**. Geben Sie das Passwort ein, das von NetScaler verwendet wird, um Ihre Benutzer gegenüber dem Active Directory zu authentifizieren.

8. Konfigurieren Sie die Authentifizierung für passive Clients, indem Sie die entsprechende Option aktivieren und die LDAP-Einstellungen konfigurieren.

HINWEIS

Die Konfiguration der Unterstützung für passive Clients ist optional.

Geben Sie die folgenden Details ein, um die Authentifizierung für passive Clients zu aktivieren:

a. **LDAP (Active Directory) Basis**. Geben Sie den Basisdomänennamen für die Domäne ein, in der sich die Benutzerkonten innerhalb des Active Directory (AD) befinden, um die Authentifizierung zu ermöglichen. Zum Beispiel, `dc=netscaler,dc=com`

b. **LDAP (Active Directory) Bind-DN**. Fügen Sie ein Domänenkonto hinzu (verwenden Sie eine E-Mail-Adresse zur Vereinfachung der Konfiguration), das über Berechtigungen zum Durchsuchen des AD-Baums verfügt. Zum Beispiel, cn=Manager,`dc=netscaler,dc=com`

c. **LDAP (Active Directory) Bind-DN-Passwort**. Geben Sie das Passwort des Domänenkontos zur Authentifizierung ein.

Einige weitere Felder, deren Werte Sie in diesem Abschnitt eingeben müssen, sind folgende:

d. **LDAP-Server (Active Directory) IP**. Geben Sie die IP-Adresse des Active Directory-Servers ein, damit die AD-Authentifizierung korrekt funktioniert.

e. **LDAP-Server-FQDN-Name**. Geben Sie den FQDN-Namen des Active Directory-Servers ein. Der FQDN-Name ist optional. Geben Sie die IP-Adresse wie in Schritt 1 oder den FQDN-Namen an.

f. **LDAP-Server Active Directory-Port**. Standardmäßig sind die TCP- und UDP-Ports für das LDAP-Protokoll 389, während der TCP-Port für Secure LDAP 636 ist.

g. **LDAP (Active Directory) Anmelde-Benutzername**. Geben Sie den Benutzernamen als „sAMAccountName“ ein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

h. **ADFS-Proxy Passive Authentifizierung VIP**. Geben Sie die IP-Adresse des virtuellen ADFS-Proxy-Servers für passive Clients ein.

HINWEIS

Die mit „*“ gekennzeichneten Felder sind Pflichtfelder.

9. Optional können Sie auch eine DNS-VIP für Ihre DNS-Server konfigurieren.

10. Klicken Sie auf **Zielinstanzen** und wählen Sie die NetScaler-Instanzen aus, um diese Microsoft ADFS-Proxy-Konfiguration bereitzustellen. Klicken Sie auf **Erstellen**, um die Konfiguration zu erstellen und auf den ausgewählten NetScaler-Instanzen bereitzustellen.

HINWEIS

Citrix empfiehlt, dass Sie vor dem Ausführen der eigentlichen Konfiguration **Probelauf** auswählen. Sie können zuerst die Konfigurationsobjekte anzeigen, die vom StyleBook auf den Ziel-NetScaler-Instanzen erstellt werden. Anschließend können Sie auf **Erstellen** klicken, um die Konfiguration auf den ausgewählten Instanzen bereitzustellen.

Erstellte Objekte

Es werden mehrere Konfigurationsobjekte erstellt, wenn die ADFS-Proxy-Konfiguration auf der NetScaler-Instanz bereitgestellt wird. Die folgende Abbildung zeigt die Liste der erstellten Objekte.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Oracle E-Business StyleBook

Oracle E-Business Suite ist die umfassendste Suite integrierter, globaler Geschäftsanwendungen. Diese Suite ermöglicht es Unternehmen, bessere Entscheidungen zu treffen, Kosten zu senken und die Leistung zu steigern, und besteht aus den folgenden Anwendungen.

- Enterprise Resource Planning (ERP)
- Kundenbeziehungsmanagement (CRM)
- Lieferkettenmanagement (SCM)

Diese Computeranwendungen werden entweder von Oracle entwickelt oder erworben. Das Oracle E-Business Suite 12.2 StyleBook ermöglicht es Ihnen, die Konfiguration auf den ausgewählten NetScaler-Instanzen bereitzustellen.

Dieses StyleBook erstellt eine Lastenausgleichskonfiguration, die einen virtuellen Lastenausgleichsserver, eine Dienstgruppe und eine Liste von Diensten umfasst. Es bindet auch die Dienste an die Dienstgruppe und die Dienstgruppe an den virtuellen Server. Sie können eine verschlüsselte Kommunikation wählen, indem Sie SSL auswählen und die SSL-Dateien und Schlüsseldateien von Ihrem lokalen System bereitstellen.

So erstellen Sie eine Konfiguration für Oracle E-Business Suite 12.2

1. Navigieren Sie in NetScaler Console zu **Applications > Configuration > StyleBooks**. Die Seite **StyleBooks** zeigt alle StyleBooks an, die in Ihrer NetScaler Console verfügbar sind. Scrollen Sie nach unten und wählen Sie **Oracle E-Business Suite 12.2**. Sie können auch die Suchoption verwenden, um das StyleBook zu suchen.
2. Klicken Sie im StyleBook-Panel auf **Create Configuration**.
3. Geben Sie den Namen der Lastenausgleichsanwendung und die virtuelle IP-Adresse im Abschnitt für die Lastenausgleichseinstellungen ein.
4. Wählen Sie das gewünschte Protokoll aus. Sie haben hier zwei Optionen – HTTP und HTTPS/SSL. Sie können auch die Portnummer eingeben.
5. Geben Sie die IP-Adressen aller Oracle E-Business Suite-Anwendungsserver im Netzwerk ein, die lastausgeglichen werden sollen. Klicken Sie auf **+**, um weitere Server-IP-Adressen hinzuzufügen.
6. Wählen Sie im Abschnitt **SSL Certificates Settings** die entsprechenden Dateien aus Ihrem lokalen Speicher aus. Sie können auch das Kontrollkästchen **Advanced Certificate Settings** aktivieren. Hier können Sie weitere Details wie den Benachrichtigungszeitraum für den

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zertifikatsablauf konfigurieren. Sie können auch den Zertifikatsablaufmonitor aktivieren oder deaktivieren.

Wählen Sie die Ziel-NetScaler-Instanz aus, auf der die Konfiguration erstellt werden soll, und klicken Sie auf **Create**.

TIPP

Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich entdeckte NetScaler-Instanzen in NetScaler Console zur Liste der verfügbaren Instanzen in diesem Fenster hinzuzufügen. Das Aktualisierungssymbol ist nur in NetScaler Console verfügbar.

Benutzerdefinierte StyleBooks erstellen und verwenden

Sie können Ihr eigenes StyleBook für Ihre Bereitstellung schreiben, es in NetScaler Console importieren und Konfigurationsobjekte erstellen. Sie können auch APIs verwenden, um Konfigurationen aus Ihren StyleBooks zu erstellen.

Dieses Dokument enthält die folgenden Informationen:

Bevor Sie beginnen

Bevor Sie mit der Erstellung von StyleBooks beginnen, stellen Sie sicher, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- NITRO API. Weitere Informationen finden Sie in der NITRO API-Dokumentation.
- YAML

StyleBook-Dateien verwenden das YAML-Format. Informationen zum YAML-Format finden Sie unter YAML-Syntax.

Im Folgenden finden Sie eine Liste von YAML-Richtlinien, die Sie beim Erstellen von StyleBooks beachten müssen:

- YAML unterscheidet Groß- und Kleinschreibung.
- YAML erfordert eine korrekte Einrückung.
- Verwenden Sie die Taste `<spacebar>`, um eine korrekte Einrückung zu erstellen. Verwenden Sie nicht die Taste `<tab>`. Die Verwendung der Taste `<tab>` führt zu einem Kompilierungsfehler beim Importieren Ihres StyleBooks in den MA Service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Verwenden Sie keine Zeichenfolgen in Anführungszeichen. Fügen Sie die Zeichenfolge nur dann in Anführungszeichen ein, wenn eine Zeichenfolge Satzzeichen (Bindestriche, Doppelpunkte usw.) enthält. Wenn Sie eine Zahl als Zeichenfolge interpretieren möchten, schließen Sie die Zahl entweder in Anführungszeichen ein oder verwenden Sie die integrierte Funktion str() von StyleBooks.
- Literale wie YES/Yes/yes/Y/y/NO/no/No/n/N, ON/On/on/OFF/Off/off und TRUE/true/truthy/ FALSE/False/false/falsely werden als Booleans betrachtet und entsprechen jeweils true und false. Um sie als Zeichenfolgen zu interpretieren, schließen Sie sie in Anführungszeichen ein. Zum Beispiel:
  - "YES"
  - "Nein"
  - "Wahr"
  - "Falsch" und so weiter.

HINWEIS

Bevor Sie Ihre StyleBook-Datei in NetScaler Console importieren, wird empfohlen, zu überprüfen, ob Ihre Datei dem YAML-Format entspricht. Citrix empfiehlt, den integrierten YAML-Validator in StyleBooks zu verwenden, um den YAML-Inhalt zu validieren und zu importieren.

Weitere Informationen finden Sie unter NITRO APIs-Dokumentation.

Aufbau eines StyleBooks

Das Schreiben von StyleBooks erfordert, dass Sie die Grammatik, Syntax und Struktur von StyleBooks verstehen. Ein typisches StyleBook hat die folgenden Abschnitte:

- **Header**: In diesem Abschnitt können Sie die Identität eines StyleBooks definieren und beschreiben, was es tut. Dies ist ein obligatorischer Abschnitt.
- **StyleBooks importieren**: In diesem Abschnitt können Sie deklarieren, auf welches andere StyleBook Sie von Ihrem aktuellen StyleBook aus verweisen möchten. Das Importieren von NetScaler NITRO-Konfigurations-StyleBooks oder anderen StyleBooks ist erforderlich, um ein StyleBook zu schreiben. Dies ist ein obligatorischer Abschnitt.
- **Parameter**: In diesem Abschnitt können Sie die Parameter definieren, die Sie in Ihrem StyleBook zum Erstellen einer Konfiguration benötigen. Er beschreibt die Eingabe, die Ihr StyleBook entgegennimmt. Dies ist ein optionaler Abschnitt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Komponenten**: In diesem Abschnitt können Sie die Entitäten (Konfigurationsobjekte) definieren, die vom StyleBook für eine bestimmte Konfiguration erstellt werden. Dieser Abschnitt gilt als Kern eines StyleBooks. Komponenten verwenden im Allgemeinen die im Parameterabschnitt bereitgestellten Eingaben, um die vom StyleBook generierte Konfiguration anzupassen. Dies ist ein optionaler Abschnitt.Ein StyleBook kann einen Parameterabschnitt, einen Komponentenabschnitt oder beides haben. Ein StyleBook, das nur den Parameterabschnitt enthält, ist nützlich, um eine Liste von Parametern zu definieren, die von anderen StyleBooks verwendet werden können. Dies fördert die Wiederverwendbarkeit von Parametergruppen über eine Reihe von StyleBooks hinweg. Ein StyleBook, das nur einen Komponentenabschnitt enthält, kann verwendet werden, wenn Sie die Werte für Attribute im StyleBook angeben möchten, anstatt Parameter zur Aufnahme von Benutzereingaben zu definieren.
- **Ausgaben**: Während der Parameterabschnitt die Eingaben des StyleBooks definiert, definiert dieser optionale Abschnitt seine Ausgaben. In diesem optionalen Ausgabeabschnitt können Sie die Komponenten angeben, die Sie Benutzern, die eine Konfiguration aus diesem StyleBook erstellen, und anderen StyleBooks, die dieses StyleBook importieren, zugänglich machen möchten. Benutzer und importierende StyleBooks können dann auf die Eigenschaften der exponierten Komponenten verweisen.
- **Operationen**: Ein StyleBook kann einen optionalen Abschnitt enthalten, um Analytics in NetScaler Console für jeden virtuellen Server zu aktivieren, der Teil des StyleBooks ist.

Die folgende Abbildung zeigt einen einfachen Überblick über ein StyleBook.

Gliederung eines StyleBooks(/en-us/netscaler-console-service/media/stylebook-outline.png)

Die folgenden Beispiele helfen Ihnen, die Grammatik und Struktur eines StyleBooks kennenzulernen und zu erfahren, wie Sie StyleBooks mit zunehmendem Komplexitätsgrad schreiben.

- StyleBook zum Erstellen eines virtuellen Lastausgleichsservers
- StyleBook zum Erstellen einer grundlegenden Lastausgleichskonfiguration
- Ein zusammengesetztes StyleBook erstellen
- Ihr StyleBook mithilfe von GUI-Attributen anpassen

Konfigurationspaket erstellen und bearbeiten

In NetScaler Console können Sie ein Konfigurationspaket aus einem StyleBook erstellen. Das Konfigurationspaket ist an das StyleBook gebunden, aus dem es erstellt wurde. Alle Aktualisierungen des Konfigurationspakets erfolgen über das StyleBook, an das es gebunden ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfigurationspaket erstellen

Gehen Sie wie folgt vor, um ein Konfigurationspaket aus einem StyleBook zu erstellen:

1. Navigieren Sie zu **Applications > Configuration > Config Packs**.
2. Klicken Sie auf **Add**.
3. Wählen Sie unter **Choose StyleBooks** die erforderlichen StyleBooks aus, aus denen Sie ein Konfigurationspaket erstellen möchten.

   Diese Seite kategorisiert StyleBooks in Standard-, Unternehmens- und benutzerdefinierte StyleBooks. Wählen Sie die entsprechenden Registerkarten aus, um die erforderlichen StyleBooks zu finden.
4. Optional können Sie einen eindeutigen **Config Key** für Ihr Konfigurationspaket angeben. Dieser Schlüssel wird als **Display Key** für dieses Konfigurationspaket angezeigt.

   - Wenn Sie einen bereits vorhandenen **Config Key** angeben, kann NetScaler Console das Konfigurationspaket nicht erstellen.
   - Wenn Sie keinen **Config Key** angeben, weist NetScaler Console automatisch die **Configpack ID** zu. Dieser Wert wird jedoch nicht als **Display Key** angezeigt.
   - Wenn Sie keinen **Config Key** angeben und einer der StyleBook-Parameter das `key`-Attribut festgelegt hat, wird dieser Parameterwert als **Display Key** angezeigt. Weitere Informationen finden Sie unter Parameters.
5. Geben Sie die erforderlichen Details wie Anwendungsname, IP-Adresse, Port oder Protokolltyp an.

   Die GUI-Felder unterscheiden sich von StyleBook zu StyleBook.
6. Wählen Sie unter **Target Instances** Instanzen oder Instanzgruppen aus, in denen Sie die Konfiguration ausführen möchten.

   HINWEIS:

   Sie können die Konfiguration auf mehr als einem NetScaler bereitstellen, indem Sie so viele Zielinstanzen angeben, wie benötigt werden.
7. Klicken Sie auf **Testlauf**.

   Die Seite **Objekte** zeigt die Objekte an, die auf den NetScaler-Instanzen erstellt, geändert oder entfernt werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Klicken Sie auf **Erstellen**

   Das Konfigurationspaket wird auf der Seite **StyleBook > Konfigurationen** angezeigt.

Wenn Sie die vorhandenen Konfigurationspakete bearbeiten möchten, wählen Sie das Konfigurationspaket aus und klicken Sie auf **Bearbeiten**.

Konfigurationen wiederverwenden, die außerhalb von StyleBooks erstellt wurden, und Konfigurationen zwischen Konfigurationspaketen teilen

Manchmal haben Sie möglicherweise NetScaler®-Konfigurationen außerhalb von Stylebooks erstellt, sei es aufgrund spezifischer betrieblicher Anforderungen oder älterer Setups. Sie können diese bereits vorhandenen Konfigurationen nun als Teil von Stylebook-Konfigurationspaketen integrieren und verwalten, was eine flexiblere und zentralisierte Verwaltung ermöglicht.

Zum Beispiel, vor dieser Funktion, wenn NetScaler bereits mit einem SSL-Profil konfiguriert ist und der Konfigurationspaketvorgang von StyleBook versucht, ein SSL-Profil mit demselben Namen zu erstellen, wäre der Konfigurationspaketvorgang mit dem Fehler "Ressource existiert bereits" fehlgeschlagen. Jetzt, da diese Funktion aktiviert ist, ist der Konfigurationspaketvorgang erfolgreich und das vorhandene SSL-Profil mit demselben Namen kann im neuen Konfigurationspaket wiederverwendet werden.

Ähnlich können auch Szenarien auftreten, in denen Ressourcen wie Netzwerkeinstellungen, Sicherheitsrichtlinien oder Teile von Anwendungskonfigurationen über mehrere Anwendungen oder Konfigurationen hinweg benötigt werden. Diese Funktion ermöglicht es Ihnen, die Konfigurationen über mehrere Konfigurationspakete hinweg zu teilen.

Um diese Funktion zu aktivieren, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Anwendungen > Konfiguration > Stylebooks**.
2. Wählen Sie auf der Seite **Stylebooks** das Stylebook aus, das Sie zum Erstellen eines neuen Konfigurationspakets verwenden werden, oder dasjenige, das mit dem Konfigurationspaket verknüpft ist, das Sie bearbeiten.
3. Klicken Sie unter **Aktion auswählen** auf **Einstellungen konfigurieren**.

4. Passen Sie die Einstellungen an, indem Sie eine oder beide der folgenden Optionen auswählen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Um die Wiederverwendung vorhandener Ressourcen auf dem NetScaler beim Erstellen von Konfigurationen zu ermöglichen, wählen Sie die Option **Wiederverwendung vorhandener Ressourcen auf dem NetScaler beim Erstellen von Konfiguration(en) zulassen**.
- Um wiederverwendete Ressourcen auf dem NetScaler beim Löschen von Konfigurationen beizubehalten, wählen Sie die Option **Wiederverwendete Ressourcen auf dem NetScaler beim Löschen von Konfiguration(en) beibehalten?**. Diese Option behält die ursprünglich außerhalb von Stylebooks auf dem NetScaler erstellten Ressourcen bei, selbst wenn das letzte Konfigurationspaket, das auf sie verweist, gelöscht wird, wodurch deren fortgesetzte Verfügbarkeit sichergestellt wird.

5. Klicken Sie auf **OK**.

Ändern des StyleBooks eines Konfigurationspakets

Manchmal müssen Sie das StyleBook aktualisieren, um Funktionen hinzuzufügen oder ein Problem zu beheben. Wenn Sie bereits Konfigurationspakete mit dem alten StyleBook erstellt haben, möchten Sie diese möglicherweise aktualisieren, um das neue aktualisierte StyleBook zu verwenden. Um ein neues StyleBook zu verwenden, ändern Sie das vorhandene StyleBook des Konfigurationspakets.

Betrachten Sie ein Beispiel-StyleBook **example-lb**, das eine grundlegende Load-Balancer-Konfiguration auf einer NetScaler-Instanz bereitstellt. Und Sie erstellen ein Konfigurationspaket CP1 aus diesem StyleBook.

Um Monitore mit der grundlegenden Load-Balancer-Konfiguration zu konfigurieren, benötigen Sie ein neues StyleBook. Erstellen Sie dazu ein **example-lb-mon** StyleBook, das die Möglichkeit beinhaltet, Monitore zusammen mit der grundlegenden Load-Balancer-Konfiguration zu konfigurieren.

Nachdem Sie ein StyleBook erstellt haben, aktualisieren Sie das vorhandene Konfigurationspaket CP1, um Monitore hinzuzufügen. Um das Konfigurationspaket zu aktualisieren, gehen Sie wie folgt vor:

1. Navigieren Sie zu **Applications > Configuration > Config Packs**.
2. Wählen Sie das Konfigurationspaket aus, für das Sie das StyleBook ändern möchten.

   Wählen Sie in diesem Beispiel CP1 aus der Liste aus.
3. Klicken Sie auf **Change StyleBook**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Wählen Sie das gewünschte StyleBook aus der Liste aus. Klicken Sie dann auf **Auswahl speichern**.
5. Klicken Sie auf **Ändern**.

   Wählen Sie in diesem Beispiel **example-lb-mon** aus der Liste aus.

   Wenn Sie das StyleBook eines Konfigurationspakets ändern, kann die Struktur der Parameter im neuen StyleBook von der des vorhandenen StyleBooks abweichen. Wenn die Parameterstruktur der des vorherigen StyleBooks ähnelt, werden die Werte der Parameter automatisch in den entsprechenden Feldern beibehalten. Andernfalls werden nur Parameter übertragen, die zwischen den beiden StyleBooks dieselbe Struktur aufweisen. Zum Beispiel derselbe Parametername, Typ, Parameter-Parent und mehr.

   HINWEIS:

   Die Seite **StyleBook-Kompatibilität** zeigt die Unterschiede in den Parametern an. Diese Seite hilft Ihnen zu entscheiden, ob Sie das StyleBook ändern oder das vorhandene StyleBook beibehalten möchten. Wenn Sie das StyleBook ändern möchten, überprüfen Sie die Änderungen und klicken Sie dann auf **Weiter**.

   Wenn im neuen StyleBook neue Parameter hinzugefügt werden, müssen Sie nach dem Ändern des StyleBooks die Werte für solche Parameter manuell angeben.

   In diesem Beispiel sind die Parameter, die auf der Konfigurationsseite für das StyleBook **example-lb** angezeigt werden, wie folgt:

   Die Parameter, die auf der Konfigurationsseite für das neue StyleBook **example-lb-mon** angezeigt werden, sind wie folgt:

   In diesem Fall behält das StyleBook die älteren Werte für die grundlegende Lastausgleichskonfiguration bei, da das neue StyleBook keine vorhandenen Parameter geändert hat. Es fügt nur die neuen Parameter hinzu. Für Monitorparameter geben Sie die erforderlichen Werte manuell an.
6. Überprüfen Sie unter **Zielinstanzen** die ausgewählten Instanzen und aktualisieren Sie die Liste bei Bedarf.
7. Klicken Sie auf **Probelauf**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Seite **Objekte** zeigt die Objekte an, die in den NetScaler-Instanzen erstellt, geändert oder entfernt werden.

8. Klicken Sie auf **OK**.

   Auf der Seite **StyleBook > Configurations** zeigt die Spalte **StyleBook Name** den neuen StyleBook-Namen für das ausgewählte Konfigurationspaket an. In diesem Fall wird **example-lb-mon** angezeigt.

Ändern des StyleBooks mit mehreren Konfigurationspaketen

Wenn Sie ein vorhandenes StyleBook ändern möchten, das mehrere Konfigurationspakete enthält, gehen Sie wie folgt vor:

1. Importieren Sie ein neues StyleBook in die NetScaler Console.

   Typischerweise hat das neue StyleBook den gleichen Namen und Namespace mit einer höheren Version als das vorhandene StyleBook. Sie können diesen Schritt jedoch überspringen, wenn Name, Namespace oder Version unterschiedlich sind.
2. Ändern Sie das StyleBook für die Konfigurationspakete, die dem vorhandenen StyleBook zugeordnet sind.

   Sie können **Change StyleBook** nur auswählen, wenn die ausgewählten Konfigurationspakete demselben StyleBook zugeordnet sind.

   Für die ausgewählten Konfigurationspakete ändert die NetScaler Console das StyleBook erfolgreich, wenn die folgenden Bedingungen erfüllt sind:

   - Alle Konfigurationsparameter des vorhandenen StyleBooks müssen im ausgewählten StyleBook vorhanden sein.
   - Die neuen Parameter aus dem ausgewählten StyleBook sind optional.

   Um den Fortschritt der ausgewählten Konfigurationspakete anzuzeigen, wählen Sie auf der Seite **Configurations** die Option **Configurations in Progress/Failed** aus.
3. Entfernen Sie das alte StyleBook aus der NetScaler Console, sobald alle Konfigurationspakete an das neue StyleBook gebunden sind.

Konfigurationspakete exportieren oder importieren

Sie können ein Konfigurationspaket wie StyleBooks exportieren oder importieren. Mit dieser Funktion können Sie die StyleBook-Konfiguration problemlos für einen anderen NetScaler Console-Server freigeben. Wenn Sie ein Konfigurationspaket exportieren, wird ein `tgz`- oder

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`zip`-Bundle auf Ihren lokalen Computer heruntergeladen. Dieses Bundle enthält eine JSON-Datei mit allen in einem Konfigurationspaket definierten Parametern.

Konfiguration exportieren

Gehen Sie wie folgt vor, um ein Konfigurationspaket zu exportieren:

1. Navigieren Sie zu **Applications > Configuration > Config Packs**.
2. Wählen Sie ein Konfigurationspaket aus, das Sie exportieren möchten.
3. Wählen Sie unter **Aktion auswählen** die Option **Konfiguration exportieren**.

4. Geben Sie im Bereich **Konfiguration exportieren** Folgendes an:

   - **Informationen zu Zielinstanzen, auf denen die Konfiguration bereitgestellt wird**: Wählen Sie diese Option, um die Informationen der Zielinstanzen in das Exportpaket aufzunehmen.
   - **StyleBook, das der Konfiguration zugeordnet ist**: Wählen Sie diese Option, um das StyleBook in das Exportpaket aufzunehmen.
   - **Passphrase zum Schutz der Exportkonfigurationsdaten**: Geben Sie eine Passphrase ein, um das Exportpaket zu verschlüsseln. Diese Passphrase schützt die sensiblen Daten eines Konfigurationspakets.
   - **Dateityp komprimieren**: Wählen Sie entweder den Dateityp **ZIP** oder **TGZ**.

5. Klicken Sie auf **Exportieren**.

   Speichern Sie das Exportpaket auf Ihrem lokalen Computer.

Konfiguration importieren

Sie können ein Konfigurationspaket von Ihrem lokalen Computer auf einen anderen NetScaler Console-Server importieren. Gehen Sie wie folgt vor, um ein Konfigurationspaket zu importieren:

1. Navigieren Sie zu **Applications > Configuration > Config Packs**.
2. Wählen Sie **Import Configuration**.
3. Wählen Sie das Importdateibündel von Ihrem Computer aus.
4. Verwenden Sie die Passphrase, die Sie beim Export angegeben haben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Optional: Wählen Sie unter „Erweiterte Optionen“ **Nur die Erstellung einer neuen Konfiguration zulassen, wenn alle Konfigurationsobjekte bereits auf NetScaler vorhanden sind**.

   Diese Option ändert die Objekte nicht, die bereits auf der NetScaler-Instanz erstellt wurden.

   Angenommen, Sie haben dieselbe NetScaler-Instanz in zwei NetScaler Console-Servern hinzugefügt. Und Sie möchten ein Konfigurationspaket von einem NetScaler Console-Server auf einen anderen Server migrieren. Verwenden Sie diese Option, um ein Konfigurationspaket zu importieren, ohne dessen Konfigurationsobjekte auf einer NetScaler-Instanz zu ändern.

   WICHTIG:

   Um diese Option zu verwenden, stellen Sie sicher, dass das angegebene Konfigurationspaket die Informationen zu den Zielinstanzen enthält. Siehe, Konfiguration exportieren.

   Diese Option migriert die Konfiguration nur, wenn alle Objekte auf der Zielinstanz vorhanden sind.

6. Klicken Sie auf **Importieren**.

Wenn Sie ein Konfigurationspaket importieren, überprüft die NetScaler Console Folgendes:

- **Zugehöriges StyleBook**: Wenn das zugehörige StyleBook nicht in der NetScaler Console vorhanden ist, importiert es das StyleBook zusammen mit dem Konfigurationspaket.
- **Zielinstanzen**: Prüft auf Zielinstanzen und stellt die Konfiguration auf den angegebenen Zielinstanzen bereit. Wenn die genannten NetScaler-Instanzen in der NetScaler Console nicht vorhanden sind, wird das Konfigurationspaket ohne Zielinstanzen importiert.
- **Quell-NetScaler Console**: Wenn Sie ein Konfigurationspaket auf demselben NetScaler Console-Server importieren, aktualisiert das ausgewählte Bundle das vorhandene Konfigurationspaket.

Konfigurationspaket als Entwurf speichern

Die Option **Als Entwurf speichern** in Konfigurationspaketen ermöglicht es Ihnen, Ihre Konfigurationsänderungen als Entwürfe zu speichern. Diese Funktion speichert die Änderungen, ohne sie sofort auf einer NetScaler-Instanz bereitzustellen.

Gehen Sie wie folgt vor, um ein Konfigurationspaket als Entwurf zu speichern:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie zu **Applications > Configuration > Config Packs**.
2. Klicken Sie auf der Seite **Configurations** auf **Add**.
3. Wählen Sie Ihr gewünschtes Stylebook aus und klicken Sie auf **Select**.
4. Klicken Sie auf der Seite **Create Configuration** auf **Save as Draft**.

Sobald das Konfigurationspaket als Entwurf gespeichert ist, werden Ihre Konfigurationsänderungen nicht direkt auf der NetScaler-Instanz bereitgestellt. Stattdessen werden die Konfigurationspakete als Entwürfe auf der Registerkarte **Draft Configurations** unter **Pending Configurations** gespeichert.

Wählen Sie auf der Registerkarte **Draft Configurations** das Konfigurationspaket aus, um die folgenden Vorgänge auszuführen:

- Bearbeiten Sie die Konfiguration des Entwurfs.
- Stellen Sie die Konfiguration auf einer NetScaler-Instanz bereit.
- Löschen Sie den Entwurf.

Sie können auch planen, wann Ihre gespeicherten Entwürfe bereitgestellt werden sollen.

Weitere Informationen finden Sie unter Erstellen eines Zeitplans für ein Konfigurationspaket.

Erstellen eines Zeitplans für ein Konfigurationspaket

Wenn Sie ein Konfigurationspaket erstellen, wird es standardmäßig automatisch auf einer NetScaler-Instanz bereitgestellt. Mit dieser Funktion können Sie die Bereitstellung von Konfigurationspaketen planen.

Führen Sie die folgenden Schritte aus, um einen Zeitplan für ein Konfigurationspaket zu erstellen:

1. Navigieren Sie zu **Applications > Configuration > Config Packs**.
2. Klicken Sie auf der Seite **Configurations** auf **Add**.
3. Wählen Sie das StyleBook aus und klicken Sie auf **Select**.
4. Wählen Sie auf der Seite **Create Configuration** unter **Execution** in der Liste **Execution Mode** die Option **Later** aus.
5. Wählen Sie die gewünschte Uhrzeit und das Datum für die Planung aus und klicken Sie auf **Submit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alle geplanten Konfigurationen werden auf der Registerkarte **Scheduled configurations** unter **Pending Configurations** gespeichert. Sie können den erstellten Zeitplan auswählen, um die Konfigurationsparameter zu bearbeiten, den Zeitplan bereitzustellen oder abzubrechen.

HINWEIS:

Die Bereitstellung eines geplanten Konfigurationspakets bricht den Zeitplan ab und führt die Konfiguration sofort aus.

Für ein bereitgestelltes Konfigurationspaket

Sie können auch einen Zeitplan erstellen, um ein bereitgestelltes Konfigurationspaket zu bearbeiten und zu löschen.

BEARBEITUNGSVORGANG FÜR EIN KONFIGURATIONSPAKET PLANEN

Um einen Zeitplan für die Bearbeitung des bereitgestellten Konfigurationspakets zu erstellen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Anwendungen > Konfiguration > Konfigurationspakete**.
2. Auf der Seite **Konfigurationen** wählen Sie ein StyleBook aus und klicken Sie auf **Bearbeiten**.
3. Auf der Seite **Konfiguration bearbeiten** bearbeiten Sie das Konfigurationspaket.
4. Wählen Sie in der Liste **Ausführungsmodus** die Option **Später** aus.
5. Wählen Sie die gewünschte Uhrzeit und das Datum für die Planung aus und klicken Sie auf **Senden**.

LÖSCHVORGANG FÜR EIN KONFIGURATIONSPAKET PLANEN

Um einen Zeitplan für das Löschen des bereitgestellten Konfigurationspakets zu erstellen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Anwendungen > Konfiguration > Konfigurationspakete**.
2. Auf der Seite **Konfigurationen** wählen Sie ein StyleBook aus und klicken Sie auf **Löschen**.
3. Wählen Sie in der Liste **Ausführungsmodus** die Option **Später** aus.
4. Wählen Sie die gewünschte Uhrzeit und das Datum für die Planung aus und klicken Sie auf **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Eine Zielinstanz von einem Konfigurationspaket trennen

Um eine Zielinstanz von einem Konfigurationspaket zu trennen, gehen Sie wie folgt vor:

1. Navigieren Sie zu **Applications > Configuration > Config Packs**.
2. Wählen Sie das Konfigurationspaket mit einer Zielinstanz aus, die Sie entfernen möchten.
3. Wählen Sie unter **Select Action** die Option **Detach Targets**.
4. Wählen Sie im Bereich **Detach Targets** die Zielinstanz aus, die Sie aus dem Konfigurationspaket entfernen möchten.

5. Klicken Sie auf **OK**.

Es wird eine Meldung angezeigt, die die Erstellung eines doppelten Konfigurationspakets bestätigt, wobei die Zielinstanz nun entfernt wurde.

Erstellen Sie Ihre StyleBooks

Der vollständige Inhalt des **example-lb** StyleBook wird Ihnen als Referenz wie folgt zur Verfügung gestellt:

```
name: example-lb

namespace: examples.stylebooks

version: "1.0"

display-name: Basic Load Balancer App

description: This is an example StyleBook that creates a load balancer
application

schema-version: "1.0"

import-stylebooks:

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters-default-sources:

  - stlb::lb

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters
```

Der vollständige Inhalt des **example-lb-mon** StyleBook wird Ihnen als Referenz wie folgt zur Verfügung gestellt:

```
name: example-lb-mon

namespace: examples.stylebooks

version: "1.0"

description: This is an example StyleBook that creates a load balancer
application with monitors

display-name: Basic Load Balancer App with Monitors

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: "1.0"
parameters-default-sources:
  - stlb::lb
parameters:
  -
    name: monitors
    label: "List of Monitors"
    description: "List of Monitors to monitor Application Servers"
    type: cmtypes::monitor[]
substitutions:
  mon-name(appname, monname): $appname + "-mon-" + $monname
components:
  -
    name: lb-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters

  -

    name: monitors-comp

    type: cmtypes::monitor

    condition: $parameters.monitors

    repeat: $parameters.monitors

    repeat-item: mon

    repeat-index: ndx

    description: Builds a list of NetScaler monitor objects and binds them
to the servicegroup of this LB config

    properties-default-sources:

      - $mon

    properties:

        monitorname: $substitutions.mon-name($parameters.lb-appname,
$mon.monitorname)

    components:

      -

        name: monitor-svcg-binding-comp

        condition:  $parameters.svc-servers
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        type: ns::servicegroup_lbmonitor_binding

        properties:

          servicegroupname: $components.lb-
comp.outputs.servicegroup.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

StyleBook zum Erstellen eines Lastausgleichs-Virtual-Servers

In diesem Beispiel entwerfen Sie ein grundlegendes StyleBook, das einen Lastausgleichs-Virtual-Server vom HTTP-Protokolltyp erstellt und auf Port 80 lauscht. Die Parameter für den Namen des virtuellen Servers, die IP-Adresse und die Lastausgleichsmethode akzeptieren benutzerdefinierte Werte, das heißt, sie sind die Parameter des StyleBooks.

Header

Die ersten sechs Zeilen eines StyleBooks bilden den Header-Abschnitt. In diesem Beispiel ist der Header-Abschnitt wie folgt geschrieben:

```
name: lb-vserver

namespace: com.example.stylebook

version: "1.0"

display-name: Load Balancing Virtual Server (HTTP)

description: "This stylebook defines a very simple load balancing HTTP
virtual server configuration"

schema-version: "1.0"
```

Der Header-Abschnitt enthält die folgenden Details:

- **name**: Ein Name für dieses StyleBook.
- **description**: Eine Beschreibung, die definiert, was dieses StyleBook tut. Diese Beschreibung wird in NetScaler Console angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **display-name**: Ein beschreibender Name für das StyleBook, der in NetScaler Console angezeigt wird.
- **namespace**: Ein Namespace ist Teil eines eindeutigen Bezeichners für ein StyleBook, um Namenskollisionen zu vermeiden.
- **schema-version**: Nimmt in dieser Version immer den Wert „1.0“ an.
- **version**: Die Versionsnummer des StyleBooks. Sie können die Versionsnummer ändern, wenn Sie das StyleBook aktualisieren.

Die Kombination aus **name**, **namespace** und **version** identifiziert ein StyleBook im System eindeutig. Sie können in NetScaler Console keine zwei StyleBooks mit derselben Kombination aus Name, Namespace und Version haben. Sie können jedoch zwei StyleBooks mit demselben Namen und derselben Version, aber unterschiedlichen Namespaces, oder mit demselben Namespace und derselben Version, aber unterschiedlichen Namen haben.

HINWEIS

Angenommen, Sie haben Ihr StyleBook aktualisiert und Sie haben eine aktualisierte Versionsnummer. Wenn Sie nun dieses StyleBook in anderen StyleBooks referenzieren (d. h. importieren), stellen Sie sicher, dass Sie die Versionsnummer auch in den anderen StyleBooks aktualisieren, damit diese die korrekte Version des importierten StyleBooks verwenden.

StyleBooks importieren

Der Abschnitt nach dem Header wird „import-stylebooks“ genannt. In diesem Abschnitt müssen Sie den Namespace und die Versionsnummer jedes anderen StyleBooks deklarieren, auf das Sie in Ihrem aktuellen StyleBook verweisen möchten. Dadurch können Sie andere StyleBooks importieren und wiederverwenden, anstatt dieselbe Konfiguration in Ihrem eigenen StyleBook neu zu erstellen.

In diesem Beispiel ist der Abschnitt „import-stylebooks“ wie folgt geschrieben:

```
import-stylebooks:

 -

  namespace: netscaler.nitro.config

  prefix: ns
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
version: "10.5"
```

Jedes StyleBook muss auf den Namespace netscaler.nitro.config verweisen, wenn es NITRO-Konfigurationsobjekte direkt verwendet. Dieser Namespace enthält alle NetScaler NITRO-Typen, wie z. B. lbvserver. Da Softwareversionen 10.5 und höher unterstützt werden, können Sie Ihr StyleBook verwenden, um Konfigurationen auf jeder NetScaler-Instanz mit Release 10.5 und höher zu erstellen und auszuführen.

Das im Abschnitt „import-stylebooks“ verwendete Präfix ist eine Kurzform, um auf die Kombination aus Namespace und Version zu verweisen. In diesem Fall bezieht sich ns auf netscaler.nitro.config der Version 10.5. In den späteren Abschnitten Ihres StyleBooks können Sie anstelle des Namespace und der Version zur Referenzierung des importierten StyleBooks die gewählte Präfixzeichenfolge, z. B. ns im obigen Beispiel, verwenden.

Die in den StyleBooks verwendete Version ist die NetScaler NITRO-Version. Ein StyleBook, das auf NITRO-Version X basiert, kann verwendet werden, um jeden NetScaler der Version X oder höher zu konfigurieren.

HINWEIS

Um sicherzustellen, dass Ihre StyleBooks zur Konfiguration jeder NetScaler-Instanz der Version 10.5 oder höher verwendet werden können, empfiehlt Citrix für maximale Kompatibilität, den NITRO 10.5-Namespace in Ihren StyleBooks zu importieren, die NITRO-integrierte StyleBooks direkt verwenden (Namespace: netscaler.nitro.config, Version: 10.5).

Es ist wichtig, dass ein StyleBook, das andere StyleBooks importiert, auf einer NITRO-Version basieren muss, die gleich oder höher ist als die StyleBooks, die es importiert. Zum Beispiel kann ein StyleBook, das auf NITRO-Version 10.5 basiert, kein StyleBook, das auf 11.1 basiert, abhängen von, verwenden oder importieren. Ein StyleBook, das auf Version 11.1 basiert, kann jedoch ein StyleBook importieren, das auf einer Version kleiner als 11.1 basiert.

Es ist auch möglich, dass ein StyleBook den NITRO-Namespace überhaupt nicht importiert. Das bedeutet, dass ein StyleBook NITRO-Komponenten nicht direkt definieren muss, sondern StyleBooks importieren (abhängen von) kann, die NITRO-Komponenten definieren. Das StyleBook, das andere StyleBooks importiert, erwirbt immer die höchste NITRO-Version in der Hierarchie seiner Abhängigkeiten. Und es wird verwendet, um NetScalers zu konfigurieren, die diese Version oder höher sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Parameter

Der Abschnitt „Parameter“ ermöglicht es Ihnen, alle Parameter zu deklarieren, die Sie in Ihrem StyleBook benötigen. Sie als StyleBook-Entwickler müssen entscheiden, welche Eingaben die Benutzer Ihres StyleBooks angeben sollen. In diesem Beispiel haben Sie Ihr StyleBook so erstellt, dass seine Benutzer den Namen des virtuellen Servers, seine IP-Adresse und die Lastverteilungsmethode angeben müssen.

Der Abschnitt „Parameter“ würde wie folgt aussehen:

```
parameters:

 -

  name: name

  label: "Application Name"

  description: "Give a name to the application configuration."

  type: string

  required: true

 -

  name: vip-ipaddress

  label: "Load Balancer IP Address"

  description: "The Application VIP that clients access"

  type: ipaddress

  required: true

 -

  name: lb-alg

  label: LB Algorithm

  description: Load Balancing Algorithm
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
type: string

default: ROUNDROBIN

allowed-values:

 - ROUNDROBIN

 - LEAST-CONNECTION
```

HINWEIS

Wenn Sie die Bezeichnung eines Parameters nicht angeben, verwendet NetScaler Console das Attribut „name“, wenn dieser Parameter angezeigt wird. Sie müssen immer eine Bezeichnung für Ihre Parameter definieren, damit Sie steuern können, wie sie in NetScaler Console angezeigt werden.

Bei der Verwendung der APIs wird der Parameter jedoch durch seinen Namen bezeichnet.
In diesem Abschnitt haben Sie drei Parameter deklariert, die durch ihre **name**-Attributwerte angegeben sind – **name** für den Namen des virtuellen Servers, **ip** für die IP-Adresse des virtuellen Servers und **lb-alg** für die Lastverteilungsmethode.

- **type** bezieht sich auf den Werttyp, den diese Parameter annehmen können. Zum Beispiel können Name und `lb-alg` einen Zeichenfolgenwert annehmen, und der IP-Wert muss vom Typ IP-Adresse sein. Parameter in einem StyleBook können von einem der folgenden integrierten Typen sein:
- **string**: Ein Array von Zeichen. Wenn keine Länge angegeben ist, kann der Zeichenfolgenwert eine beliebige Anzahl von Zeichen annehmen. Sie können die Länge eines Zeichenfolgentyps jedoch mithilfe der Attribute min-length und max-length begrenzen.
- **number**: Eine ganze Zahl. Sie können die minimale und maximale Zahl, die dieser Typ annehmen kann, mithilfe der Attribute min-value und max-value angeben.
- **boolean**: Kann entweder true oder false sein. Beachten Sie auch, dass alle Literale von YAML als Booleans betrachtet werden (zum Beispiel Yes oder No).
- **ipaddress**: Eine Zeichenfolge, die eine gültige IPv4- oder IPv6-Adresse darstellt.
- **tcp-port**: Eine Zahl zwischen 0 und 65535, die einen TCP- oder UDP-Port darstellt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **password**: Ein undurchsichtiger/geheimer Zeichenfolgenwert. Wenn NetScaler Console einen Wert für diesen Parameter anzeigt, wird er als Sternchen (*****) dargestellt.
- **certfile**: Eine Zertifikatsdatei.
- **keyfile**: Eine private Zertifikatsschlüsseldatei.
- **file**: Ein Parameter dieses Typs erfordert, dass der Benutzer eine Datei hochlädt, zum Beispiel eine Zertifikats- oder Schlüsseldatei.
- **object**: Besteht aus mehreren Elementen, und jedes dieser Elemente ist ein Parameter. Dieser Typ kann verwendet werden, um mehrere verwandte Parameter unter einem übergeordneten Parameter zu gruppieren.
- **required**: Gibt an, ob ein Parameter obligatorisch oder optional ist. Wenn er auf true gesetzt ist, ist der Parameter obligatorisch, und der Benutzer muss einen Wert für diesen Parameter angeben, wenn er Konfigurationen mit diesem StyleBook erstellt. Standardmäßig sind alle Parameter optional. In diesem Beispiel sind **name** und **ip** obligatorische Parameter, während **lb-alg** ein optionaler Parameter ist, dessen Standardwert "ROUNDROBIN" lautet.

Verwenden Sie das Attribut **default**, um einem optionalen Parameter einen Standardwert zuzuweisen. Wenn ein Benutzer beim Erstellen einer Konfiguration keinen Wert angibt, wird der Standardwert verwendet. Zum Beispiel ist für den Parameter **lb-alg** der Standardwert ROUNDROBIN.

Verwenden Sie das Attribut **allowed-values**, um spezifische Werte zu definieren, aus denen ein Benutzer beim Erstellen einer Konfiguration wählen kann. In diesem Beispiel haben Sie zwei Werte für den Parameter **lb-alg** angegeben – ROUNDROBIN und LEASTCONNECTION.

Wenn Sie Ihr StyleBook importieren und verwenden, zeigt NetScaler Console ein Formular mit diesen drei Parametern an. Die für Name und IP angezeigten Felder ermöglichen die Eingabe von Werten vom Typ String und `ipaddress`, und das Feld `lb-alg` wird als Dropdown-Liste mit ROUNDROBIN als Standardwert angezeigt.

HINWEIS

Zusätzlich zu den integrierten Typen kann ein Parameter ein anderes StyleBook als seinen Typ haben. Dies ist eine Möglichkeit, in anderen StyleBooks definierte Parameter wiederzuverwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Komponenten

Der letzte Abschnitt in diesem StyleBook wird als Komponentenabschnitt bezeichnet und gilt als der wichtigste Abschnitt im StyleBook. In diesem Abschnitt definieren Sie die Konfigurationsobjekte, die vom StyleBook erstellt werden müssen.

Für dieses Beispiel müssen Sie den Komponentenabschnitt wie folgt schreiben:

```
components:

 -

  name: lbvserver-comp

  description: This StyleBook component (a Builtin Nitro StyleBook) builds
a NetScaler lbvserver configuration object.

  type: ns::lbvserver

  properties:

   name: $parameters.name

   ipv46: $parameters.vip-ipaddress

   lbmethod: $parameters.lb-alg

   servicetype: HTTP

   port: 80
```

Dieses Beispiel enthält nur eine Komponente. Die Hauptattribute einer Komponente sind Name, Typ und Eigenschaften. Der Typ einer Komponente bestimmt, welche Eigenschaften diese Komponente bereitstellt. Komponenten sind von zwei Typen:

- **Integrierter Typ**: Dieser Typ wird vom System bereitgestellt und muss nicht definiert werden, zum Beispiel die NITRO-Entitätstypen `lbvserver` oder `servicegroup`. In diesem Beispiel verwenden Sie einen integrierten Komponententyp.
- **Zusammengesetzter Typ**: Dieser Typ ist das StyleBook, das Sie erstellt und in NetScaler Console importiert haben, oder das Standard-StyleBook, das mit NetScaler Console geliefert wird. Weitere Informationen zu zusammengesetzten StyleBooks finden Sie unter Ein zusammengesetztes StyleBook erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In diesem Beispiel haben Sie eine Komponente namens **lbvserver-comp** definiert. Diese Komponente ist vom Typ **ns::lbvserver** (ein integrierter NITRO-Typ), wobei „ns“ das Präfix ist, das sich auf den Namespace netscaler.nitro.config und die Version 10.5 bezieht, die Sie im Abschnitt „import-stylebooks“ angegeben hatten, und `lbvserver` ist eine NITRO-Ressource in diesem Namespace.

Die hier definierten **Eigenschaften** sind die Attribute der `lbvserver` Ressource. Weitere Informationen zu allen verfügbaren NetScaler NITRO-Ressourcen und deren Attributen finden Sie in der NetScaler NITRO REST API-Dokumentation.

Die Eigenschaften in diesem Abschnitt umfassen die obligatorischen Attribute der `lbvserver` Ressource und ermöglichen es Ihnen, Werte für diese Attribute anzugeben. In diesem Beispiel geben Sie statische Werte für `servicetype` und Port an, während die Eigenschaften Name, ipv46 und `lbmethod` ihre Werte von den Eingabeparametern erhalten. Im restlichen StyleBook können Sie sich auf die im Parameterabschnitt definierten Parameternamen beziehen, indem Sie den Ausdruck **$parameters.\<parameter-name\>** verwenden, zum Beispiel **$parameters.ip**.

HINWEIS

Konventionell wird das Präfix „ns“ immer verwendet, um einen NetScaler NITRO-Namespace im Abschnitt „import-stylebooks“ zu bezeichnen. Obwohl es nicht obligatorisch ist, empfiehlt Citrix, dieselbe Konvention in Ihren eigenen StyleBooks für die Konsistenz zu verwenden.

Erstellen Sie Ihr StyleBook

Nachdem Sie alle erforderlichen Abschnitte dieses StyleBooks definiert haben, fassen Sie sie alle zusammen, um Ihr erstes StyleBook zu erstellen. Kopieren Sie den StyleBook-Inhalt in einen Texteditor und speichern Sie die Datei dann als **lb-vserver.yaml**. Citrix empfiehlt, den integrierten YAML-Validator in StyleBooks zu verwenden, um den YAML-Inhalt zu validieren und zu importieren.

Der vollständige Inhalt der Datei lb-vserver.yaml ist unten wiedergegeben:

```
name: lb-vserver

namespace: com.example.stylebook

version: "1.0"

display-name: Load Balancing Virtual Server (HTTP)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
description: "This stylebook defines a very simple load balancing HTTP
virtual server configuration"

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  version: "10.5"

  prefix: ns

 -

  namespace: com.citrix.adc.stylebooks

  version: "1.0"

  prefix: stlb



parameters:

 -

  name: name

  label: "Application Name"

  description: "Give a name to the application configuration."

  type: string

  required: true

 -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  name: vip-ipaddress

  label: "Load Balancer IP Address"

  description: "The Application VIP that clients access"

  type: ipaddress

  required: true

 -

  name: lb-alg

  label: LB Algorithm

  description: Load Balancing Algorithm

  type: string

  default: ROUNDROBIN

  allowed-values:

   - ROUNDROBIN

   - LEAST-CONNECTION



components:

 -

  name: lbvserver-comp

  description: This StyleBook component (a Builtin Nitro StyleBook) builds
a NetScaler lbvserver configuration object.

  type: ns::lbvserver

  properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: $parameters.name

    ipv46: $parameters.vip-ipaddress

    lbmethod: $parameters.lb-alg

    servicetype: HTTP

    port: 80
```

Um Ihr StyleBook zum Erstellen von Konfigurationen zu verwenden, müssen Sie es in NetScaler Console importieren und dann verwenden. Weitere Informationen finden Sie unter Verwenden benutzerdefinierter StyleBooks.

Sie können dieses StyleBook auch in andere StyleBooks importieren (mithilfe des import-stylebooks-Konstrukts). Oder Sie können dieses StyleBook ändern, um weitere Parameter und Komponenten aufzunehmen, wie im nächsten Abschnitt beschrieben.

StyleBook zum Erstellen einer grundlegenden Lastausgleichskonfiguration

In diesem Abschnitt entwerfen Sie ein StyleBook, das eine Lastausgleichskonfiguration erstellt, die einen virtuellen Lastausgleichsserver, eine Dienstgruppe und eine Liste von Diensten umfasst. Das StyleBook bindet die Dienste an die Dienstgruppe und die Dienstgruppe an den virtuellen Server.

Um eine grundlegende Lastausgleichskonfiguration zu erstellen, verwenden Sie das Beispiel-StyleBook, **lb-vserver**, das Sie in StyleBook zum Erstellen eines virtuellen Lastausgleichsservers erstellt haben, und speichern Sie es als **basic-lb-config.yaml**.

Header

Um dieses StyleBook zu erstellen, aktualisieren Sie den Header-Abschnitt. Dieser Abschnitt ähnelt dem Header-Abschnitt, den Sie in StyleBook zum Erstellen eines virtuellen Lastausgleichsservers erstellt haben.

Ändern Sie den Wert von **name** in basic-lb-config. Aktualisieren Sie **description** und **display-name**, um das StyleBook zu beschreiben. Sie müssen die Werte für **namespace** und **version** nicht ändern. Da Sie den Namen geändert haben, wird ein eindeutiger Bezeichner für dieses StyleBook im System erstellt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Configuration

description: This StyleBook defines a simple load balancing configuration.

schema-version: "1.0"
```

StyleBooks importieren

Der Abschnitt import-stylebooks bleibt unverändert. Er verweist auf den netscaler.nitro.config-Namespace, um die NITRO-Konfigurationsobjekte zu verwenden.

```
import-stylebooks:

 -

 namespace: netscaler.nitro.config

 prefix: ns

 version: "10.5"
```

Parameter

Aktualisieren Sie den Parameterabschnitt, um zwei weitere Parameter hinzuzufügen.

Die Parameter definieren die Liste der Dienste oder Server und den Port, an dem die Dienste lauschen. Die ersten drei Parameter `name`, `ip` und `lb-alg` bleiben unverändert.

```
parameters:

 -

  name: name

  type: string
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  label: Application Name

  description: Give a name to the application configuration.

  required: true

 -

  name: ip

  type: ipaddress

  label: Application Virtual IP (VIP)

  description: The Application VIP that clients access

  required: true

 -

  name: lb-alg

  type: string

  label: LoadBalancing Algorithm

  description: Choose the loadbalancing algorithm (method) used for
loadbalancing client requests between the application servers.

  allowed-values:

     - ROUNDROBIN

     - LEASTCONNECTION

  default: ROUNDROBIN

 -

  name: svc-servers

  type: ipaddress[]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  label: Application Server IPs

  description: The IP addresses of all the servers of this application

  required: true

 -

  name: svc-port

  type: tcp-port

  label: Server Port

  description: The TCP port open on the application servers to receive
requests.

  default: 80
```

Der Parameter **svc-servers** wird hinzugefügt, um eine Liste von IP-Adressen der Backend-Server der Anwendung zu akzeptieren. **svc-servers** ist ein obligatorischer Parameter, wie durch **required: true** angegeben.

Der zweite Parameter, **svc-port**, bezeichnet die Portnummer, an der die Server lauschen. Die Standard-Portnummer ist 80, sofern vom Benutzer nicht anders angegeben.

Komponenten

Sie müssen auch den Komponentenabschnitt aktualisieren, um weitere Komponenten zu definieren, die die beiden neuen Parameter verwenden und die vollständige Lastausgleichskonfiguration erstellen.

Für dieses Beispiel müssen Sie den Komponentenabschnitt wie folgt schreiben:

```
components:

 -

  name: lbvserver-comp

  type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg


components:
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
   name: $parameters.name + "-svcgrp"
   servicetype: HTTP


  components:
    -
      name: lbvserver-svg-binding-comp
      type: ns::lbvserver_servicegroup_binding
      properties:
          name: $parent.parent.properties.name
          servicegroupname: $parent.properties.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

  name: members-svcg-comp

  type: ns::servicegroup_servicegroupmember_binding

  repeat: $parameters.svc-servers

  repeat-item: srv

  properties:

     ip: $srv

     port: str($parameters.svc-port)

     servicegroupname: $parent.properties.name
```

In diesem Beispiel hat die ursprüngliche Komponente **lbvserver-comp** (aus dem vorherigen Beispiel) nun eine untergeordnete Komponente namens **svcg-comp**. Die Komponente **svcg-comp** enthält ebenfalls zwei untergeordnete Komponenten. Das Verschachteln einer Komponente in einer anderen Komponente ermöglicht es der verschachtelten Komponente, Konfigurationsobjekte zu erstellen, indem sie auf Attribute in der übergeordneten Komponente verweist. Die verschachtelte Komponente kann ein oder mehrere Objekte für jedes in der übergeordneten Komponente erstellte Objekt erstellen.

Die Komponente **svcg-comp** wird verwendet, um eine Dienstgruppe auf der NetScaler-Instanz zu erstellen, indem die für die Attribute der Ressource `servicegroup` angegebenen Werte verwendet werden. In diesem Beispiel geben Sie den statischen Wert für `servicetype` an, während **name** seinen Wert vom Eingabeparameter erhält. Verweisen Sie auf den im Parameterabschnitt definierten Parameter **name** unter Verwendung der Notation **$parameters.name + "-svcgrp"**, wobei "**-svcgrp**" an den benutzerdefinierten Namen angehängt (verkettet) wird.

Die Komponente **svcg-comp** hat zwei untergeordnete Komponenten: **lbvserver-svg-binding-comp** und **members-svcg-comp**.

Die erste untergeordnete Komponente, **lbvserver-svg-binding-comp**, wird verwendet, um ein Konfigurationsobjekt zwischen der von ihrer übergeordneten Komponente erstellten Dienstgruppe und dem Lastausgleichs-Virtual-Server (`lbvserver`), der von der übergeordneten Komponente

© 1997–2026 Citrix Systems, Inc. All rights reserved.

der übergeordneten Komponente erstellt wurde, zu binden. Die Notation $parent, auch Elternreferenz genannt, wird verwendet, um auf Entitäten in den übergeordneten Komponenten zu verweisen. Zum Beispiel verweist **servicegroupname: $parent.properties.name** auf die von der übergeordneten Komponente **svcg-comp** erstellte Dienstgruppe, und **name: $parent.parent.properties.name** verweist auf den von der übergeordneten Komponente der übergeordneten Komponente **lbvserver-comp** erstellten virtuellen Server.

Die Komponente **members-svcg** wird verwendet, um Konfigurationsobjekte zwischen der Liste der Dienste und der von der übergeordneten Komponente erstellten Dienstgruppe zu binden. Die Erstellung von Bindungskonfigurationsobjekten wird durch die Verwendung des **repeat**-Konstrukts von StyleBook erreicht, um über die Liste der im Parameter **svc-servers** angegebenen Server zu iterieren. Während der Iteration erstellt diese StyleBook-Komponente ein NITRO-Konfigurationsobjekt vom Typ **servicegroup_servicegroupmember_binding** für jeden Dienst (im **repeat-item**-Konstrukt als `srv` bezeichnet) in der Dienstgruppe und setzt das Attribut **ip** in jedem NITRO-Konfigurationsobjekt auf die IP-Adresse des entsprechenden Servers.

Im Allgemeinen können Sie die Konstrukte **repeat** und **repeat-item** in einer Komponente verwenden, um diese Komponente mehrere Konfigurationsobjekte desselben Typs erstellen zu lassen. Sie können dem Konstrukt **repeat-item** einen Variablennamen zuweisen, zum Beispiel `srv`, um den aktuellen Wert in der Iteration zu bezeichnen. Dieser Variablenname wird in den Eigenschaften derselben Komponente oder in untergeordneten Komponenten als **`$<varname>`** referenziert, zum Beispiel $srv.

Im vorhergehenden Beispiel hilft die Verschachtelung von Komponenten, die Konfiguration einfach zu erstellen. Sie können die Konfiguration auch ohne Verschachtelung erstellen, wie im folgenden Beispiel gezeigt:

```
components:

 -

  name: lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name + "-lb"

   servicetype: HTTP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
  -
   name: svcg-comp
   type: ns::servicegroup
   properties:
     servicegroupname: $parameters.name + "-svcgrp"
     servicetype: HTTP
  -
   name: lbvserver-svg-binding-comp
   type: ns::lbvserver_servicegroup_binding
   properties:
    name: $components.lbvserver-comp.properties.name
    servicegroupname: $components.svcg-comp.properties.servicegroupname
  -
   name: members-svcg-comp
   type: ns::servicegroup_servicegroupmember_binding
   repeat: $parameters.svc-servers
   repeat-item: srv
   properties:
    ip: $srv
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   port: 80

   servicegroupname: $components.svcg-comp.properties.servicegroupname
```

Obwohl die Komponenten hier nicht verschachtelt sind, ist die generierte NetScaler-Konfiguration dieselbe wie die der zuvor verwendeten verschachtelten Komponenten.

Die Reihenfolge, in der die Komponenten im StyleBook deklariert werden, hat keinen Einfluss auf die Reihenfolge der Erstellung der Konfigurationsobjekte. In diesem Beispiel müssen die Komponenten **svcg-comp** und **lbvserver-comp**, obwohl zuletzt deklariert, vor der Erstellung der zweiten Komponente **lbvserver-svg-binding-comp** erstellt werden, da es in der zweiten Komponente Vorwärtsreferenzen auf diese Komponenten gibt.

HINWEIS

Konventionell sind die Namen von StyleBooks, Parametern, Substitutionen, Komponenten und Ausgaben in Kleinbuchstaben gehalten. Wenn sie aus mehreren Wörtern bestehen, werden sie durch einen „-“-Charakter getrennt. Zum Beispiel `lb-bindings`, `app-name`, `rewrite-config` und so weiter. Eine weitere Konvention ist, Komponentennamen mit der Zeichenfolge `-comp` zu versehen.

Ausgaben

In diesem Abschnitt müssen Sie angeben, was das StyleBook den Benutzern (oder in anderen StyleBooks) nach dem Erstellen einer Konfiguration zur Verfügung stellt. Sie können beispielsweise angeben, dass die `lbvserver` und die `servicegroup` Konfigurationsobjekte, die von diesem StyleBook erstellt wurden, offengelegt werden sollen.

```
outputs:

-

  name: lbvserver-comp

  value: $components.lbvserver-comp

  description: The component that builds the Nitro lbvserver configuration
object
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

  name: servicegroup-comp

  value: $components.svcg-comp

  description: The component that builds the Nitro servicegroup
configuration object
```

Der Ausgabeabschnitt eines StyleBooks ist optional. Ein StyleBook muss keine Ausgaben zurückgeben. Wenn jedoch einige interne Komponenten als Ausgaben zurückgegeben werden, ermöglicht dies StyleBooks, die dieses StyleBook importieren, mehr Flexibilität. Diese Funktionalität ist nützlich, wenn ein zusammengesetztes StyleBook erstellt wird.

HINWEIS

Es ist eine bewährte Methode, eine gesamte Komponente des StyleBooks im Ausgabeabschnitt freizulegen, anstatt nur eine einzelne Eigenschaft einer Komponente (zum Beispiel die gesamte **$components.lbvserver-comp** freizulegen, anstatt nur den Namen, **$components.lbvserver-comp.properties.name**). Fügen Sie der Ausgabe außerdem eine Beschreibung hinzu, die erklärt, was die spezifische Ausgabe darstellt.

Erstellen Sie Ihr StyleBook

Nachdem Sie alle erforderlichen Abschnitte dieses StyleBooks definiert haben, fassen Sie sie alle zusammen, um Ihr zweites StyleBook zu erstellen. Sie haben diese StyleBook-Datei bereits als **basic-lb-config.yaml** gespeichert. Citrix empfiehlt, den integrierten YAML-Validator in StyleBooks zu verwenden, um den YAML-Inhalt zu validieren und zu importieren.

Der vollständige Inhalt der Datei **basic-lb-config.yaml** wird wie folgt wiedergegeben:

```
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Configuration

description: This StyleBook defines a simple load balancing configuration.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
schema-version: "1.0"



import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  type: string

  label: LoadBalancing Algorithm

  description: Choose the loadbalancing algorithm (method) used for
loadbalancing client requests between the application servers.

  allowed-values:

     - ROUNDROBIN

     - LEASTCONNECTION

  default: ROUNDROBIN

 -

  name: svc-servers

  type: ipaddress[]

  label: Application Server IPs

  description: The IP addresses of all the servers of this application

  required: true

 -

  name: svc-port

  type: tcp-port

  label: Server Port

  description: The TCP port open on the application servers to receive
requests.

  default: 80



components:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-
 name: lbvserver-comp
 type: ns::lbvserver
 properties:
  name: $parameters.name + "-lb"
  servicetype: HTTP
  ipv46: $parameters.ip
  port: 80
  lbmethod: $parameters.lb-alg
-
 name: svcg-comp
 type: ns::servicegroup
 properties:
    servicegroupname: $parameters.name + "-svcgrp"
    servicetype: HTTP
-
 name: lbvserver-svg-binding-comp
 type: ns::lbvserver_servicegroup_binding
 properties:
  name: $components.lbvserver-comp.properties.name
  servicegroupname: $components.svcg-comp.properties.servicegroupname
-
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  name: members-svcg-comp

  type: ns::servicegroup_servicegroupmember_binding

  repeat: $parameters.svc-servers

  repeat-item: srv

  properties:

   ip: $srv

   port: 80

   servicegroupname: $components.svcg-comp.properties.servicegroupname



outputs:

-

  name: lbvserver-comp

  value: $components.lbvserver-comp

  description: The component that builds the Nitro lbvserver configuration
object

-

  name: servicegroup-comp

  value: $components.svcg-comp

  description: The component that builds the Nitro servicegroup
configuration object
```

Um Ihr StyleBook zum Erstellen von Konfigurationen zu verwenden, müssen Sie es in NetScaler Console importieren und dann verwenden. Weitere Informationen finden Sie unter Verwenden benutzerdefinierter StyleBooks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können dieses StyleBook auch in andere StyleBooks importieren und seine Eigenschaften wie im nächsten Abschnitt beschrieben verwenden.

Erstellen Sie ein zusammengesetztes StyleBook

Ein wichtiges und leistungsstarkes Merkmal von StyleBooks ist, dass sie als Bausteine für andere StyleBooks verwendet werden können. Ein StyleBook kann in ein anderes StyleBook importiert und als **Typ** bezeichnet werden, der von Komponenten des zweiten StyleBooks ähnlich einem integrierten NITRO-StyleBook verwendet wird.

Zum Beispiel können Sie das **basic-lb-config** StyleBook, das Sie im vorherigen Abschnitt erstellt haben, verwenden, um ein weiteres StyleBook namens **composite-example** zu erstellen. Um das „basic-lb-config“-StyleBook zu verwenden, müssen Sie es im neuen StyleBook im Abschnitt „import-stylebooks“ importieren.

Erstellen Sie Ihr StyleBook

Das neue StyleBook würde wie folgt aussehen:

```
name: composite-example

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Virtual Server (HTTP/RoundRobin)

description: This StyleBook defines a RoundRobin load balancing
configuration with a monitor.

schema-version: "1.0"

import-stylebooks:

  -

   namespace: netscaler.nitro.config

   version: "10.5"

   prefix: ns

  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    namespace: com.example.stylebooks
    version: "0.1"
    prefix: stlb
parameters:
  -
    name: name
    type: string
    label: Application Name
    description: Give a name to the application configuration.
    required: true
  -
    name: ip
    type: ipaddress
    label: Application Virtual IP (VIP)
    description: The Application VIP that clients access
    required: true
  -
    name: svc-servers
    type: ipaddress[]
    label: Application Server IPs
    description: The IP addresses of all the servers of this application
    required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -

    name: response-code

    type: string[]

    label: List of Response Codes

    description: List of Response Codes - Provide a list of response codes
in integer.



components:

  -

    name: basic-lb-comp

    type: stlb::basic-lb-config

    description: This component's type is another StyleBook that builds
the NetScaler lbvserver, servicegroups and services configuration objects.

    properties:

     name: $parameters.name

     ip: $parameters.ip

     svc-servers: $parameters.svc-servers

  -

     name: monit-comp

     type: ns::lbmonitor

     description: This component is a basic Nitro type (a Builtin
StyleBook) that builds the NetScaler monitor configuration object.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:
      monitorname: $parameters.name + "-mon"
      type: HTTP
      respcode: $parameters.response-code
      httprequest: "'GET /'"
      lrtm: ENABLED
      secure: "YES"

    components:
       -
         name: monit-svcgrp-bind-comp
         type: ns::servicegroup_lbmonitor_binding
         properties:
           servicegroupname: $components.basic-lb-
comp.outputs.servicegroup-comp.properties.servicegroupname
           monitor_name: $parent.properties.monitorname
```

Im Abschnitt „import-stylebooks“ importieren Sie das basic-lb-config StyleBook, indem Sie seinen Namespace und seine Version verwenden, auf die mit dem Präfix `stlb` verwiesen wird.

Im Abschnitt „components“ sind zwei Komponenten definiert. Die erste Komponente ist vom Typ **stlb::basic-lb-config**, wobei „basic-lb-config“ der Name des StyleBooks ist, das Sie in StyleBook zur Erstellung einer grundlegenden Lastverteilungskonfiguration erstellt haben. Die für diese Komponente definierten Eigenschaften entsprechen den obligatorischen Parametern, die im basic-lb-config StyleBook deklariert sind. Sie können jedoch jeden Parameter des StyleBooks verwenden (sowohl erforderliche als auch optionale). Anstatt `lbvserver`, eine Dienstgruppe sowie Dienst- und Dienstgruppenbindungen neu zu erstellen, importieren Sie das StyleBook, das

© 1997–2026 Citrix Systems, Inc. All rights reserved.

all dies als Komponente erledigt, und verwenden es, um diese Konfigurationsobjekte im neuen StyleBook zu erstellen.

Das StyleBook fügt eine zweite Komponente `monit-comp` hinzu, die die Attribute der NITRO-Ressource `lbmonitor` (ein integriertes StyleBook) verwendet, um ein Monitor-Konfigurationsobjekt zu erstellen. Es hat auch eine Unterkomponente `monit-svcgrp-bind-comp`, um das Bindungs-Konfigurationsobjekt zu erstellen, das den Monitor an die in der ersten Komponente erstellte `servicegroup` bindet. Da die in dem „basic-lb-config“-StyleBook erstellte `servicegroup` Komponente als Ausgabe verfügbar gemacht wird, kann dieses StyleBook darauf über den Ausdruck **$components.basic-lb-comp.outputs.servicegroup-comp** zugreifen. Dies ist ein Beispiel dafür, wie der Abschnitt „outputs“ von den importierenden StyleBooks verwendet werden kann, um auf Komponenten in den importierten StyleBooks zuzugreifen, auf die sie sonst keinen Zugriff gehabt hätten.

Als Nächstes kopieren Sie den StyleBook-Inhalt in einen Texteditor und speichern die Datei dann als **composite-example.yaml**. Stellen Sie sicher, dass Sie den YAML-Inhalt validieren, bevor Sie die Datei in NetScaler Console importieren. Importieren Sie sie dann in NetScaler Console und erstellen Sie eine oder mehrere Konfigurationen mit diesem StyleBook.

Citrix empfiehlt, den integrierten YAML-Validator in StyleBooks zu verwenden, um den YAML-Inhalt zu validieren und zu importieren.

GUI-Attribute in einem benutzerdefinierten StyleBook verwenden

Sie können GUI-Attribute im Parameterbereich Ihres StyleBooks hinzufügen, um die Felder intuitiv zu gestalten, wenn sie in NetScaler Console angezeigt werden.

Bezeichnung mit Tooltip für Parameter hinzufügen

Sie können einen beschreibenden Namen für den Parameter hinzufügen, indem Sie das Attribut 'label' verwenden. Fügen Sie einen Tooltip für diesen Parameter hinzu, indem Sie das Attribut 'description' verwenden.

Beispiel:

```
name: ip

label: Virtual Server IP Address

description: IP address of the virtual server that represents the load
balanced application.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
type: ipaddress

required: true
```

Einen einklappbaren Bereich für den Parameter festlegen

Wenn Sie einen Parameter vom Typ 'object' haben, können Sie das Layout mithilfe des Attributs **gui** definieren.

Beispiel-1:

```
name: svcg-advanced

label: Advanced Application Server Settings

type: object

required: false

gui:

 collapse_pane: true

 columns: 2
```

In diesem Beispiel ist das Layout ein einklappbares Objekt, bei dem Felder in zwei Spalten angezeigt werden.

Sie können auch eine Zusammenfassungsansicht eines Parameters von `type: object[]` (Liste von Objekten) als Tabelle anzeigen, wobei die inneren Parameter die Spalten darstellen. Um einen inneren Parameter in die Zusammenfassungsansicht aufzunehmen oder auszuschließen, können Sie das Attribut `summary_display` im Abschnitt `gui` wie folgt verwenden:

Beispiel-2:

```
name: settings

label: Settings

type: object[]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:

  -

    name: name

    label: Name

    description: Name of this setting

    type: string

    gui:

      summary_display: true
```

Die Benutzeroptionen als Optionsfelder festlegen

Sie können die Benutzeroptionen als Optionsfelder auflisten, indem Sie die Attribute `layout` und `allowed-values` verwenden. Wenn der Benutzer also ein Konfigurationspaket erstellt, werden die Parameterwerte als Optionsfelder angezeigt.

Standardmäßig werden die Parameterwerte als Dropdown-Menü angezeigt, wenn das Attribut 'gui' nicht angegeben ist.

```
-

    name: block-by-category-action

    label: Action

    description: Set an action if the bot is detected.

    type: string

    default: RESET

    gui:

        layout: radio

    allowed-values:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        - NONE

        - DROP

        - REDIRECT

        - RESET

        - MITIGATION
```

In diesem Beispiel werden die Benutzeroptionen zum Festlegen einer Aktion als Optionsfelder angezeigt. Und die Option **RESET** ist standardmäßig ausgewählt.

Benutzerdefinierte StyleBooks importieren

Nachdem Sie Ihr StyleBook erstellt haben, importieren Sie es in NetScaler Console, um es zu verwenden. NetScaler Console ermöglicht Ihnen den Import eines einzelnen StyleBooks im YAML-Format oder vieler StyleBook YAML-Dateien als Paket in einem .zip-, .tgz- oder .gz-Format. Das NetScaler Console-System validiert Ihre StyleBooks beim Import. Das StyleBook ist nun bereit für die Erstellung von Konfigurationen.

NetScaler Console verfügt auch über einen integrierten YAML-Editor, mit dem Sie die StyleBook YAML-Inhalte erstellen können. Der YAML-Editor ermöglicht es Ihnen, Ihre YAML-Konstrukte direkt über die NetScaler Console-GUI zu validieren. Sie müssen kein separates Tool für diese Validierungsprüfungen verwenden. Der Inhalt wird anhand von YAML-Standards validiert, und jede Abweichung wird hervorgehoben. Sie können den Inhalt dann korrigieren und versuchen, das StyleBook in NetScaler Console zu importieren. Der integrierte YAML-Editor bietet zwei Vorteile beim Schreiben Ihres eigenen StyleBooks.

- **Farbcodiert**. Der Editor zeigt den StyleBook-Inhalt gemäß den YAML-Richtlinien analysiert an. Die Farbcodierung hilft Ihnen, leicht zwischen den in den YAML-Inhalten definierten Schlüsseln und Werten zu unterscheiden.
- **YAML-Validierung**. Der Inhalt wird beim Tippen auf YAML-Fehler überprüft, und jede Abweichung wird sofort hervorgehoben. Diese Validierung ermöglicht es Ihnen, Text zu schreiben, der den YAML-Richtlinien entspricht, noch bevor Sie das StyleBook in NetScaler Console importieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Derzeit validiert der Editor den Inhalt gemäß den YAML-Richtlinien. Er validiert nicht auf Code-Korrektheit und Tippfehler.

HTML-Formatierungs-Tags in der StyleBook-Beschreibung und im Header verwenden

In der **StyleBook**-Definition können Sie ein Header-Feld einfügen und HTML-Formatierungs-Tags für den Text verwenden. Sie können auch Bilder als Teil des Headers einfügen. Der HTML-Inhalt im Header-Feld wird oben auf der Konfigurationsseite angezeigt, wenn Sie eine Konfiguration erstellen oder aktualisieren. Diese Funktion ermöglicht es Ihnen, Infografiken für das StyleBook hinzuzufügen, um das Verständnis der StyleBook-Konfiguration zu erleichtern. Wenn Sie Bilder im Header verwenden, stellen Sie sicher, dass Sie das base64-kodierte Bildformat im `<img>`-Tag verwenden.

Um Bilder in Ihrem HTML-Inhalt zu verwenden, müssen die Bilder inline sein, wie im folgenden Beispiel gezeigt. Sie können Online-Tools verwenden, um Ihre Bilder in ihr base64-kodiertes Format umzuwandeln.

```
name: cs-example

namespace: com.example.stylebooks

version: "1.2"

display-name: Content Switching Configuration

description: Example of a very simple content switching config that
creates and binds an lb to a cs

header:  <img id="b64img" src="…" />

     <h3>Operations performed by this StyleBook:</h3>

     <ul>

      <li style="list-style-type: circle"> Creates a Server </li>

      <li style="list-style-type: circle"> Creates a Service Group </li>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
       <li style="list-style-type: circle"> Creates a LBVServer </li>

      <li style="list-style-type: circle"> Creates a CS Policy and Action
</li>

     </ul>

schema-version: "1.0"
```

So importieren Sie Ihr StyleBook

1. Navigieren Sie in NetScaler Console zu **Applications** > **Configuration** > **StyleBooks**, und klicken Sie dann auf **Import New StyleBook**.
2. Klicken Sie auf eine der folgenden Optionen, um ein StyleBook zu importieren.

   - **Datei** – wählen Sie die erforderliche Datei oder das Dateibündel aus Ihrem lokalen Speicher aus.

     HINWEIS:

     In diesem Beispiel importieren Sie das `lb-vserver.yml` StyleBook, das Sie in StyleBook zum Erstellen eines virtuellen Lastausgleichsservers erstellt haben.

   - **Bundle** – Mit NetScaler Console können Sie viele StyleBooks im YAML-Format importieren. Sie können mehrere YAML-StyleBook-Dateien importieren, die in einem Zip-Format (.zip) oder Tarball-Format (.tgz, .gz) komprimiert sind.

     Ein in NetScaler Console importiertes StyleBook wird mit einem Standardsymbol in der StyleBooks-GUI angezeigt. Sie können diese Standardsymbole mit Ihren eigenen Bildern anpassen.

     Dazu:

     - Erstellen Sie einen Ordner namens `resources` unterhalb des Ordners, der Ihre StyleBook-YAML-Dateien enthält.
     - Laden Sie Ihre Symbole in den Ordner `resources` hoch.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Sie können den Ordner `resources` nicht in einen anderen Namen umbenennen.

- Wenn die Symbol-Datei und die entsprechende StyleBook-Datei denselben Namen haben, wird das Symbol automatisch dem StyleBook zugeordnet.
- Wenn die Symbol-Datei und die entsprechende StyleBook-Datei (z. B. exchange.yaml und exch.png) nicht übereinstimmen, erstellen Sie eine JSON-Datei namens „icon_mapping.json“ im Ordner `resources` wie folgt:

```
<StyleBook file name> : <icon file name>

<StyleBook file1 name> : <icon file1 name>

<StyleBook file2 name> : <icon file2 name>
```

Das Folgende ist ein Beispiel für ein StyleBook-Bundle:

- [ ] Der Ordner `resources` enthält die erforderlichen Symbole.
- [ ] In diesem Beispiel werden `sharepoint.yaml`- und `skype.yaml`-Dateien automatisch `sharepoint.jpeg` bzw. `skype.png` zugeordnet.

Um `exchange.yaml` `exch.png` zuzuordnen, geben Sie Folgendes in der Datei `icon_mapping.json` an:

```
{

"exchange.yaml":"exch.png"

}
```

Wenn ein Symbol im StyleBook-Bundle nicht verfügbar ist, wird das Standardsymbol angezeigt.

- **Raw** – Erstellen Sie den Inhalt Ihres StyleBooks im YAML-Editor.

  Sie können den StyleBook-Inhalt validieren, um Grammatikfehler im StyleBook zu überprüfen. Um den StyleBook-Inhalt zu validieren, klicken Sie auf **Inhalt validieren**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Stellen Sie beim Erstellen eines StyleBooks sicher, dass Sie die folgenden Konzepte kennen:

- NITRO API
- YAML

Weitere Informationen zum Schreiben eigener StyleBooks finden Sie unter So erstellen Sie eigene StyleBooks.

HINWEIS:

Sie können Ihr StyleBook auch in Ihrem bevorzugten Editor erstellen und den Inhalt dann zur Validierung und zum Import in den YAML-Editor kopieren und einfügen.

- **Repository synchronisieren** – Wenn Sie Ihre StyleBooks in GitHub erstellen und verwalten, verwenden Sie diese Option, damit NetScaler Console neue oder aktualisierte StyleBooks in Ihrem Repository erkennt. Wählen Sie das Repository aus, das Sie mit NetScaler Console synchronisieren möchten.

3. Optional: Wählen Sie ein Symbol für ein StyleBook aus.

   Unter **Applications > Configuration > StyleBooks** wird das importierte StyleBook mit diesem Symbol angezeigt.

4. Klicken Sie auf **Erstellen**.

   NetScaler Console validiert Ihr StyleBook nun auf alle syntaktischen und semantischen Fehler gemäß der StyleBook-Grammatik. Ihr StyleBook wird nicht in NetScaler Console importiert, wenn Fehler vorliegen.

   Wenn keine Fehler vorliegen, wird das StyleBook erfolgreich importiert und auf der Seite **StyleBooks** aufgeführt. Sie können das StyleBook anhand des Anzeigenamens identifizieren, den Sie im Kopfbereich des StyleBooks definiert haben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Wenn Sie ein Dateibündel importieren, dekomprimiert NetScaler Console den gezippten Ordner und validiert alle StyleBooks. Das Bündel wird nicht importiert, selbst wenn eine StyleBook-Datei den Validierungstest nicht besteht.

Weitere Informationen zur StyleBook-Grammatik und zur Syntax der verschiedenen Konstrukte und Attribute finden Sie unter StyleBook-Grammatik.

5. Klicken Sie auf den Link **Konfiguration erstellen**, um Konfigurationen aus diesem StyleBook zu erstellen.

   Die Seite **StyleBook** wird geöffnet, und Sie können die Werte für alle in diesem StyleBook definierten Parameter eingeben.

6. Geben Sie die erforderlichen Werte für die Parameter an.

   Im folgenden Beispiel:

   a. Geben Sie die Pflichtfelder **Anwendungsname** und **IP-Adresse des Lastenausgleichs** an.

   b. Wählen Sie den **Lastausgleichsalgorithmus** aus der Liste aus. Standardmäßig ist **ROUNDROBIN** ausgewählt.

7. Wählen Sie unter **Zielinstanzen** die IP-Adresse der NetScaler-Instanz aus, auf der Sie die Konfiguration bereitstellen möchten.

   Sie können die Konfiguration auch auf mehr als einem NetScaler bereitstellen, indem Sie so viele Zielinstanzen wie nötig angeben.

   HINWEIS:

   Um alle kürzlich erkannten NetScaler-Instanzen in NetScaler Console zu **Zielinstanzen** hinzuzufügen, wechseln Sie zur Seite **StyleBooks** und klicken Sie auf das Aktualisierungssymbol auf der rechten Seite der Seite.

8. Wenn Sie die NetScaler (NITRO)-Konfigurationsobjekte testen möchten, bevor Sie die Konfiguration bereitstellen, klicken Sie auf **Testlauf**.

   Wenn die Konfiguration gültig ist, werden die Konfigurationsobjekte basierend auf den angegebenen Werten erstellt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In diesem Beispiel erstellt das StyleBook nur ein Objekt vom Typ `lbvserver`. Dieser Lastenausgleichsserver war die einzige Komponente, die in diesem grundlegenden Beispiel-StyleBook definiert wurde.

Klicken Sie anschließend auf **Erstellen**, um die Konfiguration auf den ausgewählten NetScaler-Instanzen bereitzustellen.

Nachdem Sie die Konfiguration erfolgreich bereitgestellt haben, wird ein neues Konfigurationspaket auf der Seite **Konfigurationen** angezeigt.

Erstellen eines StyleBooks zum Hochladen von Dateien

Mit NetScaler Console StyleBooks können Sie NetScaler-Konfigurationen erstellen, die unter anderem das Hochladen von Dateien beliebigen Typs von Ihrem lokalen Dateisystem auf die NetScaler-Instanz über die NetScaler Console GUI oder die APIs umfassen können. Diese Dateien können beispielsweise Zertifikatsdateien oder Geolocation-Dateien sein. Sie können auch das Verzeichnis angeben, in das diese Dateien hochgeladen werden sollen.

StyleBook-Konfiguration

Das Folgende ist ein Beispiel-StyleBook, das beschreibt, wie eine Geolocation-Datei auf die NetScaler-Instanz hochgeladen wird. Die Geodateien werden typischerweise in GSLB-Konfigurationen zur Definition der statischen Proximity basierend auf dem geografischen Standort verwendet:

Erstellen Sie Ihr StyleBook – 1

```
name: upload-geolocations

namespace: com.citrix.adc.stylebooks.samples

version: "1.0"

display-name: GeoLocation File Upload

description: This StyleBook is used to upload a geolocation file to
NetScaler

schema-version: "1.0"



import-stylebooks:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

 namespace: netscaler.nitro.config

 version: "11.1"

 prefix: ns



parameters:

-

 name: locationfile

 label: Location File

 description: The system file path of the geolocation file on NetScaler
Console

 type: file

 required: true



components:

-

 name: upload-file-comp

 type: ns::systemfile

 properties:

    filename: $parameters.locationfile.filename

    filelocation: "/var/netscaler/inbuilt_db/"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    filecontent: base64.encode($parameters.locationfile.contents)
```

HINWEIS

Der in diesem Beispiel verwendete Parameter ist vom Typ Datei. Sie können dieses StyleBook in NetScaler Console importieren und zum Hochladen von Geolocation-Dateien verwenden.

Dieses StyleBook erfordert, dass die Datei bereits in NetScaler Console vorhanden ist (Sie hätten sie beispielsweise bereits mit einem Dienstprogramm wie SCP in NetScaler Console kopiert). Wenn Sie eine Datei über NetScaler Console auf NetScaler hochladen möchten, ohne sie zuerst in das NetScaler Console-Dateisystem zu kopieren, können Sie ein StyleBook erstellen, das zwei „String“-Parameter enthält: einen zum Angeben des auf dem NetScaler zu verwendenden Dateinamens und den anderen zum Angeben des Dateiinhaltes, und diese beiden Parameter in den upload-file-comp-Komponenten verwenden. Das Folgende ist ein alternatives StyleBook zum Hochladen einer Geolocation-Datei:

Erstellen Sie Ihr StyleBook – 2

```
name: upload-geolocations-alt

namespace: com.citrix.adc.stylebooks.samples

version: "1.0"

display-name: GeoLocation File Upload

description: This StyleBook is used to upload a geolocation file to
NetScaler

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  version: "11.1"
  prefix: ns


parameters:
 -
  name: filename
  label: Location Filename
  description: The name of the location file on the NetScaler
  type: string
  required: true
 -
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true


components:
 -
  name: upload-file-comp
  type: ns::systemfile
  properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
filename: $parameters.filename

filelocation: "/var/NetScaler/inbuilt_db/"

filecontent: base64.encode($parameters.filecontents)
```

Erstellen von Konfigurationen zum Hochladen von Dateien

Das folgende Verfahren erstellt eine Konfiguration auf einer ausgewählten NetScaler-Instanz, die eine Geolocation-Datei mit dem oben beschriebenen ersten StyleBook hochlädt.

So erstellen Sie eine Konfiguration zum Hochladen von Dateien:

1. Navigieren Sie in NetScaler Console zu **Applications** > **Configuration**, und klicken Sie auf **Create New**. Die Seite „Choose StyleBook“ zeigt alle StyleBooks an, die in Ihrer NetScaler Console verfügbar sind. Scrollen Sie nach unten und wählen Sie das importierte StyleBook aus.

   Die StyleBook-Parameter werden als Benutzeroberflächenseite angezeigt, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.
2. Geben Sie den Namen des Load Balancers und die virtuelle IP-Adresse im Abschnitt „Basic Load Balancer Settings“ ein.
3. Geben Sie im Abschnitt **Location File** den Namen oder den Speicherort der Datei ein.

   HINWEIS

   Stellen Sie sicher, dass sich die Datei in der NetScaler Console nur im Ordner des aktuellen Mandanten befindet. Verwenden Sie einen beliebigen FTP-Client, um die Datei in das NetScaler Console-Dateisystem zu kopieren.
4. Möglicherweise werden Sie aufgefordert, Ihre Benutzeranmeldeinformationen anzugeben, bevor Sie auf die Zielinstanzen zugreifen.
5. Wählen Sie die NetScaler-Zielinstanz aus, auf der die Konfiguration erstellt werden soll, und klicken Sie auf **Erstellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Citrix empfiehlt, **Testlauf** auszuwählen, um die Konfigurationsobjekte zu überprüfen, die auf der Zielinstanz erstellt werden, bevor Sie die eigentliche Konfiguration auf der Instanz ausführen.

Wenn die Erstellung des Konfigurationspakets erfolgreich ist, wird die Datei im Dateisystem der NetScaler-Instanz unter dem Speicherort /var/netscaler/inbuilt_db/ gespeichert.

HINWEIS

Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich entdeckte NetScaler-Instanzen in der NetScaler Console zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

Verwenden der NetScaler Console-API zum Erstellen eines Konfigurationspakets

Sie können die NetScaler Console-API auch verwenden, um ein Konfigurationspaket zu erstellen, das Dateien auf die ausgewählte NetScaler-Instanz hochlädt. Weitere Informationen zur Verwendung von APIs finden Sie unter Verwenden der API zum Erstellen von Konfigurationen zum Hochladen beliebiger Dateitypen.

Erstellen Sie ein StyleBook zum Hochladen von SSL-Zertifikats- und Zertifikatsschlüsseldateien

Beim Erstellen einer StyleBook-Konfiguration, die das SSL-Protokoll verwendet, müssen Sie die SSL-Zertifikatsdateien und Zertifikatsschlüsseldateien gemäß den StyleBook-Parametern hochladen. Mit StyleBook können Sie die SSL-Dateien und Schlüsseldateien direkt von Ihrem lokalen System über die NetScaler Console-GUI hochladen. Sie können auch die NetScaler Console-APIs verwenden, um Zertifikatsdateien und Schlüsseldateien hochzuladen, die NetScaler Console bereits verwaltet.

StyleBook-Konfiguration

Dieses Dokument hilft Ihnen, Ihr eigenes StyleBook – **Load Balancing Virtual Server (SSL)** mit Komponenten zum Hochladen von SSL-Zertifikaten und Schlüsseldateien zu erstellen. Das hier als Beispiel bereitgestellte StyleBook erstellt eine grundlegende Load-Balancing-Konfiguration für einen virtuellen Server auf der ausgewählten NetScaler-Instanz. Die Konfiguration verwendet das SSL-Protokoll. Um eine Konfiguration mit diesem StyleBook zu erstellen, müssen Sie den Namen und die IP-Adresse des virtuellen Servers angeben, die Parameter der Load-Balancing-Methode

© 1997–2026 Citrix Systems, Inc. All rights reserved.

auswählen und die Zertifikatsdatei und die Zertifikatsschlüsseldatei für den virtuellen Server hochladen oder eine Zertifikatsdatei und eine Zertifikatsschlüsseldatei verwenden, die bereits in der NetScaler Console vorhanden sind. Diese Parameter sind im folgenden Abschnitt „parameters“ angegeben:

```
parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: certificate
  label: "SSL Certificate File"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  description: "The file name of the SSL certificate file"

  type: certfile

 -

  name: key

  label: "SSL Certificate Key File"

  description: "The file name of the server certificate's private key
file"

  type: keyfile

 -

  name: passphrase

  label: "SSL Certificate Key Passphrase"

  description: "The password used to protect the certificate's private key
file"

  type: password
```

Zwei Komponenten werden dann im Komponentenabschnitt des StyleBooks erstellt. Die Komponente `my-lbvserver-comp` ist vom Typ `ns::lbvserver`, wobei gilt:

- „ns“ ist das Präfix, das sich auf den integrierten Namespace netscaler.nitro.config und die Version 10.5 bezieht, die Sie im Abschnitt `import-stylebooks` angegeben haben.
- `lbvserver` ist ein integriertes StyleBook in diesem Namespace. Es entspricht der NetScaler NITRO `lbvserver` Ressource desselben Namens.

Die zweite Komponente `lbvserver-certificate-comp` ist vom Typ `stlb::vserver-certs-binds`. Das Präfix `stlb` bezieht sich auf den Namespace „com.citrix.adc.stylebooks“ und die Version 1.0, die im Abschnitt „import-stylebooks“ des StyleBooks angegeben ist. Wenn der Namespace „com.citrix.adc.stylebooks“ als Ordner betrachtet werden kann, ist `vserver-certs-binds` ein weiteres StyleBook (oder eine Datei) in diesem Ordner. StyleBooks, die sich im

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Namespace „com.citrix.adc.stylebooks“ befinden, werden als Teil der NetScaler Console ausgeliefert.

Das `vserver-certs-binds` StyleBook, das von benutzerdefinierten StyleBooks verwendet wird, ermöglicht es Ihnen, die Zertifikate einfach zu konfigurieren, indem Sie die Zertifikats- und Schlüsseldateien auf die Ziel-NetScaler-Instanz hochladen und die Bindung der Zertifikats- und Schlüsseldateien an die entsprechenden virtuellen Server konfigurieren. Die Eigenschaften für diese Komponente sind der Name des virtuellen LB-Servers und die Namen der SSL-Zertifikate, die Sie beim Erstellen des Konfigurationspakets angeben.

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: SSL
   ipv46: $parameters.ip
   port: 443
   lbmethod: $parameters.lb-alg
 -
  name: lbvserver-certificate-comp
  type: stlb::vserver-certs-binds
  description: Binds lbvserver with server certificate
  properties:
   vserver-name: $components.my-lbvserver-comp.properties.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
certificates:

 -

  cert-name: $parameters.name + "-lb-cert"

  cert-file: $parameters.certificate

  ssl-inform: PEM

  key-name: $parameters.name + "-key"

  key-file: $parameters.key

  cert-password: $parameters.passphrase
```

Wenn Sie die API verwenden, um eine Konfiguration aus einem solchen StyleBook zu erstellen, verwenden Sie nur die Dateinamen (nicht den vollständigen Dateipfad). Diese Dateien sollten bereits in den Zertifikats- und Schlüsselordnern auf der NetScaler Console verfügbar sein. Die hochgeladene SSL-Zertifikatsdatei wird auf der NetScaler Console im Verzeichnis `/var/mps/tenants/.../ns_ssl_certs` gespeichert, und die SSL-Zertifikatsschlüsseldatei wird im Verzeichnis `/var/mps/tenants/.../ns_ssl_keys` auf der NetScaler Console gespeichert.

Erstellen von Konfigurationen zum Hochladen von SSL-Dateien

Das folgende Verfahren erstellt eine grundlegende Load-Balancing-Konfiguration für einen virtuellen Server auf einer ausgewählten NetScaler-Instanz unter Verwendung des SSL-Protokolls aus dem StyleBook-Beispiel. Sie können dieses Verfahren verwenden, um die SSL-Zertifikatsdateien und die Zertifikatsschlüsseldateien in der NetScaler Console hochzuladen.

So erstellen Sie eine Konfiguration zum Hochladen von Dateien:

1. Navigieren Sie in der NetScaler Console zu **Applications** > **Configuration > StyleBooks**. Die Seite **StyleBooks** zeigt alle StyleBooks an, die in Ihrer NetScaler Console verfügbar sind.
2. Scrollen Sie nach unten und wählen Sie **Load Balancing Virtual Server (SSL)** aus oder geben Sie **Load Balancing Virtual Server (SSL)** in das Suchfeld ein und drücken Sie die **Eingabetaste**.
3. Klicken Sie im StyleBook-Panel auf **Konfiguration erstellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die StyleBook-Parameter werden als Benutzeroberflächenseite angezeigt, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

4. Geben Sie im Abschnitt für die grundlegenden Load Balancer-Einstellungen den Namen des Load Balancers und die virtuelle IP-Adresse ein.
5. Wählen Sie unter **SSL-Zertifikateinstellungen** die entsprechenden Dateien aus Ihrem lokalen Speicherordner aus. Sie können die Dateien auch von der NetScaler Console auswählen.
6. Wählen Sie die Ziel-NetScaler-Instanz aus, auf der die Konfiguration erstellt werden soll, und klicken Sie auf **Erstellen**.

HINWEISE:

Sie können auch auf das Aktualisierungssymbol klicken, um kürzlich entdeckte NetScaler-Instanzen in der NetScaler Console zur verfügbaren Liste der Instanzen in diesem Fenster hinzuzufügen.

In der NetScaler Console ermöglichen Ihnen die folgenden Standard-StyleBooks, die als Teil der NetScaler Console ausgeliefert werden, die Erstellung von SSL-Unterstützung durch Hochladen der SSL-Zertifikate und -Schlüssel.

- HTTP/SSL LoadBalancing StyleBook (lb)
- HTTP/SSL LoadBalancing (mit Monitoren) StyleBook (`lb-mon`)
- HTTP/SSL Content Switched Application mit Monitoren (`cs-lb-mon`)
- Beispiel-Anwendungs-StyleBook mit CS-, LB- und SSL-Funktionen (`sample-cs-app`)

Erstellen Sie Ihr StyleBook

Der vollständige Inhalt der Datei lb-vserver-ssl.yaml wird unten angezeigt:

```
name: lb-vserver-ssl

namespace: com.example.ssl.stylebooks

version: "0.1"

description: "This stylebook defines a load balancing virtual server
configuration."

display-name: "Load Balancing Virtual Server (SSL)"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
schema-version: "1.0"



import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
 -
  namespace: com.citrix.adc.stylebooks
  prefix: stlb
  version: "1.0"


parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  name: lb-alg

  type: string

  allowed-values:

    - ROUNDROBIN

    - LEASTCONNECTION

  default: ROUNDROBIN

 -

  name: certificate

  label: "SSL Certificate File"

  description: "The file name of the SSL certificate file"

  type: certfile

 -

  name: key

  label: "SSL Certificate Key File"

  description: "The file name of the server certificate's private key
file"

  type: keyfile

 -

  name: key

  label: "SSL Certificate Key Passphrase"

  description: "The password used to protect the certificate's private key
file"

  type: password
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
    name: $parameters.name
    servicetype: SSL
    ipv46: $parameters.ip
    port: 443
    lbmethod: $parameters.lb-alg
 -
  name: lbvserver-certificate-comp
  type: stlb::vserver-certs-binds
  description: Binds lbvserver with server certificate
  properties:
   vserver-name: $ components.my-lbvserver-comp.properties.name
   certificates:
    -
     cert-name: $parameters.name + "-lb-cert"
     cert-file: $parameters.certificate
     ssl-inform: PEM
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    key-name: $parameters.name + "-key"

    key-file: $parameters.key

    cert-password: $parameters.passphrase
```

Verwenden der NetScaler Console API zum Erstellen eines Konfigurationspakets:

Sie können auch die NetScaler Console API verwenden, um ein Konfigurationspaket zu erstellen, das Zertifikats- und Schlüsseldateien auf die ausgewählte NetScaler-Instanz hochlädt. Weitere Informationen zur Verwendung von APIs finden Sie unter So verwenden Sie die API zum Erstellen von Konfigurationen zum Hochladen von Zertifikats- und Schlüsseldateien.

Anzeigen der auf der NetScaler-Instanz definierten Objekte

Nachdem die StyleBook-Konfiguration (Konfigurationspaket) in NetScaler Console erstellt wurde, klicken Sie auf **Erstellte Objekte anzeigen**, um alle auf der Ziel-NetScaler-Instanz erstellten NetScaler-Objekte anzuzeigen.

SSL-Zertifikate aus dem Zertifikatsspeicher mit StyleBooks verwalten

Der NetScaler Console-Zertifikatsspeicher hilft Ihnen, Ihre SSL-Zertifikate an einem Ort zu speichern und zu verwalten. So können Sie SSL-Zertifikate in NetScaler Console speichern und sie während der NetScaler-Konfiguration wiederverwenden.

Dieser Artikel beschreibt, wie Sie eine StyleBook-Definition erstellen, mit der Sie SSL-Zertifikate aus dem NetScaler Console-Zertifikatsspeicher hochladen und wiederverwenden können.

Parameter

Die **StyleBook**-Definition unterstützt `certkey` als neuen integrierten Parametertyp. Verwenden Sie diesen Parametertyp, um SSL-Zertifikate aus dem NetScaler Console-Zertifikatsspeicher wiederzuverwenden.

```
parameters:

-

    name: certificate
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    label: Certificate

    description: "Certificate to be bound to this virtual load balanced
application"

    type: certkey

    required: true
```

In diesem Beispiel bezieht sich der Zertifikatsparameter auf ein SSL-Zertifikat oder eine Zertifikatskette aus dem NetScaler Console-Zertifikatsspeicher.

In der **StyleBook**-Definition können Sie sich auf die folgenden Eigenschaften für einen `certkey`-Parameter beziehen:

- `certkeyname` – Ein Name des SSL-Zertifikatsschlüssels, den Sie auf einer Instanz konfigurieren möchten.
- `cert_filename` – Der Dateiname eines SSL-Zertifikats.
- `password` – Das Passwort, das bei Bedarf für den Zugriff auf ein SSL-Zertifikat erforderlich ist.
- `key_filename` – Der Dateiname eines SSL-Zertifikatsschlüssels.
- `keyfile_contents` – Der Dateiinhalt eines SSL-Zertifikats.
- `subject` – Im SSL-Zertifikat genanntes Subjekt.
- `issuer` – Es bezieht sich auf eine Behörde, die das SSL-Zertifikat ausgestellt hat.
- `certchain_certkeyname` – Manchmal werden Serverzertifikate von mehreren hierarchischen Zertifizierungsstellen (CA) signiert, was bedeutet, dass die Zertifikate eine Kette bilden.

  Verwenden Sie diese Eigenschaft, wenn der Zertifikatsspeicher eine Zertifikatskette enthält. Sie hilft Ihnen, die Zertifikate zu referenzieren und miteinander zu verbinden. Wenn Sie ein Konfigurationspaket erstellen, wird die Zertifikatskette als Liste angezeigt.

Diese Eigenschaften helfen Ihnen, die erforderlichen Komponenten in der **StyleBook**-Definition zu erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Komponenten

Wenn ein StyleBook einen `type: certkey`-Parameter hat, kann der StyleBook-Benutzer ein Zertifikat für diesen Parameter aus dem NetScaler Console-Zertifikatsspeicher bereitstellen. In diesem Workflow können Benutzer nicht nur Zertifikate aus dem NetScaler Console-Zertifikatsspeicher anzeigen und auswählen, sondern auch Folgendes tun:

- Neue Zertifikate hochladen.
- Bestehende Zertifikate aktualisieren. Zum Beispiel abgelaufene Zertifikate.
- Zertifikate entfernen.

HINWEISE

- Sie können Zertifikate im NetScaler Console-Zertifikatsspeicher auch über das NetScaler Console SSL Dashboard verwalten.
- Wenn ein SSL-Zertifikat im NetScaler Console-Zertifikatsspeicher aktualisiert wird, werden die mit dem SSL-Zertifikat verknüpften Konfigurationspakete automatisch aktualisiert.

Erstellen Sie Ihr StyleBook

Das Folgende ist ein Beispiel für eine StyleBook-Definition. Es ist eine vollständige Definition, die SSL-Zertifikate aus dem NetScaler Console-Zertifikatsspeicher verwendet. Dieses StyleBook enthält Komponenten, die die Hauptzertifikats- und Schlüsseldateien auf die NetScaler-Instanz hochladen. Wenn diese Dateien bereits auf der NetScaler-Instanz vorhanden sind, überspringt NetScaler Console die Upload-Schritte, und diese Komponenten haben keine Auswirkung.

```
name: lb-with-cert-from-certstore

namespace: com.example.stylebooks

version: "1.0"

display-name: Application using a CertStore certificate

description: This StyleBook defines a simple SSL Vserver.

schema-version: "1.0"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
import-stylebooks:
 -
    namespace: netscaler.nitro.config
    version: "13.0"
    prefix: ns


parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: certificate
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  label: Application Certificate

  description: Certificate chain and key to be bound to this application

  type: certkey

  required: true




components:

 -

    name: pem-cert-files-comp

    type: ns::systemfile

    description: This component uploads the PEM certificate file onto the
NetScaler

    condition: $parameters.certificate

    properties:

      filename: $parameters.certificate.cert_filename

      filelocation: /nsconfig/ssl

      filecontent: base64($parameters.certificate.certfile_contents)

      fileencoding: BASE64

 -

    name: pem-KEY-files-comp

    type: ns::systemfile

    description: This component uploads the PEM key file onto the
NetScaler.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    condition: $parameters.certificate

    properties:

      filename: $parameters.certificate.key_filename

      filelocation: /nsconfig/ssl

      filecontent: base64($parameters.certificate.keyfile_contents)

      fileencoding: BASE64

 -

    name: cert-files-comp

    type: ns::sslcertkey

    description: This component creates the certkey on the NetScaler using
the uploaded files.

    condition: $parameters.certificate

    properties:

      certkey:  $parameters.certificate.certkeyname

      cert: $parameters.certificate.cert_filename

      key: $parameters.certificate.key_filename

 -

  name: lbvserver-comp

  type: ns::lbvserver

  description: This component creates the lbvserver of the application.

  properties:

   name: $parameters.name + "-lbvserver"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 servicetype: SSL

 ipv46: $parameters.ip

 port: 443

 lbmethod: ROUNDROBIN

components:

    -

      name: sslvserver-comp

      type: ns::sslvserver

      description: This component configures SSL settings on the vserver

      properties:

        vservername: $parent.properties.name

        ssl3?: ENABLED

        tls1?: ENABLED

        tls11?: ENABLED

    -

     name: cert-bindings-adv-comp

     type: ns::sslvserver_sslcertkey_binding

     description: This component binds the certkey to the vserver

     condition: $parameters.certificate

     properties:

       vservername: $parent.properties.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        certkeyname: $parameters.certificate.certkeyname
```

Analysen aktivieren und Alarme auf einem in einem StyleBook definierten virtuellen Server konfigurieren

Sie können das Operations-Konstrukt verwenden, um NetScaler Console Analytics so zu konfigurieren, dass AppFlow-Datensätze für alle oder einige der Transaktionen erfasst werden, die von einer virtuellen Serverkomponente verarbeitet werden, die Teil eines StyleBooks ist. Sie können dieses Konstrukt auch verwenden, um Alarme zu konfigurieren, um Einblicke in den vom virtuellen Server verwalteten Datenverkehr zu erhalten.

Das folgende Beispiel zeigt einen Operations-Abschnitt eines StyleBooks:

```
operations:

  analytics:

   -

    name: lbvserver-ops

    properties:

      target: $components.basic-lb-comp

      filter: HTTP.REQ.URL.CONTAINS("catalog")

  alarms:

   -

    name: lbvserver-alarm

    properties:

      target: $components.basic-lb-comp

      email-profile: $parameters.emailprofile

      sms-profile: "MyProdSMS"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      rules:

       -

         metric: "total_requests"

         operator: "greaterthan"

         value: 25

         period-unit: $parameters.period

       -

         metric: "total_bytes"

         operator: "lessthan"

         value: 60

         period-unit: "day"
```

Die Attribute im Analyseabschnitt werden verwendet, um die NetScaler Console Analytics-Funktion anzuweisen, AppFlow-Datensätze auf einer virtuellen Serverkomponente zu erfassen, die durch die Zieleigenschaft identifiziert wird. Optional können Sie auch eine Filtereigenschaft angeben, die einen NetScaler Console-Richtlinienausdruck akzeptiert, um Anfragen zu filtern, für die AppFlow-Datensätze auf dem virtuellen Server erfasst werden.

Wenn ein Konfigurationspaket aus diesem StyleBook erstellt wird, wird die NetScaler Console Analytics-Funktion so konfiguriert, dass AppFlow-Datensätze auf den virtuellen Servern erfasst werden, die bei deren Erstellung im Rahmen der Erstellung eines Konfigurationspakets angegeben wurden.

Die Attribute im Alarmabschnitt werden verwendet, um Schwellenwerte festzulegen, um Alarme zu generieren und Benachrichtigungen auf dem virtuellen Server zu senden, der durch die Zieleigenschaft identifiziert wird. Im obigen Beispiel werden die Eigenschaften „email-profile“ und „SMS-profile“ verwendet, um anzugeben, wohin die Benachrichtigungen gesendet werden sollen. Der Abschnitt „rules“ definiert die Schwellenwerte. Wenn beispielsweise die vom virtuellen Server verarbeiteten Gesamtanfragen größer als 25 sind und dies für einen vom Benutzer definierten

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zeitraum gilt, wird ein Alarm ausgelöst und eine Benachrichtigung gesendet. Die „period-unit“ gibt an, wie oft ein Alarm ausgelöst wird. Sie kann die Werte Tag, Stunde oder Woche annehmen.

Sie können die folgenden Operatoren verwenden, wenn Sie den Metrikwert mit dem Schwellenwert vergleichen:

- `greaterthan` für `>`
- `lessthan` für `<`
- `greaterthanequal` für `>=`
- `lessthanequal` für `<=`

Beachten Sie, dass StyleBooks API-Namen für die Metriken verwenden und nicht die Namen, die in der NetScaler Console Analytics-GUI angezeigt werden.

Informationen zum Anzeigen und Analysieren von Daten, die auf virtuellen Servern gesammelt wurden, die als Teil eines Konfigurationspakets erstellt wurden, finden Sie in der NetScaler Console Analytics-Dokumentation.

Instanzrollen

StyleBooks unterstützt die folgenden Konfigurationen auf NetScaler-Instanzen:

- Symmetrische Konfiguration – Wenn ein Konfigurationspaket auf mehrere NetScaler-Instanzen angewendet wird und die auf allen Instanzen bereitgestellten Konfigurationen identisch sind.
- Asymmetrische Konfiguration – Wenn ein Konfigurationspaket auf mehrere NetScaler-Instanzen angewendet wird und die auf allen Instanzen bereitgestellten Konfigurationen unterschiedlich sind. Zum Beispiel muss im Standard-Microsoft Skype for Business StyleBook eine andere Konfiguration auf jeder NetScaler-Instanz bereitgestellt werden.

Die Funktion „Instanzrollen“ von StyleBooks hilft Ihnen, eine asymmetrische Konfiguration zu erstellen. Hier kann jeder NetScaler-Instanz im Konfigurationspaket eine andere Rolle zugewiesen werden. Die Rolle bestimmt die Konfigurationsobjekte des Konfigurationspakets, die die NetScaler-Instanz erhält.

Wichtige Hinweise:

- Der Satz von Instanzrollen in einem StyleBook wird bei der Erstellung des StyleBooks definiert.
- Die Rollen werden einer bestimmten NetScaler-Instanz zugewiesen, wenn das Konfigurationspaket erstellt oder aktualisiert wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Abschnitt „target-roles“

Der Abschnitt „target-roles“ wird typischerweise nach dem Abschnitt „import-StyleBooks“ und vor dem Abschnitt „parameters“ in einem StyleBook platziert. Alle vom StyleBook unterstützten Rollen werden im Abschnitt „target-roles“ deklariert.

Im folgenden StyleBook-Beispiel sind zwei Rollen im Abschnitt „target-roles“ definiert – A und B.

```
target-roles:



  -

   name: A

   name: B

     min-targets: 2

     max-targets: 5
```

Sie sehen, dass Rolle B auch zwei optionale Untereigenschaften definiert, `min-targets` und `max-targets`.

`min-targets` gibt die minimale obligatorische Anzahl von NetScaler-Instanzen an, denen diese Rolle zugewiesen werden muss, wenn ein Konfigurationspaket aus diesem StyleBook erstellt wird. `max-targets` gibt die maximale Anzahl von NetScaler-Instanzen an, denen diese Rolle zugewiesen werden kann, wenn ein Konfigurationspaket aus diesem StyleBook erstellt wird.

Werden diese Untereigenschaften nicht angegeben, gibt es keine Begrenzung für die Anzahl der NetScaler-Instanzen, die für diese Rolle konfiguriert werden können. Für min-targets = 0 ist die mit der Rolle verbundene Konfiguration optional. Für min-targets = 1 ist die Konfiguration obligatorisch, und mindestens eine NetScaler-Instanz muss für die Rolle konfiguriert werden.

Rolle „default“

Zusätzlich zu explizit definierten Rollen gibt es eine implizite Rolle, die alle StyleBooks haben. Diese implizite Rolle wird als Standardrolle bezeichnet und wird wie jede andere Rolle in einem StyleBook verwendet. Wenn ein Konfigurationspaket erstellt wird und einer NetScaler-Instanz keine spezifische Rolle zugewiesen ist, wird die Instanz implizit der Rolle „default“ zugewiesen. Die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instanz empfängt dann alle Konfigurationsobjekte, die von Komponenten generiert werden, die die Rolle „default“ haben.

Komponenten mit Rollen

Nachdem die Rollen, die ein StyleBook unterstützen kann (einschließlich der Rolle „default“), definiert sind, können die Rollen im Komponentenabschnitt eines StyleBooks verwendet werden. Wenn eine Komponente nur auf NetScaler-Instanzen bereitgestellt werden soll, die eine bestimmte Rolle spielen, können Sie das Rollenattribut als Teil der Komponente angeben, wie im folgenden Beispiel einer Komponente dargestellt:

```
-

  name: C1

  type: ns::lbvserver

  roles:

    - A

  properties:

    name: lb1

    servicetype: HTTP

    ipv46: 1.1.1.1

    port: 80
```

In diesem Beispiel generiert die Komponente ein `lbvserver` und wird auf Instanzen bereitgestellt, die die Rolle A spielen. Das Rollenattribut einer Komponente ist ein `list`, und der Komponente können mehrere Rollen zugewiesen werden. Diese Rollen wären im Abschnitt `target-roles` des StyleBooks deklariert worden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Wenn eine Komponente in einem StyleBook kein Rollenattribut angibt, werden die von der Komponente generierten Konfigurationsobjekte auf allen NetScaler-Instanzen erstellt, unabhängig von den Rollen. Sie können diese Funktion effektiv nutzen, um Konfigurationsobjekte zu erstellen, die auf alle Instanzen eines Konfigurationspakets angewendet werden können.

Betrachten Sie ein StyleBook mit zwei Rollen und vier Komponenten.

- Komponente C1 hat die Rollen A und B
- Komponente C2 hat die Rolle B
- Komponente C3 hat keine Rollen definiert
- Komponente C4 hat die Rolle „default“

Der Komponentenabschnitt dieses StyleBooks sieht wie folgt aus:

```
components:

  -

    name: C1

    type: ns::lbvserver

    roles:

      - A

      - B

    properties:

      name: lb1

      servicetype: HTTP

      ipv46: 1.1.1.1

      port: 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-
  name: C2
  type: ns::lbvserver
  roles:
    - B
  properties:
    name: lb2
    servicetype: HTTP
    ipv46: 12.12.12.12
    port: 80
-
  name: C3
  type: ns::lbvserver
  properties:
    name: lb3
    servicetype: HTTP
    ipv46: 13.13.13.13
    port: 80
-
  name: C4
  type: ns::lbvserver
  roles:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
```

Die Komponente C3 hat keine Rolle definiert, was bedeutet, dass die Komponente auf allen Instanzen bereitgestellt wird, unabhängig von ihrer Rolle. Andererseits hat Komponente C4 die Rolle „default“, was bedeutet, dass sie auf jede Instanz angewendet wird, der keine explizite Rolle zugewiesen ist.

Nehmen wir nun an, Sie möchten ein Konfigurationspaket mit diesem StyleBook erstellen und es auf fünf NetScaler-Instanzen bereitstellen. Sie können die Rollen den Instanzen auf folgende Weise zuweisen:

- Rolle A ist den Instanzen T1, T2, T3 und T4 zugewiesen
- Rolle B ist den Instanzen T2, T3 und T4 zugewiesen.
- Der Instanz T5 ist keine Rolle zugewiesen.

Die folgende Abbildung fasst die Rollenzuweisungen zusammen und zeigt die resultierende Konfiguration, die jede NetScaler-Instanz erhält:

Die Komponente C3 wird auf allen Instanzen unabhängig von der Rolle bereitgestellt, da diese Komponente kein `roles`-Attribut hatte.

Verwenden Sie die Funktion „Dry Run“, um Folgendes anzuzeigen und zu überprüfen:

- Die Zuweisung von Rollen
- Die auf jeder NetScaler-Instanz erstellten Konfigurationsobjekte

Erstellen Sie Ihr StyleBook

Der vollständige Inhalt des StyleBooks „demo-target-roles“ lautet wie folgt:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
---

name: demo-target-roles

namespace: com.example.stylebooks

version: "1.2"

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"

parameters:

  -

    name: appname

    type: string

    required: true

    key: true

target-roles:

  -

    name: A

  -

    name: B

    min-targets: 2
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    max-targets: 5
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    port: 80
-
  name: C3
  type: ns::lbvserver
  properties:
    name: lb3
    servicetype: HTTP
    ipv46: 13.13.13.13
    port: 80
-
  name: C4
  type: ns::lbvserver
  roles:
    - default
  properties:
    name: lb4
    servicetype: HTTP
    ipv46: 14.14.14.14
    port: 80
```

Die folgende Abbildung zeigt die für ein Beispiel-Konfigurationspaket erstellten Objekte:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verwenden von APIs

Bei Verwendung der REST-API können Sie Rollen für jede NetScaler-Instanz angeben, wenn Sie das Konfigurationspaket wie folgt erstellen oder aktualisieren. Geben Sie im Block „targets“ die UUID der spezifischen NetScaler-Instanz an, auf der Sie die einzelnen Komponenten bereitstellen möchten.

```
"targets": [

           {

            "id": "<ADC-UUID>",

            "roles": ["A"]

           },

          ]
```

Eine vollständige Beispiel-REST-API wird als Referenz bereitgestellt.

POST /`<IP`>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"

    },

     "targets": [

        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",

        "roles": ["A"]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        },
        {
          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",
          "roles": ["A", "B"]
        },
        {
          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
          "roles": ["A", "B"]
        },
        {
          "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
          "roles": ["A", "B"]
        },
        {
          "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
          "roles": ["default"]
        }
      ]
    }
}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Erstellen eines StyleBooks zum Ausführen von Nicht-CRUD-Operationen

StyleBooks verwalten NetScaler-Konfigurationen, indem sie die erforderlichen Konfigurationsobjekte auf den NetScaler-Instanzen berechnen. Diese Objekte werden der Instanz jedes Mal hinzugefügt, aktualisiert oder daraus entfernt, wenn Sie ein ConfigPack erstellen oder aktualisieren. Dann geben Sie den "gewünschten Zustand" an.

Einige NetScaler-Konfigurationsobjekte unterstützen jedoch einige andere Operationen als Erstellen, Aktualisieren oder Löschen (CRUD-Operationen). Beispielsweise kann ein Lastenausgleichsobjekt (`lbvserver`) oder ein NetScaler-Feature-Objekt (`nsfeature`) die Operation "Aktivieren" oder "Deaktivieren" unterstützen. Ähnlich unterstützen NetScaler `certkeys` die Operationen "Verknüpfen" und "Verknüpfung aufheben", um ein Zertifikat mit einem anderen Zertifikat zu verknüpfen oder die Verknüpfung aufzuheben. Diese Operationen an NetScaler-Objekten werden als Nicht-CRUD-Operationen bezeichnet.

Dieser Abschnitt beschreibt, wie Nicht-CRUD-Operationen an Konfigurationsobjekten, die diese unterstützen, mithilfe von StyleBooks ausgeführt werden.

HINWEIS

Die Bindung zwischen Konfigurationsobjekten (z. B. das Binden eines `certkey` an ein `lbvserver`) ist keine Nicht-CRUD-Operation, da NITRO-Bindungen als eigenständige Konfigurationsobjekte dargestellt werden. Diese Objekte werden wie jedes andere NetScaler-Konfigurationsobjekt erstellt und gelöscht.

Unterstützung der Nicht-CRUD-Operationen

Ein Konstrukt namens `meta-properties` wird in der Komponente auf derselben Ebene wie das `properties`-Konstrukt hinzugefügt. Das unterstützte Attribut in diesem Konstrukt heißt `action`. Dieses Attribut kann Werte wie `enable`, `disable`, `link`, `unlink`, `import`, `export`, `create`, `archive` und `apply` annehmen.

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  meta-properties

   action: enable

  properties:

    name: $parameters.name

    servicetype: HTTP

    ipv46: $parameters.ip

    port: 80

    lbmethod: $parameters.lb-alg
```

In diesem Beispiel ist die `my-lbvserver-comp`-Komponente vom Typ `ns::lbvserver`. Das "ns" ist das Präfix, das sich auf den Namespace netscaler.nitro.config und die Version ** 10.5 bezieht, die Sie im Abschnitt import-stylebooks angegeben haben. Das `lbvserver` ist eine NITRO-Ressource in diesem Namespace. Als implizite Aktion erstellt das StyleBook `lbvserver` und schließt dann die Operation "Aktivieren" daran ab.

Das `action` in den Meta-Eigenschaften wird am Konfigurationsobjekt nur während der Erstellung des ConfigPacks durchgeführt. Aktualisierungen des ConfigPacks führen keine Nicht-CRUD-Aktionen aus.

Sie können Ausdrücke für eine Meta-Eigenschaft angeben. Diese Ausdrücke wenden die gültigen Meta-Eigenschaftsaktionen für NetScaler-Objekte dynamisch an.

Beispiel:

```
parameters:

-

    name: meta-action-lbvserver

    type: string

    default: disable
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    allowed-values:
      - enable
      - disable


components:
  -
    name: c1
    type: ns::lbvserver
    meta-properties:
      action: $parameters.meta-action-lbvserver
    properties:
      name: $parameters.lbvserver
      ipv46: $parameters.ip
      port: 80
      servicetype: HTTP
```

In diesem Beispiel kann ein StyleBook-Benutzer beim Erstellen eines Konfigurationspakets eine gültige Meta-Eigenschaftsaktion angeben.

Bereitstellen von GSLB-Konfigurationen mithilfe von DNS-Domainnamen

Die neuen RBAC-Verbesserungen in NetScaler Console ermöglichen es nur autorisierten Anwendungsbesitzern, ihre eigenen DNS-Domains in NetScaler Console zu erstellen und zu verwalten. Sie können die App-Besitzer jetzt autorisieren, GSLB-Konfigurationen aus den DNS-Domains, die sie besitzen, mithilfe spezifischer StyleBooks zu erstellen. Wenn der ausgewählte DNS-Domainname dem Benutzer gehört, kann er beim Erstellen von GSLB-Konfigurationen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

mithilfe von GSLB-StyleBooks im NetScaler Console Anwendungs-Dashboard verwendet werden. Es gibt zwei Workflows in NetScaler Console zum Konfigurieren von GSLB-Konfigurationen.

1. **Workflow für Administratoren**. Richten Sie die RBAC-Umgebung in NetScaler Console ein. Das heißt, um GSLB-StyleBooks zu erstellen und zu importieren, müssen Sie Benutzergruppen, Richtlinien und Rollen erstellen und Benutzer der Gruppe zuweisen. Als Administrator müssen Sie diesen Workflow ausführen.
2. **Workflow für Anwendungsbesitzer**. Anwendungsbesitzer müssen GSLB-Konfigurationen mithilfe von Domainnamen erstellen, die sie besitzen.

Das folgende Flussdiagramm stellt beide Workflows dar:

Workflow für Administratoren

Als Administrator besteht Ihr Workflow zum Erstellen der RBAC-Umgebung in NetScaler Console aus den folgenden Schritten:

Erstellen Sie zunächst ein StyleBook, um GSLB-Konfigurationen auf den NetScaler-Instanzen bereitzustellen. Dieses Dokument enthält einen Beispiel-YAML-Inhalt, der Ihnen hilft, Ihr eigenes StyleBook zu erstellen – Erstellen Sie Ihr StyleBook.

Weitere Informationen zum Erstellen benutzerdefinierter StyleBooks finden Sie unter Benutzerdefinierte StyleBooks erstellen und verwenden.

HINWEIS:

NetScaler Console unterstützt ein neues Konstrukt in StyleBooks namens „allowed-dynamic-values“. Dieses Konstrukt kann verwendet werden, um dem Benutzer zu ermöglichen, aus den in NetScaler Console vorhandenen DNS-Domain-Werten aufzulisten und auszuwählen, um den Parameter „domain-name“ im StyleBook in der NetScaler Console GUI automatisch zu füllen.

Ein Beispielabschnitt für den Parameter „domain-name“ wird als Referenz bereitgestellt.

Der hier verwendete Parameter „domain-name“ ist nur ein Beispiel. Der Parameter kann in Ihrem benutzerdefinierten StyleBook unterschiedlich sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

  name: domain-name

   label: DNS Domain Name

   description: GSLB DNS Domain Name

   type: string

   required: true

   allowed-dynamic-values:

      source: local

      resource-type: dns_domain_entry
```

HINWEIS:

Derzeit wird in NetScaler Console das Konstrukt „allowed-dynamic-values“ in keinem der Standard-StyleBooks verwendet. Erstellen Sie ein neues benutzerdefiniertes GSLB StyleBook, indem Sie das Standard-GSLB StyleBook verwenden. Ersetzen Sie den Teil für den Domänennamenparameter durch das oben angegebene Beispiel. Sie können jeden Texteditor verwenden, um neue StyleBooks zu erstellen.

1. Melden Sie sich als Administrator bei NetScaler Console an.
2. Navigieren Sie zu **Applications** > **Configurations** > **StyleBooks**.
3. Klicken Sie auf **Import New StyleBook** und laden Sie das neue GSLB StyleBook in NetScaler Console hoch.

   Weitere Informationen zum Importieren von StyleBooks in NetScaler Console finden Sie unter Benutzerdefinierte StyleBooks verwenden.
4. Navigieren Sie zu **System** > **Users** > **Policies** und klicken Sie auf **Add**, um eine Zugriffsrichtlinie für die Anwendungsbesitzer wie unten gezeigt einzurichten.

   Citrix empfiehlt, dass Sie eine Zugriffsrichtlinie erstellen, um sicherzustellen, dass die Anwendungsbesitzer die von Ihnen festgelegten RBAC-Regeln nicht umgehen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Geben Sie einen Namen für die Richtlinie und eine kurze Beschreibung ein. Stellen Sie im Abschnitt „Permissions“ sicher, dass die folgenden Anzeige-/Bearbeitungsberechtigungen obligatorisch aktiviert sind.

   a. Applications > Dashboard
   b. Applications > Configurations
   c. Infrastructure > Instances
   d. Infrastructure > License Management
   e. Settings > Domain Names

   Sie können weitere Berechtigungen nach Bedarf vergeben und auf **Create** klicken.

6. Navigieren Sie zu **System** > **Benutzer** > **Rollen**, erstellen Sie eine Rolle und weisen Sie die im vorherigen Schritt erstellte Richtlinie zu.
7. Geben Sie einen Namen für die Rolle ein und geben Sie eine kurze Beschreibung an. Wählen Sie im Abschnitt Richtlinien **AppOwnerExampleAccessPolicy** aus.

8. Navigieren Sie zu **System** > **Benutzer** > **Gruppen**, erstellen Sie eine Gruppe und ordnen Sie die im vorherigen Schritt erstellte Rolle zu.
9. Geben Sie einen Namen und eine Beschreibung ein, und wählen Sie im Abschnitt Rollen **AppOwnerExampleRole** aus.

10. Klicken Sie auf **Weiter**.
11. Wählen Sie auf der Registerkarte **Autorisierungseinstellungen** die NetScaler-Instanzen aus, auf die der Anwendungsbesitzer Zugriff hat, und das neue GSLB StyleBook.

    Wiederholen Sie diesen Schritt, um so viele Benutzergruppen zu erstellen, wie Sie in Ihrer Organisation benötigen. Klicken Sie auf **Gruppe erstellen**.

12. Erstellen Sie einen Systembenutzer und weisen Sie den Benutzer einer Benutzergruppe zu. Dieses Dokument bezieht sich nur auf lokal erstellte Benutzer. Sie müssen keine Benutzer in Benutzergruppen erstellen, wenn NetScaler Console für die Verwendung externer Authentifizierung, z. B. LDAP, eingerichtet ist. Die Benutzerzuordnung zu Gruppen wird aus dem externen Authentifizierungsverzeichnis abgerufen.

    a. Navigieren Sie zu **System** > **Benutzer** > **Benutzer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Geben Sie einen Benutzernamen und ein Kennwort für den Systembenutzer ein und weisen Sie den Benutzer der Gruppe zu.

HINWEIS:

Schritt 12 ist optional und nicht erforderlich, wenn eine externe Authentifizierung wie LDAP verwendet wird.

NetScaler Console REST API für den Administrator-Workflow

REST API zum Anmelden bei NetScaler Console

```
URL: http: //<MAS_IP>/nitro/v2/config/login

HTTPMETHOD: POST



Body Payload:

{

  "login": {

    "username": "<USER_NAME>",

    "password": "<PASSWORD>",

    "session_timeout": 1800

  }

}


The response results in a session cookie header, that can be sent with the
rest of the API requests below.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-Cookie:
SESSID=##ED31F7C886E248CCDCA8F0E0AD2AA511ACCC5F46C48D6D2BCAA719A9DE62;path
=/;secure;HttpOnly
```

REST API zum Erstellen einer Zugriffsrichtlinie

```
URL: https://<MAS_IP>/nitro/v2/config/rba_policy

HTTP METHOD: POST



{

  "rba_policy": {

    "name": " AppOwnerAccessPolicy",

    "description": " ExampleCompany AppOwner Access Policy",

    "tenant_id": "7c12ec97-1472-4096-97e7-a5acb453cc5c",

    "statement": [

      {

        "access_type": true,

        "resource_type": "application",

        "operation_name": "add",

        "dependent_resources":
"mail_profile,slack_profile,smtp_server,app_category"

      },

      {

        "access_type": true,

        "resource_type": "application",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "operation_name": "get",

        "dependent_resources":
"download,smtp_server,ns_vserver_license,app_category,app_summary,app_heal
th_dashboard_details,haproxy_frontend,haproxy_backend,haproxy_frontend_sta
ts"

      },

      {

        "access_type": true,

        "resource_type": "si_app_unit",

        "operation_name": "get",

        "dependent_resources":
"download,smtp_server,app_summary,si_app_summary,si_device,security_app_da
shboard_details,si_geo_location,si_safety_app_firewall,si_safety_overview,
si_safety_security_check,si_safety_system_security,si_safety_signature"

      },

      {

        "access_type": true,

        "resource_type": "stylebooks",

        "operation_name": "get",

        "dependent_resources": "download,smtp_server,ns_vserver_license"

      },

      {

        "access_type": true,

        "resource_type": "stylebooks",

        "operation_name": "add",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "dependent_resources": "mail_profile,slack_profile,smtp_server"
      },
      {
        "access_type": true,
        "resource_type": "configpacks",
        "operation_name": "get",
        "dependent_resources":
"download,smtp_server,stylebooks,ns_vserver_license"
      },
      {
        "access_type": true,
        "resource_type": "configpacks",
        "operation_name": "add",
        "dependent_resources": "mail_profile,slack_profile,smtp_server"
      },
      {
        "access_type": true,
        "resource_type": "stylebooks_system_settings",
        "operation_name": "get",
        "dependent_resources": "download,smtp_server"
      },
      {
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "access_type": true,

        "resource_type": "stylebooks_system_settings",

        "operation_name": "add",

        "dependent_resources": "mail_profile,slack_profile,smtp_server"

      },

      {

        "access_type": true,

        "resource_type": "ns_crvserver",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_cache_redirection_report,poll_ac
tivity_status,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_crvserver",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "haproxy_frontend",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,haproxy_backend,haproxy_server"

      },

      {

        "access_type": true,

        "resource_type": "haproxy_frontend",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server"

      },

      {

        "access_type": true,

        "resource_type": "ns_server",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,ns_emon_poll_policy,poll_activity_sta
tus,ns_server,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_server",

        "operation_name": "add",

        "dependent_resources":
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_lbvserver",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_lb_vserver_report,ns_emon_poll_p
olicy,poll_activity_status,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_lbvserver",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_service",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,ns_emon_poll_policy,poll_activity_sta
tus,ns_visualizer_lb_bindings,lb_export_report"
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      },
      {
        "access_type": true,
        "resource_type": "ns_service",
        "operation_name": "add",
        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,ns_visualizer_lb_bindings,lb_export_report"
      },
      {
        "access_type": true,
        "resource_type": "ns_servicegroup",
        "operation_name": "get",
        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,ns_emon_poll_policy,poll_activity_sta
tus,ns_servicegroupmember_binding,ns_visualizer_lb_bindings,lb_export_repo
rt"
      },
      {
        "access_type": true,
        "resource_type": "ns_servicegroup",
        "operation_name": "add",
        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,ns_servicegroupmember_binding,ns_visualizer_lb_bindi
ngs,lb_export_report"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      },
      {
        "access_type": true,
        "resource_type": "ns_authenticationvserver",
        "operation_name": "get",
        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_authentication_report,poll_activ
ity_status,ns_emon_poll_policy,lb_export_report"
      },
      {
        "access_type": true,
        "resource_type": "ns_authenticationvserver",
        "operation_name": "add",
        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"
      },
      {
        "access_type": true,
        "resource_type": "syslog_messages",
        "operation_name": "get",
        "dependent_resources": "download,smtp_server"
      },
      {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "access_type": true,

        "resource_type": "ns_emon_poll_policy",

        "operation_name": "get",

        "dependent_resources": "download,poll_activity_status,smtp_server"

      },

      {

        "access_type": true,

        "resource_type": "ns_emon_poll_policy",

        "operation_name": "add",

        "dependent_resources":
"download,poll_activity_status,mail_profile,slack_profile,smtp_server"

      },

      {

        "access_type": true,

        "resource_type": "ns_visualizer_gslb_bindings",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,ns_gslbvserver_domain,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_visualizer_gslb_bindings",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,poll_activity_status,ns_emon_poll_pol
icy,ns_gslbvserver_domain,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_gslbservice",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_gslbservice",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,poll_activity_status,ns_emon_poll_pol
icy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_gslbvserver",

        "operation_name": "get",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_global_server_load_balancing_rep
ort,poll_activity_status,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_gslbvserver",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"

     },

      {

        "access_type": true,

        "resource_type": "ns_vpnvserver",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,poll_activity_statu
s,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_vpnvserver",

        "operation_name": "get",

        "dependent_resources":
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"download,DeviceAPIProxy,smtp_server,perf_ssl_vpn_report,poll_activity_sta
tus,ns_emon_poll_policy,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "ns_csvserver",

        "operation_name": "get",

        "dependent_resources":
"download,DeviceAPIProxy,smtp_server,perf_content_switching_report,ns_emon
_poll_policy,poll_activity_status,ns_visualizer_cs_bindings,lb_export_repo
rt"

      },

      {

        "access_type": true,

        "resource_type": "ns_csvserver",

        "operation_name": "add",

        "dependent_resources":
"DeviceAPIProxy,mail_profile,slack_profile,smtp_server,ns_emon_poll_policy
,poll_activity_status,ns_visualizer_cs_bindings,lb_export_report"

      },

      {

        "access_type": true,

        "resource_type": "dns_domain_entry",

        "operation_name": "get",

        "dependent_resources": ""
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      },
      {
        "access_type": true,
        "resource_type": "dns_domain_entry",
        "operation_name": "add",
        "dependent_resources": ""
      },
      {
        "access_type": true,
        "resource_type": "devicewise_detail_summary",
        "operation_name": "get",
        "dependent_resources":
"download,mps_user_heatmap,ns_event,mps_agent,active_event,smtp_server,mps
_datacenter,event_severity_report,event_device_report,ns_conf,device_event
_summary"
      },
      {
        "access_type": true,
        "resource_type": "devicewise_detail_summary",
        "operation_name": "add",
        "dependent_resources": "mail_profile,slack_profile,smtp_server"
      },
      {
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "access_type": true,

        "resource_type": "cbwanopt",

        "operation_name": "get",

        "dependent_resources":
"download,device_backup,traceroute,inventory,inventory_status,ping,mps_dat
acenter,cbwanopt_device_profile,sdwanvw_device_profile,sdwanvw_snmp_config
,sdwanvw_appflowconfig,smtp_server,cbwanopt_snmp_config,cbwanopt_appflowco
nfig,sdwanvw,tag"

      },

      {

        "access_type": true,

        "resource_type": "cbwanopt",

        "operation_name": "add",

        "dependent_resources":
"inventory,managed_device,device_backup,upload,cbwanopt_device_profile,mps
_datacenter,mail_profile,slack_profile,smtp_server,sdwanvw_device_profile,
sdwanvw_snmp_config,sdwanvw_appflowconfig,cbwanopt_snmp_config,cbwanopt_ap
pflowconfig,sdwanvw,tag"

      },

      {

        "access_type": true,

        "resource_type": "device_login",

        "operation_name": "get",

        "dependent_resources": ""

      },

      {
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "access_type": true,

        "resource_type": "ns",

        "operation_name": "get",

        "dependent_resources":
"download,ns_config_replicate,ns_conf,ns_ns_runningconfig,ns_ns_savedconfi
g,active_event,device_backup,traceroute,inventory,inventory_status,ping,ns
_device_profile,nssdx_device_profile,sdx_snmp_config,sdx_syslog_config,smt
p_server,ns_cluster,ns_snmp_config,ns_syslog_config,ns_l7_latency_config,i
ca_l7_latency_update,af_vserver_policy,ns_vserver_appflow_config,mps_datac
enter,ns_appflow_param_config,ns_ns_license,ns_ns_mode,ns_network_interfac
e,advanced_analytics_config,tag"

      },

      {

        "access_type": true,

        "resource_type": "ns",

        "operation_name": "add",

        "dependent_resources":
"inventory,ns_l7_latency_config,ica_l7_latency_update,af_vserver_policy,ns
_config_replicate,managed_device,device_backup,upload,ns_device_profile,ns
sdx_device_profile,mps_datacenter,sdx_snmp_config,sdx_syslog_config,mail_p
rofile,slack_profile,smtp_server,ns_cluster,ns_snmp_config,ns_syslog_confi
g,ns_vserver_appflow_config,ns_appflow_param_config,advanced_analytics_con
fig,tag"

      },

      {

        "access_type": true,

        "resource_type": "haproxyhost",

        "operation_name": "get",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "dependent_resources":
"download,traceroute,inventory,inventory_status,ping,mps_datacenter,smtp_s
erver,haproxy_device_profile,device_backup,tag"

      },

      {

        "access_type": true,

        "resource_type": "haproxyhost",

        "operation_name": "add",

        "dependent_resources":
"inventory,managed_device,mail_profile,slack_profile,smtp_server,mps_datac
enter,haproxy_device_profile,haproxy,device_backup,tag"

      },

      {

        "access_type": true,

        "resource_type": "docker_host",

        "operation_name": "add",

        "dependent_resources":
"inventory,ns_snmp_config,managed_device,ns,upload,mail_profile,slack_prof
ile,smtp_server,mps_datacenter,ns_device_profile,docker_nscpx_image"

      },

      {

        "access_type": true,

        "resource_type": "docker_host",

        "operation_name": "get",

        "dependent_resources":
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"download,ns_snmp_config,ns_conf,ns_ns_runningconfig,ns_ns_savedconfig,smt
p_server,mps_datacenter,ns_device_profile,traceroute,inventory,inventory_s
tatus,ping,active_event,ns_ns_license,ns_ns_mode,ns_network_interface"

      },

      {

        "access_type": true,

        "resource_type": "perf_reports",

        "operation_name": "add",

        "dependent_resources":
"mail_profile,slack_profile,smtp_server,perf_custom_dashboard"

      },

      {

        "access_type": true,

        "resource_type": "perf_reports",

        "operation_name": "get",

        "dependent_resources":
"download,smtp_server,perf_report_counters,perf_res_util_report,perf_http_
req_tcp_conn_report,perf_lb_ssl_traffic_report,perf_ip_bytes_rxtx_report,p
erf_ip_pkt_rxtx_report,perf_icmp_pkt_rxtx_report,perf_icmp_bytes_rxtx_repo
rt,perf_icmpv6_pkt_rxtx_report,perf_icmpv6_bytes_rxtx_report,perf_ipv6_byt
es_rxtx_report,perf_ipv6_pkt_rxtx_report,perf_udp_bytes_rxtx_report,perf_u
dp_packets_rxtx_report,perf_cmp_bytes_rxtx_report,perf_cmp_tcp_bytes_rxtx_
report,perf_cmp_tcp_ratiosaving_report,perf_cmp_decmp_bytes_rxtx_report,pe
rf_cmp_decmp_ratiosaving_report,perf_tcp_server_conn_report,perf_tcp_surge
len_spareconn_report,perf_http_bytes_rx_report,perf_http_gets_posts_report
,perf_ssl_transactions_hits_report,perf_ssl_client_auth_report,perf_ssl_rs
a_dhkey_report,perf_ssl_frontend_ciphers_report,perf_ssl_backend_ciphers_r
eport,perf_wsdevice_cpu_utilization_report,perf_wsdevice_send_compression_
ratio_report,perf_wsdevice_connected_plugins_report,perf_wsdevice_data_red
uction_report,perf_wsdevice_link_utilization_report,perf_wsserviceclasssta
tstable_pass_through_connection_report,perf_wsserviceclassstatstable_servi
ce_class_report,perf_wsserviceclassstatstable_acceleration_report,perf_wsl
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
inkstatstable_throughput_report,perf_wslinkstatstable_packet_loss_report,p
erf_wsappstatstable_application_report,perf_wsqosstatstable_qos_report,per
f_ssl_cpu_keyexchange_report,perf_ssl_be_rsa_dhkey_report,perf_custom_dash
board,perf_ns_throughput_report,perf_network_interface_report"

      },

      {

        "access_type": true,

        "resource_type": "perf_threshold",

        "operation_name": "get",

        "dependent_resources":
"download,perf_reports,perf_report_counters,smtp_server,sms_server,sms_pro
file"

      },

      {

        "access_type": true,

        "resource_type": "perf_threshold",

        "operation_name": "add",

        "dependent_resources":
"mail_profile,slack_profile,smtp_server,sms_server,sms_profile"

      },

      {

        "access_type": true,

        "resource_type": "perf_poll_config",

        "operation_name": "add",

        "dependent_resources": "mail_profile,slack_profile,smtp_server"
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      },
      {
        "access_type": true,
        "resource_type": "perf_poll_config",
        "operation_name": "get",
        "dependent_resources": "smtp_server,download"
      },
      {
        "access_type": true,
        "resource_type": "license_server_info",
        "operation_name": "get",
        "dependent_resources":
"sms_server,license_proxy_server,jazz_license,download,sms_profile,smtp_se
rver,user_managed_tp_vserver,managed_vserver,user_managed_vserver,haproxy_
frontend,haproxy_backend,license_file,device_license_info,license_info,ns_
authenticationvserver,ns_gslbvserver,ns_vpnvserver,ns_csvserver,ns_crvserv
er,ns_lbvserver,autoselection_preference,license_threshold,license_expiry_
info"
      },
      {
        "access_type": true,
        "resource_type": "license_server_info",
        "operation_name": "add",
        "dependent_resources":
"sms_server,license_proxy_server,jazz_license,sms_profile,mail_profile,sla
ck_profile,smtp_server,user_managed_tp_vserver,managed_vserver,upload,lice
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
nse_file,license_info,license_threshold,mas_license,user_managed_vserver,a
utoselection_preference,license_expiry_info"

      }

    ],

    "ui": [

      {

        "access_type": true,

        "name": "ApplicationsDashboard",

        "display_name": "Dashboard"

      },

      {

        "access_type": true,

        "name": "SecurityDashboard",

        "display_name": "App Security Dashboard"

      },

      {

        "access_type": true,

        "name": "Stylebooks",

        "display_name": "StyleBooks"

      },

      {

        "access_type": true,

        "name": "Stylebooks",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "display_name": "Configpacks"
      },
      {
        "access_type": true,
        "name": "StylebooksSettings",
        "display_name": "Settings"
      },
      {
        "access_type": true,
        "name": "CacheRedirection",
        "display_name": "Cache Redirection"
      },
      {
        "access_type": true,
        "name": "Servers",
        "display_name": "Servers"
      },
      {
        "access_type": true,
        "name": "VirtualServers",
        "display_name": "Virtual Servers"
      },
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{
  "access_type": true,
  "name": "Services",
  "display_name": "Services"
},
{
  "access_type": true,
  "name": "ServiceGroups",
  "display_name": "Service Groups"
},
{
  "access_type": true,
 "name": "Authentication",
  "display_name": "Authentication"
},
{
  "access_type": true,
  "name": "MonitoringAuditing",
  "display_name": "Auditing"
},
{
  "access_type": true,
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "name": "MonitoringSettings",
        "display_name": "Settings"
      },
      {
        "access_type": true,
        "name": "GSLBDomains",
        "display_name": "Domains"
      },
      {
        "access_type": true,
        "name": "GSLBServices",
        "display_name": "Services"
      },
      {
        "access_type": true,
        "name": "GSLBVirtualServer",
        "display_name": "Virtual Server"
      },
      {
        "access_type": true,
        "name": "NetScalerGateway",
        "display_name": "NetScaler Gateway"
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    },
    {
      "access_type": true,
      "name": "ContentSwitching",
      "display_name": "Content Switching"
    },
    {
      "access_type": true,
      "name": "DNSDomainNames",
      "display_name": "DNS Domain Names"
    },
    {
      "access_type": true,
      "name": "NetworkDashboard",
      "display_name": "Instances Dashboard"
    },
    {
      "access_type": true,
      "name": "NetScalerSDWANWOInstances",
      "display_name": "NetScaler SD-WAN"
    },
    {
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "access_type": true,
        "name": "InstanceOperations",
        "display_name": "Instance Operations"
      },
      {
        "access_type": true,
        "name": "NetScalerInstances",
        "display_name": "NetScaler ADC"
      },
      {
        "access_type": true,
        "name": "NetScalerCPXDockerHost",
        "display_name": "Docker Hosts"
      },
      {
        "access_type": true,
        "name": "Reports",
        "display_name": "Reports"
      },
      {
        "access_type": true,
        "name": "Thresholds",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "display_name": "Thresholds"
      },
      {
        "access_type": true,
        "name": "ReportingSettings",
        "display_name": "Settings"
      },
      {
        "access_type": true,
        "name": "Licenses",
        "display_name": "License Management"
      }
    ]
  }
}
```

REST API zum Erstellen einer Zugriffsrolle

```
URL: https://<MAS_IP>/nitro/v2/config/rba_role

HTTPMETHOD: POST



Payload:

{
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "rba_role": {
    "name": "AppOwnerRole",
    "description": "ExampleCompany App Owner Role",
    "policies": [
      "AppOwnerAccessPolicy"
    ]
  }
```

REST API zum Hochladen eines neuen GSLB StyleBooks

```
URL: https://<MAS_IP>/stylebook/nitro/v2/config/stylebooks

HTTPMETHOD: POST



Payload:

{
    "stylebook": {
      "file_name": "my-own-gslb.yaml",
      "source": "bmFtZTogZ3NsYi1kbnMtZG9tYW...aXRvcm5hbWU=",
      "encoding": "base64"
    }
  }
```

HINWEIS:

Der Name des StyleBooks kann auf Ihrem System variieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REST API zum Erstellen von Gruppen und Zuweisen ausgewählter Instanzen und StyleBooks

```
URL: https://<MAS_IP>/nitro/v2/config/mpsgroup

HTTPMETHOD: POST



Payload:

{

  "mpsgroup": {

    "id": "",

    "name": "AppOwnerGroup1",

    "description": "ExampleCompany App Owner Group",

    "roles": [

      "AppOwnerRole"

    ],

    "enable_session_timeout": false,

    "assign_all_devices": false,

    "ass ign_all_apps": false,

    "application_names_with_regex": [



    ],

    "standalone_instances_id": [

      "72c178da-47df-4426-9acc-cd6316f92506",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "c948061e-6240-4062-931c-f6988ef36e3b"
    ],
    "application_list": [


    ],
    "permission": "none",
    "application_names": [


    ],
    "authscope_props": [
      {
        "propname": "configuration_template_id",
        "propvalues": [
          "NONE"
        ]
      },
      {
        "propname": "dns_domain_entry_id",
        "propvalues": [
          "cf6631e5-2f56-4bb1-b0a5-90fabfc0e3e2",
          "b268905c-522d-47e3-a2ca-3f8d8a754373"
        ]
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      },
      {
        "propname": "stylebook_id",
        "propvalues": [
          "gslbbb963abe85936913035e1d4dd14b56f7",
          "moni72fad4494466d102b19c18ac329fa9f3"
        ]
      }
    ],
    "tenant_id": "6d024111-6636-4571-a250-d47b31aba7a8"
  }
}
```

HINWEIS:

Um die IDs für DNS-Domainnamen und GSLB StyleBooks zu erhalten, die in der obigen API-Nutzlast verwendet werden sollen, können Sie reguläre NetScaler Console APIs verwenden, um IDs abzufragen, die den Entitätsnamen entsprechen. Um beispielsweise die ID für eine DNS-Domain namens „app1.acme.com“ zu erhalten, können Sie die folgende NetScaler Console REST API verwenden.

```
URL: https://<MAS_IP>/nitro/v2/config/dns_domain_entry?filter=name:
app1.acme.com

HTTPMETHOD: GET



The ID of this domain can be extracted from the following response.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{
  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "dns_domain_entry",
  "username": "nsroot",
  "tenant_name": "Owner",
  "tenant_id": "568d8e12-1d88-42b2-8943-cbaa04826fd1",
  "resourceName": "",
  "dns_domain_entry": [
    {
      "tenant_id": "568d8e12-1d88-42b2-8943-cbaa04826fd1",
      "name": "app1.acme.com",
      "id": "3e3d85ea-1c21-49b2-97f4-60fccdbae2e0",
      "description": "app1 domain name"
    }
  ]
}
```


Ähnlich können Sie die folgende API verwenden, um die StyleBook-ID für ein StyleBook zu erhalten, dessen Namespace com.citrix.adc.stylebook, Version: 1.0, Name: `my-own-gslb` ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
URL: https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks?filter=name:my-own-gslb,namespace:com.citrix.adc.stylebooks,version:1.0

HTTPMETHOD: GET
```

Die Antwort enthält die StyleBook-Details, einschließlich des ID-Attributs.


```
{

  "stylebooks": [

    {

      "author": null,

      "builtin": "false",

      "builtins": "{"netscaler.nitro.config": "10.5"}",

      "deprecate": "false",

      "description": " This StyleBook is used to configure one or a number of NetScalers in different sites into a GSLB setup. It is assumed that the SNIP IP on each NetScaler to be used by this StyleBook as the Site IP is already configured on the appliance.",

      "display_name": "HTTP/SSL LoadBalancing StyleBook",

      "filename": "my-own-gslb.yaml",

      "hide": null,

      "id": "gslb5a748d8b7684846cf6c409ad7dea8ccf",

      "imported_by": "",

      "imported_datetime": "2018-05-25 17:20:32.848902",

      "name": "my-own-gslb",

      "namespace": "com.citrix.adc.stylebooks",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "pkg_id": "gslb5a748d8b7684846cf6c409ad7dea8ccf",
      "primary_keys": "["name"]",
      "private": "false",
      "recompile": "false",
      "schema_version": "1.0",
      "source": "LS0tIApuYW1lOiBsYgpuYW1lc…",
      "system": null,
      "tags": "",
      "tenant_id": null,
      "user_sb": "false",
      "version": "1.0"
    },
    {
      …
    }
  ]
}
```


HINWEIS:

Die obige API gibt eine Liste von StyleBooks zurück, die dem Filter entsprechen. Stellen Sie sicher, dass Sie das richtige StyleBook aus der Antwort auswählen, um die ID abzurufen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REST-API zum Erstellen eines Systembenutzers

HINWEIS:

Dieser Schritt ist optional.

```
URL: https://<MAS_IP>/nitro/v2/config/mpsuser

HTTPMETHOD: POST



Payload:

{

  "mpsuser": {

    "name": "John",

    "password": "welcome",

    "external_authentication": false,

    "enable_session_timeout": false,

    "groups": [

      "AppOwnerGroup1"

    ]

  }

}
```

Workflow für die Anwendungsbesitzer

Ihre Benutzer müssen sich als Anwendungsbenutzer mit ihren Anmeldeinformationen anmelden. Die Benutzer müssen diese Aufgabe ausführen, um ihre eigenen DNS-Domainnamen zu erstellen und das neue GSLB StyleBook zu verwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie in NetScaler Console zu **Einstellungen > Domainnamen**.
2. Klicken Sie auf **Hinzufügen**, um eine neue DNS-Domain zu erstellen. Erstellen Sie die DNS-Domains in NetScaler Console.

   HINWEIS:

   Als Administrator können Sie diese Domainnamen auch erstellen und den Benutzergruppen zuweisen.

3. Navigieren Sie zu **Anwendungen** > **Dashboard** und klicken Sie auf **Benutzerdefinierte App definieren**.
4. Geben Sie einen Namen für die Anwendung ein und wählen Sie eine Kategorie aus. Wählen Sie **Eine neue Anwendung aus einem StyleBook erstellen** und klicken Sie auf **OK**. Wählen Sie **Mein eigenes GSLB StyleBook**, um die Konfiguration auf den ausgewählten Instanzen bereitzustellen.

5. Geben Sie die für alle Parameter im StyleBook erforderlichen Werte ein.

   a. Wählen Sie den Domänennamen aus der Liste aus.

   b. Fügen Sie die GSLB-Sites Ihrer Anwendung nach Bedarf hinzu.

   c. Wählen Sie die Ziel-NetScaler-Instanzen in allen GSLB-Sites aus.

   d. Klicken Sie auf **Erstellen**, um eine GSLB-Konfiguration zu erstellen.

   HINWEIS:

   Der StyleBook-Parameter „DNS-Domänenname“ zeigt nur die Liste der DNS-Domänen an, die dem Benutzer in NetScaler Console gehören.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console REST API für den Workflow des App-Besitzers

REST API zur Anmeldung bei NetScaler Console

```
URL: http: //<MAS_IP>/nitro/v2/config/login

HTTPMETHOD: POST



Payload:

{

  "login": {

    "username": "<USER_NAME>",

    "password": "<PASSWORD>",

    "session_timeout": 1800

  }

}
```

REST API zum Erstellen von DNS-Domänennamen

```
URL: https://<MAS_IP>/nitro/v2/config/dns_domain_entry

HTTP METHOD: POST

PAYLOAD: {"dns_domain_entry":{"name":"app1.acme.com","description":"app1
acme domain"

}

}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

REST API zum Erstellen von Anwendungen mit StyleBook

```
URL: https://<MAS_IP>/nitro/v2/config/application

HTTPMETHOD: POST



Payload:

{

  "params": {

    "action": "app_discovery"

  },

  "application": {

    "id": "",

    "name": "app1",

    "app_c ategory": "ITOps",

    "stylebook_params": "{"name":"my-own-
gslb","namespace":"com.citrix.adc.stylebooks","version":"1.0","configpack_
payload":{"parameters":{"name":"app1","domain-
name":"app1.acme.com",]"ttl":"30","algorithm":"ROUNDROBIN","protocol":"HTT
P","sites":[{"name":"site1","ipaddress":"6.5.6.77","virtual-
ip":"88.6.5.44","virtual-port":"80"}]},"targets":
[ {"id":"72c178da-47df-4426-9acc-cd6316f92506"}, {"id":"0e4d0789-
bffe-4266-ba1c-09adfc61db4e"}, {"id":"b5af4455-3f06-4f56-
b0cb-3d9f868c1f94"}]}}"

  }

}
```

In der obigen Nutzlast:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die „stylebook_params“ enthalten den Namen, die Namespaces und die Version des zu verwendenden StyleBooks.
- Die „configpack_payload“ enthält die ausgefüllten Parameter des StyleBooks, wie im entsprechenden GUI-Formular oben gezeigt. NetScaler Console stellt sicher, dass nur DNS-Domänennamen, auf die der Benutzer Zugriff hat, als Werte für den Parameter „domain-name“ verwendet werden können.
- Die „targets“ enthalten die Liste der NetScaler-IDs, auf denen die GSLB-Konfiguration bereitgestellt wird (die NetScaler-Instanzen auf den GSLB-Sites).

Um die NetScaler ID zu erhalten, wenn eine Management-IP-Adresse eines NetScaler gegeben ist, können Sie die folgende NetScaler Console API verwenden:

```
URL: https://<MAS_IP>/nitro/v2/config/ns?filter=ip_address:
192.168.153.162

HTTPMETHOD: GET
```

Die Antwort-Payload enthält Informationen zu diesem NetScaler®, einschließlich seiner ID:

```
{

  "errorcode": 0,

  "message": "Done",

  …..."tenant_id": "ec0eb868-0d6b-4729-bfbd-3005dd2694c1",

  "resourceName": "",

  "ns": [

    {

      "manufacturedate": "9/30/2009",

      "is_grace": "false",

      "hostname": "youcef-ns",

      "std_bw_config": "0",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "gateway_deployment": "false",
      "gateway_ipv6": "",
      "ha_master_state": "Primary",
      "instance_available": "0",
      "device_finger_print": "",
      "instance_state": "Down",
      "reason": "Device not reachable",
      "name": "",
      "ent_bw_available": "0",
      "description": "",
      "id": "da9ffff2-c100-45f1-a913-c542718338b2",
      "mgmt_ip_address": "192.168.153.162",
      ….
    }
  ]
}
```


Erstellen Sie Ihr StyleBook

Der vollständige Inhalt der Datei „my-own-gslb.yaml“ StyleBook wird unten angezeigt: Sie können dieses benutzerdefinierte StyleBook so wie es ist verwenden oder es an Ihre Bedürfnisse anpassen, um die erforderliche GSLB-Konfiguration zu generieren. Der wichtige Parameter in diesem StyleBook namens „domain-name“ muss in jedem StyleBook vorhanden sein, um die DNS-Namen-Funktionalität nutzen zu können.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name: my-own-gslb

namespace: com.citrix.adc.stylebooks

version: "1.0"

display-name: My own GSLB StyleBook

description: This StyleBook is used to configure one or a number of
NetScalers in different sites into a GSLB setup. It is assumed that the
SNIP IP on each NetScaler to be used by this StyleBook as the Site IP is
already configured on the appliance.

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    version: "10.5"

    prefix: ns

  -

    namespace: com.citrix.adc.commontypes

    version: "1.0"

    prefix: cmtypes

parameters:

  -

    name: name

    label: Application Name

    type: string
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    required: true
    key: true


  -
    name: domain-name
    label: DNS Domain Name
    description: GSLB DNS Domain Name
    type: string
    required: true
    allowed-dynamic-values:
      source: local
      resource-type: dns_domain_entry


  -
    name: ttl
    label: TTL for the Domain
    description: Time-To-Live value (number of seconds) for the Domain
    type: number
    default: 30


  -
    name: algorithm
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    label: LB Algorithm
    description: Global Load Balancing Algorithm
    type: string
    default: ROUNDROBIN
    allowed-values:
      - ROUNDROBIN
      - STATICPROXIMITY
      - SOURCEIPHASH


  -
    name: protocol
    label: Protocol
    description: The protocol of the GSLB VIP
    type: string
    default: HTTP
    allowed-values:
      - HTTP
      - FTP
      - TCP
      - UDP
      - SSL
      - SSL_BRIDGE
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      - SSL_TCP
      - NNTP
      - ANY
      - SIP_UDP
      - SIP_TCP
      - SIP_SSL
      - RADIUS
      - RDP
      - RTSP
      - MYSQL
      - MSSQL
      - ORACLE


  -
    name: monitor
    label: LB Monitor
    description: Monitor to be bound to the GSLB service
    type: cmtypes::monitor


  -
    name: sites
    label: GSLB Sites
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    description: Provide information about the GSLB Sites

    type: object[]

    required: true

    parameters:

      -

        name: name

        label: Site Name

        type: string

        required: true

      -

        name: ipaddress

        label: Site IP Address

        description: The IP Address of this Site. Use a SNIP IP address on
the site's appliance.

        type: ipaddress

        required: true

      -

        name: public-ipaddress

        label: Site Public IP Address

        description: The Public IP Address of this Site. It NATs to the
Site's IP address

        type: ipaddress

      -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        name: virtual-ip

        label: Site VIP IP

        description: The IP Address for the GSLB Service on this site (The
VIP on this Site)

        type: ipaddress

        required: true

      -

        name: virtual-port

        label: Site VIP Port

        description: The port number for the GSLB Service (VIP) on this
site

        type: tcp-port

        default: 80



components:

  -

    name: enable-gslb-comp

    type: ns::nsfeature

    description: Enables the GSLB feature

    meta-properties:

      action: enable

    properties:

      feature: ["GSLB", "LB"]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -

    name: gslb-monitor-comp

    type: cmtypes::monitor

    condition: $parameters.monitor

    properties:

      monitorname: $parameters.name + "-" +
$parameters.monitor.monitorname + "-gslbmon"

      type: $parameters.monitor.type

      destip?: $parameters.monitor.destip

      destport?: $parameters.monitor.destport

      httprequest?: $parameters.monitor.httprequest

      send?: $parameters.monitor.send

      customheaders?: $parameters.monitor.customheaders

      respcodes?: $parameters.monitor.respcodes

      recv?: $parameters.monitor.recv

      lrtm?: $parameters.monitor.lrtm

      secure?: $parameters.monitor.secure

      interval?: $parameters.monitor.interval

      interval_units?: $parameters.monitor.interval_units

      resptimeout?: $parameters.monitor.resptimeout

      retries?: $parameters.monitor.retries

      downtime?: $parameters.monitor.downtime
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-
  name: gslb-vserver-comp
  type: ns::gslbvserver
  description: Creates a GSLB VServer config object
  properties:
    name: $parameters.name + "-gslbvserver"
    servicetype: $parameters.protocol
    lbmethod: $parameters.algorithm
  components:
    -
      name: gslb-domain-comp
      type: ns::gslbvserver_domain_binding
      properties:
        name: $parent.properties.name
        domainname: $parameters.domain-name
        ttl: $parameters.ttl
-
  name: gslb-site-comp
  type: ns::gslbsite
  description: Creates a GSLB Site config object
  repeat: $parameters.sites
  repeat-item: site
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:
      sitename: $parameters.name + "-" + $site.name + "-gslbsite"
      siteipaddress: $site.ipaddress
      publicip?: $site.public-ipaddress
    components:
      -
        name: gslb-service-comp
        type: ns::gslbservice
        description: Creates a GSLB Service
        properties:
          servicename: $parameters.name + "-" + $site.name + "-
gslbservice"
          ip: $site.virtual-ip
          servicetype: $parameters.protocol
          port: $site.virtual-port
          sitename: $parent.properties.sitename
        components:
          -
            name: gslb-vserver-service-binding-comp
            type: ns::gslbvserver_gslbservice_binding
            description: Creates a Binding between the GSLB vserver and
the GSLB Service
            properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
              name: $components.gslb-vserver-comp.properties.name

              servicename: $parent.properties.servicename

          -

            name: gslb-service-monitor-binding-comp

            type: ns::gslbservice_lbmonitor_binding

            description: Creates a Binding between the GSLB service and
the GSLB monitor

            condition: $parameters.monitor

            properties:

              servicename: $parent.properties.servicename

              monitor_name: $components.gslb-monitor-
comp.properties.monitorname
```

Sonderzeichen in ihrer wörtlichen Form in StyleBook zulassen

In der StyleBook-Definition können Sie wörtliche Zeichenfolgen verwenden, wenn Sonderzeichen in einer Zeichenfolge ihre wörtliche Form annehmen müssen. Diese Zeichenfolgen können Escape-Zeichen, Backslash, Anführungszeichen, Klammern, Leerzeichen, eckige Klammern usw. enthalten.

In StyleBooks können Sie NetScaler-Richtlinienausdrücke in ihrer wörtlichen Form mithilfe von wörtlichen Zeichenfolgen einfügen. Die Richtlinienausdrücke enthalten typischerweise Sonderzeichen. Ohne wörtliche Zeichenfolgen müssen Sie Sonderzeichen durch Aufteilen von Zeichenfolgen in Teilzeichenfolgen escapen.

Um eine wörtliche Zeichenfolge zu erstellen, schließen Sie eine Zeichenfolge wie folgt zwischen Sonderzeichen ein:

`~{string}~`

Sie können wörtliche Zeichenfolgen in den StyleBook-Ausdrücken verwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Verwenden Sie die Zeichenfolge }~ nicht in einer Eingabezeichenfolge, da diese Sequenz das Ende einer wörtlichen Zeichenfolge anzeigt.

Beispiel:

```
---

name: test-deny-url

namespace: citrix.adc.stylebooks

version: "6.2"

display-name: StyleBook for creating an AppFw profile

description: This Stylebook configures an AppFw config.

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "13.0"

parameters:

  -

    name: name

    type: string

    required: true

substitutions:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 default-deny-urls-regex:

     "Command_injection_attack": str("([ /=]|\\t|\\n)(ls|cat)([ ;'" + "\\
\"&].*)?$")

     "Command_injection_attack2": ~{([ /=]|\t|\n)(ls|rm|cat)([ ;'\"&].*)?
$}~

components:

  -

    name: appfw-profile-comp

    type: ns::appfwprofile

    properties:

      name: $parameters.name

      type: ["XML"]

    components:

          -

            name: appfw-profile-denyurl-default-binding-subcomp-all

            type: ns::appfwprofile_denyurl_binding

            properties:

                name: $parent.properties.name

                denyurl?: $substitutions.default-deny-urls-
regex["Command_injection_attack"]

                state?: "ENABLED"

          -

            name: appfw-profile-denyurl-default-binding-subcomp-all2
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            type: ns::appfwprofile_denyurl_binding

            properties:

                name: $parent.properties.name

                denyurl?: $substitutions.default-deny-urls-
regex["Command_injection_attack2"]

                state?: "ENABLED"
```

In diesem Beispiel haben die `default-deny-urls-regex` Ersetzungen einen wörtlichen Ausdruck.

- `"Command_injection_attack": str("([ /=]|\\t|\\n)(ls|cat)([ ;'" + "\\\"&].*)?$")`: StyleBook verarbeitet dies als regulären Ausdruck.
- `"Command_injection_attack2": ~{([ /=]|\t|\n)(ls|rm|cat)([ ;'\"&].*)?$}~`: StyleBook verarbeitet dies als wörtlichen Ausdruck. Die Sonderzeichen in dieser Zeichenfolge nehmen die wörtliche Form an.

Mehrere wörtliche Zeichenfolgen verketten

Sie können wörtliche Zeichenfolgen mit regulären Zeichenfolgen oder Zeichenfolgen mit Interpolationen verketten. Dabei überspringt das StyleBook die Interpretation nur für die wörtlichen Zeichenfolgen. Verwenden Sie den Plus-Operator (+) zwischen den Zeichenfolgen zum Verketten.

Beispiel:

```
value: "~{\"id\": \"}~ + %{$atom.key}% + ~{\", \"value\": \"}~ + %
{$atom.value}% + ~{\"}~"
```

In diesem Beispiel werden `%{$atom.key}%` und `%{$atom.value}%` interpretiert. Und die Interpretation wird für den Rest übersprungen.

Datenquellen verwalten

Das Definieren einer Datenquelle in NetScaler Console hilft Ihnen, Daten aus externen Quellen als Eingabe beim Erstellen oder Aktualisieren von StyleBook-Konfigurationen zu verwenden. Andernfalls müssen Sie jede vom StyleBook benötigte Eingabe explizit bereitstellen. In NetScaler Console können Sie jede verwaltete NetScaler-Instanz als Datenquelle für die Eingabe einer

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBook-Konfiguration verwenden. Sie können auch benutzerdefinierte Datenquellen definieren, die als Eingabe beim Erstellen oder Aktualisieren von Konfigurationen dienen können.

Sammlungen: Ähnlich wie eine Datenbank mehrere Tabellen haben kann, kann eine Datenquelle mehrere Sammlungen enthalten. Jede Sammlung hat einen Namen und enthält eine Liste ähnlicher Tupel, wobei jedes Tupel ein Satz von Schlüssel-Wert-Paaren ist. Zum Beispiel kann eine Sammlung aus Tupeln bestehen, wobei jedes Tupel (`<name>: <value>, <virtualip>:<value>`) hat.

Datenquellentyp: Ein Datenquellentyp unterscheidet die Art der Quelle, aus der die Daten abgerufen werden. NetScaler Console unterstützt zwei Datenquellentypen.

- **managed-adc** – Dies ist eine integrierte Datenquelle. Und sie wird zum Abrufen von Daten von jedem vorhandenen NetScaler verwendet, der von NetScaler Console verwaltet wird. Weitere Informationen finden Sie unter NetScaler-Instanz als Datenquelle verwenden.

  Sie können auch die Ziel-NetScaler-Instanz als Datenquelle verwenden. Weitere Informationen finden Sie unter Ziel-NetScaler-Instanzen als Datenquellen verwenden.
- **Benutzerdefinierter Datenquellentyp** – Sie können benutzerdefinierte Datenquellentypen definieren, bei denen Daten lokal auf NetScaler® Console gefüllt werden.

  Betrachten Sie einen Datenquellentyp `Environment`. Dieser Datenquellentyp hat zwei Datenquellen: `Production` und `Staging`. Beim Erstellen einer StyleBook-Konfiguration kann der StyleBook-Benutzer eine beliebige Datenquelle vom Typ `Environment` auswählen. Abhängig von der Auswahl werden die Datenwerte entweder von `Production` oder `Staging` als Eingabe für das StyleBook verwendet.

  Weitere Informationen finden Sie unter Benutzerdefinierte Datenquellen verwenden

Sammlungsschema: Es beschreibt, welche Art von Daten in einem Sammlungs-Tupel gespeichert werden können. Das Sammlungsschema beschreibt den Namen jedes Schlüssels im Tupel und seinen erwarteten Typ. In einer Datenbankanalogie ähnelt ein Sammlungsschema einem Datenbankschema für eine Tabelle, bei der jede Spalte einen klar definierten Namen und einen unterstützenden Typ hat.

Das folgende Diagramm ist eine allgemeine Darstellung der verschiedenen Komponenten von Datenquellen und deren Beziehungen zueinander:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Eine NetScaler-Instanz als Datenquelle verwenden

Sie können die verwalteten NetScaler-Instanzen als Datenquellen verwenden. `managed-adc` ist ein integrierter Datenquellentyp, der in NetScaler Console problemlos als Datenquelle verwendet werden kann. Jede verwaltete NetScaler-Instanz in NetScaler Console ist standardmäßig eine Datenquelle. Sie können diese Datenquellen in Ihren StyleBooks verwenden, wenn Sie beim Erstellen von Konfigurationspaketen Daten von einem vorhandenen, von NetScaler Console verwalteten NetScaler benötigen.

Geben Sie in der StyleBook-Definition den integrierten Typparameter `datum` an. Sie können die Datenquellentypen in Ihrem StyleBook verwenden. Die StyleBook-Benutzer können eine Datenquelle auswählen, die zum Abrufen von Daten aus dieser Quelle verwendet werden kann.

Verwenden der integrierten Datenquelle ohne Sammlung

```
parameters:

  - name: selected-adc

    label: Select an existing NetScaler

    type: datum

    required: true

    data-source:

      type: managed-adc
```

Im Beispiel wird der Parameter `datum` verwendet, um eine beliebige von NetScaler Console verwaltete NetScaler-Instanz auszuwählen. Die integrierte Datenquelle `managed-adc` ermöglicht es Ihnen, Daten von jeder von NetScaler Console verwalteten NetScaler-Instanz abzurufen.

In Ihrem StyleBook können Sie auf jede Konfiguration der ausgewählten NetScaler-Instanz zugreifen. Und Sie können diese Konfiguration beim Erstellen oder Aktualisieren von Konfigurationen auf derselben NetScaler-Instanz oder einer anderen NetScaler-Instanz verwenden; dies hängt von der ausgewählten Ziel-NetScaler-Instanz ab.

Auf die Sammlung aus einer Datenquelle zugreifen:

In der ausgewählten NetScaler-Instanz verwenden Sie den folgenden Ausdruck, um auf eine Sammlung zuzugreifen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$parameters.selected-adc.collections.<collection-name>
```

Beispiel:

```
$parameters.selected-adc.collections.lbvserver
```

Dieser Ausdruck gibt die Liste der `lbvserver`-Entitäten auf der ausgewählten NetScaler-Instanz zurück. Sie können diese Liste beispielsweise durchlaufen, um eine bestimmte `lbvserver` auszuwählen, die eine bestimmte Bedingung erfüllt.

Beispiel-StyleBook ohne Sammlung

```
name: add-vservers-from-managed-adc-instances

namespace: com.citrix.adc.stylebooks

version: "1.0"

schema-version: "1.0"



import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



parameters:

    -

      name: selected-adc

      label: Select a NetScaler instance
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      type: datum
      required: true
      data-source:
        type: "managed-adc"


components:
  -
    name: sslvserver-comp
    type: ns::sslvserver
    repeat: $parameters.selected-adc.collections.lbvserver
    repeat-item: lbvs
    repeat-condition: $lbvs.attributes.servicetype == "SSL"
    properties:
      name: $lbvs.attributes.name
      ssl2: DISABLED
      ssl3: DISABLED
      tls1: DISABLED
      tls11: ENABLED
      tls12: ENABLED
```

Die GUI des Konfigurationspakets zeigt die von NetScaler Console verwalteten NetScaler-Instanzen an, und StyleBook-Benutzer können beim Erstellen oder Aktualisieren des Konfigurationspakets einen beliebigen NetScaler auswählen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Integrierte NetScaler-Datenquelle ohne Sammlung(/en-us/netscaler-console-service/media/managed-adc-without-collection.png)

Dieses StyleBook verwendet den ausgewählten NetScaler und durchläuft alle `lbvserver`-Entitäten. Es wählt die virtuellen SSL-Server aus und legt die zulässigen SSL-Protokollversionen auf jedem virtuellen Server fest.

Der folgende Ausdruck ermöglicht es Ihnen, die Liste der `lbvserver`-Entitäten in der NetScaler-Instanz zu durchlaufen.

```
repeat: $parameters.selected-adc.collections.lbvserver
```

- `collections`: Bezieht sich auf alle Entitätstypen auf der NetScaler-Instanz. Zum Beispiel `csvserver`, `lbmonitor`, `servicegroup` usw.
- `lbvserver`: Bezieht sich auf die Liste der Load-Balancing-Virtual-Server-Entitäten in der NetScaler-Instanz.

Verwenden der integrierten Datenquelle mit Sammlung

```
parameters:

  - name: selected-lbvserver

    label: Select an existing lbvserver

    type: datum

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver
```

In diesem Beispiel wird der Parameter `datum` verwendet, um einem Benutzer die Auswahl sowohl der NetScaler-Instanz als auch eines spezifischen `lbvserver` aus dem Datenquellentyp `managed-adc` zu ermöglichen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Sie einen Sammlungstyp im Abschnitt `parameters` definieren, können die StyleBook-Benutzer die NetScaler-Instanz und eine spezifische Entität aus einer Sammlung auf dieser Instanz auswählen.

Zugriff auf ein Attribut des ausgewählten Elements:

Wenn der StyleBook-Benutzer einen virtuellen Server auswählt, kann der folgende Ausdruck in Ihrem StyleBook auf jedes Attribut des ausgewählten Elements zugreifen.

```
$parameters.selected-lbvserver.attributes.<attribute-name>
```

In diesem Beispiel ist das ausgewählte `datum` `lbvserver`. Sie können also auf jedes Attribut der NetScaler-Entität `lbvserver` zugreifen, wie z. B. `name`, `servicetype`, `ipv46` und so weiter.

Beispiel:

```
$parameters.selected-lbvserver.attributes.ipv46
```

Dieser Ausdruck ruft die IP des ausgewählten Load-Balancing-Virtual-Servers ab. Weitere Informationen zu den NetScaler-Entitäten (Sammlungen) und ihren Attributen finden Sie unter NetScaler NITRO API-Referenz.

Mehrere Elemente aus einer Sammlung auswählen:

Der folgende Parameterabschnitt ermöglicht StyleBook-Benutzern die Auswahl mehrerer Elemente einer Sammlung.

```
parameters:

  - name: selected-lbvservers

    label: Select existing lbvservers

    type: datum[]

    required: true

    data-source:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      type: managed-adc

      collection: lbvserver
```

In diesem Beispiel wird der Datumsparameter verwendet, um das Datenquellen-Array zu definieren. Der Benutzer kann einen oder mehrere lbvserver von einer einzelnen NetScaler®-Instanz oder über mehrere NetScaler-Instanzen hinweg auswählen.

Das folgende Code-Snippet zeigt, wie auf ausgewählte Elemente und deren Attribute zugegriffen wird.

```
components:

  - name: sslvserver-comp

    type: ns::sslvserver

    repeat:

      repeat-list: $parameters.selected-lbvservers

      repeat-item: vserverObj

    properties:

      name: $vserverObj.attributes.name

      ssl2: DISABLED

      ssl3: DISABLED

      tls1: DISABLED

      tls11: ENABLED

      tls12: ENABLED
```

Zugriff auf eine Sammlung über die Referenz des ausgewählten Elements:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können einem StyleBook-Benutzer nicht nur die Auswahl einer bestimmten Entität auf einer verwalteten NetScaler-Instanz ermöglichen, sondern auch auf jede Entität aus derselben oder anderen Sammlungen auf der ausgewählten NetScaler-Instanz zugreifen. Um auf eine andere Sammlung auf dieser NetScaler-Instanz zuzugreifen, verwenden Sie den folgenden Ausdruck im Abschnitt `components`:

```
$parameters.selected-lbvserver.datasource.collections.<collection-name>
```

Beispiel:

```
$parameters.selected-lbvserver.datasource.collections.csvserver
```

Dieser Ausdruck gibt die Liste der Content-Switching Virtual Server von der ausgewählten NetScaler-Instanz zurück.

Und der folgende Ausdruck gibt eine Liste aller Bindungen zwischen `lbvservers` und `servicegroups` zurück:

```
$parameters.selected-
lbvserver.datasource.collections.lbvserver_servicegroup_binding
```

Beispiel-StyleBook mit einer Sammlung

Das Folgende ist ein Beispiel-StyleBook, das zeigt, wie die verwaltete NetScaler-Instanz als Datenquelle verwendet wird:

```
name: bind-lb-to-servicegroup-using-ADC-as-datasource

namespace: com.citrix.adc.stylebooks

version: "1.1"

display-name: "HTTP/SSL LoadBalancing StyleBook with Service Binding"

description: "This stylebook defines a typical Load Balanced Application
configuration where we allow the user to select an existing lbvserver on
the NetScaler using datum type parameter. Then a servicegroup for the
selected lb is created if it does not exist on the NetScaler. Finally, the
selected lbvserver is bound to the service "
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



parameters:

  -

    name: selected-vserver

    label: "Select an Existing VServer"

    description: "Load Balancing Application Vservers to be bound to
service on the ADC"

    type: datum

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver



components:

  -

    name: servicegroup-discovery-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: object

    repeat: $parameters.selected-
vserver.datasource.collections.servicegroup

    repeat-item: svcgrp

    repeat-condition: $svcgrp.attributes.servicegroupname ==
 $parameters.selected-vserver.attributes.name + "-svcgrp"

    properties:

      servicegroupname: $svcgrp.attributes.servicegroupname

  -

    name: servicegroup-creation-if-not-exists-comp

    type: ns::servicegroup

    condition: not exists($components.servicegroup-discovery-comp)

    properties:

      servicegroupname: $parameters.selected-vserver.attributes.name + "-
svcgrp"

      servicetype: $parameters.selected-vserver.attributes.servicetype

    components:

      -

        name: lbvserver-servicegroup-binding

        type: ns::lbvserver_servicegroup_binding

        properties:

          name: $parameters.selected-vserver.attributes.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        servicegroupname: $parent.properties.servicegroupname
```

In diesem StyleBook prüft der Abschnitt `components` den Dienstgruppennamen, der mit dem Namen des ausgewählten Lastausgleichs-Virtual-Servers, verkettet mit `svcgrp`, übereinstimmt.

Wenn der Name des ausgewählten Lastausgleichs-Virtual-Servers `lbv1` ist, prüft dieses StyleBook die Dienstgruppe mit dem Namen `lbv1-svcgrp`. Wenn sie nicht gefunden wird, erstellt es eine Dienstgruppe `lbv1-svcgrp` und bindet sie an den Virtual Server `lbv1`.

Der folgende Ausdruck ruft die Liste der Dienstgruppen in der NetScaler-Instanz ab.

```
repeat: $parameters.selected-vserver.datasource.collections.servicegroup
```

In diesem Ausdruck:

- `datasource`: Bezieht sich auf die ausgewählte NetScaler-Instanz, die von NetScaler Console verwaltet wird.
- `collections`: Bezieht sich auf alle Entitäten in der NetScaler-Instanz.
- `servicegroup`: Bezieht sich auf die Dienstgruppen in der NetScaler-Instanz.

Sammlungsdaten filtern:

Der folgende Parameterabschnitt erklärt, wie Filter für eine integrierte Datenquellsammlung in der StyleBook-Definition angegeben werden. Er ermöglicht StyleBook-Benutzern, ein bestimmtes Element aus einer gefilterten Sammlung auszuwählen.

```
parameters:

  - name: selected-lbvserver

    label: Select an existing lbvserver

    type: datum

    required: true

    data-source:

      type: managed-adc
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    collection: lbvserver

    collection-filters:

      protocol: SSL
```

In diesem Beispiel wird der Datum-Parameter verwendet, um einem Benutzer die Auswahl sowohl der NetScaler-Instanz als auch eines bestimmten lbvserver mit SSL-Protokoll aus dem Datenquellentyp managed-adc zu ermöglichen.

Nachdem der StyleBook-Benutzer einen virtuellen Server ausgewählt hat, kann jedes Attribut des ausgewählten Elements auf die gleiche Weise aufgerufen werden, wie im vorherigen Abschnitt erläutert.

Ziel-NetScaler-Instanzen als Datenquellen verwenden

Sie können den Ziel-NetScaler Ihrer Konfiguration selbst auch als Datenquelleneingabe für Ihre Konfiguration verwenden. In diesem Szenario möchten Sie möglicherweise die vorhandene Konfiguration auf dem Ziel-NetScaler referenzieren, um neue Konfigurationen auf diesem NetScaler zu erstellen.

Um Zielinstanzen als Datenquellen zu verwenden, müssen Sie den `datum` integrierten Typparameter nicht verwenden, da keine NetScaler-Instanzen vom StyleBook-Benutzer ausgewählt werden müssen. Sie können Ausdrücke direkt im `components` Abschnitt Ihres StyleBooks schreiben, die Daten von der Ziel-NetScaler-Instanz abrufen.

Verwenden Sie den folgenden Ausdruck, um Folgendes von den Ziel-NetScaler-Instanzen abzurufen:

- Sammlungen:

  ```
  $current-target-as-datasource.collections.<collection-name>
  ```

  Beispiel:

  ```
  $current-target-as-datasource.collections.lbvserver
  ```

- Attribute:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$current-target-as-datasource.collections.attributes.<attribute>
```

Beispiel-StyleBook zur Verwendung der Ziel-NetScaler-Instanz als Datenquelle

Das Folgende ist ein Beispiel-StyleBook, das zeigt, wie die Ziel-NetScaler-Instanz als Datenquelle verwendet wird:

```
---

name: lb-add-service-with-target-adc

namespace: com.citrix.adc.stylebooks

version: "1.1"

display-name: "HTTP/SSL LoadBalancing StyleBook with Service Binding"

description: "This stylebook defines a typical Load Balanced Application
configuration."

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



components:

  -

    name: servicegroup-comp

    type: ns::servicegroup
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
properties:
  servicegroupname: "lb-demo-svcgrp"
  servicetype: "HTTP"

components:
  -
    name: lbvserver-svg-binding
    type: ns::lbvserver_servicegroup_binding
    repeat: $current-target-as-datasource.collections.lbvserver
    repeat-item: lbvsrvr
    repeat-condition: $lbvsrvr.attributes.name == "lb-demo-lb"
    properties:
      name: $lbvsrvr.attributes.name
      servicegroupname: $parent.properties.servicegroupname
```

In diesem Beispiel prüft das Konfigurationspaket die Load-Balancing-virtuellen Server in den Ziel-NetScaler-Instanzen. Und wenn die angegebene IP-Adresse des Load-Balancing-virtuellen Servers übereinstimmt, ruft es den Namen und den Dienstgruppennamen ab.

Benutzerdefinierte Datenquellen verwenden

Neben verwalteten NetScaler-Instanzen als Datenquelle können Sie benutzerdefinierte Datenquellen definieren und verwenden, wenn die Eingabedaten wiederholt zum Erstellen mehrerer Konfigurationen verwendet werden. Sie können die Eingabedaten in NetScaler Console als Datenquelle speichern. Und Sie können StyleBooks so ändern, dass sie diese Daten nutzen, ohne dass StyleBook-Benutzer wiederholt Eingaben machen müssen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bevor Sie eine benutzerdefinierte Datenquelle in Ihrer StyleBook-Definition verwenden, gehen Sie wie folgt vor, um eine benutzerdefinierte Datenquelle zu definieren:

1. Einen Datenquellentyp hinzufügen.
2. Sammlungsschema unter Datenquellentyp hinzufügen.
3. Eine Datenquelle hinzufügen.
4. Sammlungsdaten hinzufügen.

Nach dem Hinzufügen einer Datenquelle können Sie diese Datenquelle in der StyleBook-Definition verwenden. Weitere Informationen finden Sie unter Benutzerdefinierte Datenquellen in der StyleBook-Definition verwenden.

Einen Datenquellentyp hinzufügen

Geben Sie einen Datenquellentyp an, um die Quelle zu unterscheiden, aus der Daten abgerufen werden.

1. Unter **Applications > Configuration > Data Sources**.
2. Wählen Sie **Data Source Type** aus und klicken Sie auf **Add**.
3. Geben Sie den **Namen** und die **Beschreibung** für den Datenquellentyp an.
4. Klicken Sie auf **Proceed**, um den **Data Source Type** zu speichern. Klicken Sie auf **Close**, um den Workflow ohne Speichern von Änderungen zu beenden.

In diesem Beispiel ist der Datentyp der Datenquelle auf **Umgebung** festgelegt. Dieser Typ kann verwendet werden, um die Anwendungsumgebungen als Datenquellen zu definieren.

Sammlungsschema unter Datentyp der Datenquelle hinzufügen

Nach dem Hinzufügen des **Datentyps der Datenquelle** wird ein Bildschirm zur Ergänzung von **Sammlungsschemata** für ""Datentyp der Datenquelle** angezeigt.

1. Klicken Sie auf **Hinzufügen**.
2. Geben Sie den **Sammlungsnamen** für ein Sammlungsschema an.
3. Geben Sie die **Beschreibung** ein.
4. Fügen Sie bei Bedarf Attribute (Name und Typ) unter **Attributdetails** hinzu.
5. Klicken Sie auf **Erstellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In diesem Beispiel hat das Sammlungsschema **App-virtual-servers** vier Attribute. Die Sammlung, die Sie speichern möchten, muss daher diese Attribute der festgelegten Datentypen aufweisen.

Datenquelle hinzufügen

Definieren Sie eine Datenquelle für einen bestimmten Datentyp der Datenquelle.

1. Gehen Sie zu **Anwendungen > Konfiguration > Datenquellen**.
2. Wählen Sie die Registerkarte **Datenquellen** aus und klicken Sie auf **Hinzufügen**.
3. Geben Sie den **Namen** an.
4. Wählen Sie den **Datenquellentyp** aus, und geben Sie die **Beschreibung** ein.
5. Klicken Sie auf **Weiter**, um die **Datenquelle** zu speichern. Klicken Sie auf **Schließen**, um den Workflow zu beenden, ohne Änderungen zu speichern.

In diesem Beispiel wird die **Produktionsumgebung** als Datenquelle hinzugefügt.

Sammlungsdaten hinzufügen

Nach dem Hinzufügen der **Datenquelle** wird ein Bildschirm zur Eingabe der Daten für die **Datenquelle** angezeigt. Sie sehen eine Liste der **Sammlungsschemata**.

1. Wählen Sie das **Sammlungsschema** aus, dem Sie Sammlungsdaten hinzufügen möchten.
2. Klicken Sie auf **Sammlungsdaten verwalten**.
3. Fügen Sie Daten zur Sammlung hinzu. Sie können Daten einzeln hinzufügen oder eine CSV-Datei hochladen. Wenn Sie eine CSV-Datei hochladen, stellen Sie sicher, dass die Spaltennamen mit den Attributnamen des Sammlungsschemas übereinstimmen.
4. Klicken Sie auf **OK**.

Benutzerdefinierte Datenquelle ohne Sammlung verwenden

Der folgende `parameters` Abschnitt erklärt, wie eine benutzerdefinierte Datenquelle in der StyleBook-Definition ohne Sammlung definiert wird.

```
parameters:

    - name: selected-environment

      label: Select a custom datasource environment
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      type: datum

      required: true

      data-source:

        type: "Environment"
```

Die GUI des Konfigurationspakets zeigt die anwendbaren Datenquellen an, und StyleBook-Benutzer können eine davon auswählen, um ein Konfigurationspaket zu erstellen.

In diesem Beispiel wird die `Production` Datenquelle verwendet, um Daten abzurufen.

Im `Environment` Datenquellentyp verwenden Sie den folgenden Ausdruck, um auf den `App-virtual-servers` Sammlungstyp zuzugreifen:

```
$parameters.selected-environment.collections.App-virtual-servers
```

Beispiel-Snippet:

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    repeat: $parameters.selected-environment.collections.App-virtual-
servers

    repeat-item: app

    properties:

      name: $app.attributes.Name + "-lb"

      ipv46: ip($app.attributes.IPv46 )

      port: $app.attributes.Port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      servicetype: $app.attributes.Protocol

    components:



      -

        name: servicegroup-comp

        type: ns::servicegroup

        properties:

          servicegroupname: $parent.properties.name + "-svcgrp"

          servicetype: $parent.properties.servicetype



        components:

          -

            name: lbvserver-svg-binding

            type: ns::lbvserver_servicegroup_binding

            properties:

              name: $parent.parent.properties.name

              servicegroupname: $parent.properties.servicegroupname
```

Benutzerdefinierte Datenquellen mit Sammlung verwenden

Der folgende `parameters` Abschnitt erklärt, wie eine benutzerdefinierte Datenquelle in der StyleBook-Definition definiert wird. Er ermöglicht StyleBook-Benutzern, ein bestimmtes Element einer Sammlung auszuwählen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:

  - name: selected-app-vserver

    label: Select a collection from the datasource

    type: datum

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers
```

In diesem Beispiel wird der `datum` Parameter verwendet, um die benutzerdefinierte Datenquelle zu definieren. Er verwendet die `Production` Datenquelle, um Daten aus dem `App-virtual-servers` Sammlungsschema abzurufen.

Im `Environment` Datenquellentyp verwenden Sie den folgenden Ausdruck, um auf das Protokoll aus der `App-virtual-servers` Sammlung zuzugreifen:

```
$parameters.selected-app-vserver.attributes.Protocol
```

Beispiel-Snippet:

```
components:

  - name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: $parameters.selected-app-vserver.attributes.Name

      ipv46: $parameters.selected-app-vserver.attributes.IPv46

      port: $parameters.selected-app-vserver.attributes.Port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      servicetype: $parameters.selected-app-vserver.attributes.Protocol
```

Wenn Sie einen Sammlungstyp im `parameters` Abschnitt definieren, können die StyleBook-Benutzer die Datenquelle und die Sammlung auswählen.

Auswählen mehrerer Elemente aus einer Sammlung:

Der folgende Parameterabschnitt ermöglicht StyleBook-Benutzern, mehrere Elemente einer Sammlung auszuwählen.

```
parameters:

  - name: selected-app-vservers

    label: Select app-vservers from the collection

    type: datum[]

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers
```

In diesem Beispiel wird der Datumsparameter verwendet, um das benutzerdefinierte Datenquellen-Array zu definieren. Der Benutzer kann ein oder mehrere Elemente aus der Sammlung „App-virtual-servers“ aus einer einzelnen Datenquelle oder über mehrere Datenquellen hinweg auswählen.

Das folgende Code-Snippet zeigt, wie ausgewählte Elemente und ihre Attribute abgerufen werden.

```
components:

  -

   name: lbvserver-comp

   type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   repeat:
   repeat-list: $parameters.selected-app-vservers
   repeat-item: vserverObj
    properties:
      name: $vserverObj.attributes.Name
      ipv46: $vserverObj.attributes.IPv46
      port: $vserverObj.attributes.Port
      servicetype: $vserverObj.attributes.Protocol
```

Sammlungsdaten filtern:

Der folgende Parameterabschnitt erklärt, wie Filter für eine benutzerdefinierte Datenquellensammlung in der StyleBook-Definition angegeben werden. Er ermöglicht StyleBook-Benutzern, ein bestimmtes Element aus einer gefilterten Sammlung auszuwählen.

```
parameters:
  - name: selected-app-vserver
    label: Select a collection from the datasource
    type: datum
    required: true
    data-source:
      type: Environment
      collection: App-virtual-servers
      collection-filters:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        Protocol: SSL
```

In diesem Beispiel wird der Datumsparameter verwendet, um die benutzerdefinierte Datenquelle zu definieren. Sie verwendet die Datenquelle vom Typ Umgebung, um gefilterte Daten aus dem App-virtual-servers-Sammlungsschema abzurufen.

Nachdem der StyleBook-Benutzer einen virtuellen Server ausgewählt hat, kann jedes Attribut des ausgewählten Elements auf die gleiche Weise aufgerufen werden, wie im vorherigen Abschnitt erläutert.

APIs verwenden, um Konfigurationen aus StyleBooks zu erstellen

Nachdem Sie Ihr StyleBook erstellt haben, müssen Sie es entweder über die NetScaler Console GUI oder über die NetScaler Console APIs importieren. NetScaler Console validiert Ihr StyleBook beim Import. Wenn die Validierung erfolgreich ist, erscheint Ihr StyleBook im NetScaler Console StyleBook-Katalog und kann zur Erstellung von Konfigurationen verwendet werden.

Sie können nun die StyleBook APIs verwenden, um Konfigurationen basierend auf diesem StyleBook zu erstellen. Sie können jedes Tool wie das cURL-Befehlszeilentool oder die Postman Chrome-Browsererweiterung verwenden, um HTTP-Anfragen an NetScaler Console zu senden.

HINWEIS:

Die StyleBooks APIs sind auf dem Developer Portal vollständig unter Verwendung der OpenAPI-Spezifikation dokumentiert.

Beispiel 1

Betrachten Sie das `lb-vserver` StyleBook, das in StyleBook zum Erstellen eines Lastausgleichs-Virtual-Servers erstellt wurde. Verwenden Sie die folgenden REST APIs, um ein Konfigurationspaket aus diesem StyleBook zu erstellen:

HTTP-METHODE: POST

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks`

ANFRAGE-HEADER:

Content-Type: application/json

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Accept: application/json

ANFRAGE-BODY-NUTZLAST:

```
{

  "configpack":

  {

    "parameters": {

      "name": "lb1",

      "vip-ipaddress": "10.102.117.31"

    },

    "targets":

    [

      {

        "instance_id": "deecee30-f478-4446-9741-a85041903410"

      }

    ],

    "stylebook": {

            "name": "lb-vserver",

            "namespace": "com.example.stylebooks",

            "version": "1.0"

        }

  }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

In dieser HTTP-Anfrage ist die ID, deecee30-f478-4446-9741-a85041903410, die Instanz-ID der NetScaler-Instanz, auf der der Lastausgleichs-Virtual-Server lb1 mit der IP-Adresse 10.102.117.31 erstellt wird. Die Instanz-ID der NetScaler-Instanz wird von NetScaler Console abgerufen.

Um die ID einer von NetScaler Console verwalteten Instanz zu erhalten, können Sie die NetScaler Console APIs verwenden. Zum Beispiel, um die Instanz-ID einer NetScaler-Instanz abzurufen, deren IP-Adresse 192.168.153.160 ist, können Sie die folgende API verwenden:

HTTP-METHODE: GET

URL: `https://<IP>/nitro/v2/config/ns?filter=ip_address:192.168.153.160`

ANFRAGE-HEADER:

Accept: application/json

Die Antwort enthält die ID in der JSON-Nutzlast:

ERWARTETE ANTWORT-HEADER (bei Erfolg):

200 OK

Content-Type: application/json

ERWARTETER ANTWORT-BODY (bei Erfolg):

```
{

  "errorcode": 0,

  "message": "Done",

  "operation": "get",

  "resourceType": "ns",

  "username": "nsroot",

  "tenant_name": "Owner",

  "resourceName": "",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  "ns":
  [
    {
    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    "id": "deecee30-f478-4446-9741-a85041903410",
   }
 ]
}
```

Wenn die Konfiguration (Konfigurationspaket) erfolgreich erstellt wurde, erhalten Sie die folgende HTTP-Antwort:

ERWARTETE ANTWORT-HEADER (bei Erfolg):

202 OK

Content-Type: application/json

ERWARTETER ANTWORT-BODY (bei Erfolg):

```
{
  "job":
  {
    "job_id": "1460806080"
  }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

Sie haben Ihren ersten Job erstellt, der eindeutig durch die ID 1460806080 identifiziert wird. Sie können diese ID verwenden, um die Konfiguration abzufragen, zu aktualisieren oder zu löschen.

Sie können die folgende URL verwenden, um den Auftragsstatus abzufragen:

`https://<IP>/stylebook/nitro/v2/config/jobs/<jobid>`

Beispiel 2

Sie können dasselbe StyleBook verwenden, um eine weitere Konfiguration oder ein Konfigurationspaket zu erstellen und es auf denselben oder verschiedenen NetScaler-Instanzen auszuführen. Erstellen Sie in diesem Beispiel eine weitere Konfiguration und geben Sie einen anderen Namen und eine andere IP-Adresse für den virtuellen Server an. Geben Sie LEASTCONNECTION als Lastenausgleichsmethode an. Stellen Sie diese Konfiguration auf zwei NetScaler-Instanzen bereit.

Die HTTP-Anfrage lautet wie folgt:

HTTP-METHODE: POST

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks`

ANFRAGE-HEADER:

Content-Type: application/json

Accept: application/json

ANFRAGE-BODY-NUTZLAST:

```
{
  "configpack":
  {
    "parameters": {
      "name": "lb1",
      "vip-ipaddress": "10.102.117.31",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "lb-alg": "LEASTCONNECTION"
    },
    "targets":
    [
      {
        "instance_id": "deecee30-f478-4446-9741-a85041903410"
      },
      {
        "instance_id": "abcdee30-f478-4446-9741-a85041903410"
      }
    ],
    "stylebook": {
            "name": "lb-vserver",
            "namespace": "com.example.stylebooks",
            "version": "1.0"
        }
  }
}
```

In dieser HTTP-Anfrage wird der virtuelle Lastenausgleichsserver lb1 mit der IP-Adresse 10.102.117.31 auf den beiden NetScaler-Instanzen mit den IDs „deecee30-f478-4446-9741-a85041903410“ und „abcdee30-f478-4446-9741-a85041903410“ erstellt.

Nach erfolgreicher Erstellung des Konfigurationspakets wird die folgende HTTP-Antwort empfangen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERWARTETE ANTWORT-HEADER (bei Erfolg):

202 OK

Content-Type: application/json

ERWARTETER ANTWORTTEXT (bei Erfolg):

```
{

    "job": {

        "job_id": "165769629"

    }

}
```

Dieses neue Konfigurationspaket hat eine andere ID, 165769629. Sie können diese Konfiguration aktualisieren oder entfernen, indem Sie diese ID verwenden.

Beispiel 3

Betrachten Sie das StyleBook „basic-lb-config“, das Sie unter StyleBook zum Erstellen einer grundlegenden Lastenausgleichskonfiguration erstellt haben. Verwenden Sie die REST-API, um ein Konfigurationspaket aus diesem StyleBook wie folgt zu erstellen:

HTTP-METHODE: POST

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks`

ANFRAGE-HEADER:

Content-Type: application/json

Accept: application/json

ANFRAGE-BODY-NUTZLAST:

```
{

  "configpack":

  {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "parameters":
    {
      "name": "myapp",
      "ip": "10.70.122.25",
      "svc-servers": ["192.168.100.11","192.168.100.12"],
       "svc-port": 8080
    },
    "targets":
    [
     {
      "instance_id": "deecee30-f478-4446-9741-a85041903410"
     },
     {
      "instance_id": "abcdefgi-d589-4557-8632-a74032802412"
     }
    ],
    "stylebook": {
            "name": "basic-lb-config",
            "namespace": "com.example.stylebooks",
            "version": "0.1"
        }
  }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

ERWARTETE ANTWORT-HEADER (bei Erfolg):

202 OK

Content-Type: application/json

ERWARTETER ANTWORTTEXT (bei Erfolg):

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

Bei dieser HTTP-Anfrage wird die Lastverteilungskonfiguration auf zwei NetScaler-Instanzen ausgeführt. Sie können sich bei diesen NetScaler-Instanzen anmelden, um zu überprüfen, ob ein virtueller Server und eine Dienstgruppe mit zwei gebundenen Diensten erstellt wurden.

Beispiel 4

Betrachten Sie das zusammengesetzte StyleBook **composite-example**, das Sie unter Ein zusammengesetztes StyleBook erstellen erstellt haben. Verwenden Sie REST-APIs, um ein Konfigurationspaket aus diesem StyleBook wie folgt zu erstellen:

HTTP-METHODE: POST

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks`

ANFRAGE-HEADER:

Content-Type: application/json

Accept: application/json

ANFRAGE-BODY-NUTZLAST:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

  "configpack":

  {

    "parameters": {

      "name": "myapp",

      "ip": "2.2.2.2",

      "svc-servers": ["10.102.29.52","10.102.29.53"]

    },

    "targets":

    [

     {

      "id": "deecee30-f478-4446-9741-a85041903410"

     },

     {

      "id": "abcdefgg-d589-4557-8632-a74032802412"

     }

    ],

    "stylebook": {

            "name": "composite-example",

            "namespace": "com.example.stylebooks",

            "version": "0.1"

        }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

Bei dieser HTTP-Anfrage wird die Konfiguration auf zwei NetScaler-Instanzen erstellt, die durch ihre IDs repräsentiert werden. Wenn Sie sich bei den NetScaler-Instanzen anmelden, können Sie die Konfigurationsobjekte anzeigen, die vom StyleBook „basic-lb-config“ erstellt wurden, das in das StyleBook „composite-example“ importiert wurde. Sie können auch einen neuen HTTP-Monitor namens `myapp-mon` sehen, der Teil des StyleBooks „composite-example“ war.

Nach erfolgreicher Erstellung des Konfigurationspakets wird die folgende HTTP-Antwort empfangen:

ERWARTETE ANTWORT-HEADER (bei Erfolg):

202 OK

Content-Type: application/json

ERWARTETER ANTWORT-BODY (bei Erfolg):

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

Aktualisieren einer Konfiguration

Um die Konfiguration zu aktualisieren, können Sie die folgende API verwenden. Hier wird ein Backend-Server mit der IP-Adresse 10.102.29.54 zum virtuellen Lastausgleichsserver `myapp: hinzugefügt.

HTTP-METHODE: PUT

URL: `https://<IP>/stylebook/nitro/v2/config/configpacks/<configpackid>`

ANFRAGE-HEADER:

Content-Type: application/json

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Accept: application/json

ANFRAGE-BODY-NUTZLAST:

```
{

  "configpack": {

    "parameters": {

      "name": "myapp",

      "ip": "2.2.2.2",

      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]

  },

  "targets":

   [

     {

      "instance_id": "deecee30-f478-4446-9741-a85041903410"

     },

     {

      "instance_id": "abdcedff-d589-4557-8632-a74032802412"

     }

   ]

  }

}
```

Bei erfolgreicher Aktualisierung des Konfigurationspakets wird die folgende HTTP-Antwort empfangen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ERWARTETE ANTWORT-HEADER (bei Erfolg):

202 OK

Content-Type: application/json

ERWARTETER ANTWORT-BODY (bei Erfolg):

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

Löschen einer Konfiguration

Um diese Konfiguration (von allen NetScaler-Instanzen) zu löschen, können Sie die API zum Löschen eines Konfigurationspakets wie folgt verwenden:

Nach erfolgreicher Löschung des Konfigurationspakets wird die folgende HTTP-Antwort empfangen:

HTTP-METHODE: DELETE

URL: `https://<DNS-or-IP>//stylebook/nitro/v2/config/configpacks/<configpackid>`

ANFRAGE-HEADER:

Accept: application/json

ERWARTETE ANTWORT-HEADER (bei Erfolg):

202 OK

Content-Type: application/json

ERWARTETE ANTWORT-NUTZLAST (bei Erfolg):

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

Melden Sie sich bei der NetScaler-Instanz an und überprüfen Sie, dass alle Konfigurationsobjekte, die Teil dieses Konfigurationspakets sind, entfernt wurden.

Um die Konfiguration von bestimmten NetScaler-Instanzen anstatt von allen Instanzen zu entfernen, verwenden Sie den Vorgang zum Aktualisieren des Konfigurationspakets in Aktualisieren einer Konfiguration. Ändern Sie das Attribut `targets` in der JSON-Nutzlast, um die spezifischen NetScaler-Instanz-IDs zu entfernen.

Konfigurationen mit APIs erstellen

Verwenden Sie die StyleBook-API, um Konfigurationen basierend auf diesem StyleBook zu erstellen. Sie können jedes beliebige Tool wie das cURL-Befehlszeilentool oder die Postman Chrome-Browsererweiterung verwenden, um HTTP-Anfragen an NetScaler Console zu senden.

Betrachten Sie das StyleBook-Beispiel, das Sie unter So erstellen Sie ein StyleBook zum Hochladen von SSL-Zertifikats- und Zertifikatsschlüsseldateien in NetScaler Console erstellt haben, um die Zertifikats- und Schlüsseldateien hochzuladen. Verwenden Sie die REST-API, um ein Konfigurationspaket aus dem StyleBook wie folgt zu erstellen:

POST

`https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks?mode=async`

```
{

    "configpack": {

        "stylebook": {

            "name": "lb",

            "namespace": "com.citrix.adc.stylebooks",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "version": "1.1"
        },
        "parameters": {
            "lb-appname": "lbapp1",
            "lb-virtual-ip": "192.168.1.1",
            "lb-virtual-port": "443",
            "lb-service-type": "SSL",
            "svc-service-type": "HTTP",
            "svc-servers": [
                {
                    "ip": "193.1.1.1",
                    "port": "80"
                }
            ],
            "certificates": [
                {
                    "cert-name": "cert1",
                    "cert-file": {
                        "name": "c3.pem",
                        "contents": "<base64 encoded content>",
                        "encoding_type": "base64"
                    },
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    "ssl-inform": "PEM",
                    "key-file": {
                        "name": "c3.key",
                        "contents": "<base64 encoded content>",
                        "encoding_type": "base64"
                    }
                }
            ]
        },
        "targets": [
            {
                "instance_id": "1b322685-3b23-4111-a9ce-56dd1c659e4c"
            }
        ]
        }
    }
}
```

Dies gibt eine Job-ID zurück, die verwendet werden kann, um den Abschluss des Konfigurationsauftrags zu verfolgen:

```
{
    "job": {
        "job_id": "388922985"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    }

}
```

Verwenden Sie die Job-Polling-API, um den Status des Jobs herauszufinden und wann der Konfigurationsauftrag abgeschlossen ist:

GET

`https://<ADM-endpoint-name>/stylebook/nitro/v2/config/jobs/388922985`

```
200 OK

{

    "job": {

        "job_id": "388922985",

        "status": "completed",

        "progress_info": [...],

        "result": {

            "config_key": "388922985",

            "created_by": "nsroot",

            "created_datetime": "2023-01-14 01:46:05.410998",

            "created_datetimestamp": "2023-01-14 01:46:05",

            "id": "388922985",

            "incarnation_number": "0",

            "last_modified_by": "nsroot",

            "last_modified_datetime": "2023-01-14 01:46:05",

            "lock": "Y",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "name": "sample-dns-stylebook",

            "namespace": "com.citrix.adc.tests",

            "primary_keys": "{}",

            "sb_id": "samp4ed0c4c90aefaadaff6422b0c395f67f",

            "status": "completed",

            "target_devices_json": "[{\"instance_id\": \"49a45044-
ceb3-4e9d-8a5d-e3fe225d90ed\", \"id\": \"1833061454\", \"group_id\": \"\",
\"instance_ip\": \"192.168.153.165\", \"hostname\": \"ctx-adc-dc01-v-
prod-54\", \"instance_role\": \"[\\\"default\\\"]\",
\"incarnation_number\": \"0\"}]",

            "tenant_id": "1a45fd70-7ce3-4bff-8642-1bd7f7e97673",

            "version": "1.0"

        }

    }

}
```


Die Job-ID (388922985) identifiziert das Konfigurationspaket. Sie können diese ID verwenden, um die Konfiguration abzufragen, zu aktualisieren oder zu löschen.

APIs verwenden, um Konfigurationen zum Hochladen beliebiger Dateitypen zu erstellen

Sie können auch die NetScaler Console API verwenden, um ein Konfigurationspaket zu erstellen, das Dateien auf die ausgewählte NetScaler-Instanz hochlädt.

Betrachten Sie das StyleBook-Beispiel, das Sie unter How to Create a StyleBook to Upload Files to NetScaler Console erstellt haben, um Dateien beliebigen Typs hochzuladen.

Verwenden Sie die folgende REST-API, um ein Konfigurationspaket aus diesem StyleBook zu erstellen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POST `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks?mode=async`

```
{

    "configpack": {

        "stylebook": {

        "name": "filetest",

        "namespace": "test.adc.stylebook",

        "version": "1.0"

        },

        "parameters": {

            "nameoffile": "file1",

            "fileupload": {

                "name": "relate.txt",

                "contents": "base64 encoded content",

                "encoding_type": "base64"

            }

        },

        "targets": [

            {

                "instance_id": "9419667d-27b7-495a-b87a-d3b5ee747dd3"

            }

        ],
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    }

}
```

Benutzerdefinierte StyleBooks mithilfe von APIs importieren

Verwenden Sie die StyleBook-API, um benutzerdefinierte StyleBooks in NetScaler Console zu importieren. Verwenden Sie REST-APIs, um ein Konfigurationspaket aus diesem StyleBook in einem beliebigen Tool zu erstellen, z. B. dem cURL-Befehlszeilentool oder der Postman Chrome-Browsererweiterung. Sie können beispielsweise ein StyleBook mit dem Namen `example-lb` importieren, das zum Erstellen einer Lastenausgleichskonfiguration auf einer NetScaler-Instanz verwendet werden kann.

HTTP-Methode: POST

URL: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/actions/import?mode=async`

```
{

    "import": {

        "file_name": "add_dnssoarec.yaml",

        "source": "<base 64 encoded content of the sb definition>",

        "encoding": "base64"

    }

}
```

Dabei ist der Wert des Attributs `source` die Base64-Kodierung des Inhalts Ihrer StyleBook-Datei. Sie können den YAML-Inhalt Ihrer StyleBook-Datei in ein Online-Tool einfügen. Verwenden Sie beispielsweise `<https://www.browserling.com/tools/file-to-base64>`, um die Base64-Zeichenfolge zu erhalten, die Sie dann als Wert für das Attribut `source` verwenden können.

Mit diesem API-Aufruf können Sie auch eine komprimierte Tarball-Datei (.tgz-Datei) hochladen, die mehrere StyleBook-Dateien in einem API-Vorgang enthält. Gehen Sie wie folgt vor:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Ändern Sie das Attribut `file_name` in die .tgz-Datei
- Ändern Sie das Attribut `source` in die Base64-Kodierung des Inhalts Ihrer .tgz-Datei

Nachdem die API im Tool erfolgreich ausgeführt wurde, erhalten Sie eine Antwort mit einer Job-ID. Verwenden Sie diese Job-ID, um den Vorgang bis zum Abschluss zu verfolgen:

```
200 ACCEPTED
```

Antworttext:

```
{

    "job": {

        "job_id": "12345678"

    }

}
```

Verwenden Sie die Job-ID, um den Status des Vorgangs zu verfolgen:

HTTP-Methode: GET

URL: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/jobs/<job-id>`

Der Status des Jobs wird zurückgegeben:

```
200 OK
```

Antworttext:

```
{

    "job": {

        "job_id": "<job-id>",

        "progress_info": [

            {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "is_last": "true",
                "message": "No job found",
                "status": "failed"
            }
        ],
        "status": "completed"
    }
}
```


Der Statuswert „completed“ zeigt an, dass das StyleBook erfolgreich importiert wurde. Bestätigen Sie den Status der Vorgänge, indem Sie Informationen zum StyleBook abrufen:

HTTP-Methode: GET

URL: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/samples/1.0/demo-helper-object`

Die Details des importierten StyleBooks werden angezeigt:

```
200 OK
```

Antworttext:


```
{
    "stylebook": {
        "builtin_namespaces": {},
        "created_datetime": "2023-01-14 00:13:59",
        "custom": true,
        "dependencies": [],
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "deprecate": "false",

        "description": "This Stylebook is a test",

        "display_name": "Test StyleBooks",

        "encoding": "BASE64",

        "header": "Test StyleBooks",

        "icon": "''",

        "id": "demo575731aacbfc20b4ff00b3b60ea59855",

        "is_updatable": true,

        "name": "demo-helper-object",

        "namespace": "samples",

        "primary_keys": {},

        "private": false,

        "repository_name": "",

        "reverse_dependencies": [],

        "schema_version": "1.0",

        "source": "<base 64 encoded content of the stylebook definition>",

        "tenant_id": "1a45fd70-7ce3-4bff-8642-1bd7f7e97673",

        "username": "abc",

        "version": "1.0"

    }

}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benutzerdefiniertes StyleBook mithilfe der API aktualisieren

Sie können die API verwenden, um ein benutzerdefiniertes StyleBook zu aktualisieren. Wenn Sie ein StyleBook aktualisieren, können Sie Änderungen am StyleBook vornehmen, ohne dessen Version zu ändern. Sie können auch die Definitionen aktualisieren, die aus einem StyleBook-Bundle importiert wurden.

POST: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/<Namespace>/<version>/<Name>/actions/update?mode=async`

Payload:

```
{

    "update": {

        "encoding": "base64",

        "source": "<base 64 encoded content of the stylebook definition>"

}

}

    }

}
```

HINWEIS

Diese API ist asynchron und gibt eine Job-ID zurück. Die Job-ID kann verwendet werden, um den Aktualisierungsauftrag bis zum Abschluss zu verfolgen, ähnlich wie bei der API zum Importieren eines StyleBooks.

APIs zum Herunterladen benutzerdefinierter StyleBooks verwenden

Verwenden Sie die folgende StyleBooks REST-API, um ein benutzerdefiniertes StyleBook herunterzuladen:

POST `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>/actions/download`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können die API in jedem Tool ausführen, z. B. im cURL-Befehlszeilentool. Sie können auch die Postman Chrome-Browsererweiterung verwenden, nachdem Sie die Felder IP-Adresse, Name, Version und Namespace geändert haben.

Wenn Sie diese API ausführen, wird das benutzerdefinierte StyleBook als gezippte Datei auf Ihren lokalen Computer heruntergeladen.

APIs zum Herunterladen abhängiger StyleBooks und zum Angeben des Komprimierungstyps verwenden

Verwenden Sie die folgende API, um den vollständigen Baum abhängiger StyleBooks herunterzuladen und ein Komprimierungsformat (hier: .tgz) anzugeben:

POST `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>/actions/download?dependencies=true&compress_type=tgz`

Die Antwort zeigt das StyleBook und seine Abhängigkeiten (falls vorhanden) in einem Tarball an.

```
200 OK

Content-disposition: attachment; filename=samples_1.0_demo-helper-object.tgz

Content-Type: application/x-zip

....zipped content...
```

API zum Löschen benutzerdefinierter StyleBooks verwenden

Verwenden Sie die folgende StyleBooks REST API, um ein benutzerdefiniertes StyleBook zu löschen:

LÖSCHEN: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>?dependencies=true`

Wenn der Abfrageparameter für Abhängigkeiten in der URL nicht angegeben oder sein Wert auf „false“ gesetzt ist, wird nur das StyleBook gelöscht. Die StyleBook-Abhängigkeiten werden nicht gelöscht.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn das benutzerdefinierte StyleBook und seine Abhängigkeiten erfolgreich aus der NetScaler Console entfernt wurden, erhalten Sie den HTTP-Antwortstatuscode 200.

HINWEIS

Sie können kein benutzerdefiniertes StyleBook löschen, das abhängige StyleBooks hat.

Angenommen, Sie haben ein StyleBook mit dem Namen `lb-virtual-ssl-extended` in NetScaler Console erstellt. Sie haben sich später entschieden, dieses StyleBook zu löschen.

Sie können die API in jedem Tool ausführen, z. B. dem cURL-Befehlszeilentool. Sie können auch die Postman Chrome-Browsererweiterung verwenden, nachdem Sie die Felder für IP-Adresse, Name, Version und Namespace geändert haben.

APIs zum Aktualisieren eines vorhandenen Konfigurationspakets verwenden

Sie können die StyleBook-API verwenden, um die vorhandenen Konfigurationspakete in NetScaler Console zu aktualisieren.

PUT: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async`

Payload:

```
{

    "configpack": {

        "stylebook": {

            "name": "waf-adv",

            "namespace": "com.citrix.adc.stylebooks",

            "version": "1.3"

        },

        "parameters": {

            "name": "TestApp1",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "lbname": "my-lbv",
            "waf-settings": {
                "rule": "true",
                "type": [
                    "HTML"
                ],
                "profile-settings": {
                    "logeverypolicyhit": false,
                    "enablesignatures": {
                        "signaturename": "waf-sign1"
                    },
                    "sqlinjection-settings": {
                        "sqlinjectionaction": [
                            "log",
                            "stats"
                        ],
                        "sqlinjection-default-settings": {
                            "sqlinjectiontransformspecialchars": true,
                            "sqlinjectionchecksqlwildchars": true,
                            "sqlinjectiontype": "SQLSplCharANDKeyword",
                            "sqlinjectionparsecomments": "checkall",
                            "sqlinjectiongrammar": "OFF"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    }
                },
                "bufferoverflow-settings": {
                    "bufferoverflowaction": [
                        "log"
                    ],
                    "bufferoverflowmaxurllength": "2048",
                    "bufferoverflowmaxheaderlength": "4096",
                    "bufferoverflowmaxcookielength": "4096",
                    "bufferoverflowmaxquerylength": "65535",
                    "bufferoverflowmaxtotalheaderlength": "65535"
                }
            }
        }
    },
        "targets": [
        {
            "instance_id": "1b322685-3b23-4111-a9ce-56dd1c659e4c"
        }
        ]
}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

Ein HTTP-Status 202 und ein Antworttext mit einer Job-ID werden zurückgegeben. Sie können die Job-ID verwenden, um den Status des Aktualisierungsvorgangs zu verfolgen:

```
{

    "job": {

        "job_id": "1092579455"

    }

}
```

Sie können diese Job-ID (in diesem Beispiel: 1092579455) mithilfe der Jobs-Polling-API verfolgen:

GET: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/jobs/1092579455`

Der Aktualisierungsvorgang ist erfolgreich abgeschlossen, wenn die Antwort den Status "completed" enthält. Jeder andere Wert in diesem Feld zeigt das Fehlschlagen des Aktualisierungsauftrags an. Die Ursache des Fehlers ist im Objekt **progress_info** verfügbar.

```
{

    "job": {

        "job_id": "4268148987",

        "status": "completed",

        "progress_info": [

            {

                "is_last": "false",

                "message": "Validated the parameters",

                "status": "success"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            },
            {
                "is_last": "false",
                "message": "Configuration audit completed",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Computed configuration objects",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Prepared objects for applying configuration on
192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Retrieved existing data for updatable objects
on instance 192.168.153.165",
                "status": "success"
            },
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            {

                "is_last": "false",

                "message": "Applied configuration on instance
192.168.153.165",

                "status": "success"

            },

            {

                "is_last": "false",

                "message": "Retrieved data for configuration audit on
instance 192.168.153.165",

                "status": "success"

            },

            {

                "is_last": "false",

                "message": "Logged out from instance 192.168.153.165",

                "status": "success"

            },

            {

                "is_last": "true",

                "message": "Saved configpack.",

                "status": "completed"

            }

        ],
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "result": {
            "status": "completed",
            "id": "4268148987",
            "config_key": "4268148987",
            "created_by": "nsroot",
            "created_datetime": "2023-01-20 18:57:58.985435",
            "created_datetimestamp": "2023-01-20 18:57:58",
            "last_modified_by": "nsroot",
            "last_modified_datetime": "2023-01-20 19:00:32",
            "name": "sample-dns-stylebook",
            "namespace": "com.citrix.adc.tests",
            "version": "1.0"
        }
    }
}
```


APIs zum Aktualisieren von Zielinstanzen verwenden

Ändern Sie in der Payload des aktualisierten Konfigurationspakets den Abschnitt `targets`, um eine NetScaler-Instanz hinzuzufügen, zu entfernen oder zu ersetzen.

Beispiel:

Im folgenden Beispiel wird das Objekt `targets` in der Payload geändert, um der Konfiguration einen neuen Ziel-NetScaler hinzuzufügen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

    "targets": [

        {

            "instance_id": "<Existing-ADC-instance-ID>"

        },

        {

            "instance_id": "<New-ADC-instance-ID>"

        }

    ],

}
```

Wenn die Aktualisierung erfolgreich ist, wird die Konfiguration auf der neuen NetScaler-Instanz bereitgestellt. Das Ändern der Ziele einer Konfiguration ist nützlich, wenn Sie Anwendungskonfigurationen zwischen NetScalern verschieben möchten. Ändern Sie beispielsweise das Objekt `targets`, wenn ein NetScaler zur Wartung aus einer Konfiguration entfernt werden muss.

HINWEIS

Um eine Konfiguration von allen aktuellen Zielinstanzen zu entfernen, verwenden Sie ein leeres Objekt `targets`. Die NetScaler Console-Konfiguration bleibt erhalten, wird aber von allen NetScalern entfernt, auf denen sie zuvor bereitgestellt wurde. Sie können die Konfiguration bei Bedarf erneut aktualisieren, um ein oder mehrere Ziele anzugeben.

Das folgende API-Beispiel entfernt die Konfiguration von all seinen vorhandenen Zielen:

PUT: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async`

Payload:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{
    "configpack": {
        "stylebook": {
            "name": "waf-adv",
            "namespace": "com.citrix.adc.stylebooks",
            "version": "1.3"
        },
        "parameters": {
            "name": "TestApp1",
            "lbname": "my-lbv",
            "waf-settings": {
                "rule": "true",
                "type": [
                    "HTML"
                ],
                "profile-settings": {
                    "logeverypolicyhit": false,
                    "enablesignatures": {
                        "signaturename": "waf-sign1"
                    },
                    "sqlinjection-settings": {
                        "sqlinjectionaction": [
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                        "log",
                        "stats"
                    ],
                    "sqlinjection-default-settings": {
                        "sqlinjectiontransformspecialchars": true,
                        "sqlinjectionchecksqlwildchars": true,
                        "sqlinjectiontype": "SQLSplCharANDKeyword",
                        "sqlinjectionparsecomments": "checkall",
                        "sqlinjectiongrammar": "OFF"
                    }
                },
                "bufferoverflow-settings": {
                    "bufferoverflowaction": [
                        "log"
                    ],
                    "bufferoverflowmaxurllength": "2048",
                    "bufferoverflowmaxheaderlength": "4096",
                    "bufferoverflowmaxcookielength": "4096",
                    "bufferoverflowmaxquerylength": "65535",
                    "bufferoverflowmaxtotalheaderlength": "65535"
                }
            }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            }

        },

        "targets": []

    }

}
```

API zur Konfigurationsprüfung verwenden

Sie können die API verwenden, um die Änderungen, die von einem StyleBook-Konfigurationspaket vorgenommen wurden, mit der aktuellen NetScaler-Konfiguration zu vergleichen. Mit diesem Vergleich können Sie Folgendes tun:

- Die Konfigurationsabweichung zwischen dem StyleBook-Konfigurationspaket und der NetScaler-Konfiguration erkennen.
- Alle geänderten und gelöschten Objekte auf dem NetScaler identifizieren, die die vom Konfigurationspaket vorgenommenen Änderungen nicht widerspiegeln.

POST: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>/actions/audit?mode=async`

API zum Exportieren eines Konfigurationspakets verwenden

Sie können die StyleBook-API verwenden, um Konfigurationspakete aus der NetScaler Console zu exportieren. Das Exportpaket wird auf Ihrem lokalen Computer gespeichert. Es enthält die JSON-Datei mit allen in einem Konfigurationspaket definierten Parametern und allen zugehörigen Systemdateien.

POST `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>/actions/export`

Payload:

```
{

    "export": {

        "options": {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "include_stylebook": true,
            "include_targets": false,
            "compress_type": "zip",
            "password_protect": false
        },
        "passphrase": ""
    }
}
```

Sie können das Konfigurationspaket zusammen mit dem zugehörigen StyleBook und den Zielinstanzen exportieren.

Wenn Sie ein Konfigurationspaket exportieren, wird ein `tgz` - oder `zip` -Bundle auf Ihren lokalen Computer heruntergeladen. Der Bundle-Typ hängt von der angegebenen `compress_type` ab.

APIs verwenden, um das Konfigurationspaket auf ein neues StyleBook zu aktualisieren

Sie können StyleBook-APIs verwenden, um das Konfigurationspaket von einem vorhandenen StyleBook auf ein neues StyleBook zu aktualisieren.

POST `http://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/actions/upgrade?mode=async`

Payload:

```
{
    "upgrade": {
            "stylebook": {
            "name": "customer-template",
            "namespace": "neustar.citrix.adc.stylebooks",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "version": "6.2"
        },
        "configpack_ids": [
            "1644278065",
            "2750234437"
        ]
    }
}
```

In dieser Beispiel-Payload sind die aufgelisteten Konfigurationspakete 1644278065 und 2750234437. Diese Konfigurationspakete werden auf ein neues StyleBook mit dem Namen `customer-template` und der Version 6.2 aktualisiert.

Um den Status des Auftrags zur Aktualisierung des Konfigurationspakets abzurufen, verwenden Sie die Job-Polling-API:

GET: `https://<ADM-IP-address>/stylebook/nitro/v1/config/jobs/<job-ID>`

HINWEIS

Wiederholen Sie die **GET**-Methode, bis das Statusfeld im Antworttext auf **completed** (erfolgreich) oder **failed** (fehlgeschlagen) gesetzt ist.

API verwenden, um eine Zielinstanz von einem Konfigurationspaket zu trennen

Wenn Sie eine Zielinstanz von einem Konfigurationspaket trennen, werden die am Konfigurationspaket vorgenommenen Änderungen nicht auf diese Instanz bereitgestellt. Sie können die API verwenden, um eine Zielinstanz zu trennen.

POST: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>/actions/detach_targets`

Payload:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

    "detach_targets": [

        {

            "instance_id": "1b322685-3b23-4111-a9ce-56dd1c659e4c",

            "id": "1b322685-3b23-4111-a9ce-56dd1c659e4c"

        }

    ]

}
```

NetScaler-Instanz mit der API zwangsweise aus dem Konfigurationspaket löschen

Wenn die NetScaler-Instanz aus der NetScaler Console entfernt wird, ohne ihr Konfigurationspaket zu löschen, kann ein Fehler auftreten. Daher müssen Sie diese Instanz zwangsweise aus dem Konfigurationspaket löschen.

Sie können die StyleBook-API verwenden, um eine NetScaler-Instanz zwangsweise aus dem Konfigurationspaket zu löschen.

PUT: `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async&force_targets_delete=true`

```
{

    "configpack": {

        "stylebook": {

            "name": "test-policy-patset",

            "namespace": "com.citrix.adc.stylebooks",

            "version": "1.1"

        },
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "parameters": {
            "lbname": "test11"
        },
        "targets": [
            {
                "instance_id": "f9bdf101-61ec-46a7-bf09-e9ce097b7cfd",
                "instance_ip": "10.106.100.116",
                "roles": [
                    "default"
                ]
            }
        ]
    }
}
```

APIs zum Löschen von Konfigurationspaketen verwenden

Sie können die folgende StyleBook-API verwenden, um Konfigurationspakete zu löschen.

DELETE `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async`

Ein HTTP-Status 202 und eine Antwortnutzlast werden angezeigt. Die Antwortnutzlast enthält eine Job-ID, mit der Sie den Status des Löschvorgangs verfolgen können.

Die Antwortnutzlast lautet wie folgt:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

    "job": {

        "job_id": "1841028854"

    }

}
```

Um den Löschvorgang zu verfolgen, verwenden Sie die Job-Polling-API mit der Job-ID (in diesem Beispiel ist die Job-ID 1841028854):

GET `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/jobs/1841028854`

Wenn das Statusfeld in der Antwort auf „completed“ gesetzt ist, bedeutet dies, dass der Löschvorgang erfolgreich war, wie im folgenden Beispiel gezeigt:

```
{

    "job": {

        "job_id": "3920886024",

        "status": "completed",

        "progress_info": [

            {

                "is_last": "false",

                "message": "Validated the parameters",

                "status": "success"

            },

            {

                "is_last": "false",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                "message": "Configuration audit completed",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Computed configuration objects",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Prepared objects for applying configuration on
192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Retrieved existing data for updatable objects
on instance 192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Applied configuration on instance
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Retrieved data for configuration audit on
instance 192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "false",
                "message": "Logged out from instance 192.168.153.165",
                "status": "success"
            },
            {
                "is_last": "true",
                "message": "Removed configpack.",
                "status": "completed"
            }
        ]
    }
}
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Der Löschvorgang kann in den folgenden Szenarien fehlschlagen:

- Die NetScaler-Instanz, auf der die Konfiguration vorhanden ist, ist ausgefallen.
- Die NetScaler-Instanz ist für die NetScaler Console nicht erreichbar.
- Die Konfiguration ist auf dem NetScaler nicht mehr verfügbar.

Sie können die Entfernung der Konfiguration von der NetScaler Console erzwingen, auch wenn sie nicht vom NetScaler entfernt werden kann. In solchen Fällen müsste die NetScaler-Konfiguration manuell wiederhergestellt werden.

Um die Entfernung der Konfiguration von der NetScaler Console zu erzwingen, fügen Sie den Abfrageparameter „force=true“ zur API hinzu:

DELETE `https://<ADM-endpoint-name>/stylebook/nitro/v2/config/configpacks/<configpack-ID>?mode=async&force=true`.

StyleBooks-Grammatik

Sie können Ihre eigenen StyleBooks entwerfen, in NetScaler Console importieren und sie dann verwenden, um Konfigurationen entweder über die NetScaler Console GUI oder über APIs zu erstellen. Um Ihre eigenen StyleBooks erstellen zu können, müssen Sie zunächst die Grammatik und Syntax der verschiedenen Konstrukte und Attribute verstehen, die Sie verwenden können.

Dieses Dokument beschreibt die verschiedenen Konstrukte und Referenzen, die Sie beim Erstellen von StyleBooks verwenden können.

Klicken Sie in der folgenden Tabelle auf einen Abschnitt, ein Konstrukt oder einen Referenznamen, um die Details anzuzeigen.

Header	StyleBooks importieren
Parameter	Parameters-Standardquellen-Konstrukt
Substitutionen	Komponenten
Optionale Eigenschaften	Hilfskomponenten
Eigenschaften-Standardquellen	Verschachtelte Komponenten
Bedingungskonstrukt	Wiederholungskonstrukt

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wiederholungsbedingungskonstrukt	Ausgaben
Verschachtelte Wiederholungen	Elternreferenz
Parameterreferenz	Substitutionsreferenz
Komponentenreferenz	Operationen
Variablenreferenz	Alarme
Analysen	Integrierte Funktionen
Ausdrücke	Abhängigkeitserkennung
Inline-Interpolationen(/de-de/netscaler-console-service/stylebooks/stylebooks-grammar/in-place-interpolations.html)	

HINWEIS

Verwenden Sie beim Definieren von `repeat-item`, `repeat-index` oder Argumenten für Substitutionsfunktionen die folgenden reservierten Wörter nicht, um eine benutzerdefinierte Variable zu benennen, `$<var-name>`

- StyleBook, Parameter, Substitutionen, Komponenten, Eigenschaften, Ausgaben, übergeordnetes Element, selbst, Operationen, Analysen, Alarme
- repeat-item, repeat-item-0, repeat-item-1, repeat-item-2
- repeat-index, repeat-index-0, repeat-index-1, repeat-index-2
- Standard
- Rollen, Rolle, Ziele, Ziel
- Kontext, Elternkontext, Elternkontext

Informationen und Beispiele dazu, wie Sie Ihre eigenen StyleBooks entwerfen können, finden Sie unter So erstellen Sie Ihre eigenen StyleBooks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Header

Die ersten sechs Zeilen eines StyleBooks bilden den Header-Abschnitt. Dieser Abschnitt ermöglicht es Ihnen, die Identität eines StyleBooks zu definieren und zu beschreiben, was es tut. Dies ist ein obligatorischer Abschnitt.

Die folgende Tabelle beschreibt die Attribute des Header-Abschnitts:

ATTRIBUT	BESCHREIBUNG
Name	Ein Name zur Identifizierung des StyleBooks. Dieses Attribut ist obligatorisch.
Beschreibung	Eine Beschreibung, die definiert, was ein StyleBook tut. Diese Beschreibung wird in der NetScaler Console GUI angezeigt. Dies ist ein optionales Attribut.
display-name	Ein beschreibender Name für das StyleBook. Dieser Name wird in der NetScaler Console GUI angezeigt. Dies ist ein optionales Attribut.
Autor	Die Person oder Organisation, die das StyleBook erstellt. Dies ist ein optionales Attribut.
Namespace	Ein Namespace ist Teil eines eindeutigen Identifikators für ein StyleBook, um Namenskollisionen zu vermeiden. Ein Namespace kann eine beliebige Zeichenfolge sein, aber es ist eine gute Praxis, ihn zur Benennung des Unternehmens, der Abteilung oder der Einheit zu verwenden, die eine Reihe von StyleBooks erstellt oder besitzt. Zum Beispiel können Sie das folgende Format verwenden: `<company>.<department>.<unit>.stylebooks`. Dies ist ein obligatorisches Attribut.
Version	Die Versionsnummer des StyleBooks. Sie können die Versionsnummer ändern, wenn Sie ein StyleBook aktualisieren. StyleBooks unterschiedlicher Versionen können

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUT	BESCHREIBUNG
	nebeneinander existieren. Dies ist ein obligatorisches Attribut.
Schema-Version	Die Version des StyleBooks-Schemas. Sie hat den Wert „1.0“ in der aktuellen Version von NetScaler Console. Dies ist ein obligatorisches Attribut.
privat	Wenn dieses Attribut auf „true“ gesetzt ist, wird das StyleBook nicht in der NetScaler Console GUI angezeigt. Dies ist eine nützliche Einstellung für StyleBooks, die Bausteine für andere StyleBooks sind und nicht direkt von Benutzern verwendet werden sollen. Dies ist ein optionales Attribut. Sein Standardwert ist „false“.

Beispiel:

```
    name: lb


    description: "This stylebook defines a sample load balancing
configuration."


    display-name: "Load Balancing StyleBook (HTTP)"


    author: Mike Smith (ACME Infra team)


    namespace: com.example.stylebooks
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
schema-version: "1.0"



version: "0.1"
```

Die Kombination aus Name, Namespace und Version identifiziert ein StyleBook im System eindeutig. Sie können in NetScaler Console keine zwei StyleBooks mit derselben Kombination aus Name, Namespace und Version haben. Sie können jedoch zwei StyleBooks mit demselben Namen und derselben Version, aber unterschiedlichen Namespaces haben, oder mit demselben Namespace und derselben Version, aber unterschiedlichen Namen.

StyleBooks importieren

Dies ist der zweite Abschnitt Ihres StyleBooks und ermöglicht es Ihnen, zu deklarieren, auf welche anderen StyleBooks Sie von Ihrem aktuellen StyleBook aus verweisen möchten. Dadurch können Sie andere StyleBooks importieren und wiederverwenden, anstatt dieselbe Konfiguration in Ihrem eigenen StyleBook neu zu erstellen. Dies ist ein obligatorischer Abschnitt.

Sie müssen den **Namespace** und die **Versionsnummer** der StyleBooks deklarieren, auf die Sie in Ihrem aktuellen StyleBook verweisen möchten. Jedes StyleBook muss auf den Namespace netscaler.nitro.config verweisen, wenn es NITRO-Konfigurationsobjekte direkt verwendet. Dieser Namespace enthält alle NetScaler NITRO-Typen, wie z. B. `lbvserver` Service oder Monitor. StyleBooks für NetScaler-Versionen 10.5 und höher werden unterstützt, was bedeutet, dass Sie Ihr StyleBook verwenden können, um Konfigurationen auf jeder NetScaler-Instanz mit Release 10.5 oder höher zu erstellen und auszuführen.

Das in der Sektion „import-stylebooks“ verwendete Attribut **Präfix** ist eine Kurzform, um auf die Kombination aus Namespace und Version zu verweisen. Zum Beispiel kann das Präfix „ns“ verwendet werden, um auf den Namespace netscaler.nitro.config mit Version 10.5 zu verweisen. In den späteren Abschnitten Ihres StyleBooks können Sie, anstatt jedes Mal den Namespace und die Version zu verwenden, wenn Sie auf ein StyleBook mit diesem Namespace und dieser Version verweisen möchten, einfach die gewählte Präfixzeichenfolge zusammen mit dem Namen des StyleBooks verwenden, um es eindeutig zu identifizieren.

Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
import-stylebooks:

 -

   namespace: netscaler.nitro.config

   version: "10.5"

   prefix: ns

-

   namespace: com.acme.stylebooks

   version: "0.1"

   prefix: stlb
```

In diesem Beispiel wird das erste definierte Präfix „ns“ genannt und verweist auf den Namespace netscaler.nitro.config und die Version 10.5. Das zweite definierte Präfix wird `stlb` genannt und verweist auf den Namespace com.acme.stylebooks und die Version 0.1.

Nachdem Sie ein Präfix definiert haben, können Sie jedes Mal, wenn Sie auf einen Typ oder ein StyleBook verweisen möchten, das zu einem bestimmten Namespace und einer bestimmten Version gehört, die Notation **\<Namespace-Kurzform\>::\<Typname\>** verwenden. Zum Beispiel verweist **ns::lbvserver** auf den Typ `lbvserver`, der im Namespace netscaler.nitro.config, Version 10.5, definiert ist.

Wenn Sie auf ähnliche Weise auf ein StyleBook mit der Version „0.1“ im Namespace com.acme.stylebooks verweisen möchten, können Sie die Notation **stlb::\<StyleBook-Name\>** verwenden.

HINWEIS

Konventionell wird das Präfix „ns“ verwendet, um auf den NITRO-Namespace von NetScaler zu verweisen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Parameter

Dieser Abschnitt ermöglicht es Ihnen, alle Parameter zu definieren, die Sie in Ihrem StyleBook benötigen, um eine Konfiguration zu erstellen. Er beschreibt die Eingabe, die Ihr StyleBook entgegennimmt. Obwohl dieser Abschnitt optional ist, benötigen die meisten StyleBooks einen. Sie können den Parameterabschnitt verwenden, um die Felder für die Benutzer zu definieren, die das StyleBook verwenden, um eine Konfiguration auf einer NetScaler-Instanz zu erstellen.

Wenn Sie Ihr StyleBook in die NetScaler Console importieren und es zum Erstellen einer Konfiguration verwenden, nutzt die GUI diesen Abschnitt des StyleBooks, um ein Formular anzuzeigen. Dieses Formular nimmt eine Eingabe für die definierten Parameterwerte entgegen.

Der folgende Abschnitt beschreibt die Attribute, die Sie für jeden Parameter in diesem Abschnitt angeben müssen:

'Name'

Der Name des Parameters, den Sie definieren möchten. Sie können einen alphanumerischen Namen angeben.

Der Name muss mit einem Buchstaben beginnen und kann weitere Buchstaben, Zahlen, Bindestriche (-) oder Unterstriche (_) enthalten.

Beim Schreiben eines StyleBooks können Sie dieses `name` Attribut verwenden, um in anderen Abschnitten mit der Notation $parameters.\<name> auf den Parameter zu verweisen.

Obligatorisch? Ja

'Bezeichnung'

Eine Zeichenfolge, die in der NetScaler Console GUI als Name dieses Parameters angezeigt wird.

Obligatorisch? Nein

'Beschreibung'

Eine Hilfszeichenfolge, die beschreibt, wofür der Parameter verwendet wird. Die NetScaler Console GUI zeigt diesen Text an, wenn der Benutzer auf das Hilfesymbol für diesen Parameter klickt.

Obligatorisch? Nein

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'Typ'

Der Werttyp, den diese Parameter annehmen können. Parameter können einen der folgenden integrierten Typen haben:

- `string`: Ein Array von Zeichen. Wenn keine Länge angegeben ist, kann der Zeichenfolgenwert eine beliebige Anzahl von Zeichen annehmen. Sie können die Länge eines Zeichenfolgentyps jedoch mithilfe der Attribute min-length und max-length begrenzen.
- `number`: Eine ganze Zahl. Sie können die minimale und maximale Zahl, die dieser Typ annehmen kann, mithilfe der Attribute min-value und max-value angeben.
- `boolean`: Kann entweder true oder false sein. YAML betrachtet alle Literale als Booleans (zum Beispiel Yes oder No).
- `ipaddress`: Eine Zeichenfolge, die eine gültige IPv4- oder IPv6-Adresse darstellt.
- `ipnetwork`: Es besteht aus zwei Teilen. Der erste Teil ist die IP-Adresse und der zweite Teil ist die Netzmaske.

  Die Netzmaske besteht aus der Netzmaskenlänge (`netmask-len`) oder der Netzmasken-IP-Adresse (`netmask_ip`). Die Netzmaskenlänge ist eine ganze Zahl zwischen 0-32 und 0–128 für eine IPv6-Adresse. Sie wird verwendet, um die Anzahl der IP-Adressen in einem Netzwerk zu bestimmen.

  Beim Erstellen oder Aktualisieren eines Konfigurationspakets über die NetScaler Console GUI können Sie eine der folgenden Aktionen ausführen:

  - Netzmaskenlänge aktivieren und die IP-Adresse und Netzmaskenlänge eingeben
  - Netzmaskenlänge deaktivieren und die IP-Adresse und Netzmasken-IP-Adresse eingeben
- `tcp-port`: Eine Zahl zwischen 0 und 65535, die einen TCP- oder UDP-Port darstellt.
- `password`: Stellt einen undurchsichtigen/geheimen Zeichenfolgenwert dar. Wenn die NetScaler Console GUI einen Wert für diesen Parameter anzeigt, wird er als Sternchen (*****) dargestellt.
- `certfile`: Stellt eine Zertifikatsdatei dar. Dieser Wert ermöglicht es Ihnen, die Dateien direkt von Ihrem lokalen System hochzuladen, wenn Sie eine StyleBook-Konfiguration über die NetScaler Console GUI erstellen. Die hochgeladene Zertifikatsdatei wird im Verzeichnis `/var/mps/tenants/\<tenant_path>/ns_ssl_certs` in NetScaler Console gespeichert.

  Die Zertifikatsdatei wird der Liste der von NetScaler Console verwalteten Zertifikate hinzugefügt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `keyfile`: Stellt eine Zertifikatsschlüsseldatei dar. Dieser Wert ermöglicht es Ihnen, die Datei direkt von Ihrem lokalen System hochzuladen, wenn Sie eine StyleBook-Konfiguration über die NetScaler Console GUI erstellen. Die hochgeladene Zertifikatsdatei wird im Verzeichnis `/var/mps/tenants/\<tenant_path>/ns_ssl_keys` in NetScaler Console gespeichert.

  Die Zertifikatsschlüsseldatei wird der Liste der von NetScaler Console verwalteten Zertifikatsschlüssel hinzugefügt.
- `certkey`: Dieser Typ wird verwendet, um SSL-Zertifikate aus dem NetScaler Console-Zertifikatsspeicher auszuwählen. Dieser Speicher listet die vorhandenen SSL-Zertifikate auf, die auf Ihren NetScaler Console-Server hochgeladen wurden. So können Sie SSL-Zertifikate an einem Ort, nämlich dem NetScaler Console-Zertifikatsspeicher, speichern und bei Bedarf wiederverwenden.

  Beim Erstellen eines Konfigurationspakets kann ein Benutzer SSL-Zertifikate aus dem Zertifikatsspeicher hinzufügen oder auswählen. Außerdem kann der Benutzer dasselbe Zertifikat für mehrere Konfigurationspakete auswählen.
- `file`: Stellt eine Datei dar.
- `object`: Dieser Typ wird verwendet, um mehrere verwandte Parameter unter einem übergeordneten Element zu gruppieren. Geben Sie für den übergeordneten Parameter den Typ als „object“ an. Ein Parameter vom Typ „object“ kann einen verschachtelten „parameters“-Abschnitt haben, um die darin enthaltenen Parameter zu beschreiben.
- `another StyleBook`: Wenn Sie diesen Parametertyp verwenden, erwartet dieser Parameter, dass sein Wert in der Form der Parameter vorliegt, die im StyleBook definiert sind und seinen Typ angeben.

Ein Parameter kann auch eine `type` haben, die die Liste der Typen ist. Fügen Sie dazu `[]` am Ende des Typs hinzu. Wenn beispielsweise das `type`-Attribut `string[]` ist, nimmt dieser Parameter eine Liste von Zeichenfolgen als Eingabe. Sie können eine, zwei oder mehrere Zeichenfolgen für diesen Parameter angeben, wenn Sie eine Konfiguration aus diesem StyleBook erstellen.

Obligatorisch? Ja

'Netzwerk'

Für `type: ipaddress` können Sie das Attribut `network` angeben, um eine IP-Adresse automatisch aus einem NetScaler Console IPAM-Netzwerk zuzuweisen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console weist eine IP-Adresse automatisch aus dem Attribut `network` zu, wenn Sie eine StyleBook-Konfiguration erstellen.

Beispiel:

```
name: virtual-ip

label: "Load Balancer IP Address"

type: ipaddress

network: "network-1"

required: true
```

In diesem Beispiel weist das Feld `virtual-ip` automatisch eine IP-Adresse aus `network-1` zu. Die IP-Adresse wird nach dem Löschen der Konfiguration an das Netzwerk zurückgegeben.

'dynamic-allocation'

Das Attribut `dynamic-allocation` wird in der Parameterdefinition von `type:ipaddress` hinzugefügt. Verwenden Sie dieses Attribut, um die NetScaler Console IPAM-Netzwerke dynamisch aufzulisten. Dieses Attribut kann entweder `true` oder `false` als Eingabe annehmen. Für `type: ipaddress` geben Sie das Attribut `dynamic-allocation: true` an, um die NetScaler Console IPAM-Netzwerke, die sich in NetScaler Console befinden, dynamisch aufzulisten. Im Formular zur Erstellung von Konfigurationspaketen können Sie Folgendes tun:

1. Wählen Sie das erforderliche IPAM-Netzwerk aus der Liste aus.
2. Geben Sie eine IP-Adresse an, die Sie aus dem ausgewählten IPAM-Netzwerk zuweisen möchten.

   Wenn keine IP-Adresse angegeben wird, weist die NetScaler Console automatisch eine IP-Adresse aus dem ausgewählten IPAM-Netzwerk zu.

Beispiel:

```
-

  name: virtual-ip

  label: "Load Balancer IP Address"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  type: ipaddress

  dynamic-allocation: true

  required: true
```

In diesem Beispiel listet das Feld `virtual-ip` die NetScaler Console IPAM-Netzwerke auf, die sich in NetScaler Console befinden. Wählen Sie ein Netzwerk aus der Liste aus, um automatisch eine IP-Adresse aus dem Netzwerk zuzuweisen. Die IP-Adresse wird an das Netzwerk zurückgegeben, wenn die Konfiguration gelöscht wird.

'Schlüssel'

Geben Sie „true“ oder „false“ an, um zu kennzeichnen, ob dieser Parameter ein Schlüsselparameter für das StyleBook ist.

Ein StyleBook kann einen oder mehrere Parameter als „Schlüssel“-Parameter definiert haben. Die Seite **Configuration > Config Packs** zeigt den Wert des Parameters als **Anzeigeschlüssel** an.

Wenn Sie verschiedene Konfigurationspakete aus demselben StyleBook erstellen, kann jede Konfiguration einen anderen Wert für diesen Parameter haben. Dieser Wert wird als Anzeigeschlüssel in der GUI angezeigt. Mit diesem Schlüssel können Sie das Konfigurationspaket sortieren oder filtern.

Beispiel:

```
parameters:

  - name: example-appname

    type: string

    label: Application Name

    required: true

    key: true
```

Wenn ein StyleBook-Benutzer ein Konfigurationspaket erstellt, wird der Wert für den Parameter `example-appname` als Anzeigeschlüssel angezeigt. Der StyleBook-Benutzer kann diesen Schlüssel verwenden, um dieses Konfigurationspaket zu identifizieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Der **Konfigurationsschlüssel** eines Konfigurationspakets überschreibt das Schlüsselattribut, das für einen seiner Parameter festgelegt ist. Wenn ein Benutzer also einen Wert für den Konfigurationsschlüssel eingibt, wird dieser Wert in der Spalte **Anzeigeschlüssel** angezeigt.

Standardwert ist false.

Obligatorisch? Nein

'erforderlich'

Geben Sie true oder false an, um anzugeben, ob ein Parameter obligatorisch oder optional ist. Wenn er auf true gesetzt ist, ist der Parameter obligatorisch, und der Benutzer muss einen Wert für diesen Parameter angeben, wenn er Konfigurationen erstellt.

Die NetScaler Console GUI zwingt den Benutzer, einen gültigen Wert für diesen Parameter anzugeben.

Standardwert ist false.

Obligatorisch? Nein

'allowed-values'

Verwenden Sie dieses Attribut, um eine Liste gültiger Werte für einen Parameter zu definieren, wenn der Typ auf „string“ gesetzt ist.

Beim Erstellen einer Konfiguration über die NetScaler Console GUI wird der Benutzer aufgefordert, einen Parameterwert aus dieser Liste auszuwählen. Diese Liste ist statisch; der Benutzer kann nur einen Wert aus der Liste auswählen. Wenn Sie dem Benutzer erlauben möchten, Werte zur Liste hinzuzufügen, verwenden Sie das Attribut `allow-new-values`.

HINWEIS

Wenn Sie die Listenwerte als Radiooptionen anzeigen möchten, legen Sie das Attribut `layout` fest.

Beispiel 1:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

      name: ipaddress

      type: string

      allowed-values:

            -  SOURCEIP

            -  DEST IP

            -  NONE
```

Beispiel 2:

```
-

      name: TCP Port

      type: tcp-port

      allowed-values:

            -  80

            -  81

            -  8080
```

Beispiel 3:

Liste von `tcp-ports`, wobei jedes Element der Liste nur Werte haben kann, die in `allowed-values` angegeben sind.

```
-

      name: tcpports

      type: tcp-port[]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      allowed-values:
            -  80
            -  81
            -  8080
            -  8081
```

Obligatorisch? Nein

'allow-new-values'

Verwenden Sie dieses Attribut, um eine dynamische Liste für einen Parameter hinzuzufügen. Beim Erstellen oder Aktualisieren einer Konfiguration über die NetScaler Console GUI kann der Benutzer Werte zur Liste hinzufügen.

Geben Sie „true“ an, wenn der Benutzer einen Wert zur Parameterliste hinzufügen soll. Sie können die Attribute `allow-new-values` und `allowed-values` in Kombination verwenden. Diese Kombination ermöglicht es Ihnen, eine Liste vorgeschlagener Werte für einen Parameter zu definieren und auch neue Werte zu akzeptieren.

```
-
      name: port
      type: tcp-port
      allowed-values:
            -  80
            -  81
            -  8080
      allow-new-values: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In diesem Beispiel kann ein Benutzer entweder aus 80, 81, 8080 auswählen oder einen neuen Wert für den Parameter `port` eingeben, während er ein Konfigurationspaket erstellt oder aktualisiert.

'Standard'

Verwenden Sie dieses Attribut, um einem optionalen Parameter einen Standardwert zuzuweisen. Wenn ein Benutzer eine Konfiguration erstellt, ohne einen Wert anzugeben, wird der Standardwert verwendet.

Der Parameter nimmt keinen Wert an, wenn die folgenden Bedingungen erfüllt sind:

- Der Parameter hat keinen Standardwert.
- Ein Benutzer gibt keinen Wert für den Parameter an.

Beispiel 1:

```
-

      name: timeout

      type: number

      default: 20
```

Beispiel 2:

So listen Sie die Standardwerte des Parameters auf:

```
-

      name: protocols

      type: string[]

      default:

            -  TCP

            -  UDP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            -  IP
```

Beispiel 3:

```
-

      name: timeout

      type: number

      default: 20
```

Beispiel 4:

```
-

      name: tcpport

      type: tcp-port

      default: 20
```

Obligatorisch? Nein

'Muster'

Verwenden Sie dieses Attribut, um ein Muster (regulärer Ausdruck) für die gültigen Werte dieses Parameters zu definieren, wenn der Typ des Parameters "string" ist.

Beispiel:

```
-

      name: appname

      type: string

      pattern: "[a-z]+"
```

Obligatorisch? Nein

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'min-value'

Verwenden Sie dieses Attribut, um den Mindestwert für Parameter vom Typ `number` oder `tcp-port` zu definieren.

Beispiel:

```
-

      name: audio-port

      type: tcp-port

      min-value: 5000
```

Die `min-value` von Zahlen kann negativ sein. Der `min-value` für `tcp-port` muss jedoch positiv sein.

Obligatorisch? Nein

'max-value'

Verwenden Sie dieses Attribut, um den Maximalwert für Parameter vom Typ `number` oder `tcp-port` zu definieren.

Stellen Sie sicher, dass der Maximalwert größer als der Minimalwert ist, falls definiert.

Beispiel:

```
-

      name: audio-port

      type: tcp-port

      min-value: 5000

      max-value: 15000
```

Obligatorisch? Nein

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'min-length'

Verwenden Sie dieses Attribut, um die Mindestlänge von Werten zu definieren, die für einen Parameter vom Typ „string“ akzeptiert werden.

Stellen Sie sicher, dass die Mindestlänge der als Werte definierten Zeichen größer oder gleich Null ist.

Beispiel:

```
-

      name: appname

      type: string

      min-length: 3
```

Obligatorisch? Nein

'max-length'

Verwenden Sie dieses Attribut, um die Maximallänge von Werten zu definieren, die für einen Parameter vom Typ „string“ akzeptiert werden.

Stellen Sie sicher, dass die Maximallänge der Werte größer oder gleich der Länge der in `min-length` definierten Zeichen ist.

Beispiel:

```
-

      name: appname

      type: string

      max-length: 64
```

Obligatorisch? Nein

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'min-items'

Verwenden Sie dieses Attribut, um die Mindestanzahl von Elementen in einem Parameter zu definieren, der eine Liste ist.

Stellen Sie sicher, dass die Mindestanzahl der Elemente größer oder gleich Null ist.

Beispiel:

```
-

      name: server-ips

      type: ipaddress[]

      min-items: 2
```

Obligatorisch? Nein

'max-items'

Verwenden Sie dieses Attribut, um die maximale Anzahl von Elementen in einem Parameter zu definieren, der eine Liste ist.

Stellen Sie sicher, dass die maximale Anzahl der Elemente größer ist als die minimale Anzahl der Elemente, sofern definiert.

Beispiel:

```
-

      name: server-ips

      type: ipaddress[]

      min-items: 2

      max-items: 250
```

Obligatorisch? Nein

© 1997–2026 Citrix Systems, Inc. All rights reserved.

'Benutzeroberfläche'

Verwenden Sie dieses Attribut, um das Layout des Parameters in der NetScaler Console GUI anzupassen.

Obligatorisch? Nein

'Spalten'

Dieses Attribut ist ein Unterattribut des `gui` Attributs. Verwenden Sie dieses Attribut, um die Anzahl der Spalten zu definieren, in denen die `type: object[]` Parameter in der NetScaler Console GUI angezeigt werden sollen.

Obligatorisch? Nein

'Aktualisierbar'

Dieses Attribut ist ein Unterattribut des `gui` Attributs. Verwenden Sie dieses Attribut, um anzugeben, ob der Parameter aktualisiert werden kann, nachdem die Konfiguration erstellt wurde. Legen Sie dieses Attribut nur für einfache Parametertypen wie string, boolean oder number fest.

Wenn der Wert auf `false` gesetzt ist, wird das Parameterfeld ausgegraut, wenn Sie die Konfiguration aktualisieren.

Obligatorisch? Nein

'collapse_pane'

Dieses Attribut ist ein Unterattribut des `gui`-Attributs. Verwenden Sie dieses Attribut, um anzugeben, ob der Bereich, der das Layout dieses Objektparameters definiert, einklappbar ist.

Wenn der Wert auf „true“ gesetzt ist, kann der Benutzer die untergeordneten Parameter unter diesem übergeordneten Parameter erweitern oder einklappen.

Beispiel:

```
gui:


 collapse_pane: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 columns: 2
```

Beispiel eines vollständigen Parameterabschnitts:

```
parameters:

   -

      name: name

      label: Name

      description: Name of the application

      type: string

      required: true

   -

      name: ip
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      label: IP Address


      description: The virtual IP address used for this application


      type: ipaddress


      required: true


  -


      name: svc-servers


      label: Servers


      type: object\[\]


      required: true


      parameters:


        -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            name: svc-ip

            label: Server IP

            description: The IP address of the server

            type: ipaddress

            required: true

        -

            name: svc-port

            label: Server Port

            description: The TCP port of the server

            type: tcp-port

            default: 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    -

        name: lb-alg

        label: LoadBalancing Algorithm

        type: string

        allowed-values:

           - ROUNDROBIN

           - LEASTCONNECTION

        default: ROUNDROBIN

    -

        name: enable-healthcheck

        label: Enable HealthCheck?
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            type: boolean


            default: true
```

Das Folgende ist ein Beispiel, das alle Attribute einer Liste und die in früheren Abschnitten erläuterten Werte definiert:

```
      -
            name: features-list


            type: string[]


            min-length: 1


            max-length: 3


            min-items: 1


            max-items: 3


            pattern: "\[A-Z\]+"


            allowed-values:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                - SP


                - LB


                - CS


              default:


                - LB
```

'Layout'

Dieses Attribut ist ein Unterattribut des `gui`-Attributs. Verwenden Sie dieses Attribut, um die Listenwerte als Optionsfelder anzuzeigen. Setzen Sie das `layout`-Attribut im Parameterabschnitt einer StyleBook-Definition auf `radio`. Es gilt für den Parameter, der das `allowed-values`-Attribut hat. Wenn Sie ein Konfigurationspaket erstellen, zeigt die NetScaler Console GUI die Werte in der `allowed-values`-Liste als Optionsfelder an.

Beispiel:

```
-

    gui:

        layout: radio

    allowed-values:

        - One

        - Two
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        - Three
```

Die Werte „One“, „Two“ und „Three“ werden in der NetScaler Console GUI als Optionsfelder angezeigt.

'dependent-parameters'

Dieses Attribut ist ein Unterattribut des `gui`-Attributs. Es steuert dynamisch das Erscheinungsbild des Parameters oder seinen Anfangswert im StyleBook-Konfigurationsformular basierend auf dem in einem anderen Parameter angegebenen Wert.

Geben Sie dieses Attribut für einen Quellparameter an, der das Verhalten des Parameters im Formular steuert. Sie können mehrere Bedingungen einschließen, die andere Parameter steuern. Zum Beispiel kann ein Quellparameter `protocol` einen abhängigen Parameter `certificate` haben, der nur angezeigt wird, wenn der Parameterwert `protocol` `SSL` ist.

Jede Bedingung kann die folgenden Attribute haben:

- **target-parameter**: Geben Sie den Zielparameter an, auf den diese Bedingung zutrifft.
- **matching-values**: Geben Sie die Liste der Werte des Quellparameters an, die die Aktion auslösen.
- **action**: Geben Sie eine der folgenden Aktionen für den Zielparameter an:
  - `read-only`: Der Parameter wird schreibgeschützt.
  - `show`: Der Parameter wird im Formular angezeigt, wenn er ausgeblendet ist.
  - `hide`: Der Parameter wird aus dem Formular entfernt.
  - `set-value`: Der Parameterwert wird auf den im Attribut „value“ angegebenen Wert gesetzt.
- **value**: Der Wert des Zielparameters, wenn die Aktion `set-value` ist.

Wenn eine Benutzereingabe mit den angegebenen Werten des Quellparameters übereinstimmt, ändern sich das Erscheinungsbild oder der Wert des Zielparameters entsprechend der angegebenen Aktion.

Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

   name: lb-virtual-port

   label: "Load Balanced App Virtual Port"

   description: "TCP port representing the Load Balanced application"

   type: tcp-port

   gui:

     updatable: false

     dependent-parameters:

           -

             matching-values:

               - 80

             target-parameter: $parameters.lb-service-type

             action: set-value

             allowed-values:

             - HTTP

             - TCP

             - UDP


   default: 80
```

In diesem Beispiel wird der abhängige Parameter unter dem Parameter `lb-virtual-port` (Quellparameter) angegeben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn der Quellparameterwert auf `80` gesetzt ist, löst der Parameter `lb-service-type` die Aktion `set-value` aus. Dadurch kann ein Benutzer eine der folgenden Optionen auswählen:

- HTTP
- TCP
- UDP

`is_policy_expression`

Dieses Attribut ist ein Unterattribut des `gui` Attributs. Verwenden Sie dieses Attribut, um den Richtlinienausdruckseditor zum Erstellen eines Richtlinienausdrucks zu aktivieren. Setzen Sie den `is_policy_expression` auf `true` in der Parameterdefinition. Dieses Attribut kann nur für Parameter vom Typ 'string' verwendet werden.

Beispiel:

```
parameters:

  -



    name: expression

    type: string

    label: Expression

    required: true

    gui:

      is_policy_expression: true
```

Konstrukt „parameters-default-sources“

Sie können dieses Konstrukt verwenden, um Parameterdefinitionen aus anderen StyleBooks wiederzuverwenden.

Stellen Sie sich ein Szenario vor, in dem ein Parameter oder eine Gruppe von Parametern wiederholt in mehreren StyleBooks verwendet wird. Um zu vermeiden, dass diese Parameter jedes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mal neu definiert werden müssen, wenn Sie ein neues StyleBook erstellen möchten, können Sie sie einmal definieren und dann ihre Definitionen in die StyleBooks importieren, die diese Parameter benötigen, indem Sie das Konstrukt **parameters-default-sources** verwenden.

Wenn beispielsweise viele Ihrer StyleBooks eine virtuelle IP konfigurieren müssen, müssen Sie möglicherweise dieselben Parameter für virtuelle IPs in jedem neuen StyleBook definieren, das Sie erstellen. Stattdessen können Sie ein separates StyleBook erstellen, das beispielsweise `vip-params` heißt, in dem Sie alle zugehörigen Parameter definieren, wie im folgenden Beispiel gezeigt:

```
-


name: vip-params


namespace: com.acme.commontypes


version: "1.0"


description: This StyleBook defines a typical virtual IP config.


private: true


schema-version: "1.0"


parameters:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
       -

           name: lb-appname

           label: Load Balanced Application Name

          description: Name of the Load Balanced application

           type: string

           required: true

       -

           name: lb-virtual-ip

           label: Load Balanced App Virtual IP address

           description: Virtual IP address representing the Load Balanced
application

           type: ipaddress
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            required: true


        -


            name: lb-virtual-port


            label: Load Balanced App Virtual Port


            description: TCP port representing the Load Balanced
application


            type: tcp-port


            default: 80


        -


            name: lb-service-type


            label: Load Balanced App Protocol


            description: Protocol used for the Load Balanced application.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        type: string

        default: HTTP

        required: true

        allowed-values:

             - HTTP

             - SSL

             - TCP
```

Anschließend können Sie andere StyleBooks erstellen, die diese Parameter verwenden.

```
    -

    name: acme-biz-app

    namespace: com.acme.stylebooks
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
     version: "1.0"


     description: This stylebook defines the NetScaler configuration for
Biz App


     schema-version: "1.0"


     import-stylebooks:


       -


           namespace: com.acme.commontypes


           prefix: cmtypes


           version: "1.0"


     **parameters-default-sources:**


**            - cmtypes::vip-params**


     parameters:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        -

          name: monitorname

          label: Monitor Name

          description: Name of the monitor

          type: string

          required: true

        -

          name: type

          label: Monitor Type

          description: Type of the monitor

          type: string
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        required: true


        allowed-values:


          - PING


          - TCP


          - HTTP


          - HTTP-ECV


          - TCP-ECV


          - HTTP-INLINE
```

Im StyleBook `acme-biz-app` werden zunächst der Namespace und die Version des StyleBooks `vip-params` über den Abschnitt „import-stylebooks“ importiert. Anschließend wird das Konstrukt **parameters-default-sources** hinzugefügt und der StyleBook-Name, d. h. `vip-params`, angegeben. Dieser Parameter hat denselben Effekt wie die direkte Definition der Parameter des StyleBooks `vip-params` in diesem StyleBook.

Sie können Parameter aus mehreren StyleBooks einschließen, da parameters-default-sources eine Liste ist und jedes Element in der Liste ein StyleBook sein sollte.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zusätzlich zum Einschließen von Parametern aus anderen StyleBooks können Sie auch eigene Parameter mithilfe des Abschnitts „parameters“ definieren. Die vollständige Liste der Parameter des StyleBooks ist die Kombination aus Parametern, die aus anderen StyleBooks eingeschlossen wurden, und Parametern, die in diesem StyleBook definiert sind. Daher bezieht sich der Ausdruck **$parameters** auf diese Kombination von Parametern.

Wenn ein Parameter sowohl in einem importierten StyleBook als auch im aktuellen StyleBook definiert ist, überschreibt die Definition im aktuellen StyleBook die aus einem anderen StyleBook importierte Definition. Sie können diesen Ansatz effektiv nutzen, indem Sie bei Bedarf einige der importierten Parameter anpassen, während Sie den Rest der importierten Parameter unverändert verwenden.

Das Konstrukt „parameters-default-sources“ kann auch in verschachtelten Parametern verwendet werden, wie gezeigt:

```
parameters:

    -

      name: vip-details

      label: Virtual IP details

      description: Details of the Virtual IP

      type: object

      required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    parameters-default-sources:



          - cmtypes::vip-params
```

Dieser Ansatz ähnelt dem direkten Hinzufügen der Parameter des StyleBooks `vip-params` als untergeordnete Parameter des Parameters `vip-details` in diesem StyleBook.

Parameters-source-Konstrukt

Mithilfe des `parameters-source`-Konstrukts können Sie steuern, wie die importierten Parameter auf der GUI angezeigt werden, während Sie ein Konfigurationspaket erstellen. Das Folgende ist ein Beispiel-StyleBook, um dieses Konstrukt zu beschreiben:

```
parameters:

  -

    name: appname

    label: "LBVserver Name"

    description: "Name of the Load Balancer"

    type: string

    required: true

  -

   parameters-source: stlb::lb

  -

    name: vip-ipaddress

    label: "Load Balancer IP Address"

    description: "IP Address of the Load Balancer VIP"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ipaddress

    required: true
```

In diesem Beispiel wird das `parameters-source`-Konstrukt im `parameters`-Abschnitt hinzugefügt. Das `parameters-source` enthält einen Wert, der einem Listenelement im `parameters-default-sources`-Abschnitt entspricht. Mit `parameters-source` können Sie Parameter aus verschiedenen StyleBooks an den gewünschten Positionen importieren und auf der GUI rendern. Wohingegen der `parameters-default-sources`-Abschnitt die Attribute importiert und nur am Anfang der GUI gerendert wird.

Parameterbedingungen

In einer StyleBook-Definition legen Parameter die Eingabe fest, die StyleBook-Benutzer zur Erstellung eines Konfigurationspakets bereitstellen. Manchmal möchten Sie das Verhalten der Parameter wie folgt ändern:

- Einem Benutzer bestimmte Parameter nur anzeigen, wenn eine Bedingung erfüllt ist.
- Die zulässigen Werte eines Parameters sollen von einem anderen Parameter abhängen.
- Einen Parameter nur unter bestimmten Bedingungen als obligatorisch festlegen.

Verwenden Sie in diesen Fällen den Abschnitt `parameters-conditions`, um Parameterbedingungen zu definieren. Eine Parameterbedingung hat die folgenden Attribute:

- `target`: Geben Sie den Parameter an, auf den Sie eine Bedingung anwenden möchten.
- `action`: Geben Sie an, welche Aktionen ausgeführt werden sollen, wenn der Zielparameter der Bedingung entspricht. Diese Funktion unterstützt die folgenden Aktionen:
  - Parameter anzeigen oder ausblenden
  - Standardwert festlegen
  - Als Pflichtfeld festlegen
  - Zulässige Werte festlegen
  - Beschriftung des Parameters festlegen
  - Beschreibung des Parameters festlegen
  - Parameterbereich reduzieren oder erweitern
  - Legen Sie das Muster des Parameters fest

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `condition`: Geben Sie eine Bedingung an, die erfüllt werden muss.
- `value`: Legen Sie die Werte für das Attribut der Zielparameter in Abhängigkeit von der Aktion fest.

HINWEIS

Derzeit können die Parameterbedingungen nicht auf die Parameter innerhalb von Listenobjekten angewendet werden.

'anzeigen' oder 'ausblenden'

Wenn die Aktion `show` ist und die angegebene Bedingung `True` zurückgibt, wird der Zielparameter in der GUI angezeigt.

Wenn die Aktion `hide` ist und die angegebene Bedingung `True` zurückgibt, verschwindet der Zielparameter aus der GUI.

Beispiel:

```
parameters-conditions:

  -

   target: $parameters.security-settings.cert-details

   action: show

   condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

Zunächst sind die Zertifikatsdetails für den Parameter `security-settings` ausgeblendet. Wenn ein Benutzer SSL- oder SSL-Bridge-Protokolle auswählt, werden die Zertifikatsdetails angezeigt.

'Standardwert festlegen'

Wenn die Aktion `set-default` ist und die angegebene Bedingung `True` zurückgibt, wird der Wert des Zielparameters auf den Standardwert gesetzt.

Beispiel 1:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters-conditions:

  -

   target: $parameters.port

   action: set-default

   condition: $parameters.protocol == "SSL"

   value: 443

  -

   target: $parameters.port

   action: set-default

   condition: $parameters.protocol != "SSL"

   value: 80
```

Beispiel 2:

```
parameters-conditions:

  -

   target: $parameters.port

   action: set-default

   value: if-then-else($parameters.protocol == "SSL", 443, 80)
```

Wenn ein Benutzer das **SSL**-Protokoll auswählt, wird der Standardportwert auf `443` gesetzt. Für andere Protokolle wird der Standardportwert auf `80` gesetzt. Beispiel 1 und 2 liefern das gleiche Ergebnis.

'set-required'

Wenn die Aktion `set-required` ist und die angegebene Bedingung `True` zurückgibt, wird der Zielparameter zu einem Pflichtfeld, um ein Konfigurationspaket zu erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters-conditions:

  -

   target: $parameters.security-settings.cert-details

   action: set-required

   condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

Zunächst sind die Zertifikatsdetails für den Parameter `security-settings` möglicherweise nicht erforderlich. Wenn ein Benutzer die Protokolle **SSL** oder **SSL-Bridge** auswählt, werden die Zertifikatsdetails zu einem Pflichtfeld, um ein Konfigurationspaket zu erstellen.

'set-allowed-values'

Wenn die Aktion `set-allowed-values` ist und die angegebene Bedingung `True` zurückgibt, erlaubt der Zielparameter nur die Auswahl bestimmter Werte.

Beispiel-1:

```
parameters-conditions:

  -

   target: $parameters.app-name

   action: set-allowed-values

   value:

    - "SSL"

   condition: $parameters.lb-virtual-port ==  443
```

Wenn ein Benutzer `443` als virtuellen Load-Balancer-Port angibt, erlaubt der Name der Anwendung nur die Option **SSL**.

Beispiel-2;

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:

    -

      name: root-certificates

      label: "Root Certificates"

      type: object[]

      parameters:

        -

          name: certkey-name

          label: "SSL Root CertKey Name"

          type: string

          required: true

    -

      name: im-certificates

      label: "Intermediate Certificates"

      type: object[]

      parameters:

        -

          name: certkey-name

          label: "Name of Intermediate CertKey"

          type: string

          required: true

        -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          name: link-options
          label: "Link to Root or Intermediate CertKey?"
          type: string
          allowed-values:
            - Root
            - Intermediate
          default: Root
          required: true
        -
          name: link-certkey
          label: "Linked to Root/Intermediate CertKey Name"
          type: string
          required: true
parameters-conditions:
  -
    repeat: $parameters.im-certificates
    repeat-item: imcert
    parameters-conditions:
    -
      target: $imcert.link-certkey
      action: set-allowed-values
      condition: $imcert.link-options == "Root"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      value: $parameters.root-certificates[*].certkey-name

    -

      target: $imcert.link-certkey

      action: set-allowed-values

      condition: $imcert.link-options == "Intermediate"

      value: $parameters.im-certificates[*].certkey-name
```

Dieses Beispiel handelt von der Festlegung eines Werts für ein SSL-Zertifikat. Das Wiederholungskonstrukt in Parameterbedingungen iteriert über alle Zwischenzertifikate (`im-certificates`) und prüft den Parameter `link-options` jedes Zertifikats.

Wenn der Parameter `link-options` einem bestimmten Wert entspricht, werden die zulässigen Werte im Parameter `link-certkey` der jeweiligen Zertifikatsliste hinzugefügt.

Wenn beispielsweise der Parameter `link-options` `Root` ist, werden die zulässigen Werte im Parameter `link-certkey` der Liste `root-certificate` hinzugefügt.

Die folgenden Notationen werden verwendet, um Zertifikate zur Liste hinzuzufügen:

- Für Root-Zertifikate:

  ```
  $parameters.root-certificates[*].certkey-name
  ```

- Für Zwischenzertifikate:

  ```
  $parameters.im-certificates[*].certkey-name
  ```

'set-label'

Wenn die Aktion `set-label` ist und die angegebene Bedingung `True` zurückgibt, ändert sich die Beschriftung des Zielparameters in den angegebenen Text.

Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters-conditions:

  -

   target: $parameters.app-name

   action: set-label

   value: if-then-else($parameters.lb-service-type == "TCP",
"TCPApp","UDPApp")
```

Wenn ein Benutzer das Lastenausgleichsprotokoll als **TCP** auswählt, ändert sich die Beschriftung der Anwendung in **TCPApp**. Wenn der Benutzer eine andere Option auswählt, ändert sich die Beschriftung der Anwendung in **UDPApp**.

'set-description'

Wenn die Aktion `set-description` ist und die angegebene Bedingung `True` zurückgibt, ändert sich die Beschreibung des Zielparameters in den angegebenen Text. Diese Beschreibung wird im Tooltip eines Zielparameters angezeigt.

Beispiel:

```
parameters-conditions:

  -

   target: $parameters.app-name

   action: set-description

   value: if-then-else($parameters.lb-service-type == "TCP", "Select a TCP
application name","Select a UDP application name")
```

Wenn ein Benutzer das Lastenausgleichsprotokoll als **TCP** auswählt, zeigt der Tooltip der Anwendung den Text: `Select a TCP application name` an. Wenn der Benutzer eine andere Option auswählt, zeigt die Beschreibung der Anwendung `Select a UDP application name` an.

'collapse-pane' oder 'erweitern-pane'

Wenn die Aktion `collapse-pane` ist und die angegebene Bedingung `True` zurückgibt, wird der Bereich des Zielparameters in der GUI eingeklappt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn die Aktion `expand-pane` ist und die angegebene Bedingung `True` zurückgibt, wird der Bereich des Zielparameters in der GUI erweitert.

Beispiel:

```
parameters-conditions:

  -

    target: $parameters.security-settings.cert-details

    action: expand-pane

    condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

Zunächst ist der Bereich für die Zertifikatsdetails für den Parameter `security-settings` möglicherweise nicht erweitert. Wenn ein Benutzer die Protokolle **SSL** oder **SSL-Bridge** auswählt, wird der Bereich für die Zertifikatsdetails in der GUI erweitert.

'set-pattern'

Wenn die Aktion `set-pattern` ist und die angegebene Bedingung `True` zurückgibt, wird das Zielparameterfeld auf das angegebene Muster gesetzt.

Beispiel:

```
parameters-conditions:

  -

    target: $parameters.app-name

    action: set-pattern

    value: "[a-z]+"
```

In diesem Beispiel erlaubt der Name der Anwendung nur Kleinbuchstaben.

Verschachtelte Parameterbedingungen

In einer StyleBook-Definition können Sie eine Parameterbedingung innerhalb einer anderen Parameterbedingung angeben. Diese Bedingungen werden als verschachtelte

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Parameterbedingungen bezeichnet und verwenden ein Wiederholungskonstrukt, um diese Bedingungen zu definieren. Die verschachtelten Parameterbedingungen sind nützlich, wenn Sie eine Aktion für einen Parameter von einem anderen Parameter aus anwenden möchten.

Beispiel:

```
parameters-conditions:

  -

    repeat: $parameters.lbvservers

    repeat-item: lbvserver

    parameters-conditions:

      -

        target: $lbvserver.port

        action: set-allowed-values

        condition: $lbvserver.protocol == "HTTPS"

        value: $parameters.ssl-ports
```

In diesem Beispiel werden, wenn der Benutzer das HTTPS-Protokoll für einen virtuellen Lastausgleichsserver auswählt, die Portwerte dynamisch ausgefüllt. Und dies gilt für jeden virtuellen Lastausgleichsserver in der Liste.

Substitutionen

Substitutionen werden verwendet, um Kurznamen zu definieren, die komplexe Ausdrücke im StyleBook ersetzen können, wodurch das StyleBook lesbarer wird.

Substitutionen sind auch nützlich, wenn derselbe Ausdruck oder Wert wiederholt im StyleBook verwendet wird, zum Beispiel ein konstanter Wert. Die Verwendung eines Substitutionsnamens für einen Parameter ermöglicht es Ihnen, nur den Substitutionswert zu aktualisieren, anstatt alle Vorkommen des Parameters im StyleBook zu aktualisieren, was fehleranfällig sein könnte.

Substitutionen werden auch verwendet, um Zuordnungen zwischen Werten zu definieren, wie in späteren Beispielen in diesem Dokument beschrieben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Jede Substitution in der Liste besteht aus einem Schlüssel und einem Wert. Der Wert kann ein einfacher Wert, ein Ausdruck, eine Funktion oder eine Zuordnung sein.

Im folgenden Beispiel werden zwei Substitutionen definiert. Die erste ist `http-port`, die als Kurzform für 8181 verwendet werden kann. Durch die Verwendung einer Substitution können Sie im restlichen StyleBook darauf als **$substitutions.http-port** anstelle von 8181 verweisen.

Substitutionen:

`http-port: 8181`

Dies ermöglicht es Ihnen, einem Port eine mnemonische Bezeichnung zuzuweisen und diese Portnummer an einer Stelle im StyleBook zu definieren, unabhängig davon, wie oft sie verwendet wird. Wenn Sie die Portnummer auf 8080 ändern möchten, können Sie dies im Substitutionsabschnitt tun, und die Änderung wird überall dort wirksam, wo der mnemonische Name `http-port` verwendet wird. Das folgende Beispiel zeigt, wie eine Substitution in einer Komponente verwendet wird.

```
components:


 -


     name: my-lbvserver-comp


     type: ns::lbvserver


     properties:


          name: $parameters.name + "-lb"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
          servicetype: HTTP


          ipv46: $parameters.ip


          port: $substitutions.http-port


          lbmethod: $parameters.lb-alg
```

Eine Substitution kann auch ein komplexer Ausdruck sein. Das folgende Beispiel zeigt, wie zwei Substitutionen Ausdrücke verwenden.

```
substitutions:


  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS


  app-name: str("acme-") + $parameters.name + str("-app")
```

Ein Substitutionsausdruck kann auch vorhandene Substitutionsausdrücke verwenden, wie im folgenden Beispiel gezeigt.

```
substitutions:


  http-port: 8181


  app-name: str("acme-") + $parameters.name + str($substitutions.http-
port) + str("-app")
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ein weiteres nützliches Merkmal von Substitutionen sind Zuordnungen (Maps), bei denen Sie Schlüssel Werten zuordnen können. Das Folgende ist ein Beispiel für eine Map-Substitution.

```
substitutions:

    secure-port:

        true: int("443")

        false: int("80")

    secure-protocol:

        true: SSL

        false: HTTP
```

Das folgende Beispiel zeigt, wie die Zuordnungen secure-port und secure-protocol verwendet werden.

```
components:

 -

     name: my-lbvserver-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::lbvserver

    properties:

        name: $parameters.name + "-lb"

        servicetype: $substitutions.secure-protocol[$parameters.is-
secure]

        ipv46: $parameters.ip

        port: $substitutions.secure-port[$parameters.is-secure]

        lbmethod: $parameters.lb-alg
```

Wenn der Benutzer des StyleBooks hier den booleschen Wert „true“ für den Parameter `is-secure` angibt oder das entsprechende Kontrollkästchen in der NetScaler Console GUI auswählt, wird der Eigenschaft `servicetype` dieser Komponente der Wert **SSL** und der Port-Eigenschaft der Wert **443** zugewiesen. Wenn der Benutzer jedoch „false“ für diesen Parameter angibt oder das entsprechende Kontrollkästchen in der NetScaler Console GUI deaktiviert, wird der Eigenschaft `servicetype` der Wert **HTTP** und dem Port der Wert **80** zugewiesen.

Das folgende Beispiel zeigt, wie Substitutionen als Funktion verwendet werden. Eine Substitutionsfunktion kann ein oder mehrere Argumente annehmen. Argumente können von einfachem Typ sein, zum Beispiel String, Zahl, `ipaddress`, Boolean und andere Typen.

Substitutionen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

form-lb-name(name): $name + "-last"

In diesem Beispiel definieren wir eine Substitutionsfunktion „form-lb-name“, die ein String-Argument namens „name“ annimmt und es verwendet, um einen String zu erstellen, der dem String im Namensargument „-lb“ anhängt. Ein Ausdruck, der diese Substitutionsfunktion verwendet, kann wie folgt geschrieben werden:

`$substitutions.form-lb-name("my")`

Es gibt `my-lb` zurück.

Betrachten Sie ein weiteres Beispiel:

Substitutionen:

`cspol-priority(priority): 10100 - 100 * $priority`

Die Substitution `cspol-priority` ist eine Funktion, die ein Argument namens „priority“ annimmt und es zur Berechnung eines Wertes verwendet. Im Rest des StyleBooks kann diese Substitution wie im folgenden Beispiel gezeigt verwendet werden:

```
components:

  -

    name: cspolicy-binding-comp

    type: ns::csvserver_cspolicy_binding

    condition: not $parameters.is-default

    properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        name: $parameters.csvserver-name


        policyname: $components.cspolicy-comp.properties.policyname


        priority: $substitutions.cspol-
priority($parameters.pool.priority)
```

Das Folgende ist ein Beispiel für eine Substitution namens `slist`, deren Wert eine Liste ist:

```
substitutions:


  slist:


    - a


    - b


    - c
```

Der Wert einer Substitution kann auch ein Wörterbuch von Schlüssel-Wert-Paaren sein, wie im folgenden Beispiel einer Substitution namens `sdict` zu sehen ist:

```
substitutions:


  sdict:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    a: 1

    b: 2

    c: 3
```

Sie können komplexere Attribute erstellen, indem Sie Listen und Wörterbücher kombinieren. Zum Beispiel gibt eine Substitution namens `slistofdict` eine Liste von Schlüssel-Wert-Paaren zurück.

```
  slistofdict:

    -

      a: $parameters.cs1.lb1.port

      b: $parameters.cs1.lb2.port

    -

      a: $parameters.cs2.lb1.port

      b: $parameters.cs2.lb2.port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Im folgenden Beispiel gibt eine Substitution `sdictoflist` jedoch ein Schlüssel-Wert-Paar zurück, wobei der Wert selbst eine weitere Liste ist.

```
sdictoflist:

  a:

    - 1

    - 2

  b:

    - 3

    - 4
```

In Komponenten können diese Substitutionen in den Konstrukten condition, properties, repeat und repeat-condition verwendet werden.

Das folgende Beispiel einer Komponente zeigt, wie eine Substitution verwendet werden kann, um die Eigenschaften anzugeben:

```
  properties:

    a: $substitutions.slist
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      b: $substitutions.sdict


      c: $substitutions.slistofdict


      d: $substitutions.sdictoflist
```

Ein Anwendungsfall für die Definition einer Substitution, deren Wert eine Liste oder ein Wörterbuch ist, besteht darin, wenn Sie einen Content Switching Virtual Server und mehrere Load Balancing Virtual Server konfigurieren. Da alle mit demselben CS Virtual Server verbundenen LB Virtual Server eine identische Konfiguration haben könnten, können Sie die Substitutionsliste und das Wörterbuch verwenden, um diese Konfiguration zu erstellen und so eine Wiederholung der Konfiguration für jeden LB Virtual Server zu vermeiden.

Das folgende Beispiel zeigt die Substitution und die Komponente in den `cs-lb-mon` StyleBooks, um eine Content Switching Virtual Server Konfiguration zu erstellen. Beim Erstellen der Eigenschaften von `cs-lb-mon` StyleBooks gibt die komplexe Substitution „lb-properties“ die Eigenschaften der mit dem CS Virtual Server verbundenen LB Virtual Server an. Die Substitution „lb-properties“ ist eine Funktion, die den Namen, den Diensttyp, die virtuelle IP-Adresse, den Port und die Server als Parameter entgegennimmt und ein Schlüssel-Wert-Paar als Wert generiert. In der `cs-pools` Komponente weisen wir den Wert dieser Substitution einem lb-pool-Parameter für jeden Pool zu.

```
substitutions:


  cs-port[]:


    true: int("80")


    false: int("443")
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
lb-properties(name, servicetype, vip, port, servers):

  lb-appname: $name

  lb-service-type: $servicetype

  lb-virtual-ip: $vip

  lb-virtual-port: $port

  svc-servers: $servers

  svc-service-type: $servicetype

  monitors:

    -

      monitorname: $name

      type: PING
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        interval: $parameters.monitor-interval

        interval_units: SEC

        retries: 3

components:

  -

    name: cs-pools

    type: stlb::cs-lb-mon

    description: | Updates the cs-lb-mon configuration with the different
pools provided. Each pool with rule result in a dummy LB vserver, cs
action, cs policy, and csvserver_cspolicy_binding configuration.

    condition: $parameters.server-pools

    repeat: $parameters.server-pools
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    repeat-item: pool


    repeat-condition: $pool.rule


    repeat-index: ndx


    properties:


      appname: $parameters.appname + "-cs"


      cs-virtual-ip: $parameters.vip


      cs-virtual-port: $substitutions.cs-port($parameters.protocol ==
"HTTP")


      cs-service-type: $parameters.protocol


      pools:


        -


          lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP",
"0.0.0.0", 0, $pool.servers)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        rule: $pool.rule

        priority: $ndx + 1
```

Substitutionszuordnung

Sie können Substitutionen erstellen, die Schlüssel Werten zuordnen. Betrachten Sie zum Beispiel ein Szenario, in dem Sie den Standardport (Wert) definieren möchten, der für jedes Protokoll (Schlüssel) verwendet werden soll. Für diese Aufgabe schreiben Sie eine Substitutionszuordnung wie folgt.

```
substitutions:

    port:

        HTTP: 80

        DNS: 53

        SSL: 443
```

In diesem Beispiel ist HTTP 80 zugeordnet, DNS ist 53 zugeordnet und SSL ist 443 zugeordnet. Um den Port eines bestimmten Protokolls abzurufen, das als Parameter angegeben wird, verwenden Sie den Ausdruck

$substitutions.port

Der Ausdruck gibt einen Wert basierend auf dem vom Benutzer angegebenen Protokoll zurück.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wenn der Schlüssel HTTP ist, gibt der Ausdruck 80 zurück
- Wenn der Schlüssel DNS ist, gibt der Ausdruck 53 zurück
- Wenn der Schlüssel SSL ist, gibt der Ausdruck 443 zurück
- Wenn der Schlüssel nicht in der Zuordnung vorhanden ist, gibt der Ausdruck keinen Wert zurück

Durch Substitutionslisten iterieren

Im folgenden Beispiel iteriert das StyleBook durch eine Substitutionsliste namens `apps`, um eine Reihe von lbvserver-Komponenten und deren entsprechenden Dienstgruppen und gebundenen Servern zu erstellen.

```
substitutions:

  apps:

    -

      name: lb1

      vip: 1.2.3.4

      vport: 80

      protocol: HTTP

      servers:

        -

          ip: 10.8.11.11

          port: 8080

        -

          ip: 10.8.11.12

          port: 8080

    -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      name: lb2
      vip: 1.2.3.5
      vport: 81
      protocol: HTTP
      servers:
        -
          ip: 10.9.11.28
          port: 8080
        -
          ip: 10.9.11.29
          port: 8181
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    repeat: $substitutions.apps
    repeat-item: app
    properties:
      name: $app["name"]
      ipv46: $app["vip"]
      port: $app["vport"]
      servicetype: $app["protocol"]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:
  -
    name: servicegroup-comp
    type: ns::servicegroup
    properties:
      servicegroupname: $parent.properties.name + "-svg"
      servicetype: HTTP
    components:
      -
        name: servers-comp
        type: ns::server
        repeat: $app["servers"]
        repeat-item: server
        properties:
          name: $server["ip"]
          ipaddress: $server["ip"]
        components:
          -
            name: servicegroup-servicegroupmember-binding-comp
            type: ns::servicegroup_servicegroupmember_binding
            properties:
              servicegroupname:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$parent.parent.properties.servicegroupname

                servername: $parent.properties.name

                port: $server["port"]
```

Komponenten

Das Komponenten-Konstrukt in einem StyleBook gilt als der wichtigste Abschnitt im StyleBook. In diesem Abschnitt definieren Sie die zu erstellenden Konfigurationsobjekte. Mit diesem Konstrukt können Sie ein oder mehrere Konfigurationsobjekte desselben Typs erstellen.

Das Komponenten-Konstrukt kann die im Parameterabschnitt bereitgestellten Eingaben verwenden, um die vom StyleBook generierte Konfiguration anzupassen. Dies ist ein optionaler Abschnitt, obwohl die meisten StyleBooks einen Komponentenabschnitt haben.

Die folgende Tabelle beschreibt die Hauptattribute einer Komponente.

ATTRIBUT	BESCHREIBUNG
`name`	Der Name der Komponente. Sie können einen alphanumerischen Namen angeben. Der Name muss mit einem Buchstaben beginnen und kann zusätzliche Buchstaben, Zahlen, Bindestriche (-) oder Unterstriche (_) enthalten.
`description`	Eine Beschreibung der Rolle dieser Komponente im StyleBook.
`type`	Der Typ bestimmt, welche Eigenschaften diese Komponente bereitstellt. Komponenten haben zwei Arten von Typen: **Integrierter Typ**: Dieser Typ wird vom System bereitgestellt und muss nicht von Ihnen definiert werden, zum Beispiel die NITRO-Entitätstypen `lbvserver` oder `servicegroup`. Wenn eine Komponente ein Attribut vom integrierten Typ hat, erstellt sie ein Konfigurationsobjekt dieses Typs auf dem NetScaler. Wenn eine Komponente beispielsweise auf den integrierten Typ `lbvserver` verweist, erstellt diese Komponente einen virtuellen Lastausgleichsserver auf der NetScaler-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUT	BESCHREIBUNG
	Instanz, die das Ziel der Konfiguration ist. **Zusammengesetzter Typ**: Dieser Typ verweist auf ein vorhandenes StyleBook, das Sie erstellt und in NetScaler Console importiert haben. Wenn eine Komponente ein Attribut vom zusammengesetzten Typ hat, erstellt sie alle Konfigurationsobjekte, die im referenzierten StyleBook angegeben sind, auf der NetScaler-Instanz, die das Ziel der Konfiguration ist. Dies ermöglicht es Ihnen, mehrere StyleBooks zu kombinieren, wobei jedes StyleBook einen Teil der endgültigen Konfiguration erstellt. Weitere Informationen zu zusammengesetzten StyleBooks finden Sie unter Erstellen eines zusammengesetzten StyleBooks.
`meta-properties`	Meta-Eigenschaften definieren die Aktionen, die für NetScaler-Objekte ausgeführt werden sollen. Sie können statische oder dynamische Werte als gültige Meta-Eigenschaftsaktion annehmen. Wenn Sie Ausdrücke für eine Meta-Eigenschaft angeben, wendet sie die gültigen Meta-Eigenschaftsaktionen für NetScaler-Objekte dynamisch an. Dieses Attribut kann in einem StyleBook verwendet werden, wenn Sie Nicht-CRUD-Operationen an NetScaler-Objekten durchführen möchten. Weitere Informationen finden Sie unter Erstellen eines StyleBooks zur Durchführung von Nicht-CRUD-Operationen.
`properties`	Die Unterattribute, die für ein Komponententypattribut verwendet werden können. Die Eigenschaften, die für eine Komponente gültig sind, werden durch ihren Typ bestimmt. Bei einem integrierten Typ sind dies die Eigenschaften oder Attribute des entsprechenden NITRO-Objekts. Bei einer Komponente, deren Typ ein anderes StyleBook ist, d. h. ein zusammengesetzter

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUT	BESCHREIBUNG
	Typ, entsprechen die Eigenschaften den in diesem StyleBook definierten Parametern.

Beispiel:

```
components:

   -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

        name: $parameters.name

        servicetype: HTTP

        ipv46: $parameters.ip

        port: 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        lbmethod: $parameters.lb-alg
```

In diesem Beispiel haben Sie eine Komponente namens `my-lbvserver-comp` definiert. Diese Komponente ist vom Typ ns::lbvserver (ein integrierter Typ), wobei „ns“ das Präfix ist, das sich auf den Namespace `netscaler.nitro.config` und die Version 10.5 bezieht, die Sie im Abschnitt „import-stylebooks“ angegeben haben, und `lbvserver` ist eine NITRO-Ressource in diesem Namespace.

Die Eigenschaften in diesem Abschnitt umfassen vier obligatorische und ein optionales Attribut (`lbmethod`) der `lbvserver` Ressource und ermöglichen es Ihnen, Werte für diese Attribute anzugeben. In diesem Beispiel geben Sie statische Werte für `servicetype` und Port an, während die Eigenschaften Name, ipv46 und `lbmethod` ihre Werte aus den Eingabeparametern erhalten. Sie verweisen auf die im Abschnitt „parameters“ definierten Parameternamen, indem Sie die `$parameters.\<name>` Notation verwenden, zum Beispiel $parameters.ip.

Um mehr über alle verfügbaren NetScaler NITRO-Ressourcen und deren Attribute/Eigenschaften zu erfahren, lesen Sie die Dokumentation zur NetScaler NITRO REST API.

HINWEIS

Sie müssen Kleinbuchstaben für die Attributnamen von NITRO-Ressourcentypen (ihre Komponenteneigenschaften) verwenden. Andernfalls schlägt der Import eines StyleBooks fehl.

Hilfskomponenten

Die Hauptverwendung des Komponentenabschnitts in einem StyleBook besteht darin, Konfigurationsobjekte über integrierte NITRO-Typen oder ein anderes StyleBook zu generieren, das die eigentlichen Konfigurationsobjekte erstellt. Die Hilfskomponenten erstellen selbst keine Konfigurationsobjekte. Hilfskomponenten übernehmen die Eingaben aus anderen Abschnitten wie Parameterobjekten, Eigenschaften anderer Komponenten oder Ausgaben anderer Komponenten und wandeln sie in andere Formen um. Dies kann später von anderen Komponenten verwendet werden, um die eigentlichen Konfigurationsobjekte zu generieren. Eine Hilfskomponente kann von zwei Typen sein: Objekttyp oder ein anderes StyleBook, das keinen Komponentenabschnitt enthält.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Das folgende Beispiel zeigt einen Ausschnitt eines StyleBooks, das verwendet wird, um einen Lastausgleichsserver mit Monitor (`lb-mon-comp`) auf einer NetScaler-Instanz zu erstellen.

```
parameters:

  -

    name: appname

    type: string

  -

    name: ips

    type: ipaddress[]

  -

    name: vip

    type: ipaddress
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:

  -

    name: help-comp

    type: cmtypes::server-ip-port-params

    repeat:

      repeat-list: $parameters.ips

      repeat-item: server-ip

    properties:

      ip: $server-ip

      port: 80

 -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: lb-mon-comp


    type: stlb::lb-mon


    properties:


      lb-appname: $parameters.appname


      lb-virtual-ip: $parameters.vip


      lb-virtual-port: 80


      lb-service-type: HTTP


      svc-service-type: HTTP


      svc-servers: $components.help-comp.properties
```

Der Parameterabschnitt ermöglicht es Ihnen, den Namen der Anwendung und die IP-Adressen der Lastausgleichsserver einzugeben. Im Komponentenabschnitt `lb-mon-comp` erwartet der Parameter `svc-servers` des StyleBooks `lb-mon` eine Liste von Objekten, wobei jedes Element zwei Unterparameter `ip` und Port hat.

Der Parameterabschnitt dieses StyleBooks akzeptiert jedoch nur die Server-IPs über $parameters.ips. Das StyleBook geht davon aus, dass alle Server auf Port 80 laufen. Um die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lastausgleichskonfiguration mit dem StyleBook `lb-mon` zu erstellen, müssen Sie die $parameters.ips in eine Liste von Objekten umwandeln. Dies wird mit der Hilfskomponente help-comp im obigen Beispiel erreicht. Die Komponente help-comp ist vom Typ StyleBook `server-ip-port-params`. Dieses StyleBook hat keine Komponenten. Folglich erstellt es keine Konfigurationsobjekte. Die help-comp erstellt eine Wiederholungsliste über $parameters.ips und konstruiert ein Objekt, das aus `ip` und Port (der auf einen statischen Wert von 80 gesetzt ist) für jedes Element von $parameters.ips besteht. Somit wandelt help-comp eine Liste von IP-Adressen in eine Liste von Objekten um, die später in `lb-mon-comp` verwendet werden können, um die Eigenschaft `svc-servers` zuzuweisen. Das Ergebnis der help-comp wird der Eigenschaft `svc-servers` von `lb-mon-comp` zugewiesen.

Optionale Eigenschaften

Manchmal nimmt eine Eigenschaft einer Komponente ihren Wert von einem Ausdruck an, der ein einfacher Ausdruck wie eine Parameterreferenz oder ein komplexerer sein kann. Das Festlegen dieses Eigenschaftswerts ist in der Komponente optional. Sie können den Eigenschaftswert nur festlegen, wenn der Ausdruck einen tatsächlichen Wert zurückgibt, andernfalls können Sie diese Eigenschaft nicht festlegen.

Nehmen Sie zum Beispiel an, dass eine der Eigenschaften, die Sie festlegen möchten, der `lbmethod` (Lastausgleichsalgorithmus) einer Komponente ist, deren Typ ns::lbvserver ist. Der Wert der Eigenschaft `lbmethod` wird von einem vom Benutzer bereitgestellten Parameterwert übernommen, wie unten gezeigt:

```
components


  -


      name: lbvserver_comp


      type: ns::lbvserver


      properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        name: $parameters.lb-appname + "-lb"

        servicetype: $parameters.lb-service-type

        ipv46: $parameters.lb-virtual-ip

        port: 80

        lbmethod: $parameters.lb-advanced.algorithm
```

Betrachten Sie nun, dass der Parameter **lb-advanced.algorithm** ein optionaler Parameter ist. Und wenn der Benutzer keinen Wert für diesen Parameter angibt, weil er optional ist, wird der Ausdruck **$parameters.lb-advanced.algorithm** zu einem leeren Wert ausgewertet. Daher wird ein ungültiger Wert für die Eigenschaft `lbmethod` übergeben. Um eine solche Situation zu vermeiden, können Sie die Eigenschaft als optional kennzeichnen, indem Sie ihren Namen mit „?“ wie folgt versehen:

```
components

   -

     name: lbvserver_comp

     type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:

      name: $parameters.lb-appname + "-lb"

      servicetype: $parameters.lb-service-type

      ipv46: $parameters.lb-virtual-ip

      port: 80

      lbmethod?: $parameters.lb-advanced.algorithm
```

Die Verwendung von „?“ lässt die Eigenschaft weg, wenn der Ausdruck auf der rechten Seite zu nichts ausgewertet wird, was in diesem Fall einer wie folgt definierten Komponente entsprechen würde:

```
components

  -

    name: lbvserver_comp

    type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:


      name: $parameters.lb-appname + "-lb"


      servicetype: $parameters.lb-service-type


      ipv46: $parameters.lb-virtual-ip


      port: 80
```

Da **lbmethod** optional ist, führt das Weglassen immer noch zu einer gültigen Komponente. Beachten Sie, dass `lbmethod` seinen Standardwert annehmen könnte, wenn dieser in seinem Typ „ns::lbvserver“ definiert ist.

Properties-default-sources-Konstrukt

Das Properties-default-sources-Konstrukt ist analog zum Parameters-default-sources-Konstrukt. Während das Parameters-default-sources-Konstrukt die Wiederverwendung bestehender Parameter (aus anderen StyleBooks) in einem StyleBook ermöglicht, erlaubt das Properties-default-sources-Konstrukt dem Benutzer, Eigenschaften einer Komponente basierend auf bestehenden Quellen anzugeben.

Die Eigenschaften einer Komponente können über verschiedene Abschnitte des StyleBooks verteilt sein. Zum Beispiel können die Eigenschaften von Objektparametern, Substitutionen, die ein Objekt zurückgeben, Eigenschaften anderer Komponenten oder Ausgaben anderer Komponenten stammen. In solchen Fällen müssen Sie die Eigenschaften, die in anderen Abschnitten des StyleBooks vorkommen, in der Definition der Komponente neu definieren. Dies ist offensichtlich redundant und kann zu Fehlern führen. Um dieses Problem zu lösen, kann das Properties-default-sources-Konstrukt verwendet werden. Das Properties-default-sources-Konstrukt ist eine Liste, bei der jedes Element eine Quelle für bestimmte Eigenschaften der Komponente identifiziert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Betrachten Sie zum Beispiel eine Komponente, die eine `lbvserver`-Konfiguration erstellt. Diese Komponente definiert die Eigenschaften des `lbvserver` wie folgt.

```
parameters:


  -


    name: lb


    type: ns::lbvserver


components:


  -


    name: lb-comp


    type: ns::lbvserver


    properties:


      name: $parameters.lb.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      ipv46: $parameters.lb.ipv46


      port: $parameters.lb.port


      servicetype: $parameters.lb.servicetype


      lbmethod: $parameters.lb.lbmethod
```

Im obigen Beispiel ist zu beachten, dass die Werte für alle im Komponentenabschnitt definierten Eigenschaften aus dem Objekt $parameters.lb entnommen werden. Obwohl sie aus einer einzigen Quelle stammen, werden die Eigenschaften im StyleBook erneut definiert. Wenn zusätzlich ein neuer Unterparameter zum Objekt $parameters.lb hinzugefügt wird, der für die Konfiguration des `lbvserver` relevant ist, müssen Sie die Komponente lb-comp aktualisieren, um die neue Eigenschaft hinzuzufügen, die dem neuen Unterparameter entspricht.

Um die Neudefinition von Eigenschaften zu vermeiden und alle relevanten Eigenschaften einer Komponente abzurufen, ohne sie explizit im Eigenschaftenabschnitt aufzulisten, kann das Properties-default-sources-Konstrukt verwendet werden. Das obige Beispiel kann wie folgt geschrieben werden.

```
parameters:


  -


    name: lb


    type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:

  -

    name: lb-comp

    type: ns::lbvserver

    properties-default-sources:

      - $parameters.lb
```

Im obigen Beispiel führt die Verwendung des Properties-default-sources-Konstrukts zu einer Reduzierung der Größe der Komponentendefinition, und dies ermöglicht es Ihnen, eine Komponente prägnant zu definieren. Darüber hinaus werden Änderungen automatisch übernommen, jedes Mal wenn sich die Quelle der Eigenschaften der Komponente ändert. Wenn zum Beispiel eine neue Eigenschaft, sagen wir `persistencetype`, im Objekt $parameters.lb hinzugefügt wird, wird diese Eigenschaft standardmäßig zur Konfiguration von lb-comp hinzugefügt, da `persistencetype` eine Eigenschaft von `lbvserver` ist. Somit bietet das Properties-default-sources-Konstrukt eine dynamische Schnittstelle, um die Komponenten zu definieren, ohne sich um Änderungen an den Quellen der Eigenschaften der Komponente kümmern zu müssen.

Berechnung der Eigenschaften der Komponente

Dieser Abschnitt erörtert, wie die Eigenschaften abgerufen werden, wenn das Properties-default-sources-Konstrukt in einer Komponente verwendet wird. Zuerst identifiziert der StyleBooks-Compiler die Liste der Eigenschaften für eine Komponente basierend auf ihrem Typ (im obigen Beispiel `lbvserver`). Als Nächstes ruft der Compiler diese Eigenschaften aus den mehreren Quellen in der Reihenfolge ab, in der sie definiert sind (im Properties-default-sources-Abschnitt der

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Komponente). Wenn eine Eigenschaft in mehreren Quellen existiert, hat die Eigenschaft, die in der letzten Quelle erscheint, Vorrang vor anderen. Schließlich kann eine Eigenschaft, die mithilfe des Properties-default-sources-Konstrukts abgerufen wurde, im Eigenschaftenabschnitt der Komponente überschrieben werden. Es ist wichtig zu beachten, dass die Definition eines Komponentenabschnitts mindestens einen Properties-default-sources-Abschnitt oder einen Eigenschaftenabschnitt haben muss. Sie kann auch beides haben.

Verschachtelte Komponenten

Das Verschachteln einer Komponente in einer anderen Komponente ermöglicht es der verschachtelten Komponente, ihre Konfigurationsobjekte zu erstellen, indem sie sich auf Konfigurationsobjekte oder den vom übergeordneten Komponenten erstellten Kontext bezieht. Die verschachtelte Komponente kann ein oder mehrere Objekte für jedes im übergeordneten Komponenten erstellte Objekt erstellen. Das Verschachteln einer Komponente in einer anderen Komponente weist auf keine Beziehung zwischen den erstellten Konfigurationsobjekten hin. Verschachtelung ist eine Möglichkeit, die Aufgabe von Komponenten zu erleichtern, Konfigurationsobjekte innerhalb eines bestehenden Kontexts der übergeordneten Komponenten zu konstruieren.

Beispiel:

```
components:


 -


  name: my-lbvserver-comp


  type: ns::lbvserver


   properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: $parameters.name + "-lb"

    servicetype: HTTP

    ipv46: $parameters.ip

    port: 80

    lbmethod: $parameters.lb-alg

    components:

      -

       name: my-svcg-comp

       type: ns::servicegroup

       properties:

          name: $parameters.name + "-svcgrp"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            servicetype: HTTP


        components:


            -


              name: lbvserver-svg-binding-comp


              type: ns::lbvserver_servicegroup_binding


              properties:


                name: $parent.parent.properties.name


                servicegroupname: $parent.properties.name


                  -


                    name: members-svcg-comp


                    type: ns::servicegroup_servicegroupmember_binding
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                repeat:

                  repeat-list: $parameters.svc-servers

                  repeat-item: srv

                properties:

                  ip: $srv

                  port: str($parameters.svc-port)

                  servicegroupname: $parent.properties.name
```

In diesem Beispiel wird eine mehrstufige Verschachtelung verwendet. Die Komponente `my-lbvserver-comp` hat eine untergeordnete Komponente namens `my-svcg-comp`. Und die Komponente `my-svcg-comp` enthält zwei untergeordnete Komponenten. Die Komponente `my-svcg-comp` wird verwendet, um ein Dienstgruppen-Konfigurationsobjekt auf der NetScaler-Instanz zu erstellen, indem Werte für die Attribute des integrierten NITRO-Ressourcentyps „`servicegroup`“ bereitgestellt werden. Die erste untergeordnete Komponente der Komponente `my-svcg`, `lbvserver-svg-binding-comp`, wird verwendet, um die von ihrer übergeordneten Komponente erstellte Dienstgruppe an den Lastausgleichs-Virtual-Server (`lbvserver`) zu binden, der von der übergeordneten Komponente der übergeordneten Komponente erstellt wurde. Die $parent-Notation, auch als Elternreferenz bezeichnet, wird verwendet, um auf Entitäten in den übergeordneten Komponenten zu verweisen. Die zweite untergeordnete Komponente, `members-svcg-comp`, wird verwendet, um die Liste der Dienste an die von der übergeordneten Komponente erstellte Dienstgruppe zu binden. Die Bindung wird durch die Verwendung des Wiederholungskonstrukts eines StyleBooks erreicht, um die für den Parameter `svc-servers`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

angegebene Liste der Dienste zu durchlaufen. Weitere Informationen zu Wiederholungskonstrukten finden Sie unter Wiederholungskonstrukt.

Sie können dieselben Konfigurationsobjekte auch ohne die Verwendung von Komponentenverschachtelung erstellen. Weitere Informationen und Beispiele finden Sie unter StyleBook zum Erstellen einer grundlegenden Lastausgleichskonfiguration.

Bedingungskonstrukt

Sie können eine Komponente bedingt machen, indem Sie ein Bedingungskonstrukt verwenden. Der Wert eines Bedingungskonstrukts ist ein boolescher Ausdruck, der zu wahr oder falsch ausgewertet wird. Wenn die Bedingung wahr ist, wird die Komponente verwendet, um ihre Konfigurationsobjekte zu erstellen. Wenn die Bedingung falsch ist, wird die Komponente übersprungen, und es werden keine Konfigurationsobjekte durch sie erstellt. Der boolesche Ausdruck basiert oft auf Parameterwerten.

Beispiel:

```
components:

    -

      name: servicegroup-comp

      type: ns::servicegroup

      condition: $parameters.svc-server-ips

      properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
              name: $parameters.name + "-svcgrp"



              servicetype: HTTP
```

In diesem Beispiel, wenn der Benutzer einen Wert für den optionalen Parameter `svc-server-ips` angibt, dann wird die Komponente `servicegroup-comp` von der StyleBook-Engine verarbeitet. Wenn die Bedingung falsch ist, d.h. wenn der Benutzer keinen Wert für diesen Parameter angibt, wird diesem Parameter ein Nullwert zugewiesen und zu falsch ausgewertet, dann ignoriert die StyleBook-Engine die Existenz dieser Komponente, und es wird kein `servicegroup` erstellt.

Beachten Sie, dass der boolesche Ausdruck auf jedem gültigen Ausdruck basieren kann, der in StyleBooks unterstützt wird (zum Beispiel, ob eine andere Komponente vorhanden ist oder ob ein Parameter einen bestimmten Wert hat).

Das folgende Beispiel erstellt das Konfigurationsobjekt vom NITRO-Typ ns::systemfile, wenn die Bedingung als wahr ausgewertet wird.

Beispiel:

```
     components


          -



            name: pem_key_files



            type: ns::systemfile



            condition: "$components.der-certificate-files-comp or
$components.pem-certificate-files-comp"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        properties:

              filecontent: $certificate.keyfile.contents

              fileencoding: "BASE64"

              filelocation: "/nsconfig/ssl"

              filename: $certificate.keyfile.filename
```

In diesem Beispiel ist die Bedingung ein komplexer „oder“-Ausdruck, bei dem Sie möchten, dass dieses Konfigurationsobjekt vom StyleBook nur dann erstellt wird, wenn zwei andere Komponenten im StyleBook verarbeitet (nicht übersprungen) wurden, wodurch eine Abhängigkeit zwischen Komponenten entsteht.

Repeat-Konstrukt

Sie können das **repeat**-Konstrukt einer Komponente verwenden, um mehrere Konfigurationsobjekte desselben Typs zu erstellen.

Im folgenden Beispiel wird die Komponente **members-svcg-comp** verwendet, um die Liste der Dienste an die von der übergeordneten Komponente erstellte Dienstgruppe zu binden. Um ein Konfigurationsobjekt zu erstellen, das jeden Server an die Dienstgruppe bindet, verwenden Sie das **repeat**-Konstrukt, um die für den Parameter **svc-servers** angegebene Dienstliste zu durchlaufen. Während der Iteration erstellt die Komponente für jeden Dienst (im **repeat-item**-Konstrukt als **srv** bezeichnet) in der Dienstgruppe ein NITRO-Objekt vom Typ **servicegroup_servicegroupmember_binding** und setzt das Attribut **ip** in jedem NITRO-Objekt auf die IP-Adresse des entsprechenden Dienstes.

Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:

  -

      name: my-lbvserver-comp

      type: ns::lbvserver

      properties:

           name: $parameters.name + "-lb"

           servicetype: HTTP

           ipv46: $parameters.ip

           port: 80

           lbmethod: $parameters.lb-alg

           components:

                -

                   name: my-svcg-comp

                   type: ns::servicegroup

                   properties:

                        name: $parameters.name + "-svcgrp"

                        servicetype: HTTP

                   components:

                         -

                         name: lbvserver-svg-binding-comp

                         type: ns::lbvserver\servicegroup\binding

                         properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                        name: $parent.parent.properties.name

                        servicegroupname: $parent.properties.name

                    -

                    name: members-svcg-comp

                    type: ns::servicegroup\servicegroupmember\binding

                    repeat:

                      repeat-list: $parameters.svc-servers

                      repeat-item: srv

                    properties:

                        ip: $srv

                        port: $parameters.svc-port

                        servicegroupname: $parent.properties.name
```

Das **repeat** ist ein eigenständiges Objekt, und **repeat-list** sowie **repeat-item** sind Attribute für das repeat-Objekt.

- repeat-list ist ein obligatorisches Attribut, das die Liste identifiziert, über die die Komponente iteriert.
- repeat-item ist optional und wird verwendet, um dem aktuellen Element in der Iteration einen benutzerfreundlichen Namen zu geben.

Wenn nicht angegeben, kann auf das aktuelle Element mit dem Ausdruck **$repeat-item** zugegriffen werden. Die letzte Komponente im obigen Beispiel kann auch wie folgt geschrieben werden:

```
          -



          name: members-svcg-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
type: ns::servicegroup_servicegroupmember_binding

repeat:

  repeat-list: $parameters.svc-servers

properties:

      ip: $repeat-item

      port: $parameters.svc-port

      servicegroupname: $parent.properties.name
```

Zusätzlich zur Möglichkeit, sich auf das aktuelle Element während der Iteration über eine Liste zu beziehen, ist es auch möglich, sich auf den aktuellen Index des Elements in der Liste mit **repeat-index** zu beziehen. Im folgenden Beispiel wird **repeat-index** verwendet, um eine Portnummer basierend auf dem aktuellen Index zu berechnen:

```
   name: services

   type: ns::service
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            repeat:


               repeat-list: $parameters.app-services


               repeat-item: srv


            properties:


                ip: $parameters.app-ip


                port: $parameters.base-port + repeat-index


                servicegroupname: $parent.properties.name
```

Ähnlich dem **repeat-item**-Konstrukt können Sie einen anderen Variablennamen zuweisen, um auf den aktuellen Index der Iteration zu verweisen. Das vorherige Beispiel ist dem folgenden Beispiel äquivalent:

```
    -


            name: services


            type: ns::service
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            repeat:

               repeat-list: $parameters.app-services

               repeat-item: srv

               repeat-index: idx

            properties:

                ip: $parameters.app-ip

                port: $parameters.base-port + $idx

                servicegroupname: $parent.properties.name
```

Wiederholungsbedingungs-Konstrukt

Das Wiederholungsbedingungs-Konstrukt wird in jeder Iteration eines Wiederholungskonstrukts ausgewertet, und das Ergebnis bestimmt, ob das Konfigurationsobjekt in dieser Iteration erstellt oder zur nächsten Iteration übergegangen werden soll. Das folgende Beispiel zeigt die Verwendung des Wiederholungsbedingungs-Konstrukts:

Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components

   -

      name: der-key-files-comp

      type: ns::systemfile

      repeat:

      repeat-list: $parameters.certificates

      repeat-item: certificate

        repeat-condition: $certificate.ssl-inform == DER

        properties:

          filecontent: base64($certificate.keyfile.contents)

          fileencoding: BASE64
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        filelocation: /nsconfig/ssl



        filename: $certificate.keyfile.file
```

In diesem Beispiel iteriert die `der-key-files-comp`-Komponente über alle vom Benutzer angegebenen Zertifikate, erstellt aber nur Konfigurationsobjekte, die Zertifikaten mit DER-Kodierung entsprechen. In jeder Iteration wird der Wiederholungsbedingungsausdruck ausgewertet, um zu prüfen, ob die Zertifikatskodierung vom Typ DER ist. Wenn sie nicht vom Typ DER ist, wird in der aktuellen Iteration kein Konfigurationsobjekt erstellt, und die Iteration geht zum nächsten Zertifikat in der Liste über.

Verschachtelte Wiederholungen

Mit dem verschachtelten Wiederholungskonstrukt können Sie mehr als ein Wiederholungskonstrukt in jeder Komponente haben, abhängig von der Definition der Komponente. Betrachten Sie eine verschachtelte Wiederholung von zwei Ebenen. Für jedes Element in der äußeren Liste (erste Wiederholungsliste) können Sie eine Wiederholungsliste für alle Elemente der inneren Liste (zweite Wiederholungsliste) erstellen. Der StyleBook-Compiler unterstützt bis zu drei verschachtelte Wiederholungen. Jede Wiederholungsebene hat die Attribute repeat-item und repeat-index, die ihr zugeordnet sind. Sowohl die Attribute repeat-item als auch repeat-index sind optional. Zusätzlich kann jede Wiederholung auch eine repeat-condition angeben.

Beispiel:

```
parameters:


  -


      name: vips


      type: ipaddress[]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -

      name: vip-ports

      type: tcp-port[]

components:

  -

      name: lbvservers-comp

      type: ns::lbvserver

      repeat:

         repeat-list: $parameters.vips

         repeat-item: ip

         repeat:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            repeat-list: $parameters.vip-ports

            repeat-item: port

      properties:

         name: str("lb-") + str($ip) + '-' + str($port)

         servicetype: HTTP

         ipv46: $ip

         port: $port
```

In diesem Beispiel iterieren wir für jedes Element in `$parameters.vips` über alle Elemente von `$parameters.vip-ports`. Somit erstellen wir für jedes in `$parameters.vips` angegebene `ipaddress` `lbvserver` Konfigurationsobjekte für alle in $parameters.vip-ports angegebenen Ports. Der Abschnitt „properties“ definiert den Namen des Objekts mit „lb“ als Präfix für die Kombination aus IP-Adresse und Port. Daher definiert `$ip + $port` für jede Iteration eine eindeutige Kombination aus IP-Adresse und Portnummer.

Wenn das Attribut `repeat-item` nicht angegeben ist, generiert der Compiler einen Standardwert dafür. Die Standardwerte für repeat-item sind: `$repeat-item`, `$repeat-item-1`, `$repeat-item-2` für jede Wiederholungsebene. Ähnlich generiert der Compiler einen Standardwert, wenn das Attribut `repeat-index` nicht angegeben ist. Die Standardwerte für repeat-index sind: $repeat-index, $repeat-index-1 und $repeat-index-2 für jede Wiederholungsebene.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Das folgende Beispiel beschreibt die Namenskonvention bei Fehlen der Attribute repeat-item und repeat-index in einem verschachtelten Wiederholungsobjekt.

Beispiel:

```
components:


-


     name: lbvservers-comp


     type: ns::lbvserver


     repeat:


         repeat-list: $parameters.vips


         repeat:


            repeat-list: $parameters.vip-ports


     properties:


        name: str("lb-") + str($repeat-item) + '-' + str($repeat-item-1)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        servicetype: HTTP


        ipv46: $repeat-item


        port: $repeat-item-1
```

Ausgaben

Im Ausgabeabschnitt legen Sie fest, was ein StyleBook seinen Benutzern zur Verfügung stellt, nachdem es alle Konfigurationsobjekte erfolgreich erstellt hat. Der Ausgabeabschnitt eines StyleBooks ist optional. Ein StyleBook muss keine Ausgaben zurückgeben. Wenn es jedoch einige interne Komponenten als Ausgaben zurückgibt, bietet es StyleBooks, die es importieren, mehr Flexibilität, wie Sie bei der Erstellung eines zusammengesetzten StyleBooks sehen können.

Die folgende Tabelle beschreibt die Attribute, die im Ausgabeabschnitt verwendet werden.

ATTRIBUT	BESCHREIBUNG	OBLIGATORISCH
Name	Der Name der Ausgabe, die dem Konfigurationsobjekt entspricht, das Sie offenlegen möchten.	Ja
Beschreibung	Eine Textzeichenfolge, die die Ausgabe beschreibt.	Nein
Wert	Dieses Attribut gibt an, wie der Wert extrahiert wird, der von einem StyleBook zurückgegeben wird.	Ja

Beispiel:

```
outputs:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

  name: lbvserver

  description: LBVServer component

  value: $components.my-lbvserver-comp

-

  name: svc-grp

    description: ServiceGroup name

    value: $components.my-svcg.properties.name
```

In diesem Beispiel legen Sie die **lbvserver**-Komponente und den `servicegroup` **Namen** offen, die vom StyleBook erstellt würden. Der Wert der Ausgabe namens **lbvserver** ist die Komponente **my-lbvserver-comp**. Ähnlich verhält es sich: Der Wert der Ausgabe namens **svc-grp** ist der Name des `servicegroup`, der von der Komponente **my-svcg** erstellt wurde.

Parameterreferenz

Im Komponenten-Konstrukt verweisen Sie auf die im Parameterabschnitt definierten Parameter mithilfe der `$parameters.<parametername>`-Notation. Wenn `<parametername>` selbst Parameter enthält (wenn der Typ ein Objekt ist), dann müssen Sie die Notation `$parameters.<parametername>.<sub-parametername>` verwenden und so weiter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Beispiel:

```
parameters:


  -


    name: name


    label: Name


    type: string


    required: true


     -


      name: vip


      label: Virtual IP and Port


      type: object


      required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters:

  -

    name: ip

    label: Virtual IP

    description: The Virtual IP Address

    type: ipaddress

    required: true

      -

        name: port

        label: The Virtual Port

        description: The TCP port for the Virtual IP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
              type: tcp-port

              default: 80

components:

  -

    name: my-lbvserver-comp

    type: ns::lbvserver

    properties:

       name: $parameters.name

       servicetype: HTTP

       ipv46: $parameters.vip.ip
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      port: $parameters.vip.port
```

Elternreferenz

Wenn Sie verschachtelte Komponenten verwenden, können Sie mit der Notation $parent auf die übergeordnete Komponente verweisen. Wenn die übergeordnete Komponente mehrere Konfigurationsobjekte mit dem Wiederholungskonstrukt erstellt und innerhalb jeder Iteration untergeordnete Komponenten andere Konfigurationsobjekte erstellen, bezieht sich die Notation $parent immer auf die aktuelle Iteration der übergeordneten Komponente. Zum Beispiel bezieht sich $parent.properties.name auf die Eigenschaft „name“ des Konfigurationsobjekts, das in der aktuellen Iteration von der übergeordneten Komponente erstellt wurde.

Beispiel:

```
components:


 -


   name: my-lbvserver-comp


   type: ns::lbvserver


   properties:


     name: $parameters.name + "-lb"


     servicetype: HTTP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    ipv46: $parameters.ip

    port: 80

    lbmethod: $parameters.lb-alg

    components:

      -

        name: my-svcg-comp

        type: ns::servicegroup

        properties:

          name: $parameters.name + "-svcgrp"

          servicetype: HTTP

          components:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        -

          name: lbvserver-svg-binding-comp

          type: ns::lbvserver_servicegroup_binding

          properties:

             name: $parent.parent.properties.name

             servicegroupname: $parent.properties.name

               -

                 name: members-svcg-comp

                 type: ns::servicegroup_servicegroupmember_binding

                 repeat: $parameters.svc-servers

                 repeat-item: srv
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    properties:


                      ip: $srv


                      port: str($parameters.svc-port)


                      servicegroupname: $parent.properties.name
```

Sie können auch in der Hierarchie der Komponenten nach oben navigieren, indem Sie auf die Eigenschaften der Eltern von Eltern bis hin zu den Komponenten der obersten Ebene zugreifen. Zum Beispiel nimmt die Eigenschaft „name“ der Komponente **lbvserver-svg-binding-comp** ihren Wert von der Eigenschaft „name“ des Elternteils ihres Elternteils, der Komponente **my-lbvserver-comp**, indem sie die Notation **$parent.parent** verwendet.

Komponentenreferenz

In dem Komponentenkonstrukt verweisen Sie auf eine Top-Level-Komponente im StyleBook, indem Sie die Notation `$components.<componentname>` verwenden. Wenn es verschachtelte Komponenten innerhalb einer Top-Level-Komponente gibt, wird die Notation `$components.<componentname>.components.<component-name>` verwendet, um auf diese zu verweisen, und so weiter.

Beispiel:

```
components:


 -


     name: my-lbvserver-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::lbvserver

    properties:

      name: $parameters.name + "-lb"

      servicetype: HTTP

      ipv46: $parameters.ip

      port: 80

      lbmethod: $parameters.lb-alg

-

    name: my-svcg-comp

    type: ns::servicegroup

    properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        name: $parameters.name + "-svcgrp"

        servicetype: HTTP

-

    name: members-svcg-comp

    type: ns::servicegroup_servicegroupmember_binding

    repeat: $parameters.svc-servers

    repeat-item: srv

    properties:

        ip: $srv

        port: str($parameters.svc-port)

        servicegroupname: $components.my-svcg-comp.properties.name
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-

    name: lbvserver-svg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    properties:

        name: $components.my-lbvserver-comp.properties.name

        servicegroupname: $components.my-svcg-comp.properties.name
```

In diesem Beispiel müssen die Komponenten **my-svcg-comp** und **my-lbvserver-comp** erstellt werden, bevor die letzte Komponente **lbvserver-svg-binding-comp** erstellt wird, da in dieser letzten Komponente Verweise auf diese Komponenten vorhanden sind. Diese Verweise werden durch die Komponentenreferenzen bereitgestellt, die durch `$components.<componentname>` gekennzeichnet sind.

Substitutionen-Referenz

Im Abschnitt Komponenten oder im Abschnitt Operationen verweisen Sie auf Substitutionen, die im Abschnitt Substitutionen definiert sind, indem Sie die Notation **`$substitutions.<substitution-name>`** verwenden. Zum Beispiel: **$substitutions.http-port**.

Wenn eine Substitution eine Map ist, können Sie ein Element in der Map als **`$substitutions.<substitutions-name>[<map-key>]`** referenzieren. Zum Beispiel: **`$substitutions.protocol-map[$parameters.port]`**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Variablenreferenz

Wenn Sie die Konstrukte repeat und repeat-item in Komponenten verwenden, um mehrere Konfigurationsobjekte zu erstellen, können Sie dem repeat-item-Konstrukt einen Variablennamen zuweisen. Diese Variable kann dann in den Eigenschaften dieser Komponente oder in untergeordneten Komponenten unter Verwendung der Notation `$<varname>` referenziert werden. Beachten Sie, dass, wenn das repeat-Konstrukt ohne das repeat-item-Konstrukt in einer Komponente verwendet wird, eine Standardvariable namens $repeat-item verwendet werden kann, um auf die Iterationselemente zuzugreifen.

Beispiel:

```
components:

  -

    name: server-members-comp

    type: ns::server

    condition: $parameters.svc-server-domain-names

    repeat: $parameters.svc-server-domain-names

    repeat-item: server-name

    properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: $server-name + "-server"

    domain: $server-name

  components:

    -

      name: service-members-comp

      type: ns::service

      properties:

        name: $server-name + "-service"

        servername: $parent.properties.name

        servicetype: $parameters.svc-service-type

        port: $parameters.svc-server-port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Im obigen Beispiel wird dem repeat-item-Konstrukt ein Variablenname, server-name, zugewiesen. Dieser Variablenname wird in den Eigenschaften derselben Komponente und in den untergeordneten Komponenten `$<varname>` referenziert.

Operationen

Der `Operations` ist ein optionaler Abschnitt in einem StyleBook. In diesem Abschnitt können Sie NetScaler Console Analytics so konfigurieren, dass AppFlow-Datensätze für alle oder einen Teil der Transaktionen erfasst werden. Der auf einer NetScaler-Instanz mithilfe des StyleBooks erstellte virtuelle Server verarbeitet die Transaktionen. Sie können NetScaler Console auch so konfigurieren, dass Alarme ausgelöst werden, wenn bestimmte Verkehrsbedingungen auf einem virtuellen Server erfüllt sind.

Sie können NetScaler Console über StyleBooks so konfigurieren, dass Verkehrsstatistiken von den verschiedenen NetScaler Console Insights erfasst werden, die wie folgt aufgeführt sind:

- Bot Insight
- Web Insight
- Security Insight
- HDX™ Insight
- NetScaler Gateway Insight

Die unterstützten virtuellen Server sind Lastausgleichs-, Content Switching- und VPN-virtuelle Server.

Aktivieren Sie sowohl Web Insight als auch Security Insight oder eines davon für die Analyse auf einem Lastausgleichs- oder Content Switching-virtuellen Server. Für VPN-virtuelle Server müssen Sie jedoch sowohl HDX Insight als auch NetScaler Gateway Insight oder eines davon aktivieren.

Jedes NetScaler Console Insight, das auf NetScaler-Instanzen über StyleBooks aktiviert ist, verwendet ein IPFIX-Protokoll (AppFlow), um die Daten von den Instanzen an NetScaler zu senden.

Wenn Sie Web Insight aktivieren, werden außerdem „Client-Side Measurements“ auf den Lastausgleichs- und Content Switching-virtuellen Servern aktiviert. Mit dieser Funktion erfasst NetScaler Console Ladezeit- und Renderzeitmetriken für HTML-Seiten durch HTML-Injektion. Mithilfe dieser Metriken können Administratoren L7-Latenzprobleme identifizieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nachdem Sie ein bestimmtes NetScaler Console Insight aktiviert haben, rufen Sie die Seite **Anwendungsübersicht** auf, um die mit diesem Insight verbundenen Bedrohungsdetails anzuzeigen.

Beispiel 1:

Das folgende Beispiel zeigt, wie der Operations-Abschnitt in einem StyleBook geschrieben wird, um sowohl HDX Insight als auch NetScaler Gateway Insight auf einem VPN-virtuellen Server zu aktivieren:

```
name: simple-vpn-ops


namespace: com.example.stylebooks


schema-version: "1.0"


version: "0.1"


description: Test StyleBook to enable hdxinsight and gatewayinsight on a
VPN vserver


import-stylebooks:


  -


    namespace: netscaler.nitro.config
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    version: "10.5"

    prefix: ns

components:

  -

    name: vpnvserver-comp

    type: ns::vpnvserver

    properties:

      name: str("vpn-") + str($current-target.ip)

      servicetype: SSL

      ipv46: 1.1.21.37

      port: 443
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
operations:

    analytics:

      -

        name: comp-ops

        properties:

          target: $components.vpnvserver-comp

          filter: "true"

          insights:

            -

              type: hdxinsight

            -

              type: gatewayinsight
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
outputs:


  -


    name: myvpns


    value: $components.vpnvserver-comp
```

Beispiel 2:

Das folgende Beispiel zeigt, wie der Operations-Abschnitt in einem StyleBook geschrieben wird, um Web Insight, Security Insight und Bot Insight auf einem virtuellen Lastausgleichsserver zu aktivieren:

```


---

name: enable-insights

namespace: com.acme.stylebooks

description: "This StyleBook enables Web,Security & Bot Insight on Load
Balancing Vserver"

display-name: "SB Operations"

schema-version: "1.0"

version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    prefix: ns
    version: "10.5"


parameters:




 -
    name: lbname
    type: string
    required: true
  -
    name: vip
    type: ipaddress
    required: true
  -
    name: appflowfilter
    type: string
    required: true


components:
  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.lbname
      servicetype: HTTP
      ipv46: $parameters.vip
      port: 80


outputs:
  -
    name: mylb
    value: $components.my-lbvserver-comp


operations:
  analytics:
    -
      name: lbvserver-op
      properties:
        target: $outputs.mylb
        filter: $parameters.appflowfilter
        insights:
          -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            type: webinsight

          -

            type: securityinsight

          -

            type: botinsight
```

Analysen

Jedes Element im Analysebereich wird verwendet, um die NetScaler Console Analysefunktion für einen oder mehrere virtuelle Server zu konfigurieren, die in StyleBooks erstellt wurden.

Ein Element im Analysebereich hat die folgenden Attribute:

ATTRIBUT	BESCHREIBUNG	OBLIGATORISCH
Name	Name des Analyseelements.	Ja
Beschreibung	Eine Textzeichenfolge, die beschreibt, was dieses Element ist.	Nein
Bedingung	Ein boolescher Ausdruck. Wenn diese Bedingung als falsch ausgewertet wird, wird das gesamte Analyseelement übersprungen.	Nein
Wiederholung	Iteriert über eine Liste.	Nein
Wiederholungsbedingung	Ein boolescher Ausdruck. Wenn der Ausdruck als falsch ausgewertet wird, wird die aktuelle Iteration übersprungen.	Nein
Wiederholungselement	Name des Elements in der aktuellen Iteration.	Nein

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUT	BESCHREIBUNG	OBLIGATORISCH
Wiederholungsindex	Name des Indexwerts der aktuellen Iteration.	Nein
Eigenschaften	Eine Liste von Analysevorgangseigenschaften.	Ja
Ziel	Eine der Eigenschaften in der Liste. Der Zielausdruck ist der Name eines virtuellen Servers, der auf dem NetScaler konfiguriert ist und für den Analysen gesammelt werden.	Ja
Filter	Eine der Eigenschaften in der Liste. Der Wert dieses Attributs ist ein erweiterter NetScaler-Richtlinienausdruck, der verwendet wird, um die Anfragen auf dem virtuellen Server zu filtern, für den Analysen gesammelt werden. Standardmäßig werden die Analysedaten für den gesamten Datenverkehr gesammelt, der den virtuellen Server durchläuft.	Nein
Einblicke	Eine der Eigenschaften in der Liste. Der Wert dieses Attributs ist der Typ der Einblicksdaten, die vom Ziel-Virtual-Server gesammelt werden sollen. Standardmäßig werden alle zulässigen Einblicke auf den Ziel-Virtual-Servern basierend auf dem Virtual-Server-Typ konfiguriert, wie unter Ziel-	Nein

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUT	BESCHREIBUNG	OBLIGATORISCH
	Virtual-Server und Einblickstypen angegeben.	
Transportmodus	Eine der Eigenschaften in der Liste. Der Wert dieses Attributs ist entweder `logstream` oder `ipfix`. `logstream` ist der Standardwert.	Nein
clientseitige Messungen	Eine der Eigenschaften in der Liste. Der Wert dieses Attributs ist entweder ENABLED oder DISABLED. DISABLED ist der Standardwert.	Nein
http-x-forwarded-for	Eine der Eigenschaften in der Liste. Der Wert dieses Attributs ist entweder ENABLED oder DISABLED. Das Attribut aktiviert oder deaktiviert das Einfügen des X-Forwarded-For-Headers, um die Client-IP-Informationen an den Backend-Server weiterzuleiten. DISABLED ist der Standardwert.	Nein
enable-hdxinsight-for	Eine der Eigenschaften in der Liste. Der Wert dieses Attributs ist entweder ICA oder TCP. Dieses Attribut aktiviert `hdxinsight` für bestimmte Verkehrsdaten. ICA ist der Standardwert.	Nein

Beispiel 1: Analysen für einen einzelnen virtuellen Server konfigurieren

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
operations:



  analytics:

    -

    name: lbvserver-ops-comp

    properties:

        target: $components-basic-lb-comp.outputs.lbvserver-name

        filter: HTTP.REQ.URL.CONTAINS("catalog")

        transport-mode: logstream

        client-side-measurements: ENABLED

        insights:

          -

            type: webinsight

          -

            type: securityinsight
```

Beispiel 2: Analysen für eine Liste von VPN-Virtual-Servern konfigurieren

```
operations:



    analytics:

    -

      name: vpnvserver-ops-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      repeat: $outputs.staging-vpnvservers

      repeat-item: vpnvsvr

      properties:

        target: $vpnvsvr.outputs.vpnvserver

        filter: HTTP.REQ.URL.CONTAINS("catalog")

        http-x-forwarded-for: ENABLED

        insights:

          -

            type: hdxinsight

            enable-hdxinsight-for: TCP
```

Jedes Attribut im Analysebereich konfiguriert die NetScaler-Instanzen so, dass sie AppFlow-Datensätze auf dem virtuellen Server erfassen, der durch die Zieleigenschaft identifiziert wird.

Ziel-Virtual-Server und Insight-Typen

Die Ziel-Virtual-Server und die entsprechenden zulässigen Insight-Typen sind wie folgt:

ZIEL-VIRTUAL-SERVER	INSIGHT-TYP
Lastausgleichs-vServer	Web-Einblick, Sicherheits-Einblick, Bot-Einblick
CS-Server	Web-Insight, Security-Insight, Bot-Insight
VPN-Server	hdx-Einblick, gateway-Einblick

HINWEIS

IPFIX ist der Standard-Transportmodus, der zum Konfigurieren von Analysen für virtuelle Server in StyleBooks verwendet wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alarme

Der Unterabschnitt Alarme des Abschnitts Operationen hat eine ähnliche Struktur und dieselben Attribute wie der Unterabschnitt Analysen. Der einzige Unterschied liegt im Attribut Eigenschaften. Eine Liste aller Attribute (außer dem Attribut Eigenschaften) finden Sie unter Analysen.

Die folgenden Eigenschaften sind in einem Alarm-Unterabschnitt verfügbar:

ATTRIBUT	BESCHREIBUNG	OBLIGATORISCH
`target`	Ein Ausdruck, der zum Namen eines virtuellen Servers ausgewertet wird, der auf dem NetScaler konfiguriert ist und für den Alarme konfiguriert sind.	Ja
`email-profile`	Name eines E-Mail-Profils, das in der NetScaler Console Analytics-Funktion definiert ist und eine Liste von E-Mail-Adressen enthält, die Sie benachrichtigen möchten, wenn der Alarm ausgelöst wird.	Nein (entweder ein `email-profile` oder ein `sms-profile` muss definiert sein)
`sms-profile`	Name eines SMS-Profils, das in der NetScaler Console Analytics-Funktion definiert ist und eine Liste von Telefonnummern enthält, die Sie benachrichtigen möchten, wenn der Alarm ausgelöst wird.	Nein (entweder ein `email-profile` oder ein `sms-profile` muss definiert sein)
`rules`	Eine Liste von Regeln, die die Bedingungen definieren, die einen Alarm für den virtuellen Server auslösen würden, der durch die Zieleigenschaft definiert ist.	Ja

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ATTRIBUT	BESCHREIBUNG	OBLIGATORISCH
`metric`	Ein Attribut der Regel. Der Name einer Metrik, die Sie bezüglich des virtuellen NetScaler-Servers verfolgen möchten.	Ja
`operator`	Ein Attribut der Regel. Der Operator, der verwendet werden soll, um die Metrik mit dem Wert zu vergleichen. Gültige Operatoren sind `greaterthan` und `lessthan`.	Ja
`value`	Ein Attribut der Regel. Der Schwellenwert, mit dem die Metrik unter Verwendung des Operators verglichen wird. Wenn der Metrikwert diesen Schwellenwert überschreitet, werden die zugehörigen Alarme ausgelöst.	Ja
`period-unit`	Ein Attribut einer Regel. Die Häufigkeit, mit der Benutzer benachrichtigt werden sollen, wenn die Alarmregel erfüllt ist. Dieses Attribut kann die Werte Tag, Stunde oder Woche enthalten. Es bedeutet, dass, wenn die Regel erfüllt ist, ein Alarm einmal pro Zeiteinheit gesendet wird (zum Beispiel einmal täglich).	Ja

Die folgende Tabelle enthält eine Liste von Metriken, die für den NetScaler Virtual Server verfolgt werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ZÄHLER	BESCHREIBUNG	DETAILLIERTE BESCHREIBUNG	NETSCALER CONSOLE-BERECHNUNG
Für einen VPN Virtual Server			
total_requests	Gesamtzahl der VPN-Sitzungsstarts	Gesamtzahl der aktiven Sitzungen auf diesem VPN Virtual Server, die während eines vom Benutzer angegebenen Zeitintervalls gestartet wurden.	Monoton ansteigender Zähler, der bei jedem neuen Sitzungsstart erhöht wird
app_count	Anzahl der VPN-App-Starts	Gesamtzahl der eindeutigen VPN-Anwendungen auf diesem VPN Virtual Server, die während eines vom Benutzer angegebenen Zeitintervalls gestartet wurden.	Monoton ansteigender Zähler bei jedem neuen Anwendungsstart
app_launch_duration	VPN-App-Startdauer	Durchschnittliche Zeit zum Starten einer Anwendung (in Millisekunden)	Durchschnittswert, berechnet über die Startzeiten aller VPN-Anwendungen, die auf diesem virtuellen VPN-Server gestartet wurden
Andere virtuelle Server (`CS`, `LB`, `Auth`, `GSLB`)			
total_requests	Anzahl der Anfragen	Anzahl der Client-Anfragen auf diesem virtuellen Server seit	Monoton ansteigender Zähler, der bei jeder neuen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ZÄHLER	BESCHREIBUNG	DETAILLIERTE BESCHREIBUNG	NETSCALER CONSOLE-BERECHNUNG
		dem letzten Neustart der Appliance oder seit der Erstellung des virtuellen Servers, je nachdem, was aktueller ist.	Anfrage an diesen virtuellen Server inkrementiert wird.
total_bytes	Bytes	Gesamtzahl der Bytes, die über das angegebene Zeitintervall vom virtuellen Server an die NetScaler Console übertragen wurden.	Monoton ansteigender Zähler zur Erfassung der Gesamtzahl der von diesem virtuellen Server bereitgestellten Bytes.
application_response_time	Antwortzeit	Durchschnittliche Antwortzeit des virtuellen Servers.	Der Durchschnittswert der Antwortzeiten aller Anfragen, die von diesem virtuellen Server seit dem letzten Neustart der Appliance (oder seit der Erstellung des virtuellen Servers) empfangen wurden, je nachdem, was zuletzt geschehen ist.

Beispiel für einen Alarmabschnitt in einem StyleBook:

```
operations:

alarms:

 -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
name:lbvserver_alarm

properties:

    target: $outputs.lbvserver

    email-profile: $parameters.emailprofile

    sms-profile: "NetScalerSMS"

    rules:

    -

      metric: "total_requests"

      operator: "greaterthan"

      value: 25

      period-unit: weekly

      -

        metric: "total_bytes"

        operator: "lessthan"

        value: 1024

        period-unit: day
```

Ausdrücke

Eines der leistungsstärksten Merkmale eines StyleBooks ist die Verwendung von Ausdrücken. Sie können StyleBook-Ausdrücke in verschiedenen Szenarien verwenden, um dynamische Werte zu berechnen. Das folgende Beispiel ist ein Ausdruck, um einen Parameterwert mit einer Literalzeichenfolge zu verketten.

Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$parameters.appname + "-mon"
```

Dieser Ausdruck ruft den Parameter mit dem Namen `appname` ab und verkettet ihn mit der Zeichenfolge `-mon`.

HINWEIS

StyleBook unterstützt die Verwendung der reservierten Schlüsselwörter, wenn Sie Parameter und Ausdrücke in einer StyleBook-Definition definieren. Die reservierten Schlüsselwörter sind – `and`, `false`, `in`, `not`, `true` und `or`.

Die folgenden Arten von Ausdrücken werden unterstützt:

Arithmetische Ausdrücke

- Addition (+)
- Subtraktion (-)
- Multiplikation (*)
- Division (/)
- Modulo (%)

Beispiele:

- Addieren von zwei Zahlen: $parameters.a + $parameters.b
- Multiplikation zweier Zahlen: $parameters.a * 10
- Ermitteln des Rests nach der Division einer Zahl durch eine andere:

`15%10` Ergibt `5`

Zeichenfolgenausdrücke

- Zwei Zeichenfolgen verketten (+)

Beispiel:

Zwei Zeichenfolgen verketten: str("app-") + $parameters.appname

Listenausdrücke

Führt zwei Listen zusammen (+)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Beispiel:

- Zwei Listen verketten: $parameters.external-servers + $parameters.internal-servers
- Wenn `$parameters.ports-1` ist und `$parameters.port-2` ist, wird `$parameters.ports-1 + $parameters.ports-2` als Liste angezeigt.

Relationale Ausdrücke

- **==** : Prüft, ob zwei Operanden gleich sind, und gibt „true“ zurück, wenn sie gleich sind, andernfalls „false“.
- **!=** : Prüft, ob zwei Operanden unterschiedlich sind, und gibt „true“ zurück, wenn sie unterschiedlich sind, andernfalls „false“.
- **\>** : Gibt „true“ zurück, wenn der erste Operand größer als der zweite Operand ist, andernfalls „false“.
- **\>=** : Gibt „true“ zurück, wenn der erste Operand größer oder gleich dem zweiten Operanden ist, andernfalls „false“.
- **\<** : Gibt „true“ zurück, wenn der erste Operand kleiner als der zweite Operand ist, andernfalls „false“.
- **\<=** : Gibt „true“ zurück, wenn der erste Operand kleiner oder gleich dem zweiten Operanden ist, andernfalls „false“.

Beispiel:

- Verwendung des Gleichheitsoperators: `$parameters.name = = "abcd"`
- Verwendung des Ungleichheitsoperators: `$parameters.name != "default"`
- Beispiele für andere relationale Operatoren
  - `10 > 9`
  - `10 >= 10`
  - `0 < 9`
  - `10 <= 9`
  - `10 == 10`
  - `10 != 1`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Logische Ausdrücke – boolesch

- **and**: Der logische 'und'-Operator. Wenn beide Operanden wahr sind, ist das Ergebnis wahr, andernfalls ist es falsch.
- **or**: Der logische 'oder'-Operator. Wenn einer der Operanden wahr ist, ist das Ergebnis wahr, andernfalls ist es falsch.
- **not**: Der unäre Operator. Wenn der Operand wahr ist, ist das Ergebnis falsch und umgekehrt.
- **in**: Prüft, ob das erste Argument eine Teilzeichenfolge des zweiten Arguments ist
- **in**: Prüft, ob ein Element Teil einer Liste ist

HINWEIS

Sie können Ausdrücke typumwandeln, bei denen Zeichenfolgen in Zahlen (mithilfe der integrierten Funktion int()) und Zahlen in Zeichenfolgen (mithilfe der integrierten Funktion str()) konvertiert werden. Ähnlich können Sie `tcp-port` in eine Zahl (mithilfe der integrierten Funktion `int()`) und eine IP-Adresse in eine Zeichenfolge (mithilfe der integrierten Funktion str()) umwandeln.

Verwenden Sie einen Trennzeichen vor und nach jedem Operator. Sie können die folgenden Trennzeichen verwenden:

- Vor einem Operator: `space`, `tab`, `comma`, `(`, `)`, `[`, `]`
- Nach einem Operator: `space`, `tab`, `(`, `[`

Zum Beispiel:

- `abc + def`
- `100 % 10`
- `10 > 9`
- `$item in $parameters.some-list`

Splat-Ausdrücke

Ein Splat-Ausdruck `[*]` bietet eine einfachere Möglichkeit, ein bestimmtes Attribut aus einer komplexen Liste für alle Iterationen abzurufen. Sie können jetzt Splat-Ausdrücke in eine StyleBook-Definition aufnehmen.

Syntax:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
list[*].attribute
```

Dieser Ausdruck iteriert über alle Elemente der links angegebenen Liste und gibt den rechts angegebenen Attributwert zurück.

Wenn Sie eine IP-Adresse oder einen Hostnamen jedes virtuellen Servers aus der Liste abrufen möchten, können Sie die folgenden Splat-Ausdrücke verwenden:

Beispiel 1:

```
$parameters.server-members[*].hostname
```

Dieser Ausdruck gibt eine Liste von Hostnamen aller Servermitglieder zurück.

Beispiel 2:

```
$parameters.server-members[*].sub-domains[*].name
```

Dieser Ausdruck gibt eine Liste aller Namen unter den Subdomains jedes Servermitglieds zurück.

Diese Ausdrücke geben immer die Liste des am weitesten rechts stehenden Elementtyps zurück.

Wörtliche Zeichenfolgenausdrücke

Sie können wörtliche Zeichenfolgen verwenden, wenn Sonderzeichen in einer Zeichenfolge ihre wörtliche Form annehmen müssen. Diese Zeichenfolgen können Escape-Zeichen, Backslashes, Anführungszeichen, Klammern, Leerzeichen, eckige Klammern usw. enthalten. Bei wörtlichen Zeichenfolgen wird die übliche Interpretation der Sonderzeichen übersprungen. Alle Zeichen in der Zeichenfolge bleiben in ihrer wörtlichen Form erhalten.

In StyleBooks können Sie NetScaler-Richtlinienausdrücke in ihrer wörtlichen Form mithilfe wörtlicher Zeichenfolgen einfügen. Die Richtlinienausdrücke enthalten typischerweise Sonderzeichen. Ohne wörtliche Zeichenfolgen müssten Sie Sonderzeichen durch Aufteilen von Zeichenfolgen in Unterzeichenfolgen escapen.

Um eine wörtliche Zeichenfolge zu erstellen, schließen Sie eine Zeichenfolge wie folgt zwischen Sonderzeichen ein:

```
~{string}~
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können wörtliche Zeichenfolgen in den StyleBook-Ausdrücken verwenden.

HINWEIS

Verwenden Sie die Zeichenfolge `}~` nicht in einer Eingabezeichenfolge, da diese Sequenz das Ende einer wörtlichen Zeichenfolge anzeigt.

Beispiel:

```
~{HTTP.REQ.COOKIE.VALUE("jsessionid") ALT
HTTP.REQ.URL.BEFORE_STR("=").AFTER_STR(";jsessionid=") ALT
HTTP.REQ.URL.AFTER_STR(";jsessionid=")}~
```

Weitere Informationen finden Sie unter Sonderzeichen in ihrer wörtlichen Form in StyleBooks zulassen.

Zielausdrücke

In einer StyleBook-Definition können Sie den Ausdruck `$current-target` verwenden, um auf die aktuelle Ziel-NetScaler-Instanz zu verweisen. Um speziell auf eine IP-Adresse der Ziel-NetScaler-Instanz zu verweisen, verwenden Sie diesen Ausdruck wie folgt:

```
$current-target.ip
```

Beispiel:

```
components:

 -

  name: lb-comp

  type: ns::lbvserver

  properties:

    name: $current-target.ip + "-lbvserver"
```

In diesem Beispiel verwendet der Name des `lbvserver` die IP-Adresse der Ziel-NetScaler-Instanz.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Validierung des Ausdruckstyps

Die StyleBook-Engine ermöglicht jetzt eine strengere Typüberprüfung zur Kompilierungszeit, d. h. die beim Schreiben des StyleBooks verwendeten Ausdrücke werden beim Import eines StyleBooks selbst und nicht beim Erstellen des Konfigurationspakets validiert.

Alle Verweise auf Parameter, Substitutionen, Komponenten, Eigenschaften von Komponenten, Ausgaben von Komponenten, benutzerdefinierte Variablen (repeat-item, repeat-index, Argumente für Substitutionsfunktionen) usw. werden auf ihre Existenz und Typen validiert.

Beispiel für Typüberprüfungen:

Im folgenden Beispiel ist der erwartete Typ der Port-Eigenschaft des `lbvserver` StyleBooks `tcp-port`. In NetScaler Console erfolgen die Typvalidierungen zur Kompilierungszeit (Importzeit). Der Compiler stellt fest, dass String und `tcp-port` keine kompatiblen Typen sind, und daher zeigt der StyleBook-Compiler einen Fehler an und kann ein StyleBook nicht importieren oder migrieren.

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str("80")
      servicetype: HTTP
```

Um dieses StyleBook erfolgreich zu kompilieren, deklarieren Sie Folgendes als Zahl im Compiler:

`port: 80`

Beispiel für die Kennzeichnung ungültiger Ausdrücke:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Sie ein StyleBook in die NetScaler Console importieren, identifiziert der Compiler die ungültigen Ausdrücke und kennzeichnet sie. Infolgedessen kann das StyleBook nicht in die NetScaler Console importiert werden.

Im folgenden Beispiel ist der Ausdruck, der der Name-Eigenschaft in der Komponente `lb-sg-binding-comp` zugewiesen ist: `$components.lbvserver-comp.properties.lbvservername`. Es gibt jedoch keine Eigenschaft namens `lbvservername` in der Komponente `lbvserver-comp`.

```
Components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: mylb

      ipv46: 10.102.190.15

      port: 80

      servicetype: HTTP

  -

    name: sg-comp

    type: ns::servicegroup

    properties:

      servicegroupname: mysg

      servicetype: HTTP

  -

    name: lb-sg-binding-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::lbvserver_servicegroup_binding

    condition: $parameters.create-binding

    properties:

      name: $components.lbvserver-comp.properties.lbvservername

      servicegroupname: $components.sg-comp.properties.servicegroupname
```

Implizite Typumwandlung von Datentypen

Wenn Sie StyleBook-Ausdrücke für verschiedene Datentypen verwenden, wandelt die StyleBook-Engine die Ausgabe nun implizit in einen geeigneten Datentyp um. Die implizite Typumwandlung von Datentypen unterstützt binäre Operationen und Wertzuweisungen.

Beispiele für binäre Operationen:

- Das Addieren (+) zweier Variablen vom Typ `string` und `number` setzt den Ausgabedatentyp auf `string`.

`$parameters.appname + '_' + $parameters.app_instance_num`

- Das Addieren (+) zweier Variablen vom Typ `string` und `ipaddress` setzt den Ausgabedatentyp auf `string`.

`$parameters.appname + '_' + $parameters.instance_ip`

- Das Addieren (+) zweier Variablen vom Typ `ipaddress` und `number` setzt den Ausgabedatentyp auf `ipaddress`.

`$parameters.instance_ip + $parameters.number`

- Das Subtrahieren (-) zweier Variablen vom Typ `ipaddress` und `number` setzt den Ausgabedatentyp auf `ipaddress`.

`$parameters.instance_ip - $parameters.number`

- Das Multiplizieren (*) zweier Variablen vom Typ `string` und `number` setzt den Ausgabedatentyp auf `string`.

`$parameters.dummy_str * $parameters.count`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Beispiele für Wertzuweisungen:

- Wenn eine Variable als `string` Datentyp definiert ist, wird der zugewiesene Wert in den definierten Datentyp konvertiert.

```
name: $parameters.port * 3
```

- Wenn eine Variable als `portnumber` Datentyp definiert ist, wird der zugewiesene Wert mit Ausnahmen in den `portnumber` Datentyp konvertiert.

```
port: $index + $parameters.lower_limit
```

Listen indizieren

Elemente einer Liste können nun direkt durch Indizierung aufgerufen werden:

Ausdruck	Beschreibung
`$components.test-lbs[0]`	Bezieht sich auf das erste Element in der `thetest-lbs` Komponente
`$components.test-lbs[0].properties.p1`	Bezieht sich auf die Eigenschaft p1 des ersten Elements in der test-lbs Komponente
`$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname`	Bezieht sich auf die Eigenschaft `servicegroupname` des zweiten Elements in der Komponente `servicegroups`, die eine Ausgabe des ersten Elements der Komponente `lbcomps` ist.

Richtlinienausdrücke in StyleBooks

Die StyleBooks-GUI ermöglicht es Ihnen, NetScaler®-Richtlinienausdrücke zu erstellen, indem Sie Elemente aus Listen auswählen, was Ihnen hilft, Ausdrücke schneller und genauer zu erstellen.

Richtlinienausdrücke in StyleBooks ermöglichen Ihnen die Erstellung flexibler und anpassbarer Konfigurationen. Sie können Bedingungen basierend auf verschiedenen Parametern, Attributen oder Variablen festlegen. Richtlinienausdrücke werden häufig verwendet, um NetScaler-Richtlinienkonfigurationen zu implementieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RICHTLINIEN-AUSDRUCKSEDITOR IN DER STYLEBOOKS-GUI AKTIVIEREN

Um den EPA- oder Ausdrucksеditor für einen Parameter verfügbar zu machen, geben Sie das GUI-Attribut `is_policy_expression` in der Parameterdefinition an. Wenn diese Einstellung aktiviert ist (auf true gesetzt), können Sie den **Expressions Editor** aufrufen, wenn Sie einen Wert für diesen Parameter eingeben.

```
parameters:

  -

    name: expression

    type: string

    label: Expression

    required: true

    gui:

      is_policy_expression: true
```

RICHTLINIENAUSDRÜCKE ERSTELLEN UND AUFBAUEN

1. Navigieren Sie zu **Applications > Configurations > StyleBooks**. Die Seite **StyleBooks** zeigt alle StyleBooks an, die in Ihrer NetScaler Console verfügbar sind.
2. Wählen Sie ein StyleBook aus, das Richtlinienausdrücke in seinen Parametern enthält.
3. Klicken Sie auf **Create Configuration**. Geben Sie auf der Seite **Create Configuration** Werte für alle in diesem StyleBook definierten Parameter ein.
4. Klicken Sie auf das Symbol neben dem Feld **Expressions**. Die Seite **Create an expression** wird angezeigt.

5. Verwenden Sie unter **Create an expression** die intuitiven Dropdown-Menüs, um Ihren Richtlinienausdruck zu erstellen. Klicken Sie auf **Submit**.

   Wenn Sie einen benutzerdefinierten Richtlinienausdruck erstellen möchten, klicken Sie auf **EPA Editor** oder **Expression Editor**, um Ihre Ausdrücke zu erstellen. Überprüfen Sie Ihre Ausdrücke unter **Preview Expressions** und klicken Sie dann auf **Submit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Wählen Sie die Ziel-NetScaler-Instanz aus, auf der die Konfiguration bereitgestellt werden soll, und klicken Sie auf **Senden**.

In-Place-Interpolationen

Es ist nun möglich, Teile einer Zeichenfolge mithilfe eines StyleBook-Ausdrucks zu ersetzen. Wenn diese Zeichenfolgenausdrücke vom StyleBook-Compiler ausgewertet werden, wird der Teil der Zeichenfolge, der einen StyleBook-Ausdruck verwendet, durch einen Wert des Ausdrucks ersetzt. Um StyleBook-Ausdrücke in eine Zeichenfolge aufzunehmen, verwenden wir die folgende Notation:

```
"...%{...}%..."
```

Wobei die Zeichen, die zwischen „%{“ und „}%“ eingeschlossen sind, einen StyleBook-Ausdruck bilden. Diese Ausdrücke werden als „In-Place-Interpolationen“ bezeichnet.

Zum Beispiel ist die Zeichenfolge `lb-%{$parameters.appname}%-svc` ein Zeichenfolgenausdruck mit einer In-Place-Interpolation eines StyleBook-Ausdrucks. Der Wert des Zeichenfolgenausdrucks hängt vom Wert des Interpolationsausdrucks ab. Angenommen, **$parameters.appname** ist mit „app1“ zugewiesen. Dann wird der Zeichenfolgenausdruck zu **lb-app1-svc** ausgewertet. Dies ermöglicht, dass die Werte nicht fest in Zeichenfolgenausdrücken kodiert sind, sondern basierend auf den benutzerdefinierten Werten ausgewertet werden.

Ein praktischer Anwendungsfall von In-Place-Interpolationen ist die Parametrisierung von Richtlinienausdrücken in StyleBooks. Stellen Sie sich ein Szenario vor, in dem Sie einen Richtlinienausdruck schreiben möchten, der prüft, ob die HTTP-URL ein bestimmtes Wort, z. B. „jpeg“, enthält.

Dazu schreiben Sie einen Richtlinienausdruck wie folgt: „HTTP.REQ.URL.CONTAINS(\\"jpeg\\")“.

Wenn Sie nun das Objekt in der HTTP-URL parametrisieren möchten, können Sie einen Zeichenfolgenparameter im StyleBook hinzufügen, z. B. `$parameters.url-object`. Der Richtlinienausdruck wird basierend auf diesem Parameter geschrieben. Dazu verwenden Sie die Zeichenfolgenverkettung, um das Ergebnis zu erzielen. Der Ausdruck würde wie folgt aussehen:

```
str("HTTP.REQ.URL.CONTAINS(\\"" + $parameters.url-object + "\\")")
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn `$parameter.url-object` „csv“ zugewiesen ist, wird der obige Ausdruck zu „HTTP.REQ.URL.CONTAINS(\\"csv\\")“ ausgewertet. Dieser Ausdruck ist jedoch nicht leicht zu lesen. Um diese Parametrisierung leichter lesbar und verständlich zu machen, können Sie In-Place-Interpolationen verwenden.

Der Ausdruck mit In-Place-Interpolation lautet nun:

```
str("HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)")
```

Im obigen Ausdruck haben Sie einen Interpolationsausdruck verwendet, der die inneren Anführungszeichen um den Wert des $parameters.url-Objekts hinzufügt. Das Ergebnis dieses Ausdrucks ist dasselbe wie oben, aber es sieht intuitiver und näher am tatsächlichen Ergebnis aus.

Zulässige Typen innerhalb von Interpolationen

Sie können Ausdrücke verwenden, die einen Wert der folgenden Typen innerhalb von Interpolationen erzeugen: Boolean, Zahl, `tcp-port`, `ipaddress` und Zeichenfolge. Der generierte Wert wird automatisch in eine Zeichenfolge umgewandelt, wenn die Interpolationen durch das Ergebnis ersetzt werden.

Zeichenfolgenausdrücke können 0, 1 oder mehr Interpolationen enthalten. Bei einer sequenziellen Interpolation können verschiedene Teile des Zeichenfolgenausdrucks durch verschiedene StyleBook-Ausdrücke ersetzt werden. Zum Beispiel gibt die Zeichenfolge lb-%{$parameters.appname}%-%{$parameters.vip}% „lb-app1-1.1.1.1“ zurück, wenn $parameters.appname „app1“ und $parameters.vip „1.1.1.1“ ist.

Zeichenfolgenausdrücke unterstützen auch verschachtelte Interpolationen. Das heißt, ein Interpolationsausdruck kann in einem anderen Interpolationsausdruck verschachtelt werden, sodass der Wert eines Ausdrucks zu einer Eingabe für den zweiten Ausdruck werden kann.

Betrachten Sie zum Beispiel eine Zeichenfolge „%{lb-%{$parameters.port + 1}%}%“

Die interne Zeichenfolge „**%{$parameters.port + 1}%**“ gibt „lb-81“ zurück, wenn $parameters.port 80 ist. Hier ist dieser Ausdruck in einem anderen Interpolationsausdruck verschachtelt.

Die folgende Tabelle beschreibt die verschiedenen Arten von Interpolationen mit Beispielen und entsprechenden Ergebnissen. Der Wert der in den Beispielen verwendeten Parameter ist:

- $parameters.appname: "lb1"
- $parameters.vip: "1.1.1.1"
- $parameters.n1: 1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- $parameters.n2: 3

Einfache Interpolationen

AUSDRUCK	ERGEBNIS
`lb-%{$parameters.appname}%-def`	`lb-lb1-def`

Automatische Typumwandlungen

AUSDRUCK	ERGEBNIS
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-%{true}%	lb-True

Sequenzielle Interpolationen

AUSDRUCK	ERGEBNIS
%{$parameters.appname}%-%{str($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

Verschachtelte Interpolationen

AUSDRUCK	ERGEBNIS
`%{abc-%{$parameters.n1 + 1}%}%`	`abc-2`
`str("%{abc-%{$parameters.n1}%}%-%{$parameters.n2}%")`	`bc-1-3`

Interpolationen mit `quotewrap`

AUSDRUCK	ERGEBNIS
`str("%{quotewrap(abcd)}%")`	`\"abcd`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

AUSDRUCK	ERGEBNIS
`str("%{quotewrap(https://)}% +HTTP.REQ.HOSTNAME+HTTP.REQ.URL")`	`<https://"+HTTP.REQ.HOST NAME+HTTP.REQ.URL`

Escape-Zeichen in Interpolationen

Wenn die Zeichen "%{" oder "}%" Teil der Zeichenfolge sind, müssen Sie "`\`" als Escape-Zeichen angeben, damit der StyleBook-Compiler diese nicht als Interpolations-Tags auswertet.

Beispiel:

`str("%{\%\{ + str($parameters.vip) + \}\%}%") returns "%{1.1.1.1}%" if $parameters.vip is 1.1.1.1`

Die folgende Tabelle beschreibt einige weitere Ausdrücke und deren Ergebnisse:

KATEGORIE	AUSDRUCK	ERGEBNIS
Maskieren von Interpolationen	`str("% {str($parameters.n1) + \}\%}%")`	`1}%`
	`lb-% {str($parameters.n1) + \}\%}%`	`lb-1}%`
	`"%{str($parameters.n1) + \\"\\}\\%\\"}%"|1}%`	

Integrierte Funktionen

Ausdrücke in StyleBooks können integrierte Funktionen verwenden.

Zum Beispiel können Sie die integrierte Funktion `str()` verwenden, um eine Zahl in eine Zeichenfolge umzuwandeln.

`str($parameters.order)`

Oder Sie können die integrierte Funktion `int()` verwenden, um eine Zeichenfolge in eine Ganzzahl umzuwandeln.

`int($parameters.priority)`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Im Folgenden finden Sie eine Liste der in StyleBook-Ausdrücken unterstützten integrierten Funktionen mit Beispielen für deren Verwendung:

Zeichenkette()

Die Funktion `str()` wandelt das Eingabeargument in einen Zeichenfolgenwert um.

Zulässige Argumenttypen:

- `string`
- `number`
- `tcp-port`
- `boolean`
- `ipaddress`

Beispiele:

- Die `"set-" + str(10)` Funktion gibt `"set-10"` zurück.
- Die `str(10)` Funktion gibt `10` zurück.
- Die `str(1.1.1.1)` Funktion gibt `1.1.1.1` zurück.
- Die `str(True)` Funktion gibt `"True"` zurück.
- Die `str(NetScaler Console)` Funktion gibt `"NetScaler Console"` zurück.

Ganzzahl()

Die `int()` Funktion akzeptiert eine Zeichenfolge, Zahl, IP-Adresse oder `tcpport` als Argument und gibt eine Ganzzahl zurück.

Beispiele:

- Die `int("10")` Funktion gibt `10` zurück.
- Die `int(10)` Funktion gibt `10` zurück.
- Die `int(ip('0.0.4.1'))` Funktion gibt `1025` zurück.

BoolescherWert()

Die `bool()` Funktion akzeptiert einen beliebigen Typ als Argument. Wenn der Argumentwert `false`, leer oder nicht vorhanden ist, gibt diese Funktion `false` zurück.

Andernfalls gibt sie `true` zurück.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Beispiele:

- Die Funktion `bool(true)` gibt `true` zurück.
- Die Funktion `bool(false)` gibt `false` zurück.
- Die Funktion `bool($parameters.a)` gibt `false` zurück, wenn `$parameters.a` `false`, leer oder nicht vorhanden ist.

Länge()

Die Funktion `len()` akzeptiert eine Zeichenfolge oder eine Liste als Argument und gibt die Anzahl der Zeichen in einer Zeichenfolge oder die Anzahl der Elemente in einer Liste zurück.

Beispiel 1:

Wenn Sie eine Substitution wie folgt definieren:

```
items: ["123", "abc", "xyz"]
```

Die Funktion `len($substitutions.items)` gibt `3` zurück

Beispiel 2:

Die Funktion `len("NetScaler Console")` gibt `10` zurück.

Beispiel 3:

Wenn `$parameters.vips` die Werte `['1.1.1.1', '1.1.1.2', '1.1.1.3']` hat, gibt die Funktion `len($parameters.vips)` `3` zurück.

Minimum()

Die `min()` Funktion nimmt entweder eine Liste oder eine Reihe von Zahlen oder TCP-Ports als Argumente entgegen und gibt das kleinste Element zurück.

Beispiele mit einer Reihe von Zahlen/TCP-Ports:

- Die `min(80, 100, 1000)` Funktion gibt `80` zurück.
- Die `min(-20, 100, 400)` Funktion gibt `-20` zurück.
- Die `min(-80, -20, -10)` Funktion gibt `-80` zurück.
- Die `min(0, 100, -400)` Funktion gibt `-400` zurück.

Beispiele mit einer Liste von Zahlen/TCP-Ports:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Support `$parameters.ports` ist eine Liste von TCP-Ports und hat die Werte: `[80, 81, 8080]`.

  Die `min($parameters.ports)` Funktion gibt `80` zurück.

Maximum()

Die `max()` Funktion nimmt entweder eine Liste oder eine Reihe von Zahlen oder TCP-Ports als Argumente entgegen und gibt das größte Element zurück.

Beispiele mit einer Reihe von Zahlen/TCP-Ports:

- Die `max(80, 100, 1000)` Funktion gibt `1000` zurück.
- Die `max(-20, 100, 400)` Funktion gibt `400` zurück.
- Die `max(-80, -20, -10)` Funktion gibt `-10` zurück.
- Die `max(0, 100, -400)` Funktion gibt `100` zurück.

Beispiele mit einer Liste von Zahlen/TCP-Ports:

- Unterstützung `$parameters.ports` ist eine Liste von TCP-Ports und hat die Werte: `[80, 81, 8080]`.

  Die `max($parameters.ports)` Funktion gibt `8080` zurück.

bin()-Funktion

Die `bin()` Funktion nimmt eine Zahl als Argument und gibt eine Zeichenfolge zurück, die die Zahl im Binärformat darstellt.

Beispiele für Ausdrücke:

Die `bin(100)` Funktion gibt `0b1100100` zurück.

oct()-Funktion

Die `oct()` Funktion nimmt eine Zahl als Argument und gibt eine Zeichenfolge zurück, die die Zahl im Oktalformat darstellt.

Beispiele für Ausdrücke:

Die `oct(100)` Funktion gibt `0144` zurück.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

hex()-Funktion

Die `hex()` Funktion nimmt eine Zahl als Argument und gibt eine Kleinbuchstaben-Zeichenfolge zurück, die die Zahl im Hexadezimalformat darstellt.

Beispiele für Ausdrücke:

Die `hex(100)`-Funktion gibt `0x64` zurück.

klein()

Die `lower()`-Funktion akzeptiert eine Zeichenfolge als Argument und gibt dieselbe Zeichenfolge in Kleinbuchstaben zurück.

Beispiel:

Die `lower("NetScaler Console")`-Funktion gibt `NetScaler Console` zurück.

Großschreibung()

Die `upper()`-Funktion akzeptiert eine Zeichenfolge als Argument und gibt dieselbe Zeichenfolge in Großbuchstaben zurück.

Beispiel:

Die `upper("NetScaler Console")`-Funktion gibt `NetScaler Console` zurück.

Summe()

Die `sum()`-Funktion akzeptiert eine Liste von Zahlen oder `tcpports` als Argumente und gibt die Summe der Zahlen in der Liste zurück.

Beispiel 1:

Wenn Sie eine Substitution wie folgt definieren: substitutions:

```
list-of-numbers = [11, 22, 55]
```

Die `sum($substitutions.list-of-numbers)`-Funktion gibt `88` zurück.

Beispiel 2:

Wenn `$parameters.ports` `[80, 81, 82]` ist, gibt die Funktion `sum($parameters.ports)` `243` zurück.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

pow()-Funktion

Die Funktion `pow()` akzeptiert zwei Zahlen als Argumente und gibt eine Zahl zurück, die das erste Argument hoch der Potenz des zweiten Arguments darstellt.

Beispiel:

Die Funktion `pow(3,2)` gibt `9` zurück.

ip()

Die Funktion `ip()` akzeptiert eine Ganzzahl, einen String oder eine IP-Adresse als Argument und gibt die IP-Adresse basierend auf dem Eingabewert zurück.

Beispiele:

- Geben Sie eine IP-Adresse in der Funktion `ip` an:

  Die Funktion `ip(3.1.1.1)` gibt `3.1.1.1` zurück.
- Geben Sie einen String in der Funktion `ip` an:

  Die Funktion `ip('2.1.1.1')` gibt `2.1.1.1` zurück
- Geben Sie eine Ganzzahl in der Funktion `ip` an:
  - Die Funktion `ip(12)` gibt `0.0.0.12` zurück.
  - Wenn Sie eine Ganzzahl als Zeichenfolge in der `ip` Funktion angeben, gibt sie eine entsprechende IP-Adresse der Eingabe zurück.

    Die `ip('1025')` Funktion gibt `0.0.4.1` zurück.

  Diese Funktion unterstützt auch die Addition und Subtraktion von Ganzzahlen und gibt eine resultierende IP-Adresse zurück.

  - Addition: Die `ip(1025) + ip(12)` Funktion gibt `0.0.4.13` zurück.
  - Subtraktion: Die `ip('1025') - ip(12)` Funktion gibt `0.0.3.245` zurück.
  - Addition und Subtraktion kombinieren: Die `ip('1.1.1.1') + ip('1.1.1.1') – ip(2)` gibt `2.2.2.0` zurück.

ip_network()

Die `ip_network` Funktion akzeptiert IP-Adresse und Netzmaskenlänge als Argumente und gibt eine IP-Netzwerknotation zurück.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Beispiel-1:

Die `ip_network(1.1.1.1, 28)` Funktion gibt `1.1.1.1/28` zurück.

Beispiel-2:

Betrachten Sie den Wert `1.1.1.1` für `$parameters.ipaddr`. Die `ip_network($parameters.ipaddr, 30)` Funktion gibt `1.1.1.1/30` zurück.

Beispiel-3:

Betrachten Sie den Wert `24` für `$parameters.netmask-len`. Die `ip_network(23.1.12.76, $parameters.netmask-len)` Funktion gibt `23.1.12.76/24` zurück.

network_ip()

Die `network_ip()`-Funktion gibt die erste IP-Adresse des angegebenen IP-Netzwerks zurück.

Beispiel:

Die `network_ip(1.1.1.1/28)`-Funktion gibt `1.1.1.0` zurück. In diesem Beispiel ist `1.1.1.0` die erste IP-Adresse im angegebenen Netzwerk.

Subnetze()

Die `subnets()`-Funktion gibt die Liste der Subnetze aus dem angegebenen IP-Netzwerk und der Netmask-Länge zurück.

Beispiel:

Die `subnets(1.1.1.1/28, 30)`-Funktion gibt die Subnetzliste aus dem angegebenen IP-Netzwerk und der Netmask-Länge zurück. Die Ausgabe kann wie folgt aussehen:

```
[1.1.1.0/30', '1.1.1.4/30', '1.1.1.8/30', '1.1.1.12/30']
```

netmask_ip()

Die `netmask_ip()`-Funktion gibt die Netmask-IP-Adresse für das angegebene IP-Netzwerk zurück.

Beispiel:

Die `netmask_ip(1.1.1.1/28)`-Funktion gibt `255.255.255.240` zurück. Für das angegebene IP-Netzwerk ist `255.255.255.240` die Netmask-IP-Adresse.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

is_netmask_ip()

Die `is_netmask_ip()`-Funktion akzeptiert ein `ipaddress` als Eingabe. Und sie gibt `True` zurück, wenn der angegebene Wert eine gültige Netmask-IP-Adresse ist.

Beispiel 1:

Die `is_netmask_ip(255.255.255.240)` Funktion gibt `True` zurück, weil der angegebene Wert eine gültige Netzmasken-IP-Adresse ist.

Beispiel 2:

Die `is_netmask_ip(255.255.255.232)` Funktion gibt `False` zurück, weil der angegebene Wert keine gültige Netzmasken-IP-Adresse ist.

broadcast_ip()

Die `broadcast_ip()` Funktion gibt die Broadcast-IP-Adresse für das angegebene IP-Netzwerk zurück.

Beispiel:

Die `broadcast_ip(1.1.1.1/28)` Funktion gibt `1.1.1.15` zurück. Für das gegebene IP-Netzwerk ist `1.1.1.15` die Broadcast-IP-Adresse.

cidr()-Funktion

Die `cidr()` Funktion gibt die CIDR-Notation für das angegebene IP-Netzwerk zurück.

Beispiel:

Die `cidr(1.1.1.1/28)` Funktion gibt `1.1.1.0/28` zurück. Für das gegebene IP-Netzwerk ist `1.1.1.0/28` die CIDR-Notation.

is_cidr()

Die `is_cidr()` Funktion akzeptiert `ipnetwork` als Eingabe. Und sie gibt `True` zurück, wenn der angegebene Wert der CIDR-Notation des IP-Netzwerks entspricht.

Beispiel-1:

Die `is_cidr(1.1.1.0/24)` Funktion gibt `True` zurück, weil der angegebene Wert die CIDR-Notation des gegebenen Netzwerks ist.

Beispiel-2:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Funktion `is_cidr(1.1.1.1/28)` gibt `False` zurück, da die CIDR-Notation des angegebenen Netzwerks vom angegebenen Wert abweicht.

is_in_network()

Die Funktion `is_in_network()` akzeptiert die Werte `ipnetwork` und `ipaddress`. Und sie gibt `True` zurück, wenn die angegebene IP-Adresse im angegebenen IP-Netzwerk vorhanden ist.

Beispiel-1:

Die Funktion `is_in_network(1.1.1.1/24, 1.1.1.121)` gibt `True` zurück, da die Adresse `1.1.1.121` Teil des Netzwerks `1.1.1.1/24` ist.

Beispiel-2:

Die Funktion `is_in_network(1.1.1.1/28, 2.1.1.1)` gibt `Fasle` zurück, da die Adresse `2.1.1.1` nicht Teil des Netzwerks `1.1.1.1/28` ist.

base64.encode()

Die Funktion `base64.encode()` akzeptiert ein String-Argument und gibt den base64-kodierten String zurück.

Beispiel:

Die Funktion `base64.encode("abcd")` gibt `YWJjZA==` zurück.

base64.decode()

Die Funktion `base64.decode` akzeptiert einen base64-kodierten String als Argument und gibt den dekodierten String zurück.

Beispiel:

Die `base64.decode("YWJjZA==")`-Funktion gibt `abcd` zurück.

exists()-Funktion

Die `exists()`-Funktion akzeptiert ein Argument beliebigen Typs und gibt einen booleschen Wert zurück. Der Rückgabewert ist `True`, wenn die Eingabe einen Wert hat. Der Rückgabewert ist `False`, wenn das Eingabeargument keinen Wert hat (d. h. keinen Wert).

Beachten Sie, dass `$parameters.monitor` ein optionaler Parameter ist. Wenn Sie diesem Parameter beim Erstellen eines Konfigurationspakets einen Wert zuweisen, gibt die `($parameters.monitor)`-Funktion `True` zurück.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Andernfalls gibt sie `False` zurück.

Filterfunktion()

Die `filter()`-Funktion akzeptiert zwei Argumente.

Argument 1: eine Substitutionsfunktion, die ein Argument akzeptiert und einen booleschen Wert zurückgibt.

Argument 2: eine Liste.

Die Funktion gibt eine Untermenge der ursprünglichen Liste zurück, wobei jedes Element zu `True` ausgewertet wird, wenn es an die Substitutionsfunktion im ersten Argument übergeben wird.

Beispiel:

Angenommen, wir haben eine Substitutionsfunktion wie folgt definiert.

Substitutionen:

```
x(a): $a != 81
```

Diese Funktion gibt True zurück, wenn der Eingabewert nicht gleich `81` ist. Andernfalls gibt sie `False` zurück.

Angenommen, `$parameters.ports` ist `[81, 80, 81, 89]`.

Die `filter($substitutions.x, $parameters.ports)` gibt `[80, 89]` zurück, indem alle Vorkommen von `81` aus der Liste entfernt werden.

if-then-else()

Die Funktion `if-then-else()` akzeptiert drei Argumente.

Argument 1: ein boolescher Ausdruck

Argument 2: beliebiger Ausdruck

Argument 3: beliebiger Ausdruck (optional)

Wenn der Ausdruck in Argument 1 zu `True` ausgewertet wird, gibt die Funktion den Wert des als Argument 2 angegebenen Ausdrucks zurück.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Andernfalls, wenn Argument 3 angegeben ist, gibt die Funktion den Wert des Ausdrucks in Argument 3 zurück.

Wenn Argument 3 nicht angegeben ist, gibt die Funktion `no` zurück.

Beispiel 1:

Die Funktion `if-then-else($parameters.servicetype == HTTP, 80, 443)` gibt `80` zurück, wenn `$parameters.servicetype` den Wert `HTTP` hat. Andernfalls gibt die Funktion `443` zurück.

Beispiel 2:

Die Funktion `if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` gibt den Wert von `$parameters.hport` zurück, wenn `$parameters.servicetype` den Wert `HTTP` hat.

Andernfalls gibt die Funktion den Wert von `$parameters.sport` zurück.

Beispiel 3:

Die `if-then-else($parameters.servicetype == HTTP, 80)` gibt `80` zurück, wenn `$parameters.servicetype` den Wert `HTTP` hat.

Andernfalls gibt die Funktion keinen Wert zurück.

Verbinden()

Die Funktion `join()` akzeptiert zwei Argumente:

Argument 1: eine Liste von `number`, `tcp-port`, `string`, `ipaddress`

Argument 2: eine Trennzeichenfolge (optional)

Diese Funktion verbindet die Elemente der als Argument 1 angegebenen Liste zu einer Zeichenfolge, wobei jedes Element durch die als Argument 2 angegebene Trennzeichenfolge getrennt wird. Wenn Argument 2 nicht angegeben wird, werden die Elemente in der Liste zu einer Zeichenfolge verbunden.

Beispiel:

- `$parameters.ports` ist `[81, 82, 83]`.
    - Mit Trennzeichen-Argument:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Funktion `join($parameters.ports, '-')` gibt `81-82-83` zurück.

- Ohne Trennzeichen-Argument:

Die Funktion `join($parameters.ports)` gibt `818283` zurück.

Teilen()

Die `split()`-Funktion teilt eine Eingabezeichenfolge in mehrere Listen auf, abhängig von den angegebenen Trennzeichen. Wenn kein oder ein leeres (`''`) Trennzeichen angegeben ist, betrachtet diese Funktion ein Leerzeichen als Trennzeichen und teilt die Zeichenfolge in Listen auf.

Beispiele:

- Die `split('Example_string_split', 's')`-Funktion gibt `['Example_','tring_','plit']` zurück.
- Die `split('Example string split')`-Funktion gibt `['Example','string','split']` zurück.
- Die `split('Example string split', '')`-Funktion gibt `['Example','string','split']` zurück.
- Die `split('Example string')`-Funktion gibt `['Example','string']` zurück.

  Diese Funktion betrachtet aufeinanderfolgende Leerzeichen als ein einziges Leerzeichen.

abbilden()

Die `map()`-Funktion benötigt zwei Argumente;

Argument 1: eine beliebige Funktion

Argument 2: eine Liste von Elementen

Die Funktion gibt eine Liste zurück, wobei jedes Element in der Liste das Ergebnis der Anwendung der `map()`-Funktion (Argument 1) auf das entsprechende Element in Argument 2 ist.

Zulässige Funktionen in Argument 1:

- Integrierte Funktionen, die ein Argument benötigen:

  `base64.encode, base64.decode, bin, bool, exists, hex, int, ip, len, lower, upper, oct, quotewrap, str, trim, upper, url.encode, url.decode`

- Substitutionsfunktionen, die mindestens ein Argument annehmen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Beispiel:

Angenommen, $parameters.nums ist `[81, 82, 83]`.

- Zuordnen mit einer integrierten Funktion, str

  Die Funktion `map(str, $parameters.nums)` gibt `["81", "82", "83"]` zurück

  Das Ergebnis der Map-Funktion ist die Liste von Zeichenfolgen, wobei jedes Element durch Anwenden der str-Funktion auf das entsprechende Element in der Eingabeliste ($parameters.nums) berechnet wird.
- Zuordnen mit einer Substitutionsfunktion
  - Substitutionen:

    `add-10(port): $port + 10`
  - Ausdruck:

    Die Funktion `map($substitutions.add-10, $parameters.nums)` gibt eine Liste von Zahlen zurück: `[ 91, 92, 93 ]`

Das Ergebnis dieser Map-Funktion ist eine Liste von Zahlen. Jedes Element wird durch Anwenden der Substitutionsfunktion `$substitutions.add-10` auf das entsprechende Element in der Eingabeliste `($parameters.nums)` berechnet.

Zitieren()

Die Funktion `quotewrap()` nimmt eine Zeichenfolge als Argument und gibt eine Zeichenfolge zurück, nachdem ein doppeltes Anführungszeichen vor und nach dem Eingabewert hinzugefügt wurde.

Beispiel:

Die `quotewrap("NetScaler Console")`-Funktion gibt `"NetScaler Console"` zurück.

ersetzen()

Die `replace()`-Funktion akzeptiert drei Argumente:

Argument 1: ein `string` oder eine Liste der folgenden integrierten Typen:

- `string`
- `number`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `ipaddress`
- `tcp-port`
- `boolean`

Argument 2: ein einzelner Wert oder eine Liste von Werten, deren Typ mit dem in Argument 1 angegebenen Typ übereinstimmt

Argument 3: ein einzelner Wert desselben Typs wie in Argument 1 angegeben (optional)

Die `replace()`-Funktion ersetzt alle Vorkommen von Argument 2 durch Argument 3 in Argument 1.

Wenn Argument 3 nicht angegeben wird, werden alle Vorkommen von Argument 2 aus Argument 1 entfernt.

Beispiel:

- `replace('abcdef', 'def', 'xyz')`-Funktion gibt `abcxyz` zurück.

  Alle Vorkommen von `def` werden durch `xyz` ersetzt.
- `replace('abcdefabc', 'def')` gibt `abcabc` zurück.

  Da kein Argument 3 vorhanden ist, wird `def` aus der resultierenden Zeichenfolge entfernt.
- Die Funktion `replace('An#example@to%replace!characters', ['@', '#', '!', '%'], '_')` gibt `An_example_to_replace_characters` zurück.

  Die Ausgabestrings haben einen Unterstrich (_) anstelle der in `['@', '#', '!', '%']` angegebenen Zeichen.
- Die Funktion `replace([10.10.10.1, 10.10.10.2, 10.10.10.3, 10.10.10.4], [10.10.10.2, 10.10.10.4])` gibt `[10.10.10.1, 10.10.10.3]` zurück.

  Da kein Argument 3 vorhanden ist, werden `10.10.10.2` und `10.10.10.4` aus der resultierenden Liste der IP-Adressen entfernt.
- Die Funktion `replace([8080, 8081, 8082, 8083, 8084], 8083, 80)` gibt `[8080, 8081, 8082, 80, 8084]` zurück.

  Alle Vorkommen von `8083` werden durch `80` ersetzt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

trimmen()

Die Funktion `trim()` gibt eine Zeichenfolge zurück, bei der führende und nachgestellte Leerzeichen aus der Eingabezeichenfolge entfernt wurden.

Beispiel:

Die Funktion `trim(' abc ')` gibt `abc` zurück.

kürzen()

Die Funktion `truncate()` akzeptiert zwei Argumente:

Argument 1: eine Zeichenfolge

Argument 2: eine Zahl

Die Funktion gibt eine Zeichenfolge zurück, bei der die Eingabezeichenfolge in Argument 1 auf die durch Argument 2 angegebene Länge gekürzt wird.

Beispiel:

`truncate('Stylebooks', 6)` gibt `Styleb` zurück.

eindeutig()

Die Funktion `distinct()` extrahiert eindeutige Elemente aus einer Listeneingabe.

Beispiele: Wenn `$parameters.input_list` `['ADC', 'VPX', 'ADC', 'CPX']` ist, gibt die Funktion `distinct($parameters.input_list)` `['ADC', 'VPX', 'CPX']` zurück.

url.encode()

Die Funktion `url.encode()` gibt eine Zeichenfolge zurück, bei der Zeichen gemäß RFC 3986 mithilfe des ASCII-Zeichensatzes transformiert werden.

Beispiel:

Die Funktion `url.encode("a/b/c")` gibt `a%2Fb%2Fc` zurück.

url.decode()

Die Funktion `url.decode()` gibt eine Zeichenfolge zurück, bei der das URL-kodierte Argument gemäß RFC 3986 in eine reguläre Zeichenfolge dekodiert wird.

Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die `url.decode("a%2Fb%2Fc")` Funktion gibt `a/b/c` zurück.

is-ipv4()

Die `is-ipv4()` Funktion akzeptiert eine IP-Adresse als Argument und gibt den booleschen Wert `True` zurück, wenn die IP-Adresse im IPv4-Format vorliegt.

Die `is-ipv4(10.10.10.10)` Funktion gibt `True` zurück

is-ipv6()

Die `is-ipv6()` Funktion akzeptiert eine IP-Adresse als Argument und gibt den booleschen Wert `True` zurück, wenn die IP-Adresse im IPv6-Format vorliegt.

Die `is-ipv6(2001:DB8::)` Funktion gibt `True` zurück

beginntMit()

Die `startswith()` Funktion bestimmt, ob eine Zeichenfolge mit einem bestimmten Präfix beginnt. Diese Funktion erfordert zwei obligatorische Zeichenfolgenargumente.

```
startswith(str, sub_str)
```

Diese Funktion gibt `True` zurück, wenn die Zeichenfolge (`str`) mit der Unterzeichenfolge (`sub_str`) beginnt.

Beispiele:

- Die `startswith('Citrix', 'Ci')` Funktion gibt `True` zurück.
- Die `startswith('Citrix', 'iC')` Funktion gibt `False` zurück
- Die `startswith('Citrix', 'Ab')` Funktion gibt `False` zurück

endetMit()

Die `endswith()` Funktion bestimmt, ob eine Zeichenfolge mit einem bestimmten Suffix endet. Diese Funktion erfordert zwei obligatorische Zeichenfolgenargumente.

```
endswith(str, sub_str)
```

Diese Funktion gibt `True` zurück, wenn die Zeichenfolge (`str`) mit der Unterzeichenfolge (`sub_str`) endet.

Beispiele:

- Die `endswith('Citrix', 'ix')` Funktion gibt `True` zurück.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die `endswith('Citrix', 'Ix')` Funktion gibt `False` zurück.
- Die `endswith('Citrix', 'ab')` Funktion gibt `False` zurück.

enthält()

Die `contains()` Funktion bestimmt, ob eine Zeichenfolge eine bestimmte Unterzeichenfolge enthält. Diese Funktion erfordert zwei obligatorische Zeichenfolgenargumente.

Zulässige Argumenttypen:

- `string`
- `number`
- `tcp-port`
- `boolean`
- `ipaddress`

`contains(str, sub_str)`

Diese Funktion gibt `True` zurück, wenn der Unterstring (`sub_str`) irgendwo im String (`str`) enthalten ist.

Beispiele:

- Die `contains('Citrix', 'tri')` Funktion gibt `True` zurück.
- Die `contains('Citrix', 'Ci')` Funktion gibt `True` zurück.
- Die `contains('Citrix', 'ti')` Funktion gibt `False` zurück

Sie können diese Funktion auch verwenden, um zu überprüfen, ob ein bestimmtes Element zur Liste gehört.

Beispiel:

```
list_of_strings = [“Citrix”, “Core”, ”Values”, ”Integrity”]



contains($parameters.list_of_strings, “Values”)
```

In diesem Beispiel gibt die `contains()` Funktion `True` zurück, weil die Liste das Element `Values` enthält.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Teilstring()

Verwenden Sie die `substring()` Funktion, um einen Unterstring aus einem String zu extrahieren.

```
substring(str, start_index, end_index)
```

Diese Funktion erfordert die zwei obligatorischen Argumente und ein optionales Integer-Argument.

- `str` (Obligatorisch)
- `start_index` (Obligatorisch)
- `end_index` (Optional)

Diese Funktion gibt den Teilstring aus dem String (`str`) zurück, der sich zwischen den angegebenen Indexpositionen befindet. Wenn Sie die Endindexposition nicht angeben, extrahiert die Funktion den Teilstring vom Startindex bis zum Ende des Strings.

HINWEIS

Wenn Sie `end_index` angeben, schließt der Teilstring das Zeichen an der Position `end_index` aus.

Beispiel:

- Die Funktion `substring('Citrix', 2)` gibt `trix` zurück.
- Die Funktion `substring('Citrix', 10)` gibt (`''`) zurück.

  In diesem Beispiel gibt die Funktion einen leeren String zurück, da sie eine ungültige Position `start_index` hat.
- Die Funktion `substring('Citrix', 2, 4)` gibt `tr` zurück.

  In diesem Beispiel extrahiert die Funktion die Zeichen zwischen den Indexpositionen 2 und 4.
- Die Funktion `substring('Citrix', -3)` gibt `rix` zurück.

  Wenn Sie Zeichen extrahieren möchten, die sich am Ende des Strings befinden, geben Sie einen negativen Wert für das Argument `start_index` an.

  In diesem Beispiel extrahiert die Funktion den Teilstring, der die letzten drei Zeichen im String enthält.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Abgleichen()

Die `match()`-Funktion prüft, ob eine Eingabezeichenfolge dem definierten regulären Ausdrucksmuster entspricht. Diese Funktion akzeptiert reguläre Ausdrucksmuster und Suchzeichenfolgen als Argumente. Optional können Sie auch einen booleschen Typ angeben, um die Groß-/Kleinschreibung von Mustern zu ignorieren.

Beispiele:

- Die `match("\^[A-Z0-9]{2}_[A-Z0-9]{2,10}$", "A2_B2")` gibt `True` zurück.
- Die `match("\^[A-Z0-9]{2}_[A-Z0-9]{2,10}$", "a2_b2")` gibt `False` zurück.
- Die `match("\^[A-Z0-9]{2}_[A-Z0-9]{2,10}$", "a2_B2", $parameters.ignore_case)` gibt `True` zurück.

sha256()

Verwenden Sie diese Funktion, um den SHA-256-Hash für eine beliebige Zeichenfolge zu berechnen. Diese Funktion akzeptiert eine Zeichenfolgeneingabe beliebiger Länge und gibt eine Hash-Zeichenfolge fester Länge (64 Zeichen) zurück.

Beispiel:

```
components:

    -

        name: lbvserver-comp

        type: ns::lbvserver

        properties:

            name: sha256(lbserver-name)

            servicetype: SSL

            ipv46: 10.10.10.10
```

In diesem Beispiel erscheint `lbserver-name` als Hash-Zeichenfolge auf dem NetScaler-Objekt.

Diese Funktion kann auch Ausdrücke als Eingabe akzeptieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Beispiel:

```
components:

    -

        name: lbvserver-comp

        type: ns::lbvserver

        properties:

            name: sha256($parameters.lb-appname)

            servicetype: SSL

            ipv46: 10.10.10.10
```

verknüpfen()

Die `relate()`-Funktion erstellt eine Liste von Wörterbuchobjekten aus einer Reihe von Listen.

Sie akzeptiert zwei Argumente:

Argument 1: Eine Liste von Zeichenfolgen, die Schlüsselnamen darstellen.

Argument 2: Eine Liste von Listen, wobei jede Liste die Werte der entsprechenden Schlüsselnamen in Argument 1 enthält. Jede Liste in Argument 2 muss die gleiche Länge haben. Die Anzahl der Listen in Argument 2 sollte der Anzahl der Zeichenfolgen in Argument 1 entsprechen.

Beispiel:

```
name: test_relate_3

description: "Hello World StyleBook."

namespace: com.citrix.adc.stylebooks

schema-version: "1.0"

version: "1.1"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
import-stylebooks:
    -
        namespace: netscaler.nitro.config
        prefix: ns
        version: "10.5"
    -
        namespace: com.citrix.adc.stylebooks
        prefix: stlb
        version: "1.0"
        parameters:
    -
        name: namesofservers
        description: "Provide the names of LB VServers"
        type: string[]
    -
        name: listofips
        description: "Provide the list of IP Addresses"
        type: string[]
    -
        name: list_of_keys
        type: string[]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        default:

        - "name"

        - "ip"



    substitutions:

        list_of_values: [$parameters.namesofservers,$parameters.listofips]

    components:

    -

        name: svc-comp

        type: object

        properties:

        svcdetails: relate($parameters.list_of_keys,
$substitutions.list_of_values)



    -

        name: lb-comp

        type: ns::lbvserver

        repeat: $components.svc-comp.properties.svcdetails

        repeat-item: svcd

        properties:

            name: $svcd['name']

            servicetype: HTTP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            ipv46: $svcd['ip']

            port: 80
```

In diesem Beispiel:

- Der Abschnitt `parameters` enthält eine Liste namens `list_of_keys`, die `name` und `ip` enthält.
- Der Abschnitt `substitutions` enthält eine Liste namens `list_of_values`, die die folgenden zwei Listen enthält:
  - Eine Liste von Namen virtueller Server (`string`)
  - Eine Liste von IP-Adressen (`string`).

Die integrierte Funktion `relate()` akzeptiert `list_of_keys` und `list_of_values` als Argumente. Die Funktion erstellt dann eine Liste von Wörterbuchobjekten, wobei jedes Objekt einen Namen aus der ersten Liste und eine IP-Adresse aus der zweiten Liste hat.

Wenn Sie die folgende Liste virtueller Server bereitstellen:

```
["lb1","lb2"]
```

und eine Liste von IP-Adressen virtueller Server als:

```
["1.1.1.1","2.2.3.3"]
```

Die Funktion `relate()` gibt dann die folgenden Listen zurück:

```
[\{"name": "lb1", "ip": "1.1.1.1"},\{"name": "lb2", "ip": "2.2.3.3"}]
```

Das StyleBook iteriert über diese Liste von Wörterbuchobjekten im Abschnitt `components`, um die entsprechenden virtuellen Server zu erstellen.

mehrere()

Die Funktion `multiple()` akzeptiert zwei Argumente:

Argument 1: ein `number`, `string`, `boolean`, `ipaddress`, `tcp-port` oder `password`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Argument 2: ein `number`

Die Funktion `multiple(argument1, argument2)` gibt eine Liste mit vielen Kopien von Argument 1 zurück. Die Anzahl der Kopien entspricht der Zahl, die an Argument 2 übergeben wurde.

Beispiele:

- Die Funktion `multiple(10.10.10.10, 3)` gibt `[10.10.10.10, 10.10.10.10, 10.10.10.10]` zurück.
- Die Funktion `multiple(8080, 4)` gibt `[8080, 8080, 8080, 8080]` zurück.

umkehren()

Die Funktion reverse() nimmt eine Liste von Elementen als Argument entgegen und gibt eine Liste mit denselben Elementen, aber in umgekehrter Reihenfolge, zurück.

Das Argument kann eine Liste der folgenden integrierten Typen sein:

- String
- Zahl
- IP-Adresse
- IP-Netzwerk
- TCP-Port
- Boolescher Wert
- Passwort
- Objekt
- Datei
- Zertifikatsdatei
- Schlüsseldatei
- Zertifikatsschlüssel

Beispiele:

- reverse() gibt zurück.
- reverse() gibt zurück.
- reverse() gibt zurück.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Abhängigkeitserkennung

Komponenten in einem StyleBook können sich auf Eigenschaften oder Abschnitte anderer Komponenten im selben StyleBook beziehen. Komponenten sind eigenständige Blöcke und müssen nicht in der Reihenfolge geschrieben werden, in der sie ausgeführt werden sollen. Der StyleBook-Compiler prüft die Reihenfolge, in der die Komponenten geschrieben sind, und führt sie dann in einer logischen Reihenfolge aus.

Beispiel:

```
components:


  -


    name: lbvserver-comp


    type: ns::lbvserver


    properties:


      name: mylb


      ipv46: 10.102.190.15


      port: 80


      servicetype: HTTP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-
    name: lb-sg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    condition: $parameters.create-binding

    properties:

      name: $components.lbvserver-comp.properties.name

      servicegroupname: $components.sg-comp.properties.servicegroupname

-
    name: sg-comp

    type: ns::servicegroup

    properties:

      servicegroupname: mysg
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      servicetype: HTTP
```

Im obigen Beispiel sind drei Komponenten definiert: **lbvserver-comp**, **lb-sg-binding-comp** und **sg-comp**. Wenn Sie dieses StyleBook ausführen, wird zuerst `lbvserver-comp` erstellt. `lb-sg-binding-comp` bezieht sich auf `lbvserver-comp`-Eigenschaften, kann aber nicht als Nächstes erstellt werden, obwohl es die zweite im StyleBook definierte Komponente ist. Dies liegt daran, dass `lb-sg-binding-comp` auch eine Abhängigkeit von `sg-comp` hat, das noch erstellt werden muss. Infolgedessen ordnet der Compiler die Komponenten neu an, sodass die Abhängigkeiten einer Komponente zum Zeitpunkt ihrer Erstellung aufgelöst werden, und führt diese neu angeordnete Liste von Komponenten aus. Die Ausführungsreihenfolge des obigen StyleBooks ist: `lbvserver-comp`, `sg-comp` und `lb-sg-binding-comp`.

Somit muss sich der Autor eines StyleBooks keine Gedanken über die korrekte Reihenfolge der Komponenten machen. Die Komponenten können in beliebiger Reihenfolge erscheinen. Der Compiler berechnet die korrekte Ausführungsreihenfolge der Komponenten basierend darauf, wie die Komponenten aufeinander verweisen. Beachten Sie, dass dies auch für Substitutions- und Ausgabeabschnitte gilt.

Zirkuläre Abhängigkeiten

Da eine Komponente auf eine andere Komponente verweisen kann, ist es möglich, dass ein Zyklus von Abhängigkeiten in der Definition des StyleBooks eingeführt wird. Zum Beispiel, wenn Komponente A auf eine in Komponente B definierte Eigenschaft verweist, die wiederum auf eine in Komponente A definierte Eigenschaft verweist. Diese Art von Abhängigkeit wird als zirkuläre Abhängigkeit bezeichnet. Zirkuläre Abhängigkeiten können nicht automatisch aufgelöst werden. Der Autor des StyleBooks korrigiert die StyleBook-Definition manuell, um solche zirkulären Abhängigkeiten zu eliminieren. Der Compiler kann zirkuläre Abhängigkeiten erkennen – falls vorhanden – und melden.

Das folgende Beispiel zeigt eine zirkuläre Abhängigkeit von Komponenten:

```
components:


  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: $components.lb-sg-binding-comp.properties.name

      ipv46: 10.102.190.15

      port: 80

      servicetype: HTTP

  -

    name: lb-sg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    condition: $parameters.create-binding
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:

      name: mylb

      servicegroupname: $components.sg-comp.properties.servicegroupname

  -

    name: sg-comp

    type: ns::servicegroup

    properties:

      servicegroupname: mysg

      servicetype: $components.lbvserver-comp.properties.servicetype
```

Im obigen Beispiel gibt es drei Komponenten: **lbvserver-comp**, **lb-sg-binding-comp** und **sg-comp**. Die Komponente `lbvserver-comp` hängt von den Komponenten `lb-sg-binding-comp` und `lb-sg-binding` ab. Und diese Komponenten hängen von `sg-comp` ab. Die Komponente `sg-comp` hängt von `lbvserver-comp` ab. Hier bildet sich ein Zyklus von Abhängigkeiten zwischen diesen Komponenten, der nicht automatisch aufgelöst werden kann. Infolgedessen kann

© 1997–2026 Citrix Systems, Inc. All rights reserved.

dieses StyleBook nicht ausgeführt werden. Der StyleBook-Compiler erkennt dies und verhindert, dass das StyleBook in NetScaler Console importiert wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sicherheit

Die Sicherheitsfunktionen der NetScaler Console bieten Einblick in die Sicherheitslage Ihrer Anwendungen. Sie können Sicherheitsmetriken überwachen, Sicherheitsverletzungen untersuchen, Ihre APIs schützen und Web Application Firewall (WAF)-Lernfunktionen und -Empfehlungen nutzen, um Ihre Sicherheitskonfiguration zu stärken.

Die folgenden Themen helfen Ihnen beim Überwachen und Verwalten der Anwendungssicherheit:

- Dashboard für Anwendungssicherheit
  - Einheitliches Sicherheits-Dashboard
- Sicherheitsverletzungen
  - Anwendungsübersicht
  - Alle Verletzungen
- API-Sicherheit
- WAF-Lernfunktionen
- WAF-Empfehlungen

Anwendungssicherheits-Dashboard

Das Dashboard **App-Sicherheit** bietet Ihnen einen Überblick über die Sicherheitsmetriken für die erkannten Anwendungen. Dieses Dashboard zeigt die Informationen zu Sicherheitsangriffen für die erkannten Anwendungen an, z. B. Synchronisierungsangriffe, Angriffe mit kleinem Fenster und DNS-Flood-Angriffe.

So zeigen Sie die Sicherheitsmetriken im App-Sicherheits-Dashboard an:

1. Navigieren Sie zu **Sicherheit > Sicherheits-Dashboard**.
2. Wählen Sie die Instanz-IP-Adresse aus der Instanzliste aus.

   Die Berichte enthalten die folgenden Informationen für jede Anwendung:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Bedrohungsindex**. Ein einstelliges Bewertungssystem, das die Kritikalität von Angriffen auf die Anwendung angibt. Je kritischer die Angriffe auf eine Anwendung sind, desto höher ist der Bedrohungsindex für diese Anwendung. Die Werte reichen von 1 bis 7.

  Der Bedrohungsindex basiert auf Angriffsinformationen. Die angriffsbezogenen Informationen, wie z. B. Verletzungstyp, Angriffskategorie, Standort und Clientdetails, geben einen Einblick in die Angriffe auf die Anwendung. Verletzungsinformationen werden nur dann an die NetScaler Console gesendet, wenn eine Verletzung oder ein Angriff auftritt. Viele Verstöße und Schwachstellen führen zu einem hohen Bedrohungsindexwert.
- **Sicherheitsindex**. Ein einstelliges Bewertungssystem, das angibt, wie sicher Sie die NetScaler-Instanzen konfiguriert haben, um Anwendungen vor externen Bedrohungen und Schwachstellen zu schützen. Je geringer die Sicherheitsrisiken für eine Anwendung sind, desto höher ist der Sicherheitsindex. Die Werte reichen von 1 bis 7.

  Der Sicherheitsindex berücksichtigt sowohl die Konfiguration der Anwendungsfirewall als auch die NetScaler-Systemsicherheitskonfiguration. Für einen hohen Sicherheitsindexwert müssen beide Konfigurationen stark sein. Wenn beispielsweise strenge Anwendungsfirewall-Prüfungen vorhanden sind, aber keine NetScaler-Systemsicherheitsmaßnahmen, wie z. B. ein starkes Kennwort für den nsroot-Benutzer, bereitgestellt werden, wird Anwendungen ein niedriger Sicherheitsindexwert zugewiesen.

Sie können Diskrepanzen anzeigen, die im **App Security Investigator** gemeldet wurden.

Details zum Bedrohungsindex

1 - Zeigt die IP-Adresse der NetScaler-Instanz an, für die Sie Details anzeigen können.

2 - Zeigt Details wie den Bedrohungsindex-Score, die Gesamtzahl der aufgetretenen Verstöße und die Gesamtzahl der blockierten Verstöße an.

3 – Zeigt den virtuellen Server der ausgewählten Instanz an.

4 – Zeigt die Sicherheitsverletzungen basierend auf Clients an. Das Diagramm des App Security Investigator wird für jeden Client angezeigt. Sie können auf jede Client-IP klicken, um die Ergebnisse anzuzeigen.

5 – Zeigt die Verletzungen in der Kartenansicht und in der Tabellenansicht an.

6 – Zeigt die Details der Verletzung an. Wenn Sie den Mauszeiger über das Diagramm bewegen, werden Details wie Verletzungstyp, Angriffszeit und Gesamtereignisse angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Sie auf ein Blasendiagramm klicken, werden die Details auf der Seite **App Security Violation Details** angezeigt. Wenn Sie beispielsweise weitere Details zu einer Cross-Site-Script-Verletzung anzeigen möchten, klicken Sie auf das Diagramm, das für **XSS** im **App Security Investigator** angezeigt wird.

Die **App Security Violation Details** werden mit Verletzungsdetails wie Angriffszeit, Angriffskategorie, Schweregrad, URL usw. angezeigt.

Sie können auch auf die Option **Einstellungen** klicken, um die Optionen auszuwählen, die Sie anzeigen möchten.

Details zum Sicherheitsindex

Nachdem Sie die Bedrohungsgefährdung einer Anwendung überprüft haben, möchten Sie feststellen, welche Anwendungssicherheitskonfigurationen vorhanden sind und welche Konfigurationen für diese Anwendung fehlen. Sie können diese Informationen erhalten, indem Sie die Zusammenfassung des Anwendungssicherheitsindex detailliert untersuchen.

Die Zusammenfassung des Sicherheitsindex gibt Ihnen Informationen über die Wirksamkeit der folgenden Sicherheitskonfigurationen:

- **Anwendungs-Firewall-Konfiguration**. Zeigt an, wie viele Signatur- und Sicherheitseinheiten nicht konfiguriert sind.
- **NetScaler Console System Security**. Zeigt an, wie viele Systemsicherheitseinstellungen nicht konfiguriert sind.

Um die Details des **Sicherheitsindex** anzuzeigen, wählen Sie einen virtuellen Server/eine Anwendung aus und klicken Sie auf die Registerkarte **Sicherheitsindex**.

Die Details werden angezeigt.

1 – Zeigt die detaillierten Informationen für Application Firewall-Konfigurationen an.

2 – Zeigt die detaillierten Informationen zur Systemsicherheit an. Klicken Sie auf jede Sicherheitsgruppe, um Details zu Status und Citrix-Empfehlungen zu erhalten.

3 – Zeigt die Zusammenfassung für Sicherheitsprüfung und Signaturverletzung an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können auch eine Zusammenfassung der Bedrohungsumgebung anzeigen, indem Sie das security insight für virtuelle Server aktivieren und dann zu **Sicherheit > Sicherheitsverletzungen** navigieren. Weitere Informationen zum Anwendungsfall des Sicherheitsindex finden Sie unter security insight.

Einheitliches Sicherheits-Dashboard

Das **Einheitliche Sicherheits-Dashboard** ist ein zentrales Dashboard, in dem Sie Schutzmaßnahmen konfigurieren, Analysen aktivieren und die Schutzmaßnahmen für Ihre Anwendung bereitstellen können. In diesem Dashboard können Sie aus verschiedenen Vorlagenoptionen wählen und den gesamten Konfigurationsprozess in einem einzigen Workflow abschließen. Navigieren Sie zum Starten zu **Sicherheit > Sicherheits-Dashboard** und klicken Sie dann auf **Anwendung verwalten**. Auf der Seite **Anwendung verwalten** können Sie Details zu Ihren gesicherten und ungesicherten Anwendungen anzeigen.

HINWEIS:

- Wenn Sie ein neuer Benutzer sind oder noch keine Schutzmaßnahmen entweder über StyleBooks oder direkt auf NetScaler®-Instanzen konfiguriert haben, wird die folgende Seite angezeigt, nachdem Sie auf **Sicherheit > Sicherheits-Dashboard** geklickt haben.

- Sie können die Gesamtzahl der virtuellen Server anzeigen, die Schutz benötigen. Klicken Sie auf **Erste Schritte**, um Details unter **Ungesicherte Anwendungen** anzuzeigen.
- Die geeigneten virtuellen Servertypen zum Konfigurieren von Schutzmaßnahmen sind Lastausgleich und Content Switching.

Gesicherte Anwendungen

Sie können Details anzeigen, nachdem Sie Schutzmaßnahmen über das einheitliche Sicherheits-Dashboard konfiguriert haben. Weitere Informationen finden Sie unter Schutzmaßnahmen für ungesicherte Anwendungen konfigurieren.

Wenn Sie Schutzmaßnahmen bereits direkt auf den NetScaler-Instanzen oder über StyleBooks konfiguriert haben, können Sie die Anwendungen auf der Registerkarte **Gesicherte Anwendungen** anzeigen, die unter **Profil** als **Andere** gekennzeichnet sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schutzmaßnahmen für ungesicherte Anwendungen konfigurieren

HINWEIS:

Die maximal unterstützte Anzahl von Konfigurationsentitäten (Regeln) in der Blockierungsliste beträgt 32.

Wählen Sie auf der Registerkarte **Ungesicherte Anwendungen** eine Anwendung aus und klicken Sie auf **Anwendung sichern**.

Sie können eine der folgenden Optionen auswählen, um Ihre Anwendung zu schützen:

- WAF-Empfehlungsscanner – Diese Option ermöglicht es Ihnen, einen Scan Ihrer Anwendung durchzuführen. Basierend auf bestimmten Parametern des Scans schlägt das Ergebnis Ihnen Schutzmaßnahmen für Ihre Anwendung vor. Sie könnten in Betracht ziehen, diese Empfehlungen anzuwenden.
- Schutzmaßnahmen auswählen und anpassen – Diese Option ermöglicht es Ihnen, aus verschiedenen Vorlagenoptionen zu wählen oder Ihre Schutzmaßnahmen anzupassen und bereitzustellen.
  - **OWASP Top 10** – Eine vordefinierte Vorlage, die branchenübliche Schutzmaßnahmen gegen die Top-10-Sicherheitsrisiken von OWASP enthält. Weitere Informationen finden Sie unter `https://owasp.org/www-project-top-ten/`.
  - **CVE-Schutzmaßnahmen** – Sie können den Signatursatz aus der Liste der vorkonfigurierten Signaturregeln erstellen, die unter bekannten Schwachstellenkategorien klassifiziert sind. Sie können Signaturen auswählen, um die Protokoll- oder Blockierungsaktion zu konfigurieren, wenn ein Signaturmuster mit dem eingehenden Datenverkehr übereinstimmt. Die Protokollnachricht enthält die Details zur Schwachstelle.
  - **Benutzerdefinierte Schutzmaßnahmen** – Wählen Sie die Schutzmaßnahmen aus und stellen Sie sie entsprechend Ihren Anforderungen bereit.
- Bestehende Schutzmaßnahmen auswählen – Diese Option klont die Schutzmaßnahmen, die in einer bestehenden Anwendung bereitgestellt werden. Wenn Sie dieselben Schutzmaßnahmen für eine andere Anwendung bereitstellen möchten, können Sie diese Option auswählen und sie unverändert für eine andere Anwendung bereitstellen. Sie können diese Option auch als Vorlage auswählen, die Schutzmaßnahmen ändern und dann bereitstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF-Empfehlungsscanner

HINWEIS:

- Sie können nur einen Scan gleichzeitig für eine Anwendung ausführen. Um einen neuen Scan für dieselbe oder eine andere Anwendung zu starten, müssen Sie warten, bis der vorherige Scan abgeschlossen ist.
- Sie können auf **Verlauf anzeigen** klicken, um den Verlauf und den Status der vergangenen Scans anzuzeigen. Sie können auch auf **Bericht anzeigen** klicken und die Empfehlungen später anwenden.

Voraussetzungen:

- Die NetScaler-Instanz muss 13.0 41.28 oder höher (für Sicherheitsprüfungen) und 13.0 oder höher (für Signaturen) sein.
- Muss über die Premium-Lizenz verfügen.
- Muss der virtuelle Lastausgleichsserver sein.

Um mit dem WAF-Empfehlungsscan zu beginnen, müssen Sie die folgenden Informationen angeben:

1. Unter **Scan-Parameter**:
    - **Domänenname** – Geben Sie eine gültige, zugängliche IP-Adresse oder den öffentlich erreichbaren Domänennamen an, der der Anwendung zugeordnet ist. Beispiel: `www.example.com`.
    - **HTTP/HTTPS-Protokoll** – Wählen Sie das Protokoll der Anwendung aus.
    - **Traffic-Timeout** – Die Wartezeit (in Sekunden) für eine einzelne Anforderung während des Scans. Der Wert muss größer als 0 sein.
    - **URL für den Scan-Start** – Die Startseite der Anwendung, von der aus der Scan initiiert werden soll. Beispiel: `https://www.example.com/home`. Die URL muss eine gültige IPv4-Adresse sein. Wenn die IP-Adressen privat sind, müssen Sie sicherstellen, dass die private IP-Adresse von der NetScaler Console Management-IP aus zugänglich ist.
    - **Login-URL** – Die URL, an die die Anmeldedaten zur Authentifizierung gesendet werden. In HTML ist diese URL allgemein als Aktions-URL bekannt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Authentifizierungsmethode** – Wählen Sie die unterstützte Authentifizierungsmethode (Formular-basiert oder Header-basiert) für Ihre Anwendung aus.
    - Die formularbasierte Authentifizierung erfordert das Senden eines Formulars an die Login-URL mit den Anmeldeinformationen. Diese Anmeldeinformationen müssen in Form von Formularfeldern und deren Werten vorliegen. Die Anwendung teilt dann das Sitzungscookie, das zur Aufrechterhaltung der Sitzungen während des Scans verwendet wird.
    - Die Header-basierte Authentifizierung erfordert den Authentifizierungs-Header und dessen Wert im Header-Abschnitt. Der Authentifizierungs-Header muss einen gültigen Wert haben und wird zur Aufrechterhaltung der Sitzungen während des Scans verwendet. Die Formularfelder sollten bei der Header-basierten Authentifizierung leer gelassen werden.
- **Anforderungsmethode** – Wählen Sie die HTTP-Methode aus, die beim Übermitteln von Formulardaten an die Login-URL verwendet wird. Die zulässigen Anforderungsmethoden sind **POST**, **GET** und **PUT**.
- **Formularfelder** – Geben Sie die Formulardaten an, die an die Login-URL übermittelt werden sollen. Formularfelder sind nur erforderlich, wenn Sie die formularbasierte Authentifizierung auswählen. Sie müssen die Schlüssel-Wert-Paare angeben, wobei **Feldname** der Schlüssel und **Feldwert** der Wert ist. Stellen Sie sicher, dass alle für die Anmeldung erforderlichen Formularfelder, einschließlich Passwörter, korrekt hinzugefügt werden. Die Werte werden verschlüsselt, bevor sie in der Datenbank gespeichert werden. Sie können auf **Hinzufügen** klicken, um mehrere Formularfelder hinzuzufügen. Beispiel: **Feldname** – Benutzername und **Feldwert** – admin.
- **Logout-URL** – Geben Sie die URL an, die die Sitzung nach dem Zugriff beendet. Beispiel: `https://www.example.com/customer/logout`.

2. Unter **Scan-Konfigurationen**:
    - **Zu prüfende Schwachstellen** – Wählen Sie die Schwachstellen aus, die der Scanner erkennen soll. Derzeit geschieht dies für SQL-Injection- und Cross-Site-Scripting-Verstöße. Standardmäßig sind alle Verstöße ausgewählt. Nach der Auswahl der Schwachstellen simuliert das System diese Angriffe auf die Anwendung, um die potenzielle Schwachstelle zu melden. Es wird empfohlen, diese Erkennung in einer Nicht-Produktionsumgebung zu aktivieren. Alle anderen Schwachstellen werden ebenfalls gemeldet, ohne diese Angriffe auf die Anwendung zu simulieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Antwortgrößenlimit** – Der maximale Grenzwert für die Antwortgröße. Antworten, die den angegebenen Wert überschreiten, werden nicht gescannt. Der empfohlene Grenzwert beträgt 10 MB (1000000 Bytes).
- **Anfrage-Parallelität** – Die Gesamtzahl der Anfragen, die parallel an die Webanwendung gesendet werden.

3. Die Konfiguration der WAF-Scan-Einstellungen ist abgeschlossen. Sie können auf **Scan starten** klicken, um den Scanvorgang zu beginnen und warten, bis der Fortschritt abgeschlossen ist. Nach Abschluss des Scans klicken Sie auf **Bericht anzeigen**.

4. Auf der Seite mit den Scan-Ergebnissen klicken Sie auf **Empfehlung überprüfen**.

5. Überprüfen Sie die Schutzmaßnahmen oder bearbeiten/fügen Sie weitere Schutzmaßnahmen hinzu, und klicken Sie auf **Bereitstellen**.

Wenn Sie Sicherheitsprüfungen erfolgreich anwenden:

- Die Konfiguration wird auf der NetScaler-Instanz über StyleBooks angewendet, abhängig von der Version.
  - Für NetScaler 13.0 wird `unified-appsec-protection-130` StyleBook verwendet.
  - Für NetScaler 13.1 wird `unified-appsec-protection-131` StyleBook verwendet.
  - Für NetScaler 14.1 wird `unified-appsec-protection-141` StyleBook verwendet.
- Das `Appfw`-Profil wird auf Ihrem NetScaler erstellt und mithilfe von `policylabel` an die Anwendung gebunden.
- Die Signaturen sind an das AppFW-Profil gebunden, wenn die empfohlenen Signaturen bereits angewendet wurden.

HINWEIS

Sicherheitsprüfungen werden in NetScaler 13.0 41.28 oder einer späteren Version unterstützt.

Sie können überprüfen, ob die WAF-Profile und Signaturen über die Standard-StyleBooks angewendet wurden, indem Sie zu **Applications > Configuration > Config Packs** navigieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schutzmaßnahmen auswählen und anpassen

OWASP TOP 10

1 - Bietet Informationen über die Anwendung, wie IP-Adresse, Typ des virtuellen Servers, Lizenztyp, von welcher Instanz die Anwendung konfiguriert ist, und so weiter.

2 - Zeigt die ausgewählte Vorlage an. Sie können sie nach Belieben umbenennen.

3 - Zeigt die Schutzmaßnahmen an. Einige Schutzmaßnahmen erfordern zusätzliche Informationen.

4 - Zeigt den ausführlichen Protokolltyp an. Sie können die folgenden Optionen auswählen:

- **Muster**. Protokolliert nur das Verletzungsmuster.
- **Muster-Payload**. Protokolliert das Verletzungsmuster und 150 Byte zusätzliche JSON-Payload.
- **Muster, Payload, Header**. Protokolliert das Verletzungsmuster, 150 Bytes zusätzliche JSON-Payload und HTTP-Header-Informationen.

5 – Ermöglicht die Aktivierung des Überwachungsmodus. Wenn Sie den Überwachungsmodus aktivieren, wird der Datenverkehr nur protokolliert und es werden keine Gegenmaßnahmen aktiviert.

6 – Ermöglicht das Hinzufügen weiterer Schutzmaßnahmen. Klicken Sie auf **Schutzmaßnahmen hinzufügen** und überprüfen Sie diese, um sie hinzuzufügen.

7 – Ermöglicht die Auswahl einer neuen Vorlage über die Option „Vorlage ändern“.

8 – Ermöglicht das Bearbeiten oder Löschen des Schutzes.

9 – Aktiviert Analysen für die von Ihnen ausgewählten Schutzmaßnahmen. Diese Option ist standardmäßig ausgewählt. Sie können Analysen für die konfigurierten Schutzmaßnahmen unter **Sicherheit > Sicherheitsverletzungen** anzeigen.

Nachdem Sie die Schutzmaßnahmen konfiguriert haben, klicken Sie auf **Bereitstellen**.

CVE-SCHUTZMASSNAHMEN

Um die CVE-Schutzmaßnahmen bereitzustellen, klicken Sie auf **CVE-Schutz erstellen**. Wählen Sie auf der Seite **Signatursatz erstellen** die Signaturen aus der Liste aus, um die Protokoll- oder Blockierungsaktion zu konfigurieren, und klicken Sie dann auf **Speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nachdem Sie auf **Speichern** geklickt haben, können Sie die zur Konfigurationsseite hinzugefügten Signaturen anzeigen.

Sie können auch auf **Schutz hinzufügen** klicken, um der Anwendung weitere Schutzmaßnahmen hinzuzufügen. Nachdem Sie alle Schutzmaßnahmen konfiguriert haben, klicken Sie auf **Bereitstellen**.

BENUTZERDEFINIERTER SCHUTZ

Um Schutzmaßnahmen basierend auf Ihren Anforderungen bereitzustellen, klicken Sie auf **Neuen Schutz erstellen**. Wählen Sie auf der Seite **Schutzmaßnahmen hinzufügen** die Schutzmaßnahmen aus, die Sie bereitstellen möchten, und klicken Sie auf **Speichern**.

Nachdem Sie auf **Speichern** geklickt haben, überprüfen Sie die ausgewählten Schutzmaßnahmen auf der Konfigurationsseite und klicken Sie dann auf **Bereitstellen**.

Bestehende Schutzmaßnahmen auswählen

Um bestehende Schutzmaßnahmen von einer Anwendung auf eine andere bereitzustellen, wählen Sie eine bestehende Schutzmaßnahme aus der Liste aus.

Nachdem Sie eine Schutzmaßnahme ausgewählt haben, werden die bestehenden Schutzmaßnahmen geklont und auf der Konfigurationsseite angezeigt. Sie können sie je nach Bedarf ändern und dann auf **Bereitstellen** klicken.

Details zu Anwendungs-Sicherheitsverletzungen anzeigen

Webanwendungen, die dem Internet ausgesetzt sind, sind drastisch anfälliger für Angriffe geworden. NetScaler Console ermöglicht es Ihnen, umsetzbare Details zu Sicherheitsverletzungen zu visualisieren, um Anwendungen vor Angriffen zu schützen. Navigieren Sie zu **Security** > **Security Violations** für eine Single-Pane-Lösung, um:

- Anwendungen mit vollständiger Transparenz der Bedrohungsdetails in WAF-Einblicken und Bot-Einblicken visualisieren. Weitere Informationen finden Sie unter Unified Security dashboard.
- Greifen Sie auf die Anwendungs-Sicherheitsverletzungen basierend auf ihren Kategorien wie **Network**, **Bot** und **WAF** zu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Korrekturmaßnahmen ergreifen, um die Anwendungen zu sichern.

Die Seite **Security Violations** bietet die folgenden Optionen:

- **Application Overview** – Zeigt eine Übersicht mit Anwendungen an, die Gesamtverletzungen, Gesamt-WAF- und Bot-Verletzungen, Verletzungen nach Land usw. aufweisen. Weitere Informationen finden Sie unter Application overview.
- **All Violations** – Zeigt die Details zu Anwendungs-Sicherheitsverletzungen an. Weitere Informationen finden Sie unter All violations.

Einrichtung

Um die Verletzungen anzuzeigen, müssen Sie sicherstellen:

- Um mit der Konfiguration von Schutzmaßnahmen und der Aktivierung von Analysen in Ihren Anwendungen zu beginnen. Weitere Informationen finden Sie unter Unified Security dashboard.

  Wenn Sie Schutzmaßnahmen entweder über StyleBook oder direkt auf der NetScaler-Instanz konfiguriert haben, können Sie das Verfahren befolgen, um **WAF Security Violations** und **Bot Security Violations** zu aktivieren:

  a. Navigieren Sie zu **Infrastructure > Instances > NetScaler** und wählen Sie den Instanztyp aus. Zum Beispiel VPX.

  b. Wählen Sie die Instanz aus und wählen Sie aus der Liste **Select Action** die Option **Configure Analytics**.

  c. Wählen Sie die virtuellen Server aus und klicken Sie auf **Enable Security & Analytics**.

  d. Wählen Sie im Fenster **Analytics aktivieren** die Optionen **WAF-Sicherheitsverletzungen** und **Bot-Sicherheitsverletzungen** aus und klicken Sie dann auf **OK**.

- So konfigurieren Sie Detaillierte Webtransaktionseinstellungen.
- Wenn **Metrics Collector** aktiviert ist. Weitere Informationen finden Sie unter Intelligente App-Analysen konfigurieren.

Webtransaktionseinstellungen aktivieren

1. Navigieren Sie zu **Einstellungen > Analytics-Einstellungen**.

   Die Seite **Analytics-Einstellungen** wird angezeigt.

2. Klicken Sie auf **Funktionen für Analytics aktivieren**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Wählen Sie unter **Detaillierte Webtransaktionseinstellungen** die Option **Alle** aus.

4. Klicken Sie auf **OK**.

Anwendungsübersicht

Die Seite **Anwendungsübersicht** zeigt Anwendungen mit vollständiger Transparenz über die Bedrohungsdetails, die sowohl in Security Insight als auch in Bot Insight enthalten sind. Sie können auch Informationen wie die Gesamtzahl der Verstöße, die Gesamtzahl der WAF- und Bot-Verstöße, Verstöße nach Land usw. anzeigen.

1 – Zeigt die Gesamtzahl der betroffenen Anwendungen, die Gesamtzahl der Verstöße, die Gesamtzahl der WAF-Verstöße und die Gesamtzahl der Bot-Verstöße für den ausgewählten Zeitraum an.

2 – Zeigt die Details zu WAF- und Bot-Verstößen an. Klicken Sie auf die Registerkarte **WAF** und **Bot**, um die Top 5 der benutzerdefinierten oder diskreten Anwendungen basierend auf der Gesamtzahl der aufgetretenen Verstöße anzuzeigen. Klicken Sie auf **Alle anzeigen**, um alle Anwendungsdetails anzuzeigen.

3 – Zeigt die häufigsten Verstöße basierend auf deren Auftreten und den angewendeten Aktionen an.

4 – Zeigt eine geografische Kartenansicht an, die Aufschluss darüber gibt, von welchen Standorten die Verstöße ausgegangen sind.

5 – Bietet Informationen basierend auf den Verstößen.

Verstoßkategorien

WAF	BOT
Cookie-Hijacking	Scraper
XML-Inhaltstyp ableiten	Screenshot-Ersteller
Pufferüberlauf	Suchmaschine
Inhaltstyp	Dienstagent
Cookie-Konsistenz	Site-Monitor

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF	BOT
CSRF-Formular-Tagging	Geschwindigkeitstester
URL-Verweigerung	Nicht kategorisiert
Formularfeldkonsistenz	Virenscanner
Feldformate	Schwachstellenscanner
Maximale Uploads	DeviceFP-Wartezeit überschritten
Referrer-Header	Ungültiger DeviceFP
Sicherer Handel	Ungültige Captcha-Antwort
Sicheres Objekt	Tool
HTML SQL einschleusen	Captcha-Versuche überschritten
Start-URL	Gültige Captcha-Antwort
Cross-Site-Scripting	Captcha-Client stummgeschaltet
XML-DoS	Captcha-Wartezeit überschritten
XML-Format	Anforderungsgrößenlimit überschritten
XML WSI	Ratenlimit überschritten
XML SSL	Sperrliste (IP, Subnetz, Richtlinienausdruck)
XML-Anhang	Zulassungsliste (IP, Subnetz, Richtlinienausdruck)
XML SOAP-Fehler	Null-Pixel-Anforderung
XML-Validierung	Quell-IP
Sonstige	Host
IP-Reputation	Crawler
HTTP-DOS	Feed-Fetcher

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF	BOT
TCP Small Window	Link-Checker
Signaturverletzung	Marketing
Dateiupload-Typ	Geostandort
JSON-Cross-Site-Scripting	URL
JSON-SQL	
JSON-DOS	
Befehlsinjektion	
Sperr-Schlüsselwort	
JSON-Block-Schlüsselwort	
Grammatik für Befehlsinjektion	

WAF-Verletzungsdetails anzeigen

Klicken Sie auf eine Anwendung aus den **Top Applications** oder aus der Option **View All**, um die WAF-Details anzuzeigen.

HINWEIS:

Wenn Sie eine benutzerdefinierte App auswählen, können Sie die konsolidierten Anwendungsdetails auf der Seite **Security Overview** anzeigen. Wählen Sie aus der Liste eine Anwendung aus, um Details für die ausgewählte Anwendung anzuzeigen.

Die Seite **Security Overview** für die ausgewählte Anwendung wird angezeigt. Unter **WAF** können Sie Folgendes anzeigen:

- Eine grafische Ansicht, die die Gesamtanzahl der Verstöße, den Bedrohungsindex-Score und den Sicherheitsindex-Score für die Anwendung anzeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Klicken Sie auf **View Details**, um die Konfigurationsdetails der Application Firewall und der NetScaler System Security anzuzeigen.

- Die Verstöße basierend auf Typen, Schweregrad und angewendeten Aktionen.

  Klicken Sie auf **Logs**, um Details basierend auf dem Schweregrad oder der ergriffenen Maßnahme anzuzeigen. Sie können auch die Client-IP-Adresse anzeigen.

  Sie können auch das Suchtextfeld verwenden, in dem Sie Details nach Ihren Anforderungen anzeigen können. Wenn Sie auf das Suchfeld klicken, zeigt das Suchfeld eine Liste mit Suchvorschlägen an.

- Die Verstöße, die die Anwendung betreffen. Unter **Verstoßdetails** können Sie die betroffenen Verstoßdetails anzeigen.

  HINWEIS

  Für eine benutzerdefinierte App werden Verstöße angezeigt, die für alle Anwendungen gelten. Sie können eine Anwendung aus der Liste auswählen, um die für die ausgewählte Anwendung betroffenen Verstöße anzuzeigen.

  Klicken Sie auf jeden Verstoß, um Details wie die folgenden anzuzeigen:

  - **Was ist passiert** – Zeigt die Gesamtzahl der Vorkommen sowie das Datum und die Uhrzeit des letzten Vorkommens an.
  - **Ereignisdetails** – Zeigt eine geografische Karte an, die die Client-IP und andere Verstoßdetails wie Verstoßtyp, Client-IP, Standort usw. anzeigt.

Bot-Verstoßdetails anzeigen

Wählen Sie auf der Registerkarte **Bot** eine Anwendung aus den **Top-Anwendungen** oder aus der Option **Alle anzeigen** aus, um die Bot-Details anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Wenn Sie eine benutzerdefinierte App auswählen, können Sie die konsolidierten Anwendungsdetails auf der Seite **Sicherheitsübersicht** anzeigen. Wählen Sie aus der Liste eine Anwendung aus, um Details für die ausgewählte Anwendung anzuzeigen.

Die Seite **Sicherheitsübersicht** für die ausgewählte Anwendung wird angezeigt. Unter **Bot** können Sie Folgendes anzeigen:

- Ein Diagramm, das die Gesamtzahl der Bots, die Gesamtzahl der schlechten Bots, die Gesamtzahl der guten Bots und das Gesamtverhältnis zwischen menschlichen Benutzern und Bots, die auf die Anwendung zugreifen, anzeigt.

- Die Verstöße basierend auf den Bot-Typen, dem Schweregrad und den angewendeten Aktionen.

  Klicken Sie auf **Protokolle**, um Details basierend auf dem Schweregrad oder den ergriffenen Maßnahmen anzuzeigen. Wenn ein erkannter Bot ein Bot vom Typ Signatur ist, können Sie weitere Details wie Bot-Entwickler und Signatur-ID anzeigen. Die Signatur-ID ermöglicht es Ihnen, zu identifizieren, ob der erkannte Bot ein guter Bot oder ein schlechter Bot ist.

  HINWEIS:

  Wenn ein erkannter Bot ein anderer Bot-Typ als ein Signatur-Bot ist, werden die Signatur-ID und der Bot-Entwickler als N/A angezeigt.

  Sie können auch das Suchtextfeld verwenden, in dem Sie Bot-Details nach Ihren Anforderungen anzeigen können. Wenn Sie auf das Suchfeld klicken, erhalten Sie eine Liste mit Suchvorschlägen.

- Die Verstöße, die die Anwendung betreffen. Unter **Verstoßdetails** können Sie die betroffenen Verstoßdetails anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Für eine benutzerdefinierte App werden Verstöße angezeigt, die für alle Anwendungen gelten. Sie können eine Anwendung aus der Liste auswählen, um die für die ausgewählte Anwendung betroffenen Verstöße anzuzeigen.

Klicken Sie auf jeden Verstoß, um Details anzuzeigen, wie zum Beispiel:

- **Was ist passiert** – Zeigt die Gesamtzahl der Vorkommen und das Datum und die Uhrzeit des letzten Vorkommens an.
- **Ereignisdetails** – Zeigt eine geografische Karte an, die die Client-IP und andere Verstoßdetails wie Verstoßtyp, Client-IP, Standort usw. angibt.

HINWEIS:

Unter **WAF** und **Bot** können Sie Analysen für Content Switching Virtual Server anzeigen, die an Load Balancing Virtual Server gebunden sind. Klicken Sie auf den Content Switching Virtual Server, und unter **Gebundener Lastausgleichsserver** können Sie die Liste der Lastausgleichsserver anzeigen, die an den Content Switching Virtual Server gebunden sind.

Ereignisverlauf anzeigen

Sie können die Signaturaktualisierungen in **Ereignissen** anzeigen, wenn:

- Neue Signaturen in NetScaler-Instanzen hinzugefügt werden.
- Bestehende Signaturen in NetScaler-Instanzen aktualisiert werden.

Automatische Signaturaktualisierung

NetScaler Console sucht automatisch nach neuen Signaturaktualisierungen und wendet diese auf die verwalteten NetScaler-Instanzen an.

Das folgende Diagramm zeigt, wie die Signaturen aus der AWS-Cloud abgerufen, auf NetScaler aktualisiert und die Zusammenfassung der Signaturaktualisierung in NetScaler Console angezeigt wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alle Verstöße

Die Seite **Alle Verstöße** zeigt die Details zu Anwendungssicherheitsverstößen basierend auf den Kategorien **Netzwerk**, **WAF** und **Bot** an. Um die Sicherheitsverstöße in NetScaler Console anzuzeigen, stellen Sie sicher, dass Sie alle erforderlichen Einstellungen aktiviert haben. Weitere Informationen finden Sie in der Prozedur unter Einrichtung.

Verstoßkategorien

NetScaler Console ermöglicht Ihnen die Anzeige der folgenden Verstöße. Unter **Verstoßdetails** können Sie auf jede Registerkarte für Verstöße klicken, um die Verstoßdetails anzuzeigen.

NETZWERK	WAF	BOT
HTTP Slow Loris	Inhaltstyp XML ableiten	Scraper
DNS Slow Loris	Pufferüberlauf	Screenshot-Ersteller
HTTP Slow Post	Inhaltstyp	Suchmaschine
NXDomain-Flood-Angriff	Cookie-Konsistenz	Service-Agent
HTTP-Desynchronisationsangriff	CSRF-Formular-Tagging	Website-Monitor
Bleichenbacher-Angriff	URL-Verweigerung	Geschwindigkeitstester
Segment-Smack-Angriff	Formularfeld-Konsistenz	Tool
SYN-Flood-Angriff	Feldformate	Nicht kategorisiert
Small Window Attack	Referrer-Header	Virenscanner
	Cross-Site-Scripting	Schwachstellenscanner
	XML DoS	DeviceFP-Wartezeit überschritten
	XML-Format	Ungültiges DeviceFP
	XML WSI	Ungültige Captcha-Antwort
	XML SSL	Captcha-Versuche überschritten

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETZWERK	WAF	BOT
	XML-Anhang	Gültige Captcha-Antwort
	XML-SOAP-Fehler	Captcha-Client stummgeschaltet
	XML-Validierung	Captcha-Wartezeit überschritten
	Sonstige	Anforderungsgrößenlimit überschritten
	IP-Reputation	Ratenlimit überschritten
	HTTP-DOS	Sperrliste (IP, Subnetz, Richtlinienausdruck)
	TCP Small Window	Zulassungsliste (IP, Subnetz, Richtlinienausdruck)
	Signaturverletzung	Null-Pixel-Anfrage
	Dateiupload-Typ	Quell-IP
	JSON-Cross-Site-Scripting	Host
	JSON-SQL	Geostandort
	JSON-DoS	URL
	Befehlsinjektion	Crawler
	Cookie-Hijacking	Feed-Fetcher
	Schlüsselwortblockierung	Link-Checker
	JSON-Schlüsselwortblockierung	Marketing
	Sicherer Handel	
	Sicheres Objekt	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETZWERK	WAF	BOT
	HTML SQL einschleusen	
	Start-URL	
	Grammatik für Befehlsinjektion	
	Grammatik für JSON SQL-Injektion	

Dashboard für Sicherheitsverletzungen

Im Dashboard für Sicherheitsverletzungen können Sie Folgendes anzeigen:

- Gesamtzahl der auf allen NetScaler-Instanzen und -Anwendungen aufgetretenen Verletzungen. Die Gesamtzahl der Verletzungen wird basierend auf dem ausgewählten Zeitraum angezeigt.

- Gesamtzahl der Verletzungen in jeder Kategorie.

- Gesamtzahl der betroffenen NetScaler-Instanzen, Gesamtzahl der betroffenen Anwendungen und Top-Verletzungen basierend auf der Gesamtzahl der Vorkommen und der betroffenen Anwendungen.

Details zur Verletzung

Für jede Verletzung überwacht NetScaler Console das Verhalten über einen bestimmten Zeitraum und erkennt Verletzungen bei ungewöhnlichem Verhalten. Klicken Sie auf jede Registerkarte, um die Details zur Verletzung anzuzeigen. Sie können Details wie die folgenden anzeigen:

- Die Gesamtzahl der Vorkommen, das letzte Vorkommen und die Gesamtzahl der betroffenen Anwendungen
- Unter Ereignisdetails können Sie Folgendes anzeigen:
  - Die betroffene Anwendung. Sie können die Anwendung auch aus der Liste auswählen, wenn zwei oder mehr Anwendungen von Verletzungen betroffen sind.
  - Das Diagramm, das Verletzungen anzeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Empfohlene Aktionen**, die Ihnen vorschlagen, das Problem zu beheben.
- Weitere Details zur Verletzung, wie z. B. die Uhrzeit des Vorkommens und die Erkennungsmeldung.

WAF-Lernfunktion

NetScaler Web App Firewall (WAF) schützt Ihre Webanwendungen vor böswilligen Angriffen wie SQL-Injection und Cross-Site-Scripting. Um Datenschutzverletzungen zu verhindern und den richtigen Sicherheitsschutz zu bieten, müssen Sie Ihren Datenverkehr auf Bedrohungen und umsetzbare Echtzeitdaten zu Angriffen überwachen. Manchmal können die gemeldeten Angriffe Fehlalarme sein, die als Ausnahme behandelt werden müssen.

Die Lern-Engine in NetScaler Console ist ein Filter für sich wiederholende Muster, der es WAF ermöglicht, das Verhalten (die normalen Aktivitäten) Ihrer Webanwendungen zu lernen. Basierend auf der Überwachung generiert die Engine eine Liste vorgeschlagener Regeln oder Ausnahmen für jede Sicherheitsprüfung, die auf den HTTP-Verkehr angewendet wird.

Es ist viel einfacher, Entspannungsregeln mit der Lern-Engine bereitzustellen, als sie manuell als notwendige Entspannungen bereitzustellen.

Die folgende Abbildung erläutert die allgemeinen Informationen zur Funktionsweise der WAF-Lernfunktion in NetScaler Console:

1 – NetScaler-Instanzen mit ihren WAF-Profilen

2 – Konfigurieren Sie ein Lernprofil in NetScaler Console, fügen Sie die WAF-Profile hinzu und wählen Sie aus, ob die Entspannungsregeln automatisch oder manuell bereitgestellt werden sollen

3 – Der Administrator kann die Entspannungsregeln in NetScaler Console validieren und entscheiden, ob sie bereitgestellt oder übersprungen werden sollen

Erste Schritte

Um die Lernfunktion bereitzustellen, müssen Sie:

- Aktivieren Sie das zentralisierte Lernen in der NetScaler-Instanz. Führen Sie den folgenden Befehl in der NetScaler-Instanz aus:

  ```
  set appfw settings -centralizedLearning ON
  ```

- Stellen Sie sicher, dass die NetScaler-Instanzversion **13.0-76.6** oder höher ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Konfigurieren Sie ein Web App Firewall-Profil (eine Reihe von Sicherheitseinstellungen) auf Ihrer NetScaler Appliance. Weitere Informationen finden Sie unter Erstellen von Web App Firewall-Profilen.

Nachdem Sie das zentralisierte Lernen aktiviert und das WAF-Profil konfiguriert haben, generiert NetScaler Console eine Liste von Ausnahmen (Relaxationen) für die konfigurierte Sicherheitsprüfung. Als Administrator können Sie die Liste der Ausnahmen in NetScaler Console überprüfen und entscheiden, ob Sie sie bereitstellen oder überspringen möchten.

Mit der WAF-Lernfunktion in NetScaler Console können Sie:

- Ein Lernprofil mit den folgenden Sicherheitsprüfungen konfigurieren:
  - Start-URL
  - Cookie-Konsistenz
  - Kreditkarte

    HINWEIS

    Für die Sicherheitsprüfung der Kreditkarte müssen Sie die `doSecureCreditCardLogging` in der NetScaler-Instanz konfigurieren und sicherstellen, dass die Einstellung **OFF** ist.

  - Inhaltstyp
  - Formularfeld-Konsistenz
  - Feldformate
  - CSRF-Formular-Tagging
  - HTML-Cross-Site-Scripting
  - HTML-SQL-Injection

    HINWEIS

    Für die HTML-SQL-Injection-Prüfung müssen Sie `set -sqlinjectionTransformSpecialChars ON` und `set -sqlinjectiontype sqlspclcharorkeywords` in der NetScaler-Instanz konfigurieren.

  - HTML-Befehlsinjektion

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Nur in NetScaler-Instanz 13.0-72.12 oder höher unterstützt.

- JSON-SQL

HINWEIS

Nur in NetScaler-Instanz 13.1-14.10 oder höher unterstützt.

- JSON-Befehlsinjektion

HINWEIS

Nur in NetScaler-Instanz 13.1-14.10 oder höher unterstützt.

- JSON-XSS

HINWEIS

Nur in NetScaler-Instanz 13.1-14.10 oder höher unterstützt.

- Überprüfen Sie die Entspannungsregeln in der NetScaler Console und entscheiden Sie, die erforderlichen Maßnahmen zu ergreifen (Bereitstellen oder Überspringen).
- Erhalten Sie die Benachrichtigungen über E-Mail, Slack und ServiceNow
- Verwenden Sie die Seite **Aktionsübersicht**, um Entspannungsdetails anzuzeigen

So verwenden Sie die WAF-Lernfunktion in NetScaler Console:

1. Lernprofil konfigurieren
2. Entspannungsregeln verwalten
3. Die WAF-Lern-Aktionsübersichtsseite verwenden

WAF-Empfehlungen

NetScaler Web App Firewall (WAF)-Profile und WAF-Signaturen schützen Ihre Webanwendungen vor bösartigen Angriffen. WAF-Signaturen bieten spezifische, konfigurierbare Regeln, um den Schutz Ihrer Websites vor bekannten Angriffen zu vereinfachen. Eine Signatur stellt ein Muster dar,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

das eine Komponente eines bekannten Angriffs auf ein Betriebssystem, einen Webserver, eine Website, einen XML-basierten Webdienst oder eine andere Ressource ist. Um Ihre Anwendung mithilfe von Signaturen zu schützen, müssen Sie die Regeln überprüfen, aktivieren und konfigurieren, die Sie anwenden möchten.

Ebenso müssen Sie, um Datenschutzverletzungen zu verhindern und den richtigen Sicherheitsschutz in der Anwendung zu gewährleisten, ein WAF-Profil mit Sicherheitsprüfungen erstellen. Wenn Sie ein WAF-Profil in der NetScaler-Instanz erstellen, kann der Datenverkehr:

- Mit den genannten Sicherheitsprüfungen generiert werden
- Nicht mit den genannten Sicherheitsprüfungen generiert werden

Die Instanz empfängt möglicherweise andere Angriffe, aber Sie haben diese Sicherheitsprüfung in den WAF-Profilen möglicherweise nicht aktiviert.

Als Administrator müssen Sie verstehen, wie Sie die richtigen Signaturen aktivieren und die richtigen WAF-Profile erstellen, um die Webanwendung zu schützen. Die Identifizierung der richtigen Signaturen und WAF-Profile kann in einigen Szenarien eine schwierige Aufgabe sein.

Die NetScaler Console WAF-Empfehlung scannt die Anwendung auf Schwachstellen und generiert die folgenden Empfehlungen:

- WAF-Profil
- WAF-Signatur

Weitere Informationen finden Sie unter WAF-Profil und WAF-Signaturen.

Die WAF-Empfehlungsdatenbank wird regelmäßig aktualisiert, um neue Schwachstellen aufzunehmen. Sie können scannen und dann die Aktivierung der erforderlichen Empfehlungen auswählen. Sie können alle Signaturen und Sicherheitsprüfungen aktivieren, dies kann jedoch zu Fehlalarmen führen und die Leistung der NetScaler-Instanz beeinträchtigen. Daher wird empfohlen, nur die erforderlichen Sicherheitsprüfungen und Signaturen auszuwählen. Die WAF-Empfehlungs-Engine erkennt auch automatisch, welche Signaturen und Sicherheitsprüfungen für die Anwendung aktiviert werden müssen.

HINWEIS

Die NetScaler-Instanz muss **13.0 41.28 oder höher** (für Sicherheitsprüfungen) und **13.0 oder höher** (für Signaturen) sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Voraussetzungen

Die Anwendungen:

- Müssen über die Premium-Lizenz verfügen.
- Muss der virtuelle Lastausgleichsserver sein.

WAF-Scan-Einstellungen konfigurieren

Navigieren Sie in NetScaler Console zu **Security > WAF Recommendation** und klicken Sie unter **Applications** auf **Start Scan**, um die WAF-Scan-Einstellungen für eine Anwendung zu konfigurieren.

Auf der Seite WAF-Empfehlungen:

- **Domänenname** – Geben Sie den öffentlich zugänglichen/öffentlich erreichbaren Domänennamen an, der mit der Anwendungs-VIP verknüpft ist. Beispiel: `www.example.com`.

  Hinweis

  > Start-URL, Anmelde-URL und Abmelde-URL müssen mit der angegebenen Domäne übereinstimmen.

- **Traffic und Start-URL** – Geben Sie die URL-Details der Anwendung (Server) an.
  - **HTTP/HTTPS-Protokoll** – Wählen Sie das Protokoll der Anwendung aus.
  - **Traffic-Timeout** – Die Wartezeit (in Sekunden) für eine einzelne Anforderung während des Scans. Der Wert muss größer als 0 sein.
  - **Start-URL** – Die Startseite der Anwendung, um den Scan zu initiieren. Beispiel: `https://www.example.com/home`. Die URL muss eine gültige IPv4-Adresse sein. Wenn die IP-Adressen privat sind, müssen Sie sicherstellen, dass die private IP-Adresse von der NetScaler Console Management-IP aus zugänglich ist.

- **Login-URLs** – Geben Sie die Anmeldeinformationen und URLs (falls vorhanden) an, um auf die Anwendung zuzugreifen.
  - **Login-URL** – Die URL, an die die Anmeldedaten zur Authentifizierung gesendet werden. In HTML ist diese URL allgemein als Aktions-URL bekannt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Authentifizierungsmethode** – Wählen Sie die unterstützte Authentifizierungsmethode (Formular-basiert oder Header-basiert) für Ihre Anwendung aus.
  - Die formularbasierte Authentifizierung erfordert das Absenden eines Formulars an die Login-URL mit den Anmeldeinformationen. Diese Anmeldeinformationen müssen in Form von Formularfeldern und deren Werten vorliegen. Die Anwendung teilt dann das Sitzungscookie, das zur Aufrechterhaltung von Sitzungen während des Scans verwendet wird.
  - Die Header-basierte Authentifizierung erfordert den Authentifizierungs-Header und dessen Wert im Header-Abschnitt. Der Authentifizierungs-Header muss einen gültigen Wert haben und wird zur Aufrechterhaltung von Sitzungen während des Scans verwendet. Die Formularfelder sollten für die Header-basierte Authentifizierung leer gelassen werden.
- **Anforderungsmethode** – Wählen Sie die HTTP-Methode, die beim Übermitteln von Formulardaten an die Login-URL verwendet wird. Die zulässigen Anforderungsmethoden sind POST, GET und PUT.
- **Formularfelder** – Geben Sie die Formulardaten an, die an die Login-URL übermittelt werden sollen. Formularfelder sind nur erforderlich, wenn Sie die formularbasierte Authentifizierung auswählen. Sie müssen die Schlüssel-Wert-Paare angeben, wobei der Feldname der Schlüssel und der Feldwert der Wert ist. Stellen Sie sicher, dass alle für die Anmeldung erforderlichen Formularfelder korrekt hinzugefügt werden, einschließlich Passwörter. Die Werte werden vor der Speicherung in der Datenbank verschlüsselt. Sie können auf die Schaltfläche „Hinzufügen“ klicken, um mehrere Formularfelder hinzuzufügen. Zum Beispiel: Feldname – Benutzername und Feldwert – admin.
- **HTTP-Header** – Die HTTP-Header können für eine erfolgreiche Anmeldung erforderlich sein. Sie müssen die Schlüssel-Wert-Paare angeben, wobei der Header-Name der Schlüssel und der Header-Wert der Wert ist. Sie können auf die Schaltfläche „Hinzufügen“ klicken, um mehrere HTTP-Header hinzuzufügen. Einer der am häufigsten benötigten HTTP-Header ist der Content-Type-Header.

- **Logout-URLs** – Geben Sie die URL an, die die Sitzung nach dem Zugriff beendet. Zum Beispiel: `https://www.example.com/customer/logout`.

- **Schwachstelle** – Wählen Sie die Schwachstellen aus, die der Scanner erkennen soll. Derzeit wird dies für SQL-Injection- und Cross-Site-Scripting-Verletzungen durchgeführt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Standardmäßig sind alle Verletzungen ausgewählt. Nach der Auswahl der Schwachstellen simuliert es diese Angriffe auf die Anwendung, um die potenzielle Schwachstelle zu melden. Es wird empfohlen, diese Erkennung zu aktivieren, die sich nicht in der Produktionsumgebung befindet. Alle anderen Schwachstellen werden ebenfalls gemeldet, ohne diese Angriffe auf die Anwendung zu simulieren.

- **Zusätzliche Einstellungen**
  - **Anfrage-Parallelität** – Die Gesamtzahl der parallel an die Webanwendung gesendeten Anfragen.
  - **Scan-Tiefe** – Die Tiefe der Webanwendung, bis zu der der Scan durchgeführt werden muss. Bei einer Scan-Tiefe von 2 werden beispielsweise die Start-URL und alle in dieser URL gefundenen Links gescannt. Sie müssen einen Wert größer oder gleich 1 angeben.
  - **Antwortgrößenlimit** – Das maximale Limit für die Antwortgröße. Alle Antworten, die den angegebenen Wert überschreiten, werden nicht gescannt. Das empfohlene Limit beträgt 3 MB (300000 Bytes).

Die Konfiguration der WAF-Scaneinstellungen ist abgeschlossen. Sie können auf **Scannen** klicken, um den Scanvorgang zu starten, oder auf **Für später speichern**, um die Konfigurationen zu speichern und später zu scannen.

WAF-Scan-Empfehlungsprozess

Wenn Sie den Scan starten, führt die WAF-Empfehlungs-Engine Folgendes aus:

- Scannt die bereitgestellte Webanwendung über die angegebene URL.
- Überprüft die Webanwendung, um die von der Webanwendung verwendeten Technologien zu ermitteln.
- Simuliert Sicherheitsangriffe auf die Webanwendung, um potenzielle Schwachstellen zu erkennen.
- Empfiehlt Signaturen basierend auf den erkannten Webtechnologien.
- Empfiehlt Sicherheitsprüfungen basierend auf gefundenen Schwachstellen und der Analyse des Datenverkehrs.
- Analysiert die Antworten der Webanwendung, um detailliertere Einstellungen zu generieren.

Die folgenden Sicherheitsprüfungen werden unterstützt:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Pufferüberlauf
- Feldformate
- Kreditkarte
- Cookie-Konsistenz
- HTML-SQL-Injection
- HTML-Cross-Site-Scripting
- Formularfeld-Konsistenz
- CSRF-Formular-Tagging

Scanbericht anzeigen

Nach Abschluss des Scans klicken Sie auf **Bericht anzeigen**, um die Ergebnisse anzuzeigen.

Das Scanergebnis liefert:

- **WAF-Empfehlung** – Ermöglicht Ihnen, die Zusammenfassung der für die Anwendung empfohlenen Signaturen und Sicherheitsprüfungen anzuzeigen.
- **Scan-Erkennungen** – Ermöglicht Ihnen, die gesammelten Informationen wie Technologien und Details zu Verletzungen, die an der Anwendung durchgeführt wurden, anzuzeigen. Klicken Sie auf **Details anzeigen**, um Informationen zu den Erkennungen und weitere Details des Scans anzuzeigen.

Klicken Sie unter **WAF-Empfehlung** auf **Empfehlung überprüfen**, um die Details für **Sicherheitsprüfungen** und **Signaturen** anzuzeigen.

Die empfohlenen Sicherheitseinstellungen schlagen die empfohlenen Sicherheitsprüfungen und Signaturen für die Anwendung vor. Sie können die Empfehlungen aus der Liste bearbeiten und auf **anzeigen oder bearbeiten** klicken, um Details anzuzeigen oder Änderungen gemäß den Anforderungen zu bearbeiten. Die Option „Auf Standard zurücksetzen“ setzt alle vorgenommenen Änderungen zurück und stellt die ursprünglichen Empfehlungen wieder her.

Nachdem Sie die Details überprüft haben, klicken Sie auf **Empfehlung anwenden**. Die Empfehlungen werden mithilfe der StyleBooks konfiguriert. Sie müssen sicherstellen, dass Sie die Empfehlung in den Registerkarten **Sicherheitsprüfungen** und **Signatur** separat anwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Es wird empfohlen, zuerst die Signaturen und dann die Sicherheitsprüfungen anzuwenden. Dadurch werden die Signaturen automatisch an das Profil gebunden.

Wenn Sie Signaturen erfolgreich anwenden:

- Die Konfiguration wird über das `appfw-import-object` StyleBook auf die NetScaler-Instanz angewendet.
- Die Signaturdatei mit den konfigurierten Empfehlungen wird in die NetScaler-Instanz importiert.

HINWEIS

Signaturen werden in NetScaler 13.0 oder einer späteren Version unterstützt.

Bevor Sie mit der Anwendung der Empfehlungen für die **Sicherheitsprüfung** fortfahren, navigieren Sie zu **Applications > Configuration > Config Packs** und stellen Sie sicher, dass das Signaturen-Configpack erfolgreich erstellt wurde.

Wenn Sie Sicherheitsprüfungen erfolgreich anwenden:

- Die Konfiguration wird über StyleBooks auf die NetScaler-Instanz angewendet, abhängig von der NetScaler-Version. Für NetScaler 13.0 wird das `waf-default-130` StyleBook verwendet und für NetScaler 13.1 wird das `waf-default-131` Stylebook verwendet.
- Das `Appfw` Profil wird auf Ihrem NetScaler erstellt und mithilfe des `policylabel` an die Anwendung gebunden.
- Die Signaturen werden an das appfw-Profil gebunden, wenn die empfohlenen Signaturen bereits angewendet wurden.

HINWEIS

Sicherheitsprüfungen werden in NetScaler 13.0 41.28 oder einer späteren Version unterstützt.

Nachdem Sie die Empfehlung (Sicherheitsprüfungen und Signaturen) angewendet haben, können Sie die folgende Bestätigungsmeldung anzeigen:

WAF-Bestätigung(/en-us/netscaler-console-service/media/wre-confirmation.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können überprüfen, ob die WAF-Profile und Signaturen über die Standard-StyleBooks angewendet wurden, indem Sie zu **Anwendungen > Konfiguration > Konfigurationspakete** navigieren.

WAF-StyleBooks(/en-us/netscaler-console-service/media/wre-stylebooks.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway

Die Gateway-Funktionen von NetScaler Console bieten Einblick in den Benutzerzugriff und die Virtual-Desktop-Erfahrung über Ihre NetScaler Gateway-Bereitstellungen hinweg. Sie können Anmelde- und Zugriffsfehler beheben, die HDX™ Virtual-Desktop-Erfahrung überwachen und Schwellenwerte und Warnungen konfigurieren.

Die folgenden Themen helfen Ihnen beim Überwachen und Verwalten von Gateway-Analysen:

- Gateway Insight
  - Beheben von Gateway Insight-Problemen
- HDX Insight
  - HDX Insight-Datenerfassung aktivieren
  - Schwellenwerte erstellen und Warnungen für HDX Insight konfigurieren
  - HDX Insight-Berichte und -Metriken anzeigen
  - Beheben von HDX Insight-Problemen
- Metrikinformationen für Schwellenwerte

Gateway Insight

In einer NetScaler Gateway-Bereitstellung ist die Transparenz der Benutzerzugriffsdetails für die Fehlerbehebung bei Zugriffsproblemen unerlässlich. Als Netzwerkadministrator möchten Sie wissen, wann sich ein Benutzer nicht bei NetScaler Gateway anmelden kann, und Sie möchten die Benutzeraktivität und die Gründe für Anmeldefehler erfahren. Diese Informationen sind jedoch in der Regel nicht verfügbar, es sei denn, der Benutzer sendet eine Anfrage zur Problemlösung.

Gateway Insight bietet Einblick in die Fehler, die allen Benutzern, unabhängig vom Zugriffsmodus, beim Anmelden bei NetScaler Gateway begegnen. Sie können jederzeit eine Liste aller verfügbaren Benutzer, die Anzahl der aktiven Benutzer, die Anzahl der aktiven Sitzungen sowie die von allen Benutzern verwendeten Bytes und Lizenzen anzeigen. Sie können die Endpunktanalyse (EPA), Authentifizierungs-, Single Sign-On (SSO)- und Anwendungsstartfehler für einen Benutzer anzeigen. Sie können auch die Details aktiver und beendeter Sitzungen für einen Benutzer anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway Insight bietet auch Einblick in die Gründe für das Fehlschlagen des Anwendungsstarts bei virtuellen Anwendungen. Dies verbessert Ihre Fähigkeit, Anmelde- oder Anwendungsstartfehler jeglicher Art zu beheben. Sie können die Anzahl der gestarteten Anwendungen, die Anzahl der gesamten und aktiven Sitzungen sowie die von den Anwendungen verbrauchten Gesamtbytes und die Bandbreite anzeigen. Sie können Details zu Benutzern, Sitzungen, Bandbreite und Startfehlern für eine Anwendung anzeigen.

Sie können jederzeit die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die Gesamtbytes und die Bandbreite anzeigen, die von allen Gateways verwendet werden, die mit einer NetScaler Gateway-Appliance verbunden sind. Sie können die EPA-, Authentifizierungs-, Single Sign-On- und Anwendungsstartfehler für ein Gateway anzeigen. Sie können auch die Details aller Benutzer, die einem Gateway zugeordnet sind, und deren Anmeldeaktivität anzeigen.

Alle Protokollmeldungen werden in der NetScaler Console-Datenbank gespeichert, sodass Sie Fehlerdetails für jeden beliebigen Zeitraum anzeigen können. Sie können auch eine Zusammenfassung der Anmeldefehler anzeigen und feststellen, in welcher Phase des Anmeldevorgangs ein Fehler aufgetreten ist.

Hinweise:

- Gateway Insight wird in den folgenden Bereitstellungen unterstützt:
  - Access Gateway
  - Unified Gateway
- Die Version und der Build von NetScaler Console müssen gleich oder neuer sein als die der NetScaler Gateway-Appliance.
- Berichte von Gateway Insight für eine Stunde können für NetScaler-Instanzen mit einer Advanced-Lizenz angezeigt werden. Eine Premium-Lizenz ist erforderlich, um Gateway Insight-Berichte über eine Stunde hinaus anzuzeigen.

Einschränkungen:

- NetScaler Gateway unterstützt Gateway Insight nicht, wenn die Authentifizierungsmethode als zertifikatbasierte Authentifizierung konfiguriert ist.
- Erfolgreiche Benutzeranmeldungen, Latenz und Details auf Anwendungsebene für virtuelle ICA-Anwendungen und Desktops sind nur auf dem HDX™ Insight Users-Dashboard sichtbar.
- Im Double-Hop-Modus ist die Sichtbarkeit von Fehlern auf der NetScaler Gateway Appliance in der zweiten DMZ nicht verfügbar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Probleme beim Desktop-Zugriff über das Remote Desktop Protocol (RDP) werden nicht gemeldet.
- Die Gateway Insight-Datensätze für die SAML-Authentifizierung werden nicht gemeldet.
- Gateway Insight wird für die folgenden Authentifizierungstypen unterstützt. Wenn andere Authentifizierungstypen als diese verwendet werden, können Sie Abweichungen in Gateway Insight feststellen.
  - Lokal
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - Natives OTP
  - OAuth

Gateway Insight aktivieren

Um Gateway Insight für Ihre NetScaler Gateway Appliance zu aktivieren, müssen Sie die NetScaler Gateway Appliance zuerst zu NetScaler Console hinzufügen. Anschließend müssen Sie AppFlow für den virtuellen Server aktivieren, der die VPN-Anwendung darstellt. Informationen zum Hinzufügen von Geräten zu NetScaler Console finden Sie unter Instanzen hinzufügen.

HINWEIS

Um Fehler bei der Endpunktanalyse (EPA) in NetScaler Console anzuzeigen, müssen Sie die Protokollierung der AppFlow-Authentifizierung, -Autorisierung und des Zugriffssteuerungs-Benutzernamens auf der NetScaler Gateway Appliance aktivieren.

AppFlow für einen virtuellen Server in NetScaler Console aktivieren

1. Navigieren Sie zu **Einstellungen > Lizenzierungs- und Analysekonsfiguration**.
2. Klicken Sie unter **Zusammenfassung der virtuellen Serveranalysen** auf **Analysen konfigurieren**.
3. Wählen Sie auf der Seite **Alle virtuellen Server** den virtuellen NetScaler Gateway-Server aus, und klicken Sie auf **Sicherheit & Analysen aktivieren**.
4. Wählen Sie **Gateway Insight** aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Klicken Sie auf **Speichern**.

AppFlow-Benutzernamenprotokollierung auf einer NetScaler Gateway-Appliance über die GUI aktivieren

1. Navigieren Sie zu **Konfiguration > System > AppFlow® > Einstellungen**, und klicken Sie dann auf **AppFlow-Einstellungen ändern**.
2. Wählen Sie im Bildschirm **AppFlow-Einstellungen konfigurieren** die Option **AAA-Benutzername** aus, und klicken Sie dann auf **OK**.

Gateway Insight-Berichte anzeigen

In NetScaler Console können Sie Berichte für alle Benutzer, Anwendungen und Gateways anzeigen, die mit den NetScaler Gateway-Appliances verknüpft sind, und Sie können Details für einen bestimmten Benutzer, eine Anwendung oder ein Gateway anzeigen. Im Abschnitt **Übersicht** können Sie die Fehler bei EPA, SSO, Authentifizierung und Anwendungsstart anzeigen. Sie können auch eine Zusammenfassung der verschiedenen Sitzungsmodi anzeigen, die von Benutzern zum Anmelden verwendet werden, die Clienttypen und die Anzahl der Benutzer, die sich jede Stunde angemeldet haben.

HINWEIS:

Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, der Gruppe Zugriff auf Anwendungsebene gewähren und Benutzer der Gruppe zuweisen. NetScaler Console Analytics unterstützt jetzt die autorisierungsbasierte Autorisierung über virtuelle IP-Adressen. Ihre Benutzer können jetzt Berichte für alle Insights nur für die Anwendungen (virtuelle Server) sehen, für die sie autorisiert sind. Weitere Informationen zu Gruppen und zum Zuweisen von Benutzern zu einer Gruppe finden Sie unter Gruppen in NetScaler Console konfigurieren.

EPA-, SSO-, Authentifizierungs-, Autorisierungs- und Anwendungsstartfehler anzeigen

1. Navigieren Sie in NetScaler Console zu **Gateway > Gateway Insight**.
2. Wählen Sie den Zeitraum aus, für den Sie die Benutzerdetails anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.
3. Klicken Sie auf die Registerkarten EPA (Endpunktanalyse), Authentifizierung, Autorisierung, SSO (Einmaliges Anmelden) oder Anwendungsstart, um die Fehlerdetails anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EPA-Bericht(/en-us/netscaler-console-service/media/gateway-insight-reports-failure.png)

Zusammenfassung der Sitzungsmodi, Clients und der Benutzeranzahl anzeigen

Navigieren Sie in NetScaler Console zu **Gateway > Gateway Insight** und scrollen Sie nach unten, um die Berichte anzuzeigen.

Berichtszusammenfassung(/en-us/netscaler-console-service/media/gateway-insight-reports-summary.png)

Anmeldeaktivität(/en-us/netscaler-console-service/media/gateway-insight-reports-logon-activity.png)

Benutzer

Sie können einen vollständigen Bericht für die Benutzer anzeigen, die den NetScaler Gateway-Appliances zugeordnet sind. Sie können die EPA-, Authentifizierungs-, SSO-, Anwendungsstartfehler usw. für einen Benutzer anzeigen.

Sie können auch eine konsolidierte Ansicht aller aktiven und beendeten Benutzersitzungen visualisieren.

Gateway Insight-Verbesserungen(/en-us/netscaler-console-service/media/gateway-insight-improvements.png)

Als Administrator ermöglicht Ihnen diese Ansicht:

- Alle Benutzerdetails in einer Ein-Fenster-Visualisierung anzeigen
- Die Komplexität beim Auswählen jedes Benutzers und Anzeigen der aktiven und beendeten Sitzungen beseitigen

Benutzerdetails anzeigen

1. Navigieren Sie in der NetScaler Console zu **Gateway > Gateway Insight > Users**.
2. Wählen Sie den Zeitraum aus, für den Sie die Benutzerdetails anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.
3. Sie können die Anzahl der aktiven Benutzer, die Anzahl der aktiven Sitzungen und die von allen Benutzern während des Zeitraums übertragenen Bytes anzeigen.

   Gateway Insight jetzt(/en-us/netscaler-console-service/media/gw-now.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scrollen Sie nach unten, um eine Liste der verfügbaren Benutzer und aktiven Benutzer anzuzeigen.

Aktive Benutzer(/en-us/netscaler-console-service/media/gateway-insight-reports-active-users.png)

Klicken Sie auf der Registerkarte **Users** oder **Active Users** auf einen Benutzer, um die folgenden Benutzerdetails anzuzeigen:

- **Benutzerdetails** – Sie können Einblicke für jeden Benutzer anzeigen, der mit den NetScaler Gateway-Appliances verknüpft ist. Navigieren Sie zu **Gateway** > **Gateway Insight** > **Users** und klicken Sie auf einen Benutzer, um Einblicke für den ausgewählten Benutzer anzuzeigen, z. B. Sitzungsmodus, Betriebssystem und Browser.

  Benutzerdetails(/en-us/netscaler-console-service/media/gw-user-details.png)
- **Benutzer und Anwendungen für das ausgewählte Gateway** – Navigieren Sie zu **Gateway** > **Gateway Insight** > **Gateway** und klicken Sie auf einen Gateway-Domänennamen, um die Top 10 Anwendungen und Top 10 Benutzer anzuzeigen, die mit dem ausgewählten Gateway verknüpft sind.

  Benutzer und Anwendung(/en-us/netscaler-console-service/media/gw-user-app.png)
- **Weitere Optionen für Anwendungen und Benutzer anzeigen** – Bei mehr als 10 Anwendungen und Benutzern können Sie auf das Mehr-Symbol in Anwendungen und Benutzern klicken, um alle Benutzer- und Anwendungsdetails anzuzeigen, die mit dem ausgewählten Gateway verknüpft sind.
- **Details durch Klicken auf das Balkendiagramm anzeigen** – Wenn Sie auf ein Balkendiagramm klicken, können Sie die entsprechenden Details anzeigen. Navigieren Sie beispielsweise zu **Gateway > Gateway Insight > Gateway** und klicken Sie auf das Gateway-Balkendiagramm, um die Gateway-Details anzuzeigen.

  Balkendiagramm(/en-us/netscaler-console-service/media/bar-graph.png)
- Die Benutzer **Aktive Sitzungen** und **Beendete Sitzungen**.

  ▢
- Der Gateway-Domainname und die Gateway-IP-Adresse in **Aktive Sitzungen**.

  ▢
- Die Anmeldedauer des Benutzers.

  ▢
- Der Grund für die Abmeldesitzung des Benutzers. Die Abmeldegründe können sein:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Sitzung abgelaufen
- Abgemeldet wegen internem Fehler
- Abgemeldet, weil inaktive Sitzung abgelaufen ist
- Benutzer hat sich abgemeldet
- Administrator hat die Sitzung beendet

Suchleiste und Geo-Kartenansicht

Sie können anzeigen:

- Eine Suchleiste, mit der Sie Ergebnisse basierend auf dem Benutzernamen filtern können. Navigieren Sie zu **Gateway > Gateway Insight > Benutzer**, um die Suchleiste für **Benutzer** und **Aktive Benutzer** anzuzeigen. Platzieren Sie den Mauszeiger auf der Suchleiste, wählen Sie **Benutzername** aus und geben Sie einen Benutzernamen ein, um die Ergebnisse zu filtern.

- Eine Geokarte, die die Benutzerinformationen basierend auf dem geografischen Standort der Benutzer anzeigt. Als Administrator ermöglicht Ihnen diese Geokarte, die Zusammenfassung der gesamten Benutzer, Anwendungen und Sitzungen für einen bestimmten Standort anzuzeigen.

  a. Navigieren Sie zu **Gateway > Gateway Insight**, um die Geokarte anzuzeigen
  b. Klicken Sie auf ein Land. Zum Beispiel: Vereinigte Staaten

     Die Geokarte zeigt Details wie Benutzerliste, aktive Sitzungen, beendete Sitzungen und Anwendungen für das ausgewählte Land an.

Anwendungen

Sie können die Anzahl der gestarteten Anwendungen, die Anzahl der gesamten und aktiven Sitzungen sowie die Anzahl der gesamten Bytes und die von den Anwendungen verbrauchte Bandbreite anzeigen. Sie können Details zu den Benutzern, Sitzungen, der Bandbreite und Startfehlern für eine Anwendung anzeigen.

Anwendungsdetails anzeigen

1. Navigieren Sie in NetScaler Console zu **Gateway > Gateway Insight > Anwendungen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Wählen Sie den Zeitraum aus, für den Sie die Anwendungsdetails anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.

Sie können nun die Anzahl der gestarteten Anwendungen, die Anzahl der gesamten und aktiven Sitzungen sowie die Anzahl der gesamten Bytes und die von den Anwendungen verbrauchte Bandbreite anzeigen.

Scrollen Sie nach unten, um die Anzahl der Sitzungen, die Bandbreite und die gesamten Bytes anzuzeigen, die von ICA® und anderen Anwendungen verbraucht werden.

Auf der Registerkarte **Andere Anwendungen** können Sie in der Spalte **Name** auf eine Anwendung klicken, um Details zu dieser Anwendung anzuzeigen.

Gateways

Sie können die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die gesamten Bytes und die Bandbreite, die von allen Gateways einer NetScaler Gateway Appliance zu einem bestimmten Zeitpunkt verwendet werden, anzeigen. Sie können die EPA-, Authentifizierungs-, Single Sign-On- und Anwendungsstartfehler für ein Gateway anzeigen. Sie können auch die Details aller Benutzer, die einem Gateway zugeordnet sind, und deren Anmeldeaktivitäten anzeigen.

Gateway-Details anzeigen

1. Navigieren Sie in der NetScaler Console zu **Gateway > Gateway Insight > Gateways**.
2. Wählen Sie den Zeitraum aus, für den Sie die Gateway-Details anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.

Sie können nun die Anzahl der Gateways, die Anzahl der aktiven Sitzungen, die gesamten Bytes und die Bandbreite, die von allen Gateways einer NetScaler Gateway Appliance zu einem bestimmten Zeitpunkt verwendet werden, anzeigen.

Scrollen Sie nach unten, um die Gateway-Details wie Gateway-Domänenname, Name des virtuellen Servers, NetScaler-IP-Adresse, Sitzungsmodi und Gesamtbytes anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können auf ein Gateway in der Spalte **Gateway-Domänenname** klicken, um die EPA-, Authentifizierungs-, Single Sign-On- und Anwendungsstartfehler sowie weitere Details für ein Gateway anzuzeigen.

Sie können auch eine Geo-Karte für Gateways anzeigen, mit der Sie Benutzer nach einem bestimmten Standort filtern können.

1. Navigieren Sie zu **Gateway > Gateway Insight > Gateways**
2. Wählen Sie einen Gateway-Domänennamen aus, um die Geo-Karte anzuzeigen
3. Klicken Sie auf ein Land. Zum Beispiel, Vereinigte Staaten

   Die Geo-Karte zeigt Details wie Benutzerliste, aktive Sitzungen, beendete Sitzungen und Anwendungen für das ausgewählte Land an.

Berichte exportieren

Sie können die Gateway Insight-Berichte mit allen in der GUI angezeigten Details im PDF-, JPEG-, PNG- oder CSV-Format auf Ihrem lokalen Computer speichern. Sie können den Export der Berichte auch in bestimmten Intervallen an angegebene E-Mail-Adressen planen.

HINWEIS

- Benutzer mit schreibgeschütztem Zugriff können keine Berichte exportieren.
- Geo-Kartenberichte werden nur exportiert, wenn die NetScaler Console über eine Internetverbindung verfügt.

Einen Bericht exportieren

1. Klicken Sie auf der Registerkarte **Dashboard** im rechten Bereich auf die Schaltfläche **Exportieren**.
2. Wählen Sie unter **Jetzt exportieren** das gewünschte Format aus und klicken Sie dann auf **Exportieren**.

So planen Sie den Export:

1. Klicken Sie auf der Registerkarte **Dashboard** im rechten Bereich auf die Schaltfläche **Exportieren**.
2. Geben Sie unter **Export planen** die Details an und klicken Sie auf **Planen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Konfigurieren Sie die E-Mail-Servereinstellungen, bevor Sie den Bericht planen, indem Sie zu **System** > **Benachrichtigungen** > **E-Mail** navigieren und auf **Hinzufügen** klicken.

So fügen Sie einen E-Mail-Server oder eine E-Mail-Verteilerliste hinzu:

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System** > **Benachrichtigungen** > **E-Mail**.
2. Wählen Sie im rechten Bereich **E-Mail-Server**, um einen E-Mail-Server hinzuzufügen, oder wählen Sie **E-Mail-Verteilerliste**, um eine E-Mail-Verteilerliste zu erstellen.
3. Geben Sie die Details an und klicken Sie auf **Erstellen**.

So exportieren Sie das gesamte Gateway Insight-Dashboard:

1. Klicken Sie auf der Registerkarte **Dashboard** im rechten Bereich auf die Schaltfläche **Exportieren**.
2. Wählen Sie unter **Jetzt exportieren** das **PDF**-Format und klicken Sie dann auf **Exportieren**.

Gateway Insight-Anwendungsfälle

Die folgenden Anwendungsfälle zeigen, wie Sie Gateway Insight verwenden können, um Einblick in die Zugriffsdetails, Anwendungen und Gateways der Benutzer auf NetScaler Gateway-Appliances zu erhalten.

1. Benutzer kann sich nicht bei der NetScaler Gateway-Appliance oder bei den internen Webservern anmelden

Sie sind ein NetScaler Gateway-Administrator, der NetScaler Gateway-Appliances über NetScaler Console überwacht, und Sie möchten sehen, warum sich ein Benutzer nicht anmelden kann oder in welcher Phase des Anmeldevorgangs der Fehler aufgetreten ist.

NetScaler Console ermöglicht es Ihnen, die Fehlerdetails der Benutzeranmeldung in den folgenden Phasen des Anmeldevorgangs anzuzeigen:

- Authentifizierung
- Endpunktanalyse (EPA)
- Einmaliges Anmelden

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In NetScaler Console können Sie nach einem bestimmten Benutzer suchen und dann alle Details für diesen Benutzer anzeigen.

So suchen Sie nach einem Benutzer:

Navigieren Sie in NetScaler Console zu **Gateway > Gateway Insight**, und geben Sie im Textfeld **Search for Users** den Benutzer ein, den Sie suchen möchten.

Authentifizierungsfehler

Sie können Authentifizierungsfehler wie falsche Anmeldeinformationen oder keine Antwort vom Authentifizierungsserver anzeigen. Wenn Sie eine zweistufige Authentifizierung eingerichtet haben, können Sie sehen, ob die primäre, sekundäre oder beide Stufen der Authentifizierung fehlgeschlagen sind.

Details zu Authentifizierungsfehlern anzeigen

1. Navigieren Sie in NetScaler Console zu **Gateway > Gateway Insight**.
2. Wählen Sie im Abschnitt **Overview** den Zeitraum aus, für den Sie die Authentifizierungsfehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.
3. Klicken Sie auf die Registerkarte **Authentication**. Sie können die Anzahl der Authentifizierungsfehler zu einem bestimmten Zeitpunkt im Diagramm **Failures** anzeigen.

Scrollen Sie nach unten, um Details zu jedem Authentifizierungsfehler anzuzeigen, z. B. **Username, Client IP Address, Error Time, Authentication type, Authentication Server IP Address** und mehr aus der Tabelle auf derselben Registerkarte. Die Spalte **Error Description** in der Tabelle zeigt den Grund für den Anmeldefehler an, und die Spalte **State** zeigt an, in welcher Phase einer zweistufigen Authentifizierung der Fehler aufgetreten ist.

Sie können in der Spalte **Username** auf einen Benutzer klicken, um die Authentifizierungsfehler und andere Details für diesen Benutzer anzuzeigen.

Sie können die Tabelle anpassen, um Spalten mithilfe der Einstellungsoption hinzuzufügen oder zu löschen.

EPA-Fehler

Sie können EPA-Fehler in der Vor- oder Nachauthentifizierungsphase anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EPA-Fehlerdetails anzeigen

1. Navigieren Sie in NetScaler Console zu **Gateway > Gateway Insight**.
2. Wählen Sie im Abschnitt Übersicht den Zeitraum aus, für den Sie die EPA-Fehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.
3. Klicken Sie auf die Registerkarte **EPA (End Point Analysis)**. Die Anzahl der EPA-Fehler zu einem bestimmten Zeitpunkt können Sie im Diagramm **Fehler** anzeigen.

Scrollen Sie nach unten, um Details zu jedem EPA-Fehler anzuzeigen, wie z. B. **Benutzername, NetScaler IP-Adresse, Gateway IP-Adresse, VPN, Fehlerzeit, Richtlinienname, Gateway-Domänenname** und mehr aus der Tabelle auf derselben Registerkarte. Die Spalte **Fehlerbeschreibung** in der Tabelle zeigt den Grund für den EPA-Fehler an, und die Spalte **Richtlinienname** zeigt die Richtlinie an, die zum Fehler geführt hat.

Sie können auf einen Benutzer in der Spalte **Benutzername** klicken, um die EPA-Fehler und andere Details für diesen Benutzer anzuzeigen.

Sie können die Tabelle anpassen, um Spalten mithilfe der Einstellungsoption hinzuzufügen oder zu löschen.

HINWEIS

NetScaler Gateway meldet die EPA-Fehler nicht, wenn der Ausdruck „clientSecurity“ als VPN-Sitzungsrichtlinienregel konfiguriert ist.

SSO-Fehler

Sie können alle SSO-Fehler in jeder Phase für einen Benutzer anzeigen, der über die NetScaler Gateway-Appliance auf Anwendungen zugreift.

SSO-Fehlerdetails anzeigen

1. Navigieren Sie in NetScaler Console zu **Gateway > Gateway Insight**.
2. Wählen Sie im Abschnitt Übersicht den Zeitraum aus, für den Sie die SSO-Fehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Klicken Sie auf die Registerkarte **SSO (Single Sign On)**. Sie können die Anzahl der SSO-Fehler zu einem bestimmten Zeitpunkt im Diagramm „Fehler“ anzeigen.

Scrollen Sie nach unten, um Details zu jedem SSO-Fehler anzuzeigen, wie z. B. **Benutzername, NetScaler IP-Adresse, Fehlerzeit, Fehlerbeschreibung, Ressourcenname** und mehr aus der Tabelle auf derselben Registerkarte.

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die SSO-Fehler und andere Details für diesen Benutzer anzuzeigen.

Sie können die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen, indem Sie die Option „Einstellungen“ verwenden.

2. Nach erfolgreicher Anmeldung bei NetScaler Gateway kann ein Benutzer keine virtuelle Anwendung starten

Bei einem Fehler beim Starten einer Anwendung können Sie die Gründe dafür einsehen, z. B. eine unzugängliche Secure Ticket Authority (STA) oder einen Citrix Virtual App-Server oder ein ungültiges STA-Ticket. Sie können den Zeitpunkt des Fehlers, die Fehlerdetails und die Ressource anzeigen, für die die STA-Validierung fehlgeschlagen ist.

Details zu Fehlern beim Anwendungsstart anzeigen

1. Navigieren Sie in NetScaler Console zu **Gateway > Gateway Insight**.
2. Wählen Sie im Abschnitt **Übersicht** den Zeitraum aus, für den Sie die SSO-Fehler anzeigen möchten. Sie können den Zeitschieberegler verwenden, um den ausgewählten Zeitraum weiter anzupassen. Klicken Sie auf **Go**.
3. Klicken Sie auf die Registerkarte **Anwendungsstart**. Sie können die Anzahl der Fehler beim Anwendungsstart zu einem bestimmten Zeitpunkt im Diagramm **Fehler** anzeigen.

Scrollen Sie nach unten, um Details zu jedem Fehler beim Anwendungsstart anzuzeigen, wie z. B. **NetScaler IP-Adresse, Fehlerzeit, Fehlerbeschreibung, Ressourcenname, Gateway-Domänenname** und mehr, aus der Tabelle auf derselben Registerkarte. Die Spalte **Fehlerbeschreibung** in der Tabelle zeigt die IP-Adresse des STA-Servers an, und die Spalte **Ressourcenname** zeigt die Details der Ressource an, für die die STA-Validierung fehlgeschlagen ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können in der Spalte **Benutzername** auf einen Benutzer klicken, um die Fehler beim Anwendungsstart und andere Details für diesen Benutzer anzuzeigen.

Sie können die Tabelle anpassen, um Spalten hinzuzufügen oder zu löschen, indem Sie die Option Einstellungen verwenden.

3. Nachdem eine neue Anwendung erfolgreich gestartet wurde, möchte ein Benutzer die von dieser Anwendung verbrauchten Gesamtbytes und die Bandbreite anzeigen

Nachdem Sie eine neue Anwendung erfolgreich gestartet haben, können Sie in NetScaler Console die von dieser Anwendung verbrauchten Gesamtbytes und die Bandbreite anzeigen.

Gesamtbytes und Bandbreite, die von einer Anwendung verbraucht werden, anzeigen

Navigieren Sie in NetScaler Console zu **Gateway > Gateway Insight > Applications**, scrollen Sie nach unten und klicken Sie auf der Registerkarte **Other Applications** auf die Anwendung, für die Sie die Details anzeigen möchten.

Sie können die Anzahl der Sitzungen und die Gesamtanzahl der Bytes anzeigen, die von dieser Anwendung verbraucht werden.

Sie können auch die Bandbreite anzeigen, die von dieser Anwendung verbraucht wird.

4. Ein Benutzer hat sich erfolgreich bei NetScaler Gateway angemeldet, kann aber nicht auf bestimmte Netzwerkressourcen im internen Netzwerk zugreifen

Mit Gateway Insight können Sie feststellen, ob der Benutzer Zugriff auf die Netzwerkressourcen hat oder nicht. Sie können auch den Namen der Richtlinie anzeigen, die zum Fehler geführt hat.

Benutzerzugriff auf Ressourcen anzeigen

1. Navigieren Sie in NetScaler Console zu **Gateway > Gateway Insight > Applications**.
2. Scrollen Sie auf dem angezeigten Bildschirm nach unten, und wählen Sie auf der Registerkarte **Andere Anwendungen** die Anwendung aus, bei der sich der Benutzer nicht anmelden konnte.

Ressourcenzugriff(/en-us/netscaler-console-service/media/use-cases-resource-access.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Auf dem angezeigten Bildschirm scrollen Sie nach unten, und in der Tabelle **Benutzer** werden alle Benutzer angezeigt, die Zugriff auf diese Anwendung haben.

Ressourcenzugriff1(/en-us/netscaler-console-service/media/use-cases-resource-access-users.png)

5. Verschiedene Benutzer verwenden möglicherweise unterschiedliche NetScaler Gateway-Bereitstellungen oder melden sich über verschiedene Zugriffsmodi bei NetScaler Gateway an. Der Administrator muss Details zu den Bereitstellungstypen und Zugriffsmodi anzeigen können

Mit Gateway Insight können Sie eine Zusammenfassung der verschiedenen Sitzungsmodi, die von Benutzern zur Anmeldung verwendet werden, der Clienttypen und der Anzahl der pro Stunde angemeldeten Benutzer anzeigen. Sie können auch feststellen, ob die Bereitstellung eines Benutzers ein Unified Gateway oder eine klassische NetScaler Gateway-Bereitstellung ist. Bei Unified Gateway-Bereitstellungen können Sie den Namen und die IP-Adresse des Content Switching Virtual Servers sowie den Namen des VPN Virtual Servers anzeigen.

Zusammenfassung der Sitzungsmodi, Clienttypen und Anzahl der angemeldeten Benutzer anzeigen

1. Navigieren Sie in NetScaler Console zu **Gateway > Gateway Insight**.
2. Scrollen Sie im Abschnitt **Übersicht** nach unten, um die Diagramme **Sitzungsmodus, Betriebssysteme, Browser** und **Benutzeranmeldeaktivität** anzuzeigen, die die verschiedenen Sitzungsmodi, die von Benutzern zur Anmeldung verwendet werden, die Clienttypen und die Anzahl der pro Stunde angemeldeten Benutzer darstellen.

Sitzung(/en-us/netscaler-console-service/media/use-cases-deployment-types-access-modes-summary.png)

Sitzung1(/en-us/netscaler-console-service/media/use-cases-deployment-types-access-modes-user-log-activity.png)

Beheben von Gateway Insight-Problemen

Wenn die Gateway Insight-Lösung nicht wie erwartet funktioniert, könnte das Problem bei einem der folgenden Punkte liegen. Beachten Sie die Checklisten in den jeweiligen Abschnitten zur Fehlerbehebung.

- Gateway Insight-Konfiguration.
- Konnektivitätsproblem zwischen NetScaler und NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Datensatzgenerierung in NetScaler.
- Validierungen in NetScaler Console.

Checkliste für die Gateway Insight-Konfiguration

- Stellen Sie sicher, dass die AppFlow-Funktion in NetScaler aktiviert ist. Weitere Informationen finden Sie unter AppFlow aktivieren.
- Überprüfen Sie die Gateway Insight-Konfiguration in der laufenden NetScaler-Konfiguration.

  Führen Sie den Befehl `show running | grep -i <appflow_policy>` aus, um die Gateway Insight-Konfiguration zu überprüfen. Stellen Sie sicher, dass der Bindungstyp REQUEST ist. Zum Beispiel;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

- Stellen Sie für Single-Hop-, Access Gateway- oder Unified Gateway-Bereitstellungen sicher, dass die Gateway Insight AppFlow-Richtlinie an den virtuellen VPN-Server gebunden ist, über den der VPN-Verkehr fließt. Weitere Informationen finden Sie unter HDX Insight-Datenerfassung aktivieren.
- Überprüfen Sie den Parameter `appflowlog` im virtuellen NetScaler Gateway/VPN-Server. Weitere Informationen finden Sie unter AppFlow für virtuelle Server aktivieren.

Checkliste für die Konnektivität zwischen NetScaler und NetScaler Console

- Überprüfen Sie den Status des AppFlow-Collectors in NetScaler. Weitere Informationen finden Sie unter So überprüfen Sie den Konnektivitätsstatus zwischen NetScaler und AppFlow Collector.
- Überprüfen Sie die Treffer der Gateway Insight AppFlow®-Richtlinie.

  Führen Sie den Befehl `show appflow policy <policy_name>` aus, um die Treffer der AppFlow-Richtlinie zu überprüfen.

  Sie können auch in der GUI zu **System > AppFlow > Policies** navigieren, um die Treffer der AppFlow-Richtlinie zu überprüfen.
- Überprüfen Sie, ob eine Firewall die AppFlow-Ports 4739 oder 5557 blockiert.

Datensatzgenerierung in der NetScaler-Checkliste

- Führen Sie den Befehl `nsconmsg -d stats -g ai_tot` aus und überprüfen Sie die Statistikinkremente in NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Erfassen Sie `nstrace`-Protokolle und suchen Sie nach CFLOW-Paketen, um zu bestätigen, dass NetScaler AppFlow-Datensätze exportiert.

Validierungen in NetScaler Console

- Führen Sie den Befehl `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` aus, um die Protokolle zu überprüfen und zu bestätigen, dass NetScaler Console AppFlow-Datensätze empfängt.
- Stellen Sie sicher, dass die NetScaler-Instanz zu NetScaler Console hinzugefügt wurde.
- Stellen Sie sicher, dass der virtuelle NetScaler Gateway/VPN-Server in NetScaler Console lizenziert ist.

Gateway Insight-Statistiken

Die folgenden Gateway Insight-Statistiken sind verfügbar.

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled

Wenden Sie sich an den technischen Support von Citrix

Für eine schnelle Lösung stellen Sie sicher, dass Sie die folgenden Informationen haben, bevor Sie sich an den technischen Support von Citrix wenden:

- Details der Bereitstellung und Netzwerktopologie.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler- und NetScaler Console-Versionen.
- Tech-Support-Bundle für NetScaler und NetScaler Console.
- `nstrace`-Erfassung während des Problems.

Bekannte Probleme

Siehe NetScaler-Versionshinweise für bekannte Probleme bei Gateway Insight.

HDX™ Insight

HDX Insight bietet End-to-End-Transparenz für den HDX-Datenverkehr zu Citrix Virtual Apps and Desktops, der NetScaler passiert. Es ermöglicht Administratoren auch, Echtzeit-Client- und Netzwerklatenzmetriken, Verlaufsberichte, End-to-End-Leistungsdaten anzuzeigen und Leistungsprobleme zu beheben. Die Verfügbarkeit von Echtzeit- und Verlaufs-Transparenzdaten ermöglicht es NetScaler Console, eine Vielzahl von Anwendungsfällen zu unterstützen.

Damit Daten angezeigt werden, müssen Sie AppFlow auf Ihren virtuellen NetScaler Gateway-Servern aktivieren. AppFlow kann über das **IPFIX**-Protokoll oder die **Logstream**-Methode bereitgestellt werden.

HINWEIS

Damit ICA®-Roundtrip-Zeitberechnungen protokolliert werden können, aktivieren Sie die folgenden Richtlinieneinstellungen:

- ICA-Roundtrip-Berechnung
- ICA-Roundtrip-Berechnungsintervall
- ICA-Roundtrip-Berechnung für inaktive Verbindungen

Wenn Sie auf einen einzelnen Benutzer klicken, sehen Sie jede HDX-Sitzung, aktiv oder beendet, die der Benutzer innerhalb des ausgewählten Zeitrahmens durchgeführt hat. Weitere Informationen umfassen mehrere Latenzstatistiken und die während der Sitzung verbrauchte Bandbreite. Sie können auch Bandbreiteninformationen von einzelnen virtuellen Kanälen wie Audio, Druckerzuordnung und Clientlaufwerkszuordnung abrufen.

Sie können auch eine konsolidierte Ansicht aller aktiven und beendeten Sitzungen von Benutzern visualisieren.

Als Administrator ermöglicht Ihnen diese Ansicht:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Alle Benutzerdetails in einer Single-Pane-Visualisierung anzeigen
- Die Komplexität eliminieren, jeden Benutzer auszuwählen und die aktiven und beendeten Sitzungen anzuzeigen

HINWEIS

Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, der Gruppe Zugriff auf Anwendungsebene gewähren und Benutzer der Gruppe zuweisen. NetScaler Console Analytics unterstützt jetzt die Autorisierung basierend auf virtuellen IP-Adressen. Ihre Benutzer können nun Berichte für alle Insights nur für die Anwendungen (virtuelle Server) sehen, für die sie autorisiert sind. Weitere Informationen zu Gruppen und zum Zuweisen von Benutzern zu einer Gruppe finden Sie unter Konfigurieren von Gruppen in NetScaler Console.

Sie können auch zu **HDX Insight** > **Anwendungen** navigieren und auf **Startdauer** klicken, um die Startzeit der Anwendung anzuzeigen. Sie können auch den User Agent aller verbundenen Benutzer anzeigen, indem Sie zu **HDX Insight > Benutzer** navigieren.

HINWEIS

HDX Insight unterstützt Admin-Partitionen, die in NetScaler-Instanzen mit Softwareversion 12.0 konfiguriert sind.

Die folgenden Thin Clients unterstützen HDX Insight:

- WYSE Windows-basierte Thin Clients
- WYSE Linux-basierte Thin Clients
- WYSE ThinOS-basierte Thin Clients
- 10ZiG Ubuntu-basierte Thin Clients

Ermitteln der Grundursache für langsame Leistungsprobleme

Szenario 1

Benutzer erlebt Verzögerungen beim Zugriff auf Citrix Virtual Apps and Desktops

Die Verzögerungen können auf Latenz im Servernetzwerk, durch das Servernetzwerk verursachte ICA-Verkehrsverzögerungen oder Latenz im Clientnetzwerk zurückzuführen sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Um die Grundursache des Problems zu ermitteln, analysieren Sie die folgenden Metriken:

- WAN-Latenz
- DC-Latenz
- Host-Verzögerung

So zeigen Sie die Client-Metriken an:

1. Wählen Sie auf der Registerkarte **Analytics** die Option **HDX Insight** > **Benutzer**.
2. Scrollen Sie nach unten, wählen Sie den Benutzernamen und wählen Sie den Zeitraum aus der Liste aus. Der Zeitraum kann ein Tag, eine Woche, ein Monat sein, oder Sie können den Zeitraum, für den Sie die Daten anzeigen möchten, sogar anpassen.
3. Das Diagramm zeigt die ICA-RTT- und DC-Latenzwerte des Benutzers für den angegebenen Zeitraum als Grafik an.

4. Bewegen Sie in der Tabelle **Aktuelle Anwendungssitzungen** den Mauszeiger über den **RTT**-Wert und notieren Sie die Werte für Host-Verzögerung, DC-Latenz und WAN-Latenz.
5. Klicken Sie in der Tabelle **Aktuelle Anwendungssitzungen** auf das Hop-Diagrammsymbol, um Informationen zur Verbindung zwischen Client und Server anzuzeigen, einschließlich der Latenzwerte.

Zusammenfassung:

In diesem Beispiel beträgt die **DC-Latenz** 751 Millisekunden, die **WAN-Latenz** 52 Millisekunden und die **Host-Verzögerung** 6 Sekunden. Dies deutet darauf hin, dass der Benutzer aufgrund der durchschnittlichen Latenz, die durch das Servernetzwerk verursacht wird, eine Verzögerung erfährt.

Szenario 2

Benutzer erfährt Verzögerung beim Starten einer Anwendung auf Citrix Virtual Apps™ oder Desktops

Die Verzögerung kann auf Latenz im Servernetzwerk, ICA-Verkehrsverzögerungen durch das Servernetzwerk, Latenz im Clientnetzwerk oder die zum Starten einer Anwendung benötigte Zeit zurückzuführen sein.

Um die Grundursache des Problems zu identifizieren, analysieren Sie die folgenden Metriken:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- WAN-Latenz
- DC-Latenz
- Host-Verzögerung

So zeigen Sie die Benutzermetriken an:

1. Navigieren Sie zu **Gateway** > **HDX Insight** > **Benutzer**.
2. Scrollen Sie nach unten und klicken Sie auf den Benutzernamen.
3. Beachten Sie in der grafischen Darstellung die Werte für WAN-Latenz, DC-Latenz und RTT für die jeweilige Sitzung.
4. Beachten Sie in der Tabelle **Aktuelle Anwendungssitzungen**, dass die Host-Verzögerung hoch ist.

Zusammenfassung:

In diesem Beispiel beträgt die **DC-Latenz** 1 Millisekunde, die **WAN-Latenz** 12 Millisekunden, aber die **Host-Verzögerung** 517 Millisekunden. Eine hohe RTT bei niedrigen DC- und WAN-Latenzen deutet auf einen Anwendungsfehler auf dem Host-Server hin.

HINWEIS

HDX Insight zeigt auch weitere Benutzermetriken an, wie z. B. WAN-Jitter und serverseitige Neuübertragungen, wenn Sie NetScaler Console mit Software 11.1 Build 51.21 oder höher verwenden. Um diese Metriken anzuzeigen, navigieren Sie zu **Gateway** > **HDX Insight** > **Benutzer**, und wählen Sie einen Benutzernamen aus. Die Benutzermetriken werden in der Tabelle neben dem Diagramm angezeigt.

Geokarte für HDX Insight

Die Geokartenfunktion in NetScaler Console zeigt die Nutzung von Webanwendungen an verschiedenen geografischen Standorten auf einer Karte an. Als Administrator können Sie diese Informationen nutzen, um Trends bei der Anwendungsnutzung zu verstehen und für die Kapazitätsplanung.

Die Geokarte liefert Informationen zu den folgenden Metriken, spezifisch für ein Land, einen Bundesstaat und eine Stadt:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Gesamtzahl der Zugriffe: Gesamtzahl der Zugriffe auf eine Anwendung.
- Bandbreite: Gesamtbandbreite, die beim Bedienen von Clientanfragen verbraucht wird
- Antwortzeit: Durchschnittliche Zeit, die zum Senden von Antworten auf Clientanfragen benötigt wird.

Die Geokarte liefert Informationen, die zur Lösung verschiedener Anwendungsfälle verwendet werden können, wie die folgenden:

- Region mit der maximalen Anzahl von Clients, die auf eine Anwendung zugreifen
- Region mit der höchsten Antwortzeit
- Region, die die meiste Bandbreite verbraucht

NetScaler Console **aktiviert automatisch** Geokarten für private IP-Adressen oder öffentliche IP-Adressen, wenn Sie **Web Insight** aktivieren.

Einen privaten IP-Block erstellen

NetScaler Console kann den Standort eines Clients erkennen, wenn die private IP-Adresse des Clients zum NetScaler Console-Server hinzugefügt wird. Wenn beispielsweise die IP-Adresse eines Clients in den Bereich eines privaten IP-Adressblocks fällt, der mit Stadt A verknüpft ist, erkennt NetScaler Console, dass der Datenverkehr für diesen Client aus Stadt A stammt.

So erstellen Sie einen IP-Block:

1. Navigieren Sie in NetScaler Console zu **Einstellungen > Analyseeinstellungen > IP-Blöcke**, und klicken Sie dann auf **Hinzufügen**.
2. Auf der Seite **IP-Blöcke erstellen** geben Sie die folgenden Parameter an:
    - **Name**. Geben Sie einen Namen für den privaten IP-Block an
    - **Start-IP-Adresse**. Geben Sie den niedrigsten IP-Adressbereich für den IP-Block an.
    - **End-IP-Adresse**. Geben Sie den höchsten IP-Adressbereich für den IP-Block an.
    - **Land**. Wählen Sie das Land aus der Liste aus.
    - **Region**. Basierend auf dem Land wird die Region automatisch ausgefüllt, Sie können aber Ihre Region auswählen.
    - **Stadt**. Basierend auf der Region wird die Stadt automatisch ausgefüllt, Sie können aber Ihre Stadt auswählen.
    - **Stadtbreitengrad** und **Stadtlängengrad**. Basierend auf der von Ihnen ausgewählten Stadt werden Breitengrad und Längengrad automatisch ausgefüllt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Klicken Sie auf **Erstellen**, um den Vorgang abzuschließen.

Öffentliche IP-Blöcke

NetScaler Console kann auch den Client-Standort erkennen, wenn der Client eine öffentliche IP-Adresse verwendet. NetScaler Console verfügt über eine integrierte CSV-Datei für Standorte, die den Standort basierend auf dem IP-Adressbereich des Clients abgleicht. Um öffentliche IP-Blöcke zu verwenden, müssen Sie lediglich die Erfassung von **Geodaten aktivieren** auf der Seite „Insight konfigurieren“ aktivieren.

Hinweis

NetScaler Console benötigt eine Internetverbindung, um die Geomaps für einen bestimmten geografischen Standort anzuzeigen. Eine Internetverbindung ist auch erforderlich, um die GeoMap in den Formaten .pdf, .png oder .jpg zu exportieren.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu exportieren, klicken Sie oben rechts auf dieser Seite auf das Symbol **Exportieren**. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren**. Um den Bericht im PDF-, JPEG-, PNG- oder CSV-Format anzuzeigen und zu speichern.
2. Wählen Sie die Registerkarte **Export planen**. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu senden.

HINWEIS

- Wenn Sie die Wiederholung **Wöchentlich** auswählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie die Wiederholung **Monatlich** auswählen, stellen Sie sicher, dass Sie alle Tage, an denen der Bericht geplant werden soll, durch Kommas getrennt eingeben.

So konfigurieren Sie eine Geomap für Rechenzentren:

Auf der Registerkarte **Infrastruktur** navigieren Sie zu **Sites** > **Private IP-Blöcke**, um Geomaps für einen bestimmten Standort zu konfigurieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Anwendungsfall

Betrachten Sie ein Szenario, in dem die Organisation ABC zwei Niederlassungen hat, eine in Santa Clara und die andere in Indien.

Die Benutzer in Santa Clara verwenden die NetScaler Gateway-Appliance unter SClara.x.com, um auf VPN-Verkehr zuzugreifen. Die indischen Benutzer verwenden die NetScaler Gateway-Appliance unter India.x.com, um auf VPN-Verkehr zuzugreifen.

In einem bestimmten Zeitintervall, sagen wir von 10 Uhr morgens bis 17 Uhr nachmittags, verbinden sich die Benutzer in Santa Clara mit SClara.x.com, um auf VPN-Verkehr zuzugreifen. Die meisten Benutzer greifen auf dasselbe NetScaler Gateway zu, was zu einer Verzögerung beim Verbindungsaufbau zum VPN führt, sodass einige Benutzer stattdessen eine Verbindung zu India.x.com herstellen, anstatt zu SClara.x.com.

Ein NetScaler-Administrator, der den Datenverkehr analysiert, kann die Geomap-Funktionalität verwenden, um den Datenverkehr im Büro in Santa Clara anzuzeigen. Die Karte zeigt, dass die Antwortzeit im Büro in Santa Clara hoch ist, da das Büro in Santa Clara nur eine NetScaler Gateway-Appliance besitzt, über die Benutzer auf VPN-Verkehr zugreifen können. Der Administrator könnte daher beschließen, ein weiteres NetScaler Gateway zu installieren, damit die Benutzer zwei lokale NetScaler Gateway-Appliances haben, über die sie auf das VPN zugreifen können.

Einschränkungen

Wenn NetScaler-Instanzen über eine Advanced-Lizenz verfügen, werden die in NetScaler Console für HDX Insight festgelegten Schwellenwerte nicht ausgelöst, da Analysedaten nur für 1 Stunde gesammelt werden.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu exportieren, klicken Sie auf das Symbol **Exportieren** oben rechts auf dieser Seite. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren**. Um den Bericht im PDF-, JPEG-, PNG- oder CSV-Format anzuzeigen und zu speichern.
2. Wählen Sie die Registerkarte **Export planen**. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu senden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

- Wenn Sie die Wiederholung **Wöchentlich** auswählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie die Wiederholung **Monatlich** auswählen, stellen Sie sicher, dass Sie alle Tage, an denen der Bericht geplant werden soll, durch Kommas getrennt eingeben.

HDX™ Insight-Datenerfassung aktivieren

HDX Insight ermöglicht dem Administrator, ein außergewöhnliches Benutzererlebnis zu bieten, indem es eine End-to-End-Transparenz für den ICA-Datenverkehr bietet, der die NetScaler-Appliance durchläuft.

HDX Insight bietet überzeugende und leistungsstarke Funktionen für Business Intelligence und Fehleranalyse für das Netzwerk, virtuelle Desktops, Anwendungen und die Anwendungsarchitektur. HDX Insight kann Benutzerprobleme sofort beheben, Daten über virtuelle Desktop-Verbindungen sammeln, AppFlow®-Datensätze generieren und diese als visuelle Berichte darstellen.

Die Konfiguration zur Aktivierung der Datenerfassung in den NetScaler-Instanzen unterscheidet sich je nach Position der Appliance in der Bereitstellungstopologie. Dieses Thema enthält die folgenden Details:

- Aktivieren der Datenerfassung zur Überwachung von NetScaler-Instanzen, die im transparenten Modus bereitgestellt werden
- Aktivieren der Datenerfassung für NetScaler Gateway-Appliances, die im Single-Hop-Modus bereitgestellt werden
- Aktivieren der Datenerfassung für NetScaler Gateway-Appliances, die im Double-Hop-Modus bereitgestellt werden
- Aktivieren der Datenerfassung zur Überwachung von NetScalern, die im LAN-Benutzermodus bereitgestellt werden

Datenerfassung für im Single-Hop-Modus bereitgestellte NetScaler Gateway Appliances aktivieren

Wenn NetScaler Gateway im Single-Hop-Modus bereitgestellt wird, befindet sich das NetScaler Gateway am Netzwerkrand und leitet ICA-Verbindungen an die Desktop-Bereitstellungsinfrastruktur weiter. Diese Bereitstellung ist die einfachste und häufigste

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bereitstellung. Dieser Modus bietet Sicherheit, wenn ein externer Benutzer versucht, auf das interne Netzwerk einer Organisation zuzugreifen. Im Single-Hop-Modus greifen Benutzer über ein virtuelles privates Netzwerk (VPN) auf die NetScaler Appliances zu.

Um mit der Erfassung der Berichte zu beginnen, müssen Sie die NetScaler Gateway Appliance zum NetScaler Console-Inventar hinzufügen und AppFlow auf NetScaler Console aktivieren. Die folgende Abbildung zeigt eine im Single-Hop-Modus bereitgestellte NetScaler Console

AppFlow-Funktion über NetScaler Console aktivieren

1. Navigieren Sie zu **Infrastruktur** > **Instanzen**, und wählen Sie die NetScaler-Instanz aus, für die Sie Analysen aktivieren möchten.
2. Wählen Sie aus der Liste **Aktion auswählen** die Option **Analysen konfigurieren**.
3. Wählen Sie die VPN-virtuellen Server aus und klicken Sie auf **Analysen aktivieren**.
4. Wählen Sie **Web Insight**.
5. Klicken Sie auf **OK**.

HINWEIS

Die folgenden Befehle werden im Hintergrund ausgeführt, wenn Sie AppFlow® im Single-Hop-Modus aktivieren. Diese Befehle werden hier explizit zu Fehlerbehebungszwecken angegeben.

- `add appflow collector \<name\> -IPAddress \<ip\_addr\>`
- `add appflow action \<name\> -collectors \<string\>`
- `set appflow param -flowRecordInterval \<secs\>`
- `disable ns feature AppFlow`
- `enable ns feature AppFlow`
- `add appflow policy \<name\> \<rule\> \<expression\>`
- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Datenerfassung zur Überwachung von NetScalern im transparenten Modus aktivieren

Wenn ein NetScaler im transparenten Modus bereitgestellt wird, können die Clients direkt auf die Server zugreifen, ohne einen dazwischengeschalteten virtuellen Server. Wenn eine NetScaler Appliance im transparenten Modus in einer Citrix Virtual Apps and Desktops-Umgebung bereitgestellt wird, wird der ICA-Datenverkehr nicht über ein VPN übertragen.

Nachdem Sie den NetScaler zum NetScaler Console-Bestand hinzugefügt haben, müssen Sie AppFlow für die Datenerfassung aktivieren. Die Aktivierung der Datenerfassung hängt vom Gerät und dem Modus ab. In diesem Fall müssen Sie NetScaler Console als AppFlow-Collector auf jeder NetScaler Appliance hinzufügen und eine AppFlow-Richtlinie konfigurieren, um den gesamten oder spezifischen ICA-Datenverkehr zu erfassen, der durch die Appliance fließt.

HINWEIS

- Sie können die Datenerfassung auf einem im transparenten Modus bereitgestellten NetScaler nicht über das NetScaler Console-Konfigurationsprogramm aktivieren.
- Detaillierte Informationen zu den Befehlen und ihrer Verwendung finden Sie unter Befehlsreferenz.
- Informationen zu Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke.

Die folgende Abbildung zeigt die Netzwerkbereitstellung einer NetScaler Console, wenn ein NetScaler im transparenten Modus bereitgestellt wird:

So konfigurieren Sie die Datenerfassung auf einer NetScaler Appliance über die Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Melden Sie sich an einer Appliance an.
2. Geben Sie die ICA-Ports an, an denen die NetScaler Appliance auf Datenverkehr lauscht.

   ```
   set ns param --icaPorts \<port\>...
   ```

   Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set ns param -icaPorts 2598 1494
```

HINWEIS

- Mit diesem Befehl können Sie bis zu 10 Ports angeben.
- Die Standardportnummer ist 2598. Sie können die Portnummer bei Bedarf ändern.

3. Fügen Sie NetScaler Insight Center als AppFlow-Collector auf der NetScaler Appliance hinzu.

```
add appflow collector <name> -IPAddress <ip_addr>
```

Beispiel:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

HINWEIS

Um die auf der NetScaler Appliance konfigurierten AppFlow-Collectoren anzuzeigen, verwenden Sie den Befehl **show appflow collector**.

4. Erstellen Sie eine AppFlow®-Aktion und ordnen Sie den Collector der Aktion zu.

```
add appflow action <name> -collectors <string> ...
```

Beispiel:

```
add appflow action act -collectors MyInsight
```

5. Erstellen Sie eine AppFlow-Richtlinie, um die Regel für die Generierung des Datenverkehrs festzulegen.

```
add appflow policy <policyname> <rule> <action>
```

Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add appflow policy pol true act
```

6. Binden Sie die AppFlow-Richtlinie an einen globalen Bindungspunkt.

```
bind appflow global <policyname> <priority> -type <type>
```

Beispiel:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

HINWEIS

Der Wert von **type** muss ICA_REQ_OVERRIDE oder ICA_REQ_DEFAULT sein, um auf ICA®-Datenverkehr angewendet zu werden.

7. Legen Sie den Wert des Parameters flowRecordInterval für AppFlow auf 60 Sekunden fest.

```
set appflow param -flowRecordInterval 60
```

8. Speichern Sie die Konfiguration.

```
save ns config
```

Datenerfassung für im Double-Hop-Modus bereitgestellte NetScaler Gateway Appliances aktivieren

Der NetScaler Gateway Double-Hop-Modus bietet zusätzlichen Schutz für das interne Netzwerk einer Organisation, da ein Angreifer mehrere Sicherheitszonen oder demilitarisierte Zonen (DMZ) durchdringen müsste, um die Server im sicheren Netzwerk zu erreichen.

Als Administrator können Sie mit NetScaler Console Folgendes analysieren:

- Die Anzahl der Hops (NetScaler Gateway Appliances), durch die die ICA-Verbindungen laufen
- Die Details zur Latenz bei jeder TCP-Verbindung und wie sie sich im Vergleich zur gesamten vom Client wahrgenommenen ICA®-Latenz verhält

Die folgende Abbildung zeigt, dass die NetScaler Console und NetScaler Gateway in der ersten DMZ im selben Subnetz bereitgestellt werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Das NetScaler Gateway in der ersten DMZ verarbeitet Benutzerverbindungen und führt die Sicherheitsfunktionen eines SSL VPN aus. Dieses NetScaler Gateway verschlüsselt Benutzerverbindungen, bestimmt, wie die Benutzer authentifiziert werden, und steuert den Zugriff auf die Server im internen Netzwerk.

Das NetScaler Gateway in der zweiten DMZ dient als NetScaler Gateway Proxy-Gerät. Dieses NetScaler Gateway ermöglicht es dem ICA-Datenverkehr, die zweite DMZ zu durchqueren, um Benutzerverbindungen zur Serverfarm herzustellen.

Die NetScaler Console kann entweder im Subnetz, das zur NetScaler Gateway Appliance in der ersten DMZ gehört, oder im Subnetz, das zur NetScaler Gateway Appliance in der zweiten DMZ gehört, bereitgestellt werden.

Im Double-Hop-Modus erfasst NetScaler Console TCP-Datensätze von einer Appliance und ICA-Datensätze von der anderen Appliance. Nachdem Sie die NetScaler Gateway Appliances zum NetScaler Console-Inventar hinzugefügt und die Datenerfassung aktiviert haben, exportiert jede Appliance die Berichte, indem sie die Hop-Anzahl und die Verbindungs-Ketten-ID verfolgt.

Damit NetScaler Console identifizieren kann, welche Appliance Datensätze exportiert, wird jede Appliance mit einer Hop-Anzahl und jede Verbindung mit einer Verbindungs-Ketten-ID versehen. Die Hop-Anzahl stellt die Anzahl der NetScaler Gateway Appliances dar, durch die der Datenverkehr von einem Client zu den Servern fließt. Die Verbindungs-Ketten-ID stellt die End-to-End-Verbindungen zwischen Client und Server dar.

NetScaler Console verwendet die Hop-Anzahl und die Verbindungs-Ketten-ID, um die Daten von beiden NetScaler Gateway Appliances zu korrelieren und die Berichte zu generieren.

Um NetScaler Gateway Appliances, die in diesem Modus bereitgestellt werden, zu überwachen, müssen Sie zuerst das NetScaler Gateway zum NetScaler Console-Inventar hinzufügen, AppFlow auf NetScaler Console aktivieren und dann die Berichte auf dem NetScaler Console-Dashboard anzeigen.

Datenerfassung auf NetScaler Console aktivieren

Wenn Sie NetScaler Console so konfigurieren, dass die ICA-Details von beiden Appliances erfasst werden, sind die erfassten Details redundant. Um diese Situation zu vermeiden, müssen Sie AppFlow für TCP auf der ersten NetScaler Gateway Appliance und dann AppFlow für ICA auf der zweiten Appliance aktivieren. Dadurch exportiert eine der Appliances ICA-AppFlow-Datensätze und die andere Appliance TCP-AppFlow-Datensätze. Dies spart auch Verarbeitungszeit beim Parsen des ICA-Datenverkehrs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So aktivieren Sie die AppFlow-Funktion über NetScaler Console:

1. Navigieren Sie zu **Infrastructure** > **Instances**, und wählen Sie die NetScaler-Instanz aus, für die Sie Analysen aktivieren möchten.
2. Wählen Sie in der Liste **Select Action** die Option **Configure Analytics** aus.
3. Wählen Sie die virtuellen Server aus, und klicken Sie auf **Enable Security & Analytics**.
4. Wählen Sie Web **Insight**
5. Klicken Sie auf **OK**.

NetScaler Gateway Appliances für den Datenexport konfigurieren

Nach der Installation der NetScaler Gateway Appliances müssen Sie die folgenden Einstellungen auf den NetScaler Gateway Appliances konfigurieren, um die Berichte an NetScaler Console zu exportieren:

- Konfigurieren Sie virtuelle Server der NetScaler Gateway Appliances in der ersten und zweiten DMZ so, dass sie miteinander kommunizieren.
- Binden Sie den virtuellen NetScaler Gateway Server in der zweiten DMZ an den virtuellen NetScaler Gateway Server in der ersten DMZ.
- Aktivieren Sie Double Hop auf dem NetScaler Gateway in der zweiten DMZ.
- Deaktivieren Sie die Authentifizierung auf dem virtuellen NetScaler Gateway Server in der zweiten DMZ.
- Aktivieren Sie eine der NetScaler Gateway Appliances, um ICA-Datensätze zu exportieren.
- Aktivieren Sie die andere NetScaler Gateway Appliance, um TCP-Datensätze zu exportieren:
- Verbindungsverkettung auf beiden NetScaler Gateway Appliances aktivieren.

NetScaler Gateway über die Befehlszeilenschnittstelle konfigurieren:

1. Konfigurieren Sie den virtuellen NetScaler Gateway Server in der ersten DMZ so, dass er mit dem virtuellen NetScaler Gateway Server in der zweiten DMZ kommuniziert.

   VPN-NextHop-Server hinzufügen \<name\> \<nextHopIP\> \<nextHopPort\> \[**-secure** (ON|OFF)\] \[**-imgGifToPng**\] ...

   ```
   add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Binden Sie den virtuellen NetScaler Gateway Server in der zweiten DMZ an den virtuellen NetScaler Gateway Server in der ersten DMZ. Führen Sie den folgenden Befehl auf dem NetScaler Gateway in der ersten DMZ aus:

   VPN-vServer binden \<name\> **-nextHopServer** \<name\>

   ```
   bind vpn vserver vs1 -nextHopServer nh1
   ```

3. Double Hop und AppFlow auf dem NetScaler Gateway in der zweiten DMZ aktivieren.

   set vpn vserver \<name\> \[**- doubleHop** (AKTIVIERT |DEAKTIVIERT)\] \[**- appflowLog** (AKTIVIERT |DEAKTIVIERT)\]

   ```
   set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
   ```

4. Authentifizierung auf dem virtuellen NetScaler Gateway Server in der zweiten DMZ deaktivieren.

   set vpn vserver\<name\> \[**-authentication** (EIN|AUS)\]

   ```
   set vpn vserver vs -authentication OFF
   ```

5. Aktivieren Sie eine der NetScaler Gateway Appliances zum Exportieren von TCP-Datensätzen.

   bind vpn vserver\<Name\> \[**-policy**\<Zeichenfolge\> **-priority**\<positive_Ganzzahl\>\] \[**-type**\<Typ\>\]

   ```
   bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
   OTHERTCP\_REQUEST
   ```

6. Aktivieren Sie die andere NetScaler Gateway Appliance zum Exportieren von ICA-Datensätzen:

   bind vpn vserver\<Name\> \[**-policy**\<Zeichenfolge\> **-priority**\<positive_Ganzzahl\>\] \[**-type**\<Typ\>\]

   ```
   bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA\_REQUEST
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Verbindungsverkettung auf beiden NetScaler Gateway Appliances aktivieren:

   set appFlow Parameter \[**-connectionChaining** (ENABLED|DISABLED)\]

   ```
   set appflow param -connectionChaining ENABLED
   ```

Konfigurieren von NetScaler Gateway mithilfe des Konfigurationsdienstprogramms:

1. Konfigurieren Sie das NetScaler Gateway in der ersten DMZ so, dass es mit dem NetScaler Gateway in der zweiten DMZ kommuniziert, und binden Sie das NetScaler Gateway in der zweiten DMZ an das NetScaler Gateway in der ersten DMZ.

   a. Klicken Sie auf der Registerkarte **Konfiguration** auf erweitern **NetScaler Gateway** und dann auf **Virtuelle Server**.

   b. Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und erweitern Sie in der Gruppe „Erweitert“ **Veröffentlichte Anwendungen**.

   c. Klicken Sie auf **Next Hop Server** und binden Sie einen Next Hop Server an die zweite NetScaler Gateway Appliance.

2. Aktivieren Sie Double Hop auf dem NetScaler Gateway in der zweiten DMZ.

   a. Klicken Sie auf der Registerkarte **Konfiguration** auf erweitern **NetScaler Gateway** und dann auf **Virtuelle Server**.

   b. Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und klicken Sie in der Gruppe **Grundeinstellungen** auf das Bearbeitungssymbol.

   c. erweitern Sie **Mehr**, wählen Sie **Double Hop** und klicken Sie auf **OK**.

3. Deaktivieren Sie die Authentifizierung auf dem virtuellen Server auf dem NetScaler Gateway in der zweiten DMZ.

   a. Klicken Sie auf der Registerkarte **Konfiguration** auf erweitern **NetScaler Gateway** und dann auf **Virtuelle Server**.

   b. Doppelklicken Sie im rechten Bereich auf den virtuellen Server, und klicken Sie in der Gruppe **Grundeinstellungen** auf das Bearbeitungssymbol.

   c. erweitern Sie **Mehr**, und deaktivieren Sie **Authentifizierung aktivieren**.

4. Aktivieren Sie eine der NetScaler Gateway Appliances, um TCP-Datensätze zu exportieren.

   a. Auf der Registerkarte **Configuration** erweitern **NetScaler Gateway** und klicken Sie auf **Virtual Servers**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Im rechten Bereich doppelklicken Sie auf den virtuellen Server, und in der Gruppe „Advanced“ erweitern Policies.

c. Klicken Sie auf das +-Symbol und wählen Sie aus der Liste **Choose Policy AppFlow®** und aus der Liste **Choose Type Other TCP Request**.

d. Klicken Sie auf **Continue**.

e. Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Close**.

5. Aktivieren Sie die andere NetScaler Gateway Appliance für den Export von ICA-Datensätzen:

a. Auf der Registerkarte **Configuration** erweitern **NetScaler Gateway** und klicken Sie auf **Virtual Servers**.

b. Im rechten Bereich doppelklicken Sie auf den virtuellen Server, und in der Gruppe **Advanced** erweitern **Policies**.

c. Klicken Sie auf das +-Symbol und wählen Sie aus der Liste **Choose Policy AppFlow** und aus der Liste **Choose Type Other TCP Request**.

d. Klicken Sie auf **Continue**.

e. Fügen Sie eine Richtlinienbindung hinzu, und klicken Sie auf **Close**.

6. Aktivieren Sie die Verbindungsverkettung auf beiden NetScaler Gateway Appliances.

a. Auf der Registerkarte **Configuration** navigieren Sie zu **System** > **Appflow**.

b. Im rechten Bereich, in der Gruppe **Settings**, klicken Sie auf **Change Appflow Settings**.

c. Wählen Sie **Connection Chaining** und klicken Sie auf **OK**.

Datenerfassung zur Überwachung von NetScalern im LAN-Benutzermodus aktivieren

Externe Benutzer, die auf Citrix Virtual App- oder Desktop-Anwendungen zugreifen, müssen sich am NetScaler Gateway authentifizieren. Interne Benutzer müssen jedoch möglicherweise nicht zum NetScaler Gateway umgeleitet werden. Auch bei einer Bereitstellung im transparenten Modus muss der Administrator die Routing-Richtlinien manuell anwenden, damit die Anfragen an die NetScaler Appliance umgeleitet werden.

Um diese Herausforderungen zu überwinden und damit LAN-Benutzer direkt eine Verbindung zu Citrix Virtual Apps- und Desktops-Anwendungen herstellen können, können Sie die NetScaler Appliance im LAN-Benutzermodus bereitstellen, indem Sie einen virtuellen Cache-Umleitungsserver konfigurieren. Der virtuelle Cache-Umleitungsserver fungiert als SOCKS-Proxy auf der NetScaler Gateway Appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die folgende Abbildung zeigt die NetScaler Console, die im **LAN-Benutzermodus** bereitgestellt wird.

HINWEIS

Die NetScaler Gateway Appliance muss den Agenten erreichen können.

Um NetScaler Appliances zu überwachen, die in diesem Modus bereitgestellt werden, fügen Sie zuerst die NetScaler Appliance zum NetScaler Insight-Inventar hinzu, aktivieren Sie AppFlow und zeigen Sie dann die Berichte auf dem Dashboard an.

Nachdem Sie die NetScaler Appliance zum NetScaler Console-Inventar hinzugefügt haben, müssen Sie AppFlow für die Datenerfassung aktivieren.

HINWEIS

- Sie können die Datenerfassung auf einem im LAN-Benutzermodus bereitgestellten NetScaler nicht über das NetScaler Console-Konfigurationsdienstprogramm aktivieren.
- Ausführliche Informationen zu den Befehlen und ihrer Verwendung finden Sie unter Befehlsreferenz.
- Informationen zu Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke.

So konfigurieren Sie die Datenerfassung auf einer NetScaler Appliance über die Befehlszeilenschnittstelle:

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Melden Sie sich bei der NetScaler Appliance an.
2. Fügen Sie einen virtuellen Server für die Weiterleitung von Proxy-Cache-Umleitungen mit der Proxy-IP und dem Port hinzu und geben Sie den Diensttyp als HDX an.

   ```
   add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType
   <cachetype>] [ - cltTimeout <secs>]
   ```

   Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add cr vserver cr1 HDX 10.12.2.2 443 –cacheType FORWARD –cltTimeout 180
```

HINWEIS

Wenn Sie über eine NetScaler Gateway Appliance auf das LAN-Netzwerk zugreifen, fügen Sie eine Aktion hinzu, um eine Richtlinie anzuwenden, die dem VPN-Verkehr entspricht.

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]



add vpn trafficPolicy** \<name\> \<rule\> \<action\>
```

Beispiel:

```
add vpn trafficAction act1 tcp -HDX ON



add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. Fügen Sie NetScaler Console als AppFlow-Collector auf der NetScaler Appliance hinzu.

```
add appflow collector** \<name\> **-IPAddress** \<ip\_addr\>
```

Beispiel:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

4. Erstellen Sie eine AppFlow®-Aktion und verknüpfen Sie den Collector mit der Aktion.

```
add appflow action** \<name\> **-collectors** \<string\> ...
```

Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add appflow action act -collectors MyInsight
```

5. Erstellen Sie eine AppFlow-Richtlinie, um die Regel für die Generierung des Datenverkehrs festzulegen.

   ```
   add appflow policy** \<policyname\> \<rule\> \<action\>
   ```

   Beispiel:

   ```
   add appflow policy pol true act
   ```

6. Binden Sie die AppFlow-Richtlinie an einen globalen Bindungspunkt.

   ```
   bind appflow global** \<policyname\> \<priority\> **-type** \<type\>
   ```

   Beispiel:

   ```
   bind appflow global pol 1 -type ICA_REQ_DEFAULT
   ```

   HINWEIS

   Der Wert von type muss ICA_REQ_OVERRIDE oder ICA_REQ_DEFAULT sein, um auf ICA®-Datenverkehr angewendet zu werden.

7. Legen Sie den Wert des Parameters flowRecordInterval für AppFlow auf 60 Sekunden fest.

   ```
   set appflow param -flowRecordInterval 60
   ```

   Beispiel:

   ```
   set appflow param -flowRecordInterval 60
   ```

8. Speichern Sie die Konfiguration.

   ```
   save ns config
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwellenwerte erstellen und Warnungen für HDX™ Insight konfigurieren

HDX™ Insight auf NetScaler Console ermöglicht Ihnen die Überwachung des HDX-Datenverkehrs, der die NetScaler-Instanzen durchläuft. NetScaler Console ermöglicht es Ihnen, Schwellenwerte für verschiedene Zähler festzulegen, die zur Überwachung des Insight-Datenverkehrs verwendet werden. Sie können auch Regeln konfigurieren und Warnungen in NetScaler Console erstellen.

Der HDX-Datenverkehrstyp ist mit verschiedenen Entitäten wie Anwendungen, Desktops, Gateways, Lizenzen und Benutzern verknüpft. Jede Entität kann verschiedene Metriken enthalten, die mit ihr verbunden sind. Zum Beispiel ist die Anwendungsentität mit mehreren Treffern, der von der Anwendung verbrauchten Bandbreite und der Antwortzeit des Servers verbunden. Eine Benutzerentität kann mit WAN-Latenz, DC-Latenz, ICA® RTT und der von einem Benutzer verbrauchten Bandbreite verbunden sein.

Die Schwellenwertverwaltung für HDX™ Insight in NetScaler Console ermöglichte es Ihnen, proaktiv Regeln zu erstellen und Warnungen zu konfigurieren, wenn die festgelegten Schwellenwerte überschritten wurden. Diese Schwellenwertverwaltung wurde nun erweitert, um eine Gruppe von Schwellenwertregeln zu konfigurieren. Sie können jetzt die Gruppe anstelle einzelner Regeln überwachen. Eine Schwellenwertregelgruppe besteht aus einer oder mehreren benutzerdefinierten Schwellenwertregeln für Metriken, die aus Entitäten wie Benutzern, Anwendungen und Desktops ausgewählt wurden. Jede Regel wird anhand eines erwarteten Werts überwacht, den Sie beim Erstellen der Regel eingeben. Bei der Benutzerentität kann die Schwellenwertgruppe auch einer Geolocation zugeordnet werden.

Eine Warnung wird in NetScaler Console nur generiert, wenn alle Regeln in der konfigurierten Schwellenwertgruppe verletzt werden. Sie können beispielsweise eine Anwendung hinsichtlich der Gesamtzahl der Sitzungsstarts und auch hinsichtlich der Anwendungsstartanzahl als eine Schwellenwertgruppe überwachen. Eine Warnung wird nur generiert, wenn beide Regeln verletzt werden. Dies ermöglicht es Ihnen, realistischere Schwellenwerte für eine Entität festzulegen.

Einige Beispiele sind wie folgt aufgeführt:

- Schwellenwertregel 1: ICA RTT (Metrik) für Benutzer (Entität) muss \<= 100 ms sein
- Schwellenwertregel 2: WAN-Latenz (Metrik) für Benutzer (Entität) muss \<= 100 ms sein

Ein Beispiel für eine Schwellenwertgruppe kann sein: {Schwellenwertregel 1 + Schwellenwertregel 2}

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Um eine Regel zu erstellen, müssen Sie zuerst die Entität auswählen, die Sie überwachen möchten. Wählen Sie dann beim Erstellen einer Regel eine Metrik aus. Sie können beispielsweise die Anwendungsentität auswählen und dann **Gesamtzahl der Sitzungsstarts oder Anzahl der App-Starts** auswählen. Sie können eine Regel für jede Kombination aus einer Entität und einer Metrik erstellen. Verwenden Sie die bereitgestellten Vergleichsoperatoren (\>, \<, \>= und \<=) und geben Sie einen Schwellenwert für jede Metrik ein.

HINWEIS

Wenn Sie nicht mehrere Entitäten in einer einzigen Gruppe überwachen möchten, müssen Sie für jede Entität eine separate Schwellenwertregelgruppe erstellen.

Wenn der Wert eines Zählers den Wert eines Schwellenwerts überschreitet, generiert NetScaler Console ein Ereignis, um eine Schwellenwertüberschreitung anzuzeigen, und für jedes Ereignis wird eine Warnung erstellt.

Sie müssen konfigurieren, wie Sie die Warnung erhalten. Sie können die Warnung so einstellen, dass sie in NetScaler Console angezeigt wird, oder die Warnung als E-Mail oder beides oder als SMS auf Ihrem Mobilgerät erhalten. Für die letzten beiden Aktionen müssen Sie den E-Mail-Server oder den SMS-Server in NetScaler Console konfigurieren.

Schwellenwertgruppen können auch Geolocations für die geospezifische Überwachung der Benutzerentität zugeordnet werden.

Beispielanwendungsfälle

ABC Inc. ist ein globales Unternehmen mit Niederlassungen in über 50 Ländern. Das Unternehmen verfügt über zwei Rechenzentren, eines in Singapur und das andere in Kalifornien, die die Citrix Virtual Apps and Desktops hosten. Mitarbeiter des Unternehmens greifen weltweit über das NetScaler Gateway und GSLB-basierte Umleitung auf die Citrix Virtual Apps and Desktops zu. Eric, der Citrix Virtual Apps and Desktops-Administrator für ABC Inc., möchte die Benutzererfahrung für alle seine Niederlassungen verfolgen, um die Bereitstellung von Apps und Desktops für den Zugriff von überall und jederzeit zu optimieren. Eric möchte auch die Metriken der Benutzererfahrung wie ICA RTTs und Latenzen überprüfen und Abweichungen proaktiv melden.

Die Benutzer von ABC Inc. sind verteilt. Einige Benutzer befinden sich in der Nähe des Rechenzentrums, während andere weiter entfernt sind. Da die Benutzerbasis weit verteilt ist, variieren auch die Metriken und die entsprechenden Schwellenwerte an diesen Standorten. Zum

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Beispiel kann der ICA RTT für einen Standort in der Nähe des Rechenzentrums 5–10 ms betragen, während er für einen entfernten Standort etwa 100 ms betragen kann.

Mit der Verwaltung von Schwellenwertregelgruppen für HDX Insight kann Eric standortspezifische Schwellenwertregelgruppen für jeden Standort festlegen und per E-Mail oder SMS über Verstöße pro Bereich benachrichtigt werden. Eric kann auch die Verfolgung mehrerer Metriken innerhalb einer Schwellenwertregelgruppe kombinieren und die Grundursache auf Kapazitätsprobleme eingrenzen, falls vorhanden. Eric kann nun proaktiv jede Abweichung verfolgen, ohne sich um die Komplexität kümmern zu müssen, alle Citrix Virtual Apps and Desktops nach HDX Insight-Portfoliometriken manuell zu durchsuchen.

Schwellenwertregelgruppe erstellen und Warnungen für HDX Insight mit NetScaler Console konfigurieren

1. Navigieren Sie in NetScaler Console zu **Einstellungen > Analytikeinstellungen > Schwellenwerte**. Klicken Sie auf der sich öffnenden Seite **Schwellenwerte** auf **Hinzufügen**.
2. Geben Sie auf der Seite **Schwellenwerte und Warnungen erstellen** die folgenden Details an:

   a. **Name**. Geben Sie einen Namen für die Erstellung eines Ereignisses ein, für das NetScaler Console eine Warnung generiert.

   b. **Traffic Type**. Wählen Sie aus der Liste **HDX** aus.

   c. **Entität**. Wählen Sie aus der Liste die Kategorie oder den Ressourcentyp aus. Die Entitäten unterscheiden sich für jeden zuvor ausgewählten Verkehrstyp.

   d. **Referenzschlüssel**. Ein Referenzschlüssel wird automatisch basierend auf dem von Ihnen ausgewählten Verkehrstyp und der Entität generiert.

   e. **Dauer**. Wählen Sie aus der Liste das Zeitintervall aus, für das Sie die Entität überwachen möchten. Sie können die Entitäten für eine Stunde, einen Tag oder eine Woche überwachen.

   ▢

3. **Schwellenwertregelgruppe für alle Entitäten erstellen:**

   Für HDX-Verkehr müssen Sie eine Regel erstellen, indem Sie auf **Regel hinzufügen** klicken. Geben Sie die Werte in das sich öffnende Pop-up-Fenster **Regeln hinzufügen** ein.

   ▢

   Sie können mehrere Regeln erstellen, um jede Entität zu überwachen. Das Erstellen mehrerer Regeln in einer einzigen Gruppe ermöglicht es Ihnen, die Entitäten als Gruppe von

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwellenwertregeln anstatt als einzelne Regeln zu überwachen. Klicken Sie auf **OK**, um das Fenster zu schließen.

4. **Konfigurieren der Geolocation-Tagging für die Entität Benutzer:**

   Optional können Sie im Abschnitt **Geo-Details konfigurieren** einen standortbasierten Alarm für die Benutzerentität erstellen. Die folgende Abbildung zeigt ein Beispiel für die Erstellung eines Geolocation-basierten Tagging zur Überwachung der WAN-Latenzleistung für Benutzer an der Westküste der Vereinigten Staaten.

5. Klicken Sie auf **Schwellenwerte aktivieren**, damit NetScaler Console mit der Überwachung der Entitäten beginnen kann.
6. Optional können Sie Aktionen wie E-Mail- und Slack-Benachrichtigungen konfigurieren.
7. Klicken Sie auf **Erstellen**, um eine Schwellenwertregelgruppe zu erstellen.

HDX™ Insight-Berichte und -Metriken anzeigen

HDX Insight bietet vollständige Transparenz der Berichte und Metriken zum HDX-Datenverkehr auf Ihren NetScaler-Instanzen.

Sie können die HDX-Metriken für jede ausgewählte Entität anzeigen. Die Ansichten umfassen die folgenden Entitätskategorien:

- **Benutzer**: Zeigt die Berichte für alle Benutzer an, die innerhalb des ausgewählten Zeitintervalls auf Citrix Virtual Apps and Desktops zugreifen.
- **Anwendungen**: Zeigt die Berichte für die Gesamtzahl der Anwendungen und alle zugehörigen relevanten Informationen an, z. B. die Gesamtzahl der Anwendungsstarts innerhalb des angegebenen Zeitintervalls.
- **Instanzen**: Zeigt die Berichte zu den NetScaler-Instanzen an, die als Gateways für eingehenden Datenverkehr fungieren.
- **Gateway Virtual Servers**: Zeigt die Berichte für alle virtuellen Server an.
- **Desktops**: Zeigt die Berichte für die Desktops an, die im ausgewählten Zeitrahmen verwendet wurden.
- **Lizenzen**: Zeigt die Berichte für die insgesamt verwendeten SSL-VPN-Lizenzen innerhalb des angegebenen Zeitfensters an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Ab Version **14.1-51.x** oder höher können Sie wichtige Metriken wie aktive Sitzungen, Desktops und gestartete Anwendungen auf der Ebene des VPN-Virtual-Servers überwachen. Eine Liste aller virtuellen Server finden Sie unter **Gateway > HDX Insight > Gateway Virtual Servers**.

Dieses Dokument enthält Folgendes:

- Benutzeransicht Berichte und Metriken
- Anwendungsansicht Berichte und Metriken
- Desktop-Ansicht Berichte und Metriken
- Berichte und Metriken der Instanzansicht
- Berichte und Metriken der Lizenzansicht

Berichte und Metriken der Anwendungsansicht

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf die Citrix Virtual Apps. Navigieren Sie zu **Gateway** > **HDX Insight** > **Applications**

Zusammenfassende Ansicht

Die zusammenfassende Ansicht zeigt die Berichte für alle Anwendungen an, die während des ausgewählten Zeitraums angemeldet sind.

Alle Metriken/Berichte weisen, sofern nicht explizit anders angegeben, die entsprechenden Werte für den ausgewählten Zeitraum auf.

LINIENDIAGRAMM

METRIKEN	BESCHREIBUNG
Sitzungen	Gesamtzahl der Sitzungen innerhalb eines bestimmten Zeitintervalls.
Startdauer	Durchschnittliche Zeit, die zum Starten einer Anwendung benötigt wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ZUSAMMENFASSENDER ANWENDUNGSBERICHT

METRIKEN	BESCHREIBUNG
Name	Name der Citrix Virtual App.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual App-Sitzungen im angegebenen Zeitintervall.
Gesamtzahl der App-Starts	Gesamtzahl der gestarteten Citrix Virtual App-Anwendungen im angegebenen Zeitintervall.
Startdauer	Durchschnittliche Zeit, die zum Starten der Citrix Virtual App benötigt wird.

BERICHT ÜBER AKTIVE ANWENDUNGEN

METRIKEN	BESCHREIBUNG
Name	Name der Citrix Virtual App.
Status	Zeigt den Status der Anwendung an: Grün-Aktiv, Rot-Inaktiv
#Aktive Sitzungen	Anzahl der aktiven Benutzersitzungen, die diese App in einem bestimmten Zeitintervall verwenden.
#Aktive Apps	Anzahl der aktiven Sitzungen für diese Anwendung.

SCHWELLENWERTBERICHT

Der Schwellenwertbericht stellt die Anzahl der überschrittenen Schwellenwerte dar, bei denen die *Entität* im ausgewählten Zeitraum als Anwendung ausgewählt ist.

LINIENDIAGRAMM

METRIKEN	BESCHREIBUNG
Aktive Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Startdauer	Durchschnittliche Zeit zum Starten einer Anwendung.

BERICHT ÜBER AKTUELLE SITZUNGEN

METRIKEN	BESCHREIBUNG
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Host-Verzögerung	Durchschnittliche Verzögerung im ICA-Datenverkehr, der durch die NetScaler geleitet wird, verursacht durch das Servernetzwerk.
Bandbreite pro Intervall	Die von der Sitzung in diesem bestimmten Zeitintervall verbrauchte Bandbreite.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Bytes pro Intervall	Anzahl der von der Sitzung in diesem bestimmten Zeitintervall verbrauchten Bytes.
Startzeit	Sitzungsstartzeit.
Betriebszeit	Sitzungsdauer.
Client-IP-Adresse	IP des Endbenutzers.
Server-IP-Adresse	Backend-/Citrix Virtual App Server-IP.
NetScaler-IP-Adresse	NetScaler Management-IP (NSIP).
Client-Typ	Citrix Workspace-Typ – Citrix Windows Client.
Client-Version	Citrix Workspace-Version.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
MSI	Boolesch (Ja/Nein). Zeigt an, ob die Sitzung Multi-Stream-ICA ist.
Sitzungswiederverbindungen	Anzahl der Wiederverbindungen der Sitzung.
ACR-Zähler	Gesamtzahl der automatischen Wiederverbindungen eines Clients mit getrennten Sitzungen.
Benutzerzugriffstyp	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway Benutzer-/Transparenzmodus.
Land	Land, aus dem die Sitzung hergestellt wurde.
Region	Region, aus der die Sitzung hergestellt wurde.
Stadt	Stadt, von der aus die Sitzung eingerichtet wurde.
USB-Status	Aktiv/Inaktiv – Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der gestoppten USB-Instanzen	Die Anzahl der gestoppten USB-Instanzen.
Client-Hostname	Der Hostname des Clients.
HA-Failover-Anzahl	Anzahl der aufgetretenen HA-Failover.
Grund für die Beendigung	Zeigt den Grund für eine Sitzungsbeendigung an. Zum Beispiel: ICA-Sitzungs-Timeout, Sitzung vom Benutzer beendet.
ICA RTT	ICA RTT ist die Bildschirmverzögerung, die der Benutzer während der Interaktion mit einer Anwendung oder einem Desktop erlebt, die jeweils auf Citrix Virtual App oder Desktop gehostet wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
WAN-Latenz	Latenz, die durch die Clientseite des Netzwerks verursacht wird. Das heißt, von NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die durch die Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler zu den Back-End-Servern.
Gesamtbytes	Gesamtbytes, die vom Benutzer während des ausgewählten Zeitraums verbraucht wurden.
Serverseitige Neuübertragungen	Die Anzahl der neu übertragenen Pakete auf der Verbindung zwischen NetScaler und dem Back-End-Server.
Clientseitige Neuübertragungen	Die Anzahl der neu übertragenen Pakete auf der Verbindung zwischen NetScaler und dem Endbenutzer. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern weist auf eine hohe Bandbreitenauslastung aufgrund von Neuübertragungen hin.
Clientseitiges Zero-Window-Größenereignis	Dieser Zähler gibt an, wie oft der Client ein TCP-Fenster der Größe Null angekündigt hat.
Clientseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitiges Zero-Window-Size-Ereignis	Dieser Zähler gibt an, wie oft der Server ein TCP-Fenster der Größe Null angekündigt hat.
Serverseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout bei der Verbindung zwischen NetScaler und dem Back-End-Server aufgetreten ist.
Benutzername	Der Benutzername des Benutzers, der auf diese spezielle Citrix Virtual App zugreift.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Sitzungs-ID	Eindeutige Kennung für die Citrix Virtual App-Sitzung.
Sitzungstyp	Wird „Anwendung“ sein.
Status	Sitzungsstatus: Grün für aktiv, Rot für inaktiv.
Maximale Verletzungslatenz	Der höchste Wert der L7-Latenz, wenn eine Überschreitung eines definierten Schwellenwerts für ein festgelegtes Zeitintervall auftritt.
Durchschnittliche Überschreitungslatenz	Der Durchschnittswert der L7-Latenz, wenn sich das System in einem Zustand "L7-Latenz überschritten" befindet.
Anzahl der L7-Schwellenwertüberschreitungen	Die Häufigkeit, mit der eine L7-Schwellenwertüberschreitung aufgetreten ist.
L7-Client-seitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem ICA-Client und der NetScaler-Instanz beobachtet wird. Diese Metrik ist nützlich, wenn Nicht-Citrix-Geräte im Bereitstellungspfad vorhanden sind.
L7-Server-seitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem NetScaler-Gerät und der Citrix Virtual App beobachtet wird. Diese Metrik ist nützlich, wenn Nicht-Citrix-Geräte im Bereitstellungspfad vorhanden sind.

SITZUNGSANSICHT PRO ANWENDUNG

Die Sitzungsansicht pro Anwendung zeigt Berichte für eine bestimmte ausgewählte Anwendungssitzung an.

So zeigen Sie die Sitzungsberichte an:

1. Navigieren Sie zu **Gateway** > **HDX™ Insight** > **Applications**.
2. Wählen Sie einen bestimmten Benutzer aus dem **Application Summary Report** aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Eine Sitzung aus dem Bericht der aktuellen Sitzungen ausgewählt.

LINIENDIAGRAMM

METRIKEN	BESCHREIBUNG
Sitzungswiederverbindungen	Anzahl der Wiederverbindungen der Sitzung.
ACR-Zähler	Gesamtzahl der automatischen Wiederverbindungen von Clients mit getrennten Sitzungen.
ICA-RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die bzw. der jeweils auf Citrix Virtual App oder Desktop gehostet wird.
WAN-Latenz	Latenz, die durch die Clientseite des Netzwerks verursacht wird. Das heißt, von NetScaler zum Endbenutzer.
Serverseitiges Zero-Window-Size-Ereignis	Latenz, die durch die Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler zu den Back-End-Servern.
Bandbreite pro Intervall	Die Bandbreite, die von der Sitzung in diesem bestimmten Zeitintervall verbraucht wurde.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Back-End-Server erneut übertragen wurden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen wurden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos sein wird, weist aber auf eine hohe Bandbreitenauslastung aufgrund von Neuübertragungen hin.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Serverseitiges Zero-Window-Size-Ereignis	Dieser Zähler gibt an, wie oft der Server ein TCP-Fenster der Größe Null angekündigt hat.
Clientseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung zwischen NetScaler und dem Back-End-Server aufgetreten ist.
Clientseitiges Zero-Window-Size-Ereignis	Dieser Zähler gibt an, wie oft der Client ein TCP-Fenster der Größe Null angekündigt hat.

BENUTZER-BALKENDIAGRAMM

Das **Benutzer**-Balkendiagramm stellt die Benutzer dar, die bei dieser bestimmten App angemeldet sind.

Berichte und Metriken der Desktop-Ansicht

Die Berichte und Metriken in dieser Ansicht konzentrieren sich auf den Citrix Virtual Desktop. Navigieren Sie zu **Gateway** > **HDX™ Insight** > **Desktop**

Zusammenfassende Ansicht

Die zusammenfassende Ansicht zeigt die Berichte für alle Citrix Virtual Desktops™, die während des ausgewählten Zeitraums angemeldet sind.

Alle unten aufgeführten Metriken/Berichte zeigen, sofern nicht explizit anders erwähnt, die entsprechenden Werte für den ausgewählten Zeitraum an.

LINIENDIAGRAMM

METRIKEN	BESCHREIBUNG
Aktive Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps- und Desktops-Sitzungen an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die bzw. der jeweils auf Citrix Virtual App oder Desktop gehostet wird.
WAN-Latenz	Latenz, verursacht durch die Client-Seite des Netzwerks. Das heißt, von NetScaler zum Endbenutzer.
DC-Latenz	Latenz, verursacht durch die Serverseite des Netzwerks. Das heißt, von NetScaler zu den Back-End-Servern.
Bandbreite	Gesamtanzahl der Bytes pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt wurden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Back-End-Server erneut übertragen wurden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen wurden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos sein wird, sondern weist auf eine hohe Bandbreitenauslastung aufgrund von Neuübertragungen hin.
Clientseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
	zwischen NetScaler und dem Back-End-Server aufgetreten ist.
Clientseitiges Zero-Window-Größenereignis	Dieser Zähler gibt an, wie oft der Client ein TCP-Fenster der Größe Null angekündigt hat.
Server-seitiges Zero-Window-Ereignis	Dieser Zähler gibt an, wie oft der Server ein TCP-Fenster der Größe Null angekündigt hat.

DESKTOP-ZUSAMMENFASSUNGSBERICHT

METRIKEN	BESCHREIBUNG
Aktive Sitzungen	Gesamtzahl der aktiven Citrix Virtual Desktop-Sitzungen innerhalb eines bestimmten Zeitintervalls.
Aktive Desktops	Gesamtzahl der aktiven Citrix Virtual Desktops innerhalb eines bestimmten Zeitintervalls.
ICA RTT	ICA RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die bzw. der auf Citrix Virtual App oder Desktop gehostet wird.
WAN-Latenz	Latenz, die durch die Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die durch die Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler zu den Back-End-Servern.
Bandbreite	Gesamtanzahl der Bytes pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Gesamt-Bytes	Gesamtanzahl der vom Benutzer im ausgewählten Zeitraum verbrauchten Bytes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SCHWELLENWERTBERICHT

Der Schwellenwertbericht stellt die Anzahl der überschrittenen Schwellenwerte dar, wobei die *Entität* im ausgewählten Zeitraum als Desktop ausgewählt ist.

Pro-Desktop-Ansicht

Die Pro-Desktop-Ansicht bietet detaillierte Berichte zur Endbenutzererfahrung für einen ausgewählten Citrix Virtual Desktop.

So navigieren Sie zur jeweiligen Desktop-Ansicht:

1. Navigieren Sie zu **Gateway > HDX Insight > Desktop**.
2. Wählen Sie einen bestimmten **Desktop** aus dem **Desktop-Zusammenfassungsbericht** aus.

LINIENDIAGRAMM

METRIKEN	BESCHREIBUNG
Aktive Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die bzw. der jeweils auf Citrix Virtual App oder Desktop gehostet wird.
WAN-Latenz	Latenz, die durch die Clientseite des Netzwerks verursacht wird. Das heißt, von NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die durch die Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler zu Back-End-Servern.
Bandbreite	Gesamtanzahl der Bytes pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Back-End-Server erneut übertragen wurden.
Client-seitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen wurden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern weist auf eine hohe Bandbreitenauslastung aufgrund von Neuübertragungen hin.
Client-seitiger schneller RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Server-seitiger schneller RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung zwischen NetScaler und dem Back-End-Server aufgetreten ist.
Client-seitiges Zero-Window-Size-Ereignis	Dieser Zähler gibt an, wie oft der Client ein TCP-Fenster der Größe Null angekündigt hat.
Server-seitiges Zero-Window-Size-Ereignis	Dieser Zähler gibt an, wie oft der Server ein TCP-Fenster der Größe Null angekündigt hat.

BERICHT ÜBER DESKTOP-BENUTZER

Diese Tabelle bietet Einblicke in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Desktop-Startanzahl und Bandbreite sortiert werden.

METRIKEN	BESCHREIBUNG
Name	Name des Citrix Virtual Desktops.
Anzahl der Desktop-Starts	Anzahl der Desktop-Starts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Bandbreite	Gesamtzahl der Bytes pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls verwendet wurden.
DC-Latenz	Latenz, die durch die Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler zu den Back-End-Servern.
WAN-Latenz	Latenz, die durch die Clientseite des Netzwerks verursacht wird. Das heißt, von NetScaler zum Endbenutzer.
ICA-RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die bzw. der auf Citrix Virtual App oder Desktop gehostet wird.

BERICHT ÜBER AKTIVE/INAKTIVE BENUTZER-DESKTOPS

Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählungen sortiert werden.

METRIKEN	BESCHREIBUNG
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Host-Verzögerung	Durch das Servernetzwerk verursachte durchschnittliche Verzögerung im ICA-Datenverkehr, der die NetScaler passiert.
Bandbreite pro Intervall	Die von der Sitzung in diesem bestimmten Zeitintervall verbrauchte Bandbreite.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Bytes pro Intervall	Anzahl der Bytes, die von der Sitzung in diesem bestimmten Zeitintervall verbraucht wurden.
Startzeit	Sitzungsstartzeit.
Betriebszeit	Sitzungsdauer.
Client-IP-Adresse	IP des Endbenutzers.
Server-IP-Adresse	Backend-/Citrix Virtual App-Server-IP.
NetScaler-IP-Adresse	NetScaler Management-IP (NSIP).
Client-Typ	Citrix Workspace-Typ – Citrix Windows Client
Client-Version	Citrix Workspace-Version.
MSI	Boolesch (Ja/Nein). Zeigt an, ob die Sitzung Multi-Stream ICA ist.
Sitzungswiederverbindungen	Anzahl der Wiederverbindungen der Sitzung.
ACR-Zähler	Gesamtzahl der automatischen Wiederverbindungen von Benutzern durch einen Client mit getrennten Sitzungen.
Benutzerzugriffstyp	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway Benutzer-/Transparenzmodus.
Land	Land, aus dem die Sitzung hergestellt wurde.
Region	Region, aus der die Sitzung hergestellt wurde.
Stadt	Stadt, aus der die Sitzung hergestellt wurde.
USB-Status	Aktiv/Inaktiv – Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Anzahl der gestoppten USB-Instanzen	Die Anzahl der gestoppten USB-Instanzen.
Client-Hostname	Der Hostname des Clients.
HA-Failover-Anzahl	Anzahl der aufgetretenen HA-Failover.
Grund für die Beendigung	Zeigt den Grund für die Beendigung einer Sitzung an. Zum Beispiel: ICA-Sitzungs-Timeout, Sitzung vom Benutzer beendet.
ICA-RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die bzw. der auf Citrix Virtual Apps oder Desktops gehostet wird.
WAN-Latenz	Latenz, die durch die Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die durch die Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler zu den Back-End-Servern.
Gesamtbytes	Gesamtbytes, die vom Benutzer während des ausgewählten Zeitraums verbraucht wurden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Back-End-Server erneut übertragen wurden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen wurden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos sein wird, sondern weist auf eine hohe Bandbreitenauslastung aufgrund von Neuübertragungen hin.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Clientseitiges Zero-Window-Size-Ereignis	Dieser Zähler gibt an, wie oft der Client ein Zero-TCP-Fenster angekündigt hat.
Clientseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitiges Zero-Window-Size-Ereignis	Dieser Zähler gibt an, wie oft der Server ein Null-TCP-Fenster angekündigt hat.
Serverseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout bei der Verbindung zwischen NetScaler und dem Back-End-Server aufgetreten ist.
VDI-Image-Name	Name des Citrix Virtual Desktops, mit dem der Benutzer verbunden ist
Diagramm	

Ansicht pro Desktopsitzung

Die Ansicht pro Desktopsitzung bietet Berichte für eine bestimmte ausgewählte Citrix Virtual Desktop-Sitzung.

So navigieren Sie zur Desktopsitzungsansicht:

1. Navigieren Sie zu **Gateway** > **HDX Insight** > **Desktop**.
2. Wählen Sie einen bestimmten Desktop aus dem **Desktop-Zusammenfassungsbericht** aus.
3. Wählen Sie eine Sitzung aus dem Bericht der aktuellen Sitzungen aus.

ZEITACHSEN-DIAGRAMM

Die Ansicht pro Benutzersitzung bietet Berichte für die Sitzung eines bestimmten ausgewählten Benutzers.

So zeigen Sie die Metriken für die Sitzung eines ausgewählten Benutzers an:

1. Navigieren Sie zu **Gateway** > **HDX Insight** > **Benutzer**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Wählen Sie einen bestimmten Benutzer aus dem Abschnitt **Benutzerübersichtsbericht** aus.
3. Wählen Sie eine Sitzung aus der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** aus.

METRIKEN	BESCHREIBUNG
Sitzungswiederverbindungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
ACR-Zählungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die bzw. der auf Citrix Virtual App oder Desktop gehostet wird.
WAN-Latenz	Latenz, die durch die Clientseite des Netzwerks verursacht wird. Das heißt, von NetScaler zum Endbenutzer.
DC-Latenz	Latenz, verursacht durch die Serverseite des Netzwerks. Das heißt, von NetScaler zu den Back-End-Servern.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Back-End-Server erneut übertragen wurden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen wurden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, sondern weist auf eine hohe Bandbreitenauslastung aufgrund von Neuübertragungen hin.
Clientseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
	zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung zwischen NetScaler und dem Back-End-Server aufgetreten ist.
Bandbreite pro Intervall	Die von der Sitzung in diesem bestimmten Zeitintervall verbrauchte Bandbreite.
Serverseitiges Zero-Window-Size-Ereignis	Dieser Zähler gibt an, wie oft der Server ein TCP-Fenster der Größe Null angekündigt hat.
Client-seitiges Zero-Window-Größenereignis	Dieser Zähler gibt an, wie oft der Client ein TCP-Fenster der Größe Null angekündigt hat.

BERICHT ZUGEHÖRIGER DESKTOPSITZUNGEN

Die folgenden Metriken können nach Bandbreite pro Intervall, Sitzungswiederverbindungen und ACR-Zählungen sortiert werden.

METRIKEN	BESCHREIBUNG
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Host-Verzögerung	Durch das Servernetzwerk verursachte durchschnittliche Verzögerung im ICA-Datenverkehr, der die NetScaler passiert.
Bandbreite pro Intervall	Die von der Sitzung in diesem bestimmten Zeitintervall verbrauchte Bandbreite.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Bytes pro Intervall	Anzahl der von der Sitzung in diesem bestimmten Zeitintervall verbrauchten Bytes.
Startzeit	Sitzungsstartzeit.
Betriebszeit	Sitzungsdauer.
Client-IP-Adresse	IP des Endbenutzers.
Server-IP-Adresse	IP des Backend-/Citrix Virtual App-Servers.
NetScaler-IP-Adresse	NetScaler Management IP (NSIP).
Clienttyp	Workspace-Typ – Citrix Windows Client
Clientversion	Citrix Workspace-Version.
MSI	Boolesch (Ja/Nein). Gibt an, ob die Sitzung Multi-Stream ICA ist.
Sitzungswiederverbindungen	Anzahl der Wiederverbindungen der Sitzung.
ACR-Zähler	Gesamtzahl der automatischen Wiederverbindungen von Clients mit getrennten Sitzungen.
Benutzerzugriffstyp	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel NetScaler Gateway Benutzer-/Transparenzmodus.
Land	Land, aus dem die Sitzung hergestellt wurde.
Region	Region, aus der die Sitzung hergestellt wurde.
Stadt	Stadt, aus der die Sitzung hergestellt wurde.
USB-Status	Aktiv/Inaktiv – Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Anzahl der gestoppten USB-Instanzen	Die Anzahl der gestoppten USB-Instanzen.
Client-Hostname	Der Hostname des Clients.
HA-Failover-Anzahl	Anzahl der HA-Failover-Vorgänge.
Grund für die Beendigung	Zeigt den Grund für die Beendigung einer Sitzung an. Zum Beispiel: ICA-Sitzungs-Timeout, Sitzung vom Benutzer beendet.
ICA RTT	ICA RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die jeweils auf Citrix Virtual App oder Desktop gehostet wird.
WAN-Latenz	Latenz, die durch die Clientseite des Netzwerks verursacht wird. Das heißt: von NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die durch die Serverseite des Netzwerks verursacht wird. Das heißt: von NetScaler zu den Back-End-Servern.
Gesamt-Bytes	Gesamt-Bytes, die vom Benutzer während des ausgewählten Zeitraums verbraucht wurden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Back-End-Server erneut übertragen wurden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen wurden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos sein wird, sondern weist auf eine hohe Bandbreitenauslastung aufgrund von Neuübertragungen hin.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Clientseitiges Zero-Window-Ereignis	Dieser Zähler gibt an, wie oft der Client ein TCP-Fenster der Größe Null angekündigt hat.
Clientseitiger schneller RTO	Anzahl der Male, bei denen der Retransmission-Timeout bei der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitiges Zero-Window-Ereignis	Dieser Zähler gibt an, wie oft der Server ein TCP-Fenster der Größe Null angekündigt hat.
Serverseitiger schneller RTO	Anzahl der Male, bei denen der Retransmission-Timeout bei der Verbindung zwischen NetScaler und dem Back-End-Server aufgetreten ist.
VDI-Image-Name	Name des Citrix Virtual Desktops, mit dem der Benutzer verbunden ist

Berichte und Metriken der Benutzeransicht

Die Berichte und Metriken in dieser Ansicht werden pro Citrix Virtual App- oder Desktop-Benutzer angezeigt.

Navigieren Sie zu **Gateway** > **HDX™ Insight** > **Benutzer**

Zusammenfassende Ansicht

Die zusammenfassende Ansicht zeigt die Berichte für alle Benutzer an, die sich während des ausgewählten Zeitraums angemeldet haben. Alle Metriken/Berichte in dieser Ansicht zeigen die entsprechenden Werte für den ausgewählten Zeitraum an, sofern nicht anders angegeben.

So ändern Sie den ausgewählten Zeitraum:

1. Verwenden Sie die Liste der Zeiträume oder den Zeitschieberegler, um das gewünschte Zeitintervall festzulegen.
2. Klicken Sie auf **Go**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LINIENDIAGRAMM

METRIKEN	BESCHREIBUNG
Aktive Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps- und Desktops-Sitzungen an.
Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die bzw. der jeweils auf Citrix Virtual App oder Desktop gehostet wird.
WAN-Latenz	Latenz, verursacht durch die Clientseite des Netzwerks. Das heißt, von NetScaler zum Endbenutzer.
DC-Latenz	Latenz, verursacht durch die Serverseite des Netzwerks. Das heißt, von NetScaler zu Back-End-Servern.
Bandbreite	Gesamtbits pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Back-End-Server neu übertragen wurden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer neu übertragen wurden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos sein wird, weist aber auf eine hohe Bandbreitenauslastung aufgrund von Neuübertragungen hin.
Clientseitiger schneller RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
	zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout bei der Verbindung zwischen NetScaler und dem Back-End-Server aufgetreten ist.
Clientseitiges Zero-Window-Size-Ereignis	Dieser Zähler gibt an, wie oft der Client ein TCP-Fenster der Größe Null angekündigt hat.
Serverseitiges Zero-Window-Size-Ereignis	Dieser Zähler gibt an, wie oft der Server ein TCP-Fenster der Größe Null angekündigt hat.

BENUTZERÜBERSICHTSBERICHT

Im Folgenden sind die Metriken aufgeführt, die für diesen Bericht spezifisch sind.

METRIKEN	BESCHREIBUNG
# Aktive Sitzungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
# Aktive Apps	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die bzw. der auf Citrix Virtual App oder Desktop gehostet wird.
WAN-Latenz	Latenz, die durch die Clientseite des Netzwerks verursacht wird. Das heißt, von NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die durch die Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler zu den Back-End-Servern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Bandbreite	Gesamtzahl der Bits pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Back-End-Server erneut übertragen wurden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen wurden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos sein wird, deutet aber auf eine hohe Bandbreitenauslastung aufgrund von Neuübertragungen hin.
Clientseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitiges schnelles RTO	Anzahl der Neuübertragungs-Timeouts, die auf der Verbindung zwischen NetScaler und dem Back-End-Server aufgetreten sind.
Clientseitiges Zero-Window-Größenereignis	Dieser Zähler gibt an, wie oft der Client ein Zero-TCP-Fenster angekündigt hat.
Serverseitiges Zero-Window-Größenereignis	Dieser Zähler gibt an, wie oft der Server ein Zero-TCP-Fenster angekündigt hat.
Gesamtzahl der App-Starts	Gesamtzahl der vom Benutzer während des ausgewählten Zeitraums gestarteten Apps.
Gesamtbytes	Gesamtbytes, die vom Benutzer während des ausgewählten Zeitraums verbraucht wurden.
Aktive Desktops	Gesamtzahl der aktiven Citrix Virtual Desktops während eines bestimmten Zeitintervalls.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

KANÄLE

Kanäle stellen die Gesamtbandbreite oder die Gesamtbytes dar, die von jedem virtuellen ICA®-Kanal in Form eines Donut-Diagramms verbraucht werden. Sie können die Metriken auch nach Bandbreite oder Gesamtbytes sortieren.

BENUTZERAGENTEN

Benutzeragenten stellen die gesamte Bandbreite/Gesamtbits dar, die von jedem Endpunkt in Form eines Donut-Diagramms verbraucht werden. Sie können die Metriken auch nach Bandbreite oder Gesamtbytes sortieren.

ANZAHL DER SCHWELLENWERTÜBERSCHREITUNGEN

Die Metriken zur Anzahl der Schwellenwertüberschreitungen stellen die Anzahl der in dem ausgewählten Zeitraum überschrittenen Schwellenwerte dar.

WELTKARTE

Die Weltkartenansicht in HDX Insight ermöglicht es Administratoren, historische und aktive Benutzerdetails aus geografischer Sicht anzuzeigen. Die Administratoren können eine Weltansicht des Systems erhalten, zu einem bestimmten Land und weiter zu Städten navigieren, indem sie einfach auf die Region klicken. Die Administratoren können weiter nach Stadt und Bundesland filtern, um Informationen anzuzeigen. Ab NetScaler Console Version 12.0 und höher können Sie zu Benutzern navigieren, die von einem geografischen Standort aus verbunden sind.

Die folgenden Details können auf der Weltkarte in HDX Insight angezeigt werden, und die Dichte jeder Metrik wird in Form einer Heatmap dargestellt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Gesamtbytes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ansicht pro Benutzer

Die Ansicht pro Benutzer bietet detaillierte Berichte zur Endbenutzererfahrung für jeden bestimmten ausgewählten Benutzer.

So navigieren Sie zu den Metriken eines bestimmten Benutzers:

1. Navigieren Sie zu **Gateway** > **HDX Insight** > **Benutzer**.
2. Wählen Sie einen bestimmten Benutzer aus dem Benutzerübersichtsbericht aus.

LINIENDIAGRAMM

Das Liniendiagramm zeigt die Zusammenfassung aller Metriken für den bestimmten ausgewählten Benutzer während des ausgewählten Zeitraums an.

BERICHT ÜBER AKTUELLE/BEENDETE SITZUNGEN

Dieser Bericht bezieht sich auf alle aktuellen/beendeten Benutzersitzungen für den ausgewählten Benutzer. Diese Metriken können nach Startzeit, Sitzungswiederverbindungen und ACR-Anzahl sortiert werden.

METRIKEN	BESCHREIBUNG
Sitzungs-ID	Eine eindeutige Identität für eine ICA-Sitzung.
Sitzungstyp	Anwendung/Desktop.
Status	Grün/Rot für aktive/inaktive Sitzungen.
Host-Verzögerung	Durchschnittliche Verzögerung im ICA-Datenverkehr, der die NetScaler passiert und durch das Servernetzwerk verursacht wird.
Bandbreite pro Intervall	Die von der Sitzung in diesem bestimmten Zeitintervall verbrauchte Bandbreite.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Bytes pro Intervall	Anzahl der von der Sitzung in diesem bestimmten Zeitintervall verbrauchten Bytes.
Startzeit	Sitzungsstartzeit.
Betriebszeit	Sitzungsdauer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Client-IP-Adresse	IP des Endbenutzers.
Server-IP-Adresse	IP des Back-End-/Citrix Virtual App-Servers.
NetScaler-IP-Adresse	NetScaler Management-IP (NSIP).
Clienttyp	Workspace-Typ – Citrix Windows Client
Clientversion	Workspace-Version.
MSI	Boolesch (Ja/Nein). Gibt an, ob die Sitzung Multi-Stream ICA ist.
Sitzungswiederverbindungen	Anzahl der Wiederverbindungen der Sitzung.
ACR-Zähler	Gesamtzahl der automatischen Wiederverbindungen eines Clients mit getrennten Sitzungen.
Benutzerzugriffstyp	Zeigt den Zugriffsmodus der ICA-Sitzung an. Zum Beispiel: NetScaler Gateway Benutzer-/Transparenzmodus.
Land	Land, aus dem die Sitzung hergestellt wurde.
Region	Region, aus der die Sitzung hergestellt wurde.
Stadt	Stadt, aus der die Sitzung hergestellt wurde.
USB-Status	Aktiv/Inaktiv - Grün/Rot.
Anzahl der akzeptierten USB-Instanzen	Die Anzahl der akzeptierten USB-Instanzen.
Anzahl der abgelehnten USB-Instanzen	Die Anzahl der abgelehnten USB-Instanzen.
Anzahl der beendeten USB-Instanzen	Die Anzahl der beendeten USB-Instanzen.
Client-Hostname	Der Hostname des Clients.
HA-Failover-Anzahl	Anzahl der aufgetretenen HA-Failover.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Grund für die Beendigung	Zeigt den Grund für die Beendigung einer Sitzung an. Zum Beispiel: ICA-Sitzungs-Timeout, Sitzung vom Benutzer beendet.
ICA-RTT	ICA-RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die bzw. der auf Citrix Virtual App oder Desktop gehostet wird.
WAN-Latenz	Latenz, die durch die Client-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler zum Endbenutzer.
DC-Latenz	Latenz, die durch die Server-Seite des Netzwerks verursacht wird. Das heißt, von NetScaler zu den Back-End-Servern.
Gesamt-Bytes	Gesamt-Bytes, die vom Benutzer im ausgewählten Zeitraum verbraucht wurden.
Neuübertragungen auf Serverseite	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Back-End-Server erneut übertragen wurden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen wurden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos sein wird, sondern weist auf eine hohe Bandbreitenauslastung aufgrund von Neuübertragungen hin.
Clientseitiges Zero-Window-Ereignis	Dieser Zähler gibt an, wie oft der Client ein Zero-TCP-Fenster angekündigt hat.
Clientseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Serverseitiges Zero-Window-Ereignis	Dieser Zähler gibt an, wie oft der Server ein Zero-TCP-Fenster angekündigt hat.
Serverseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung zwischen NetScaler und dem Back-End-Server aufgetreten ist.

UNTERSTÜTZUNG FÜR EDT IN HDX INSIGHT

NetScaler Console unterstützt jetzt Enlightened Data Transport (EDT) zur Anzeige von Analysen für HDX Insight. Das heißt, NetScaler Console unterstützt jetzt sowohl das UDP- als auch das TCP-Protokoll. Die EDT-Unterstützung für NetScaler Gateway gewährleistet eine hochauflösende In-Session-Benutzererfahrung von virtuellen Desktops für Benutzer, die Citrix Workspace ausführen.

HDX Insight zeigt jetzt die Anzahl der EDT-Sitzungen und Nicht-EDT-Sitzungen als Teil des Berichts über aktive Sitzungen an. Die Tabelle „Benutzer“ zeigt einen detaillierten Bericht aller Benutzer im System an. Die Tabelle zeigt Metriken wie WAN-Latenz, DC-Latenz, Neuübertragungen, RTOs, und einige dieser Metriken sind für Benutzer, die EDT-Sitzungen haben, nicht verfügbar, da sie derzeit aus dem TCP-Stack berechnet werden. Daher werden sie als „NA“ angezeigt.

Ein neues Donut-Diagramm wurde eingeführt, damit Sie die vom Benutzer verbrauchte Bandbreite und auch die Gesamtzahl der Bytes basierend auf dem von den Benutzern verwendeten Protokolltyp sehen können.

HDX INSIGHT-METRIKEN VERFÜGBAR AB NETSCALER CONSOLE 12.0 UND HÖHER

L7 CLIENT-SEITIGE LATENZ	DIE DURCHSCHNITTLICHE L7-LATENZ, DIE ZWISCHEN DEM ICA-CLIENT UND DER NETSCALER-INSTANZ BEOBACHTET WIRD. DIESE METRIK IST NÜTZLICH, WENN NICHT-CITRIX-GERÄTE IM BEREITSTELLUNGSPFAD VORHANDEN SIND.
L7 Server-seitige Latenz	Die durchschnittliche L7-Latenz, die zwischen dem NetScaler-Gerät und der Citrix Virtual App

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L7 CLIENT-SEITIGE LATENZ	DIE DURCHSCHNITTLICHE L7-LATENZ, DIE ZWISCHEN DEM ICA-CLIENT UND DER NETSCALER-INSTANZ BEOBACHTET WIRD. DIESE METRIK IST NÜTZLICH, WENN NICHT-CITRIX-GERÄTE IM BEREITSTELLUNGSPFAD VORHANDEN SIND.
	beobachtet wird. Diese Metrik ist nützlich, wenn Nicht-Citrix-Geräte im Bereitstellungspfad vorhanden sind.
Maximale Verletzungslatenz	Der höchste Wert der L7-Latenz, wenn eine Überschreitung eines definierten Schwellenwerts für ein festgelegtes Zeitintervall auftritt.
Durchschnittliche Verletzungslatenz	Der Durchschnittswert der L7-Latenz, wenn sich das System in einem Zustand der „L7-Latenzverletzung“ befindet.
Anzahl der L7-Schwellenwertüberschreitungen	Die Häufigkeit, mit der eine L7-Schwellenwertüberschreitung aufgetreten ist.

DESKTOP-BENUTZER

Diese Tabelle gibt Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Desktop-Startanzahl und Bandbreite sortiert werden.

METRIKEN	BESCHREIBUNG
Name	Name des Citrix Virtual Desktops.
Anzahl der Desktop-Starts	Anzahl der Desktop-Starts.
Bandbreite	Gesamtzahl der Bits pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls benötigt werden.
DC-Latenz	Latenz, die durch die Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler zu den Back-End-Servern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
WAN-Latenz	Latenz, die durch die Clientseite des Netzwerks verursacht wird. Das heißt, von NetScaler zum Endbenutzer.
ICA RTT	ICA RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erfährt, die bzw. der auf Citrix Virtual App oder Desktop gehostet wird.

ANWENDUNGEN

Ein Balkendiagramm, das Anwendungen nach Aktiv, Gesamtzahl der Sitzungsstarts, Gesamtzahl der Anwendungsstarts und Startdauer sortiert darstellt.

INSTANZEN

Ein Balkendiagramm, das NetScaler-Instanzen nach Aktiv und Gesamtanzahl der Anwendungen sortiert darstellt

KANÄLE

Kanäle stellen die Gesamtbandbreite oder die von jedem virtuellen ICA-Kanal verbrauchten Gesamtbits in Form eines Donut-Diagramms dar. Sie können die Metriken auch nach Bandbreite oder Gesamtbits sortieren.

BENUTZERAGENTEN

Benutzeragenten stellen die Gesamtbandbreite/Gesamtbits dar, die von jedem Endpunkt in Form eines Donut-Diagramms verbraucht werden. Sie können die Metriken auch nach Bandbreite oder Gesamtbits sortieren.

Ansicht pro Benutzersitzung

Die Ansicht pro Benutzersitzung bietet Berichte für die Sitzung eines bestimmten ausgewählten Benutzers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So zeigen Sie die Metriken für die Sitzung eines ausgewählten Benutzers an:

1. Navigieren Sie zu **Gateway** > **HDX Insight** > **Benutzer**.
2. Wählen Sie einen bestimmten Benutzer aus dem Abschnitt **Benutzerübersichtsbericht** aus.
3. Wählen Sie eine Sitzung aus der Spalte **Aktuelle Sitzungen** oder **Beendete Sitzungen** aus.

ZEITACHSENDIAGRAMM

METRIKEN	BESCHREIBUNG
Sitzungswiederverbindungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual Apps and Desktops-Sitzungen an.
ACR-Zählungen	Diese Zahl gibt die Anzahl der aktiven Citrix Virtual App-Sitzungen an.
ICA RTT	ICA RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die bzw. der auf Citrix Virtual App oder Desktop gehostet wird.
WAN-Latenz	Latenz, verursacht durch die Client-Seite des Netzwerks. Das heißt, von NetScaler zum Endbenutzer.
DC-Latenz	Latenz, verursacht durch die Serverseite des Netzwerks. Das heißt, von NetScaler zu den Back-End-Servern.
Sitzungsbandbreite	Die von der Sitzung verbrauchte Bandbreite, unabhängig vom Zeitintervall.
Serverseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Back-End-Server erneut übertragen wurden.
Clientseitige Neuübertragungen	Die Anzahl der Pakete, die auf der Verbindung zwischen NetScaler und dem Endbenutzer erneut übertragen wurden. Ein hoher Wert dieser Metrik bedeutet nicht, dass die Benutzererfahrung nicht nahtlos ist, deutet

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
	aber auf eine hohe Bandbreitenauslastung aufgrund von Neuübertragungen hin.
Clientseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung zwischen NetScaler und dem Endbenutzer aufgetreten ist.
Serverseitiges schnelles RTO	Anzahl der Male, bei denen das Neuübertragungs-Timeout auf der Verbindung zwischen NetScaler und dem Back-End-Server aufgetreten ist.
Bandbreite pro Intervall	Die von der Sitzung während dieses bestimmten Zeitintervalls verbrauchte Bandbreite.
Serverseitiges Zero-Window-Größenereignis	Dieser Zähler gibt an, wie oft der Server ein Zero-TCP-Fenster angekündigt hat.
Clientseitiges Zero-Window-Größenereignis	Dieser Zähler gibt an, wie oft der Client ein Zero-TCP-Fenster angekündigt hat.

AKTIVE ANWENDUNG

Der Abschnitt **Aktive Anwendungen** zeigt die aktiven Anwendungen des ausgewählten Benutzers an. Diese Anwendungen können auch nach der Anzahl der aktiven Sitzungen und den Startdauern sortiert werden.

VERWANDTE SITZUNGEN

Der Abschnitt Verwandte Sitzungen zeigt die verwandten Sitzungen der Sitzungen des ausgewählten Benutzers an. Die Beziehung kann als gemeinsame Server oder gemeinsamer NetScaler ausgewählt werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Berichte und Metriken der Instanzansicht

Die Berichte und Metriken in der Instanzansicht konzentrieren sich auf eine oder mehrere NetScaler-Instanzen.

So navigieren Sie zur Instanzansicht:

1. Melden Sie sich mit einem unterstützten Webbrowser bei Ihrer NetScaler Console an.
2. Navigieren Sie zu **Gateway** > **HDX™ Insight** > **Instanzen**.

Instanz-Zusammenfassungsansicht

Diese Ansicht wird als Zusammenfassungsansicht bezeichnet, da sie die Berichte für alle NetScaler-Instanzen anzeigt, die zur NetScaler Console hinzugefügt wurden.

Alle diese Metriken/Berichte haben, sofern nicht explizit anders angegeben, die entsprechenden Werte für den ausgewählten Zeitraum.

INSTANZ-BALKENDIAGRAMM

Dieses Diagramm zeigt die Instanz im Vergleich zur Gesamtzahl der Sitzungsstarts und der Gesamtanzahl der Apps aus der Liste oben rechts auf der Diagrammfläche.

ZUSAMMENFASSENDER BERICHT ZU INSTANZEN/AKTIVEN INSTANZEN

METRIKEN	BESCHREIBUNG
Name	Hostname der NetScaler-Instanz.
IP-Adresse	NetScaler-IP-Adresse.
Gesamtzahl der gestarteten Sitzungen	Gesamtzahl der eindeutigen Benutzersitzungen, die in einem bestimmten Zeitintervall erstellt wurden.
Gesamtzahl der Apps	Gesamtzahl der eindeutigen Anwendungen, die in einem bestimmten Zeitintervall gestartet wurden.
Typ	N/A

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SCHWELLENWERTBERICHT

Der Schwellenwertbericht stellt die Anzahl der überschrittenen Schwellenwerte dar, wobei die *Entität* im ausgewählten Zeitraum als Instanz ausgewählt ist. Weitere Informationen finden Sie unter Schwellenwerte und Warnungen erstellen.

ÜBERSPRUNGENE FLOWS

Ein übersprungener Flow ist ein Datensatz, bei dem die Analyse der ICA®-Verbindung übersprungen wurde. Dieser Flow kann aus mehreren Gründen auftreten, z. B. bei der Verwendung nicht unterstützter Citrix Virtual App- oder Desktop-Versionen, nicht unterstützter Workspace-Versionen oder Workspace-Typen usw. Diese Tabelle zeigt die IP-Adresse und die Anzahl der übersprungenen Flows. Diese Workspaces sind möglicherweise nicht Teil der zugelassenen Workspaces. Daher werden diese Sitzungen von der Überwachung ausgeschlossen.

Weitere Informationen zu Problemen im Zusammenhang mit der ICA-Analyse finden Sie unter Problem bei der Datensatzgenerierung für HDX/ICA-Datenverkehr in der NetScaler-Checkliste

WELTANSICHT

Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, historische und aktive Benutzerdetails aus geografischer Sicht anzuzeigen. Die Administratoren können eine Weltansicht des Systems erhalten und durch Klicken auf die Region zu einem bestimmten Land und weiter zu Städten navigieren. Die Administratoren können die Informationen auch nach Stadt und Bundesland detaillierter anzeigen. Ab NetScaler Console Version 12.0 und höher können Sie zu Benutzern navigieren, die von einem geografischen Standort aus verbunden sind.

Die folgenden Details können auf der Weltkarte in HDX Insight angezeigt werden, und die Dichte jeder Metrik wird in Form einer Heatmap dargestellt:

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Gesamt-Bytes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ansicht pro Instanz

Die Ansicht pro Instanz bietet detaillierte Berichte zur Endbenutzererfahrung für eine bestimmte ausgewählte NetScaler-Instanz.

So navigieren Sie zur Instanzansicht:

1. Navigieren Sie zu **Gateway** > **HDX Insight** > **Instanzen**.
2. Wählen Sie eine bestimmte Instanz aus dem **Instanz-Zusammenfassungsbericht** aus.

LINIENDIAGRAMM

METRIKEN	BESCHREIBUNG
IP-Adresse	Dies stellt die NetScaler-IP-Adresse der ausgewählten Instanz dar.
Gesamtzahl der Sitzungsstarts	Gesamtzahl der aktiven Citrix Virtual App-Sitzungen im angegebenen Zeitintervall.
Gesamtzahl der Apps	Gesamtzahl der eindeutigen Anwendungen, die in einem bestimmten Zeitintervall gestartet wurden.

ANWENDUNGS-BALKENDIAGRAMM

Zeigt die Top 5 Anwendungen basierend auf aktiven Apps, der Gesamtzahl der Sitzungsstarts, der Gesamtzahl der App-Starts oder der Startdauer an.

BENUTZER-BALKENDIAGRAMM

Das Benutzer-Balkendiagramm zeigt die Top 5 Benutzer basierend auf den folgenden Kriterien an

- Bandbreite
- WAN-Latenz
- DC-Latenz
- ICA-RTT

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BERICHT ÜBER DESKTOP-BENUTZER

Diese Tabelle gibt Einblick in die Citrix Virtual Desktop-Sitzungen für einen bestimmten Benutzer. Diese Metriken können nach Desktop-Startanzahl und Bandbreite sortiert werden.

METRIKEN	BESCHREIBUNG
Name	Der Name des Citrix Virtual Desktops.
Anzahl der Desktop-Starts	Anzahl der Desktop-Starts.
Bandbreite	Gesamtzahl der Bytes pro Sekunde, die für die End-to-End-Kommunikation während des ausgewählten Zeitintervalls verwendet wurden.
DC-Latenz	Latenz, die durch die Serverseite des Netzwerks verursacht wird. Das heißt, von NetScaler zu den Back-End-Servern.
WAN-Latenz	Latenz, die durch die Clientseite des Netzwerks verursacht wird. Das heißt, von NetScaler zum Endbenutzer.
ICA RTT	ICA RTT ist die Bildschirmverzögerung, die der Benutzer bei der Interaktion mit einer Anwendung oder einem Desktop erlebt, die bzw. der auf Citrix Virtual App oder Desktop gehostet wird.

Desktop-Benutzerbericht(/en-us/netscaler-console-service/media/hdx-dekstop-user.png)

WELTANSICHT

Die Weltkartenansicht in HDX Insight ermöglicht es den Administratoren, die Details zu historischen und aktiven Benutzern aus geografischer Sicht anzuzeigen. Die Administratoren können eine Weltansicht des Systems erhalten, zu einem bestimmten Land und durch Klicken auf die Region weiter zu Städten navigieren. Die Administratoren können weiter detaillierte Informationen nach Stadt und Bundesland anzeigen. Ab NetScaler Console Version 12.0 und höher können Sie zu Benutzern navigieren, die von einem geografischen Standort aus verbunden sind.

Die folgenden Details können auf der Weltkarte in HDX Insight angezeigt werden, und die Dichte jeder Metrik wird in Form einer Heatmap dargestellt:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ICA RTT
- WAN-Latenz
- DC-Latenz
- Bandbreite
- Gesamtbytes

Berichte und Metriken der Lizenzansicht

Die Lizenzansicht liefert Details zu den NetScaler Gateway-Lizenzinformationen. Navigieren Sie zu **Gateway** > **HDX Insight** > **Lizenzen**.

Liniendiagramm

METRIKEN	BESCHREIBUNG
Verwendete Lizenzen	Die NetScaler Gateway CCU-Lizenzen, die während des ausgewählten Zeitraums verwendet werden. Jede Zählung stellt die Anzahl der Benutzersitzungen dar. Dies ist unabhängig von den Anwendungs- und Desktopsitzungen, die von diesem Benutzer gestartet wurden.
Gesamtzahl der Lizenzen	Gesamtzahl der NetScaler Gateway CCU-Lizenzen, die dem Kunden zur Verfügung stehen.

Schwellenwertbericht

Der Schwellenwertbericht zeigt die Anzahl der überschrittenen Schwellenwerte, wobei die *Entität* als Lizenz im ausgewählten Zeitraum ausgewählt ist.

Fehlerbehebung bei HDX™ Insight-Problemen

Wenn die HDX Insight-Lösung nicht wie erwartet funktioniert, könnte das Problem bei einem der folgenden Punkte liegen. Beachten Sie die Checklisten in den jeweiligen Abschnitten zur Fehlerbehebung.

- HDX Insight-Konfiguration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Konnektivität zwischen NetScaler und NetScaler Console.
- Datensatzgenerierung für HDX/ICA-Datenverkehr in NetScaler.
- Erfassung von Datensätzen in NetScaler Console.

HDX Insight-Konfigurations-Checkliste

- Stellen Sie sicher, dass die AppFlow-Funktion in NetScaler aktiviert ist. Einzelheiten finden Sie unter AppFlow aktivieren.
- Überprüfen Sie die HDX Insight-Konfiguration in der NetScaler-Laufzeitkonfiguration.

  Führen Sie den Befehl `show running | grep -i <appflow_policy>` aus, um die HDX Insight-Konfiguration zu überprüfen. Stellen Sie sicher, dass der Bindungstyp ICA REQUEST ist. Zum Beispiel:

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  Für den transparenten Modus muss der Bindungstyp ICA_REQ_DEFAULT sein. Zum Beispiel:

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```
- Für Single-Hop-/Access Gateway- oder Double-Hop-Bereitstellungen stellen Sie sicher, dass die HDX Insight AppFlow-Richtlinie an den virtuellen VPN-Server gebunden ist, über den der HDX/ICA-Datenverkehr läuft.
- Für den transparenten Modus oder den LAN-Benutzermodus stellen Sie sicher, dass die ICA®-Ports 1494 und 2598 eingestellt sind.
- Überprüfen Sie, ob der `appflowlog` Parameter im NetScaler Gateway oder VPN Virtual Server für Access Gateway oder Double-Hop-Bereitstellung aktiviert ist. Details finden Sie unter AppFlow für virtuelle Server aktivieren.
- Überprüfen Sie, ob „Connection Chaining“ im Double-Hop NetScaler aktiviert ist. Details finden Sie unter Konfigurieren von NetScaler Gateway Appliances zum Exportieren von Daten.
- Wenn nach einem HA-Failover die HDX Insight-Details übersprungen werden, überprüfen Sie, ob der ICA-Parameter „enableSRonHAFailover“ aktiviert ist. Details finden Sie unter Sitzungszuverlässigkeit auf einem NetScaler Hochverfügbarkeitspaar.

Checkliste zur Konnektivität zwischen NetScaler und NetScaler Console

- Überprüfen Sie den AppFlow-Collector-Status in NetScaler. Details finden Sie unter So überprüfen Sie den Konnektivitätsstatus zwischen NetScaler und AppFlow Collector.
- Überprüfen Sie die Treffer der HDX Insight AppFlow®-Richtlinie.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Führen Sie den Befehl `show appflow policy <policy_name>` aus, um die Treffer der AppFlow-Richtlinie zu überprüfen.

Sie können auch in der GUI zu **System > AppFlow > Policies** navigieren, um die Treffer der AppFlow-Richtlinie zu überprüfen.

- Überprüfen Sie, ob eine Firewall die AppFlow-Ports 4739 oder 5557 blockiert.

Checkliste zur Datensatzgenerierung für HDX/ICA-Verkehr in NetScaler

Führen Sie den Befehl `tail -f /var/log/ns.log | grep -i "default ICA Message"` zur Protokollvalidierung aus. Basierend auf den generierten Protokollen können Sie diese Informationen zur Fehlerbehebung verwenden.

- Protokoll: **Überspringen der ICA-Verbindungsanalyse – HDX Insight wird für diesen Host nicht unterstützt**

  Ursache: Nicht unterstützte Citrix Virtual Apps and Desktops-Versionen

  Problemumgehung: Aktualisieren Sie die Citrix Virtual Apps and Desktops-Server auf eine unterstützte Version.
- Protokoll: **Client-Typ 0x53 empfangen, NICHT UNTERSTÜTZT**

  Ursache: Nicht unterstützte Version der Citrix Workspace-App

  Lösung: Aktualisieren Sie die Citrix Workspace-App auf eine unterstützte Version.
- Protokoll: **Error from erweitern Packet - Skipping all hdx processing for this flow**

  Ursache: Problem beim Entpacken des ICA-Datenverkehrs

  Lösung: Für diese ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wird.
- Protokoll: **Invalid transition: NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT"**

  Ursache: Problem beim Parsen des ICA-Handshakes

  Lösung: Für diese spezielle ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wird.
- Protokoll: **Missing EUEM ICA RTT**

  Ursache: Kanaldaten der Endbenutzer-Erfahrungsüberwachung können nicht geparst werden

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lösung: Stellen Sie sicher, dass der Dienst für die Endbenutzer-Erfahrungsüberwachung auf den Citrix Virtual Apps and Desktops-Servern gestartet ist. Stellen Sie sicher, dass Sie die unterstützten Versionen der Citrix Workspace-App verwenden.

- Protokoll: **Invalid Channel Header**

  Ursache: Kanalheader kann nicht identifiziert werden

  Lösung: Für diese spezielle ICA-Sitzung sind keine Berichte verfügbar, bis eine neue Sitzung eingerichtet wird.

- Protokoll: **Skip code**

  Wenn Sie einen der folgenden Werte für den Überspringcode sehen, dann werden die Insight-Details übersprungen.

  Überspringcode 0 zeigt an, dass der Datensatz erfolgreich aus NetScaler exportiert wurde.

ÜBERSPRINGCODE	FEHLERMELDUNG	FEHLERURSACHE
100	NS_ICA_ERR_NULL_FRAG	Fehler bei der Verarbeitung von ICA-Fragmenten, wahrscheinlich aufgrund von Speicherbedingungen
101	NS_ICA_ERR_INVALID_HS_CMD	Ungültiger Handshake-Befehl empfangen
102	NS_ICA_ERR_REDUC_PARAM_CNT	Ungültiger Parameter für die Initialisierung des V3-Expanders angegeben
103	NS_ICA_ERR_REDUC_INIT	V3-Expander konnte nicht korrekt initialisiert werden
104	NS_ICA_ERR_REDUC_PARAM_BYTES	Nicht genügend Bytes, um einem Kanal einen Coder zuzuweisen
105	NS_ICA_ERR_INVALID_CHANNEL	Ungültige ICA-Kanalnummer
106	NS_ICA_ERR_INVALID_DECODER	Ungültiger Decoder für einen Kanal angegeben

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÜBERSPRINGCODE	FEHLERMELDUNG	FEHLERURSACHE
107	NS_ICA_ERR_INVALID_TW_PARAM	Ungültige Parameteranzahl für den Thinwire-Kanal angegeben
108	NS_ICA_ERR_INVALID_TW_DECODER	Ungültiger Decoder für Thinwire-Kanal
109	NS_ICA_ERR_REDUC_NO_DECODER	Kein Decoder für Kanal definiert
110	NS_ICA_ERR_REDUC_V3_EXPANDER	Fehler beim erweiternieren der Kanaldaten
111	NS_ICA_ERR_REDUC_BYTES_V3_OOR	Expander-Fehler: Mehr Bytes verbraucht als verfügbar
112	NS_ICA_ERR_REDUC_BYTES_OOR	Fehler: Überlauf unkomprimierter Daten
113	NS_ICA_ERR_REDUC_INVALID_CMD	Undefinierter Expander-Befehl
114	NS_ICA_ERR_CGP_FILL_HOLE	Fehler beim Verarbeiten von geteilten CGP-Frames
115	NS_ICA_ERR_MEM_NSB_ALLOC	NSB-Zuweisungsfehler – aufgrund geringer Speicherkapazität
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	Speicherzuweisungsfehler für Expander-Kontext
117	NS_ICA_ERR_ICA_OLD_SERVER	Alter Server, Capability-Blöcke werden nicht unterstützt
118	NS_ICA_ERR_PIR_MANY_FRAG	Paket-Init-Anforderung ist fragmentiert, kann nicht verarbeitet werden

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÜBERSPRINGCODE	FEHLERMELDUNG	FEHLERURSACHE
119	NS_ICA_ERR_INIT_ICA_CAPS	Fehler bei der Initialisierung der ICA-Funktion
120	NS_ICA_ERR_NO_MSI_SUPPORT	Host unterstützt die MSI-Funktion nicht. Gilt für XenApp-Versionen niedriger als 6.5 oder XenDesktop-Versionen niedriger als 5.0
121	NS_ICA_ERR_CGP_INVALID_CMD	Ungültiger CGP-Befehl gefunden
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	Unzureichende Bytes über den Kanal
123	NS_ICA_ERR_CHANNEL_DATA	Falsche Daten auf dem EUEM-, CONTROL- oder SEAMLESS-Kanal
124	NS_ICA_ERR_INVALID_PURE_CMD	Ungültiger Befehl beim Verarbeiten von reinen ICA-Kanaldaten empfangen
125	NS_ICA_ERR_INVALID_PURE_LEN0	Ungültige Länge beim Verarbeiten von reinen ICA-Kanaldaten festgestellt
126	NS_ICA_ERR_INVALID_PURE_LEN	Ungültige Länge beim Verarbeiten von reinen ICA-Kanaldaten festgestellt
127	NS_ICA_ERR_INVALID_CLNT_DATA	Ungültige Datenlänge vom Client empfangen
128	NS_ICA_ERR_MSI_GUID_SZ	Fehler bei der MSI GUID-Größe
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	Ungültiger Kanal-Header erkannt

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÜBERSPRINGCODE	FEHLERMELDUNG	FEHLERURSACHE
130	NS_ICA_ERR_CGP_PARSE_RECONNECT_ID	Abruf der wiederhergestellten Sitzung fehlgeschlagen
131	NS_ICA_ERR_DISABLE_SR_NON_NS_RECONNECT	Fehler beim Deaktivieren von SR
132	NS_ICA_ERR_REDUC_NOT_V3	Nicht unterstützte ICA Reducer-Version
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Komprimierung deaktiviert, vom Host nicht berücksichtigt
134	NS_ICA_ERR_IDENT_PROTO	ICA- oder CGP-Protokoll kann nicht identifiziert werden, tritt bei falschen Receivern auf
135	NS_ICA_ERR_INVALID_SIGNATURE	Falsche ICA-Signatur oder Magic String
136	NS_ICA_ERR_PARSE_RAW	Fehler beim Parsen des ICA-Handshake-Pakets
137	NS_ICA_ERR_INCOMPLETE_PKT	Unvollständiges Paket im Handshake empfangen
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	ICA-Frame ist zu groß, überschreitet 1.460 Bytes
139	NS_ICA_ERR_FORWARD	Fehler beim Weiterleiten der ICA-Daten
140	NS_ICA_ERR_MAX_HOLES	CGP-Befehl kann nicht verarbeitet werden, da er über die unterstützte Grenze hinaus aufgeteilt ist
141	NS_ICA_ERR_ASSEMBLE_FRAME	ICA-Frame kann nicht korrekt wiederhergestellt werden

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÜBERSPRINGCODE	FEHLERMELDUNG	FEHLERURSACHE
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	ICA-Parsing für diesen Arbeitsbereich (Client) übersprungen, da er nicht in der Zulassungsliste enthalten ist
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	Parsing-Status für Client-Wiederverbindungs-Cookie kann nicht erkannt werden
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	Ungültige Länge des Wiederverbindungs-Cookies nach Client-Wiederverbindung erkannt
145	NS_ICA_ERR_INVALID_RECONNECT_ID	Client-Wiederverbindungs-Cookie hat die erforderliche Einschränkung nicht erfüllt
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	Ungültige Workspace-Versionszeichenfolge vom Client empfangen
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	Ungültige Produkt-ID vom Client empfangen
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	Ungültige Kanallänge nach der Erweiterung
149	NS_ICA_ERR_SPECIAL_THINWIRE	Dekomprimierungsfehler
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	Es wurden unzureichende Bytes für den nahtlosen Befehl festgestellt.
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Es wurden unzureichende Bytes für den EUEM-Befehl festgestellt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÜBERSPRINGCODE	FEHLERMELDUNG	FEHLERURSACHE
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	Ungültiges Ereignis für die nahtlose Kanalanalyse
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Ungültiges Ereignis für die CTRL-Kanal-Analyse
154	NS_ICA_ERR_EUEM_INVALID_EVENT	Ungültiges Ereignis für die EUEM-Kanal-Analyse
155	NS_ICA_ERR_USB_INVALID_EVENT	Ungültiges Ereignis für die USB-Kanal-Analyse
156	NS_ICA_ERR_PURE_INVALID_EVENT	Ungültiges Ereignis für die reine Kanal-Analyse
157	NS_ICA_ERR_VCP_INVALID_EVENT	Ungültiges Ereignis für die virtuelle Kanal-Analyse
158	NS_ICA_ERR_ICAP_INVALID_EVENT	Ungültiges Ereignis für die ICA-Datenanalyse
159	NS_ICA_ERR_CGPP_INVALID_EVENT	Ungültiges Ereignis für die CGP-Datenanalyse
160	NS_ICA_ERR_BASICCRYPT_INVALIDSTATE	Ungültiger Zustand für einen Krypto-Befehl bei der Basisverschlüsselung
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	Ungültiger Krypto-Befehl bei der Basisverschlüsselung
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	Ungültiger Zustand für einen Krypto-Befehl bei der RC5-Verschlüsselung
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	Ungültiger Krypto-Befehl bei der RC5-Verschlüsselung
164	NS_ICA_ERR_ADVCRYPT_ENC	Fehler bei der RC5-Verschlüsselung/-Entschlüsselung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÜBERSPRINGCODE	FEHLERMELDUNG	FEHLERURSACHE
165	NS_ICA_ERR_ADVCRYPT_DEC	Fehler bei der RC5-Verschlüsselung/-Entschlüsselung
166	NS_ICA_ERR_SERVER_NOT_REDUCER_V3	VDA unterstützt Reducer Version 3 nicht
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Workspace unterstützt Reducer Version 3 nicht
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Unerwartete Anzahl von Bytes im ICA-Handshake
169	NS_ICA_ERR_HIGHER_RECONSEQ	Höhere CGP-Wiederaufnahmesequenznummer vom Peer nach erneuten Verbindungen
170	NS_ICA_ERR_DESCSRINFO_ABSENT	ICA-Parsing-Status nach erneuter Verbindung kann nicht wiederhergestellt werden
171	NS_ICA_ERR_NSAP_PARSING	Fehler beim Parsen von Insight-Kanaldaten
172	NS_ICA_ERR_NSAP_APP	Fehler beim Parsen von App-Details aus Insight-Kanaldaten
173	NS_ICA_ERR_NSAP_ACR	Fehler beim Parsen der ACR-Details aus den Insight-Kanaldaten
174	NS_ICA_ERR_NSAP_SESSION_END	Fehler beim Parsen der Sitzungsendedetails aus den Insight-Kanaldaten
175	NS_ICA_ERR_NON_NSAP_SN	ICA-Parsing auf dem Dienstknoten wurde aufgrund fehlender Insight-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ÜBERSPRINGCODE	FEHLERMELDUNG	FEHLERURSACHE
		Kanalunterstützung übersprungen
176	NS_ICA_ERR_NON_NSAP_CLIENT	NSAP wird vom Client nicht unterstützt
177	NS_ICA_ERR_NON_NSAP_SERVER	NSAP wird vom VDA nicht unterstützt
178	NS_ICA_ERR_NSAP_NEG_FAIL	Fehler bei der NSAP-Datenverhandlung
179	NS_ICA_ERR_SN_RECONNECT_TKT_FETCH	Fehler beim Abrufen des Service-Reconnect-Tickets im Service-Knoten
180	NS_ICA_ERR_SN_HIGHER_RECONSEQ	Fehler beim Empfangen einer höheren Reconnect-Sequenznummer im Service-Knoten
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONNSAP	Fehler beim Deaktivieren von HDX Insight für Nicht-NSAP-Verbindungen

Beispielprotokolle:

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49 GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]"
```

```
Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41 GMT ns-223 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow: Session GUID [4e3a91175ebcbe686baf175eec7e0200], Client IP/Port [10.105.232.40/60059], Server IP/Port [10.106.40.219/2598], MSI Client Cookie [Non-MSI], Session setup time [01/09/2020:22:55:39 GMT], Client Type [0x0052], Receiver Version [19.12.0.23],
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`User [user1], Client [10.105.232.40], Server [10.106.40.219], Ctx Flags [0x8820220008], Track Flags [0x1600010c040], Skip Code [171]"`

Fehlerzähler

Verschiedene Zähler werden bei der ICA-Analyse erfasst. Die folgende Tabelle listet die verschiedenen Zähler für die ICA-Analyse auf. Führen Sie den Befehl `nsconmsg –g hdx –d statswt0` aus, um die Zählerdetails anzuzeigen.

HDX-ZÄHLERNAME	ZWECK	KATEGORIE (STATS/ ERROR/DIAGNOSTICS)
hdx_tot_ica_conn	Gibt die Gesamtzahl der von NS erkannten reinen ICA-Verbindungen an. Wird immer dann erhöht, wenn eine ICA-Verbindung basierend auf der ICA-Signatur auf einer Client-PCB erkannt wird.	Stats
hdx_tot_cgp_conn	Gibt die Gesamtzahl der von NS erkannten CGP-Verbindungen an (Sitzungszuverlässigkeit EIN). Wird immer dann erhöht, wenn eine CGP-Verbindung basierend auf der CGP-Signatur auf einer Client-PCB erkannt wird.	Stats
hdx_dbg_tot_udt_conn	Gibt die Gesamtzahl der von NS erkannten UDP-ICA-Verbindungen an.	Stats
hdx_dbg_tot_nsap_conn	Gibt die Gesamtzahl der von NS erkannten NSAP-unterstützten Verbindungen an.	Statistiken
hdx_tot_skip_conn	Gibt an, wie viele ICA-Verbindungen vom Parser aufgrund einer ungültigen	Statistiken

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX-ZÄHLERNAME	ZWECK	KATEGORIE (STATS/ ERROR/DIAGNOSTICS)
	ICA- oder CGP-Signatur übersprungen wurden.	
hdx_dbg_active_conn	Gesamtzahl der aktiven EDT-/CGP-/ICA-Verbindungen zu diesem Zeitpunkt.	Statistiken
hdx_dbg_active_nsap_conn	Gesamtzahl der aktiven EDT-/CGP-/ICA-NSAP-Verbindungen zu diesem Zeitpunkt.	Statistiken
hdx_dbg_skip_appflow_disabled	Gesamtzahl der Instanzen, bei denen AppFlow aufgrund der Deaktivierung von AppFlow von einer Sitzung getrennt wurde.	Statistiken/Diagnose
hdx_dbg_transparent_user	Gesamtzahl der transparenten Benutzerzugriffe	Statistiken/Diagnose
hdx_dbg_ag_user	Gesamtzahl der Access Gateway-Benutzerzugriffe	Statistiken/Diagnose
hdx_dbg_lan_user	Gesamtzahl der LAN-Benutzermodus-Zugriffe	Statistiken/Diagnose
hdx_basic_enc	Gibt die Anzahl der ICA-Verbindungen an, die eine einfache Verschlüsselung verwenden	Statistiken/Diagnose
hdx_advanced_enc	Gibt die Anzahl der ICA-Verbindungen an, die eine erweiterte RC5-basierte Verschlüsselung verwenden	Statistiken/Diagnose
hdx_dbg_reconnected_session	Gesamtzahl der Wiederverbindungsanfragen	Statistiken/Diagnose

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX-ZÄHLERNAME	ZWECK	KATEGORIE (STATS/ ERROR/DIAGNOSTICS)
	vom Client ohne NetScaler-Fehler	
hdx_dbg_host_rejected_ns_reconnect	Gesamtzahl der Hosts, die Wiederverbindungsanfragen vom Client abgelehnt haben	Statistiken/Diagnose
hdx_euem_available	Gibt die Anzahl der Verbindungen an, für die der End User Experience Monitoring-Kanal verfügbar ist. Der End User Experience Monitoring-Kanal ist erforderlich, um Statistiken wie ICA RTT zu erfassen.	Statistiken/Diagnose
hdx_err_disabled_sr	Die Sitzungszuverlässigkeit ist mit dem `nsapimgr`-Regler deaktiviert. Die Sitzung funktioniert für diese Sitzung nicht.	Fehler
hdx_err_skip_no_msi	Der XA/XD-Server verfügt nicht über die MSI-Funktionalität. Dies deutet auf eine ältere Serverversion hin, HDX Insight überspringt diese Verbindung.	Fehler
hdx_err_skip_old_server	Alte, nicht unterstützte Serverversion	Fehler
hdx_err_clnt_not_whitelist	Client-Empfänger nicht in der Zulassungsliste, HDX Insight überspringt diese Verbindung	Fehler
hdx_sm_ica_cam_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CAM_CHANNEL	Diagnose

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX-ZÄHLERNAME	ZWECK	KATEGORIE (STATS/ ERROR/DIAGNOSTICS)
hdx_sm_ica_usb_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_USB_CHANNEL	Diagnose
hdx_sm_ica_clip_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CLIP_CHANNEL	Diagnose
hdx_sm_ica_ccm_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CCM_CHANNEL	Diagnose
hdx_sm_ica_cdm_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CDM_CHANNEL	Diagnose
hdx_sm_ica_com1_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_COM1_CHANNEL	Diagnose
hdx_sm_ica_com2_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_COM2_CHANNEL	Diagnose
hdx_sm_ica_cpm_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_CPM_CHANNEL	Diagnose
hdx_sm_ica_lpt1_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_LPT1_CHANNEL	Diagnose

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX-ZÄHLERNAME	ZWECK	KATEGORIE (STATS/ ERROR/DIAGNOSTICS)
hdx_sm_ica_lpt2_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_LPT2_CHANNEL	Diagnose
dx_dbg_sm_ica_msi_disabled	Gesamtzahl der Fälle, in denen MSI über die SmartAccess-Richtlinie deaktiviert ist	Diagnose
hdx_sm_ica_file_channel_disabled	Gesamtzahl der über die SmartAccess-Richtlinie deaktivierten NS_ICA_FILE_CHANNEL	Diagnose
hdx_dbg_usb_accept_device	Gesamtzahl der akzeptierten USB-Geräte	Diagnose
hdx_dbg_usb_reject_device	Gesamtzahl der abgelehnten USB-Geräte	Diagnose
hdx_dbg_usb_reset_endpoint	Gesamtzahl der zurückgesetzten USB-Endpunkte	Diagnose
hdx_dbg_usb_reset_device	Gesamtzahl der zurückgesetzten USB-Geräte	Diagnose
hdx_dbg_usb_stop_device	Gesamtzahl der gestoppten USB-Geräte	Diagnose
hdx_dbg_usb_stop_device_response	Gesamtzahl der Antworten von gestoppten USB-Geräten	Diagnose
hdx_dbg_usb_device_gone	Gesamtzahl der entfernten USB-Geräte	Diagnose
hdx_dbg_usb_device_stopped	Gesamtzahl der gestoppten USB-Geräte	Diagnose

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nstrace-Validierung

Überprüfen Sie das CFLOW-Protokoll, um alle AppFlow-Datensätze zu sehen, die NetScaler verlassen.

Checkliste zur Datensatzpopulation in NetScaler Console

- Führen Sie den Befehl `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` aus und überprüfen Sie die Protokolle, um zu bestätigen, dass NetScaler Console AppFlow-Datensätze empfängt.
- Bestätigen Sie, dass die NetScaler-Instanz zu NetScaler Console hinzugefügt wurde.
- Überprüfen Sie, ob der virtuelle NetScaler Gateway/VPN-Server in NetScaler Console lizenziert ist.
- Stellen Sie sicher, dass die Multi-Hop-Parametereinstellung für Double-Hop aktiviert ist.
- Stellen Sie sicher, dass NetScaler Gateway für den zweiten Hop in einer Double-Hop-Bereitstellung freigegeben ist.

Bevor Sie den technischen Support von Citrix kontaktieren

Für eine schnelle Lösung stellen Sie sicher, dass Sie die folgenden Informationen haben, bevor Sie den technischen Support von Citrix kontaktieren:

- Details zur Bereitstellung und Netzwerktopologie.
- NetScaler- und NetScaler Console-Versionen.
- Citrix Virtual Apps and Desktops Serverversionen.
- Client-Workspace-Versionen.
- Anzahl der aktiven ICA-Sitzungen, als das Problem auftrat.
- Tech Support-Bundle, das durch Ausführen des Befehls `show techsupport` an der NetScaler-Eingabeaufforderung erfasst wurde.
- Tech Support-Bundle, das für NetScaler Console erfasst wurde.
- Paket-Traces, die auf allen NetScaler erfasst wurden. Um einen Paket-Trace zu starten, geben Sie `start nstrace -size 0'` ein. Um einen Paket-Trace zu stoppen, geben Sie `stop nstrace` ein.
- Sammeln Sie Einträge in der ARP-Tabelle des Systems, indem Sie den Befehl `show arp` ausführen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bekannte Probleme

Beachten Sie die NetScaler-Versionshinweise für bekannte Probleme mit HDX Insight.

Metrikinformationen für Schwellenwerte

Sie können Schwellenwerte erstellen und benachrichtigt werden, sobald der Schwellenwert überschritten wird. In einer typischen Bereitstellung können Sie Schwellenwerte festlegen, um:

- Verschiedene Anwendungsmetriken verfolgen
- Planung erleichtern
- Benachrichtigt werden, wenn der Metrikwert der Anwendungen den festgelegten Schwellenwert überschreitet

So konfigurieren Sie den Schwellenwert:

1. Navigieren Sie zu **Einstellungen > Analyse-Einstellungen > Schwellenwerte**.
2. Klicken Sie auf der Seite **Schwellenwerte** auf **Hinzufügen**.

Web

METRIKEN	ENTITÄT	BESCHREIBUNG
Anwendungen	Treffer	Gesamtzahl der Treffer, die von einem virtuellen Server (Anwendung) empfangen wurden
	Bandbreite (MB)	Gesamte Bandbreite, die vom virtuellen Server (Anwendung) verbraucht wird
	Antwortzeit (ms)	Die Zeit, die der virtuelle Server zum Antworten benötigt
Clients	Anfragen	Die vom Client empfangene Gesamtanfrage
	Renderzeit (ms)	Die Zeit, die der Client zum Rendern der Serverantwort benötigt

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	ENTITÄT	BESCHREIBUNG
	Client-Netzwerklatenz	Die Zeit, die für Anfragen aus dem Client-Netzwerk benötigt wird
Geräte	Treffer	Gesamtzahl der von einem Gerät empfangenen Treffer. Zum Beispiel: Laptop, Mobiltelefon
	Bandbreite (MB)	Gesamte Bandbreite, die von einem Gerät verbraucht wird
Domänen	Treffer	Gesamtzahl der Treffer, die von einer Netzwerkdomäne empfangen wurden
	Bandbreite (MB)	Gesamte Bandbreite, die von einer Netzwerkdomäne verbraucht wird
	Antwortzeit (ms)	Die Zeit, die eine Netzwerkdomäne benötigt, um Anfragen zu beantworten
Betriebssystem	Treffer	Gesamtzahl der Treffer, die von einem Betriebssystem empfangen wurden
	Bandbreite (MB)	Gesamte Bandbreite, die von einem Betriebssystem verbraucht wird
	Renderzeit (ms)	Die Zeit, die ein Betriebssystem benötigt, um die Serverantwort zu rendern
Anfragemethoden	Treffer	Gesamtzahl der von einer Anfragemethode empfangenen Anfragen. Zum Beispiel: GET, POST

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	ENTITÄT	BESCHREIBUNG
	Bandbreite (MB)	Gesamtbandbreite, die von einer Anfragemethode verbraucht wird
Antwortstatus	Treffer	Gesamtzahl der Treffer, die mit Antwortcodes empfangen wurden
	Bandbreite (MB)	Gesamtbandbreite, die vom Antwortcode verbraucht wird
Server	Treffer	Gesamtzahl der von einem Server empfangenen Anfragen/Treffer
	Bandbreite (MB)	Gesamtbandbreite, die von einem Server verbraucht wird
	Server-Netzwerklatenz (ms)	Die Zeit, die für Anfragen aus dem Servernetzwerk benötigt wird
	Server-Verarbeitungszeit (ms)	Die Zeit, die ein Server benötigt, um auf Anfragen zu antworten
URLs	Treffer	Gesamtzahl der Treffer, die eine URL erhalten hat. Zum Beispiel: www.Citrix.com
	Ladezeit (ms)	Die Zeit, die eine URL benötigt, um vom Server geladen zu werden
	Renderzeit (ms)	Die Zeit, die die URL zum Rendern und Anzeigen benötigt
Benutzeragenten	Treffer	Gesamtzahl der Anfragen, die ein Benutzeragent erhalten

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	ENTITÄT	BESCHREIBUNG
		hat. Zum Beispiel: Chrome-Webbrowser
	Bandbreite (MB)	Gesamte Bandbreite, die vom Benutzeragenten verbraucht wird
	Renderzeit (ms)	Die Zeit, die der Benutzeragent zum Rendern der Serverantwort benötigt

Sicherheit

METRIK	ENTITÄT	BESCHREIBUNG
Anwendungen	Bedrohungsindex	Ein einstelliges Bewertungssystem, das die Kritikalität von Angriffen auf die Anwendung angibt. Je kritischer die Angriffe auf eine Anwendung sind, desto höher ist der Bedrohungsindex für diese Anwendung. Die Werte reichen von 1 bis 7.
	Sicherheitsindex	Ein einstelliges Bewertungssystem, das angibt, wie sicher Sie die NetScaler-Instanzen konfiguriert haben, um Anwendungen vor externen Bedrohungen und Schwachstellen zu schützen. Je geringer die Sicherheitsrisiken für eine Anwendung sind, desto höher ist der Sicherheitsindex. Die Werte reichen von 1 bis 7.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

APPANALYTICS

METRIK	ENTITÄT	BESCHREIBUNG
Anwendungen	AppScore	App Score definiert, wie gut eine Anwendung funktioniert, und zeigt an, ob die Anwendung hinsichtlich der Reaktionsfähigkeit gut funktioniert. Die Werte reichen von 0 bis 80.

HDX™

Informationen zu HDX-Schwellenwerten finden Sie unter Schwellenwerte erstellen und Warnmeldungen für HDX Insight

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastruktur

Die Infrastrukturfunktionen von NetScaler Console ermöglichen Ihnen die Überwachung und Verwaltung Ihrer NetScaler-Instanzen. Sie können die Infrastrukturintegrität analysieren, Instanzen und Ereignisse verwalten, SSL-Zertifikate handhaben, Konfigurations- und Upgrade-Aufträge ausführen und Instanzen in Ihrem Netzwerk bereitstellen.

Die folgenden Themen helfen Ihnen bei der Überwachung und Verwaltung Ihrer Infrastruktur:

- Infrastruktur-Analysen
- Instanzverwaltung
- Ereignisse
- SSL-Dashboard
- Konfiguration
- Upgrade-Aufträge
- Netzwerkfunktionen
- Netzwerkberichterstattung
- Bereitstellung
- Orchestrierung

Infrastruktur-Analysen

Ein wichtiges Ziel für Netzwerkadministratoren ist die Überwachung von NetScaler-Instanzen. NetScaler-Instanzen bieten interessante Einblicke in die Nutzung und Leistung von Anwendungen und Desktops, auf die über sie zugegriffen wird. Administratoren müssen die NetScaler-Instanz überwachen und die von jeder NetScaler-Instanz verarbeiteten Anwendungsflüsse analysieren. Administratoren müssen auch in der Lage sein, mögliche Probleme bei der Konfiguration, Einrichtung, Konnektivität, Zertifikaten und anderen Auswirkungen auf die Anwendungsnutzung oder -leistung zu beheben. Zum Beispiel kann eine plötzliche Änderung des Anwendungsverkehrsmusters auf eine Änderung der SSL-Konfiguration zurückzuführen sein, wie die Deaktivierung eines SSL-Protokolls. Administratoren müssen in der Lage sein, die Korrelation zwischen diesen Datenpunkten schnell zu erkennen, um Folgendes sicherzustellen:

- Die Anwendungsverfügbarkeit befindet sich in einem optimalen Zustand

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Es gibt keine Probleme mit Ressourcenverbrauch, Hardware, Kapazität oder Konfigurationsänderungen
- Es gibt keine ungenutzten Bestände
- Es gibt keine abgelaufenen Zertifikate

Die Funktion „Infrastruktur-Analysen“ vereinfacht den Prozess der Datenanalyse, indem sie mehrere Datenquellen korreliert und zu einem messbaren Score quantifiziert, der den Zustand einer Instanz definiert. Mit dieser Funktion erhalten Administratoren einen zentralen Anlaufpunkt, um das Problem, dessen Ursprung und mögliche Abhilfemaßnahmen zu verstehen, die sie durchführen können.

Infrastruktur-Analysen in NetScaler Console

Die Funktion „Infrastruktur-Analysen“ sammelt alle von den NetScaler-Instanzen erfassten Daten und quantifiziert sie zu einem **Instanz-Score**, der den Zustand der Instanzen definiert. Der Instanz-Score wird in einer Tabellenansicht oder als Kreispackungs-Visualisierung zusammengefasst. Die Funktion „Infrastruktur-Analysen“ hilft Ihnen, die Faktoren zu visualisieren, die zu einem Problem auf den Instanzen geführt haben oder führen könnten. Diese Visualisierung hilft Ihnen auch, die Maßnahmen zu bestimmen, die ergriffen werden müssen, um das Problem und dessen Wiederauftreten zu verhindern.

Instanz-Score

Der Instanz-Score gibt den Zustand einer NetScaler-Instanz an. Ein Score von 100 bedeutet eine perfekt funktionierende Instanz ohne Probleme. Der Instanz-Score erfasst verschiedene Ebenen potenzieller Probleme auf der Instanz. Er ist eine quantifizierbare Messung des Instanzzustands, und mehrere „Gesundheitsindikatoren“ tragen zu diesem Score bei.

Gesundheitsindikatoren sind die Bausteine des Instanz-Scores, wobei der Score periodisch für einen vordefinierten „Überwachungszeitraum“ berechnet wird, basierend auf allen in diesem Zeitfenster erkannten Indikatoren. Derzeit berechnet die Infrastrukturanalyse den Instanz-Score einmal pro Stunde basierend auf den von den Instanzen gesammelten Daten. Ein Indikator kann als jede Aktivität (ein Ereignis oder ein Problem) definiert werden, die zu einer der folgenden Kategorien auf den Instanzen gehört.

- Systemressourcenindikatoren
- Indikatoren für kritische Ereignisse
- SSL-Konfigurationsindikatoren
- Indikatoren für Konfigurationsabweichungen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Erläuterung der Zustandsindikatoren

- Indikatoren für Systemressourcen

  Im Folgenden sind die kritischen Systemressourcenprobleme aufgeführt, die auf NetScaler-Instanzen auftreten und von NetScaler Console überwacht werden können.

  - **Hohe CPU-Auslastung**. Die CPU-Auslastung hat den oberen Schwellenwert in der NetScaler-Instanz überschritten.
  - **Hohe Speicherauslastung**. Die Speicherauslastung hat den oberen Schwellenwert in der NetScaler-Instanz überschritten.
  - **Hohe Festplattenauslastung**. Die Festplattenauslastung hat den oberen Schwellenwert in der NetScaler-Instanz überschritten.
  - **Festplattenfehler**. Es liegen Fehler auf Festplatte 0 oder Festplatte 1 des Hypervisors vor, auf dem die NetScaler-Instanz installiert ist.
  - **Stromausfall**. Die Stromversorgung ist ausgefallen oder von der NetScaler-Instanz getrennt.
  - **SSL-Kartenfehler**. Die auf der Instanz installierte SSL-Karte ist ausgefallen.
  - **Flash-Fehler**. Auf der NetScaler-Instanz wurden Compact-Flash-Fehler festgestellt.
  - **NIC-Verwerfungen**. Die von der NIC-Karte verworfenen Pakete haben den oberen Schwellenwert in der NetScaler-Instanz überschritten.

Weitere Informationen zu diesen Systemressourcenfehlern finden Sie unter Instanz-Dashboard.

- Indikatoren für kritische Ereignisse

  Die folgenden kritischen Ereignisse werden durch die Ereignisse unter der Ereignisverwaltungsfunktion von NetScaler Console identifiziert, die mit kritischer Schwere konfiguriert sind.

  - **HA-Synchronisierungsfehler**. Die Konfigurationssynchronisierung zwischen den NetScaler-Instanzen in Hochverfügbarkeit ist auf dem sekundären Server fehlgeschlagen.
  - **HA keine Heartbeats**. Der primäre Server in einem Paar von NetScaler-Instanzen in Hochverfügbarkeit empfängt keine Heartbeats vom sekundären Server.
  - **HA schlechter sekundärer Status**. Der sekundäre Server in einem Paar von NetScaler-Instanzen in Hochverfügbarkeit befindet sich im Status „Down“, „Unknown“ oder „Stay secondary“.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **HA-Versionskonflikt**. Die Version der NetScaler-Software-Images, die auf einem Paar von NetScaler-Instanzen in Hochverfügbarkeit installiert sind, stimmt nicht überein.
- **Cluster-Synchronisierungsfehler**. Die Konfigurationssynchronisierung zwischen den NetScaler-Instanzen im Cluster-Modus ist fehlgeschlagen.
- **Cluster-Versionskonflikt**. Die Version der NetScaler-Software-Images, die auf den NetScaler-Instanzen im Cluster-Modus installiert sind, stimmt nicht überein.
- **Cluster-Propagierungsfehler**. Die Weitergabe von Konfigurationen an alle Instanzen in einem Cluster ist fehlgeschlagen.

HINWEIS:

Sie können Ihre Liste kritischer SNMP-Ereignisse erstellen, indem Sie die Schweregrade der Ereignisse ändern. Weitere Informationen zum Ändern der Schweregrade finden Sie unter Ändern des gemeldeten Schweregrads von Ereignissen, die auf NetScaler-Instanzen auftreten.

Weitere Informationen zu Ereignissen in NetScaler Console finden Sie unter Ereignisse.

- SSL-Konfigurationsindikatoren
  - **Nicht empfohlene Schlüsselstärke**. Die Schlüsselstärke der SSL-Zertifikate entspricht nicht den NetScaler®-Standards.
  - **Nicht empfohlener Aussteller**. Der Aussteller des SSL-Zertifikats wird von Citrix nicht empfohlen.
  - **SSL-Zertifikate abgelaufen**. Das in der NetScaler-Instanz installierte SSL-Zertifikat ist abgelaufen.
  - **SSL-Zertifikate laufen bald ab**. Das in der NetScaler-Instanz installierte SSL-Zertifikat läuft in der nächsten Woche ab.
  - **Nicht empfohlene Algorithmen**. Die Signaturalgorithmen der in der NetScaler-Instanz installierten SSL-Zertifikate entsprechen nicht den NetScaler-Standards.

Weitere Informationen zu SSL-Zertifikaten finden Sie unter SSL-Dashboard.

- Indikatoren für Konfigurationsabweichungen
  - **Konfigurationsabweichungsvorlage**. Es gibt eine Abweichung (nicht gespeicherte Änderungen) in der Konfiguration von den Audit-Vorlagen, die Sie mit spezifischen Konfigurationen erstellt haben, die Sie auf bestimmten Instanzen prüfen möchten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Standard-Konfigurationsabweichung**. Es gibt eine Abweichung (nicht gespeicherte Änderungen) in der Konfiguration von den Standardkonfigurationsdateien.

Weitere Informationen zu Konfigurationsabweichungen und zum Ausführen von Audit-Berichten zur Überprüfung von Konfigurationsabweichungen finden Sie unter Audit-Berichte anzeigen..

NetScaler-Kapazitätsprobleme anzeigen

Wenn eine NetScaler-Instanz den Großteil ihrer verfügbaren Kapazität verbraucht hat, kann es beim Verarbeiten des Client-Datenverkehrs zu Paketverlusten kommen. Durch das Verständnis solcher NetScaler-Kapazitätsprobleme können Sie proaktiv zusätzliche Lizenzen zuweisen, um die NetScaler-Leistung zu stabilisieren. Weitere Informationen finden Sie unter Kapazitätsprobleme in einer NetScaler-Instanz anzeigen.

Wert der Gesundheitsindikatoren

Die Indikatoren werden basierend auf ihren Werten wie folgt in hochprioritäre Indikatoren und niedrigprioritäre Indikatoren eingeteilt:

Die Gesundheitsindikatoren innerhalb derselben Indikatorengruppe haben unterschiedliche Gewichtungen. Ein Indikator kann stärker zu einer niedrigeren Instanzbewertung beitragen als ein anderer Indikator. Zum Beispiel senkt eine hohe Speicherauslastung die Instanzbewertung stärker als eine hohe Festplattenauslastung, eine hohe CPU-Auslastung und NIC-Verwerfungen. Wenn bei einer Instanz eine größere Anzahl von Indikatoren erkannt wird, ist die Instanzbewertung geringer.

Der Wert eines Indikators wird basierend auf den folgenden Regeln berechnet. Der Indikator gilt als auf eine der folgenden drei Arten erkannt:

1. **Basierend auf einer Aktivität**. Zum Beispiel wird ein Systemressourcenindikator ausgelöst, wenn ein Stromausfall auf der Instanz auftritt, und dieser Indikator reduziert den Wert der Instanzbewertung. Wenn der Indikator gelöscht wird, wird die Strafe aufgehoben, und die Instanzbewertung steigt.
2. **Basierend auf der Überschreitung des Schwellenwerts**. Zum Beispiel wird ein Systemressourcenindikator ausgelöst, wenn die NIC-Karte Pakete verwirft und der Schwellenwert überschritten wird.
3. **Basierend auf der Überschreitung des niedrigen und hohen Schwellenwerts**. Hier kann ein Indikator auf zwei Arten ausgelöst werden:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wenn der Wert des Indikators zwischen dem niedrigen und hohen Schwellenwert liegt, wobei eine teilweise Strafe auf den Instanz-Score erhoben wird.
- Wenn der Wert den hohen Schwellenwert überschreitet, wobei eine volle Strafe auf den Instanz-Score erhoben wird.
- Es wird keine Strafe auf den Instanz-Score erhoben, wenn der Wert unter einen niedrigen Schwellenwert fällt.

Beispielsweise ist die CPU-Auslastung ein Systemressourcenindikator, der ausgelöst wird, wenn der Auslastungswert den niedrigen Schwellenwert und auch wenn der Wert den hohen Schwellenwert überschreitet.

Dashboard für Infrastruktur-Analysen

Navigieren Sie zu **Infrastruktur > Infrastruktur-Analysen**.

Die Infrastruktur-Analysen können in einem **Kreispack**-Format oder einem **Tabellen**-Format angezeigt werden. Sie können zwischen den beiden Formaten wechseln.

- In der Tabellenansicht können Sie nach einer Instanz suchen, indem Sie den Hostnamen oder die IP-Adresse in die Suchleiste eingeben.
- Standardmäßig zeigt die Seite „Infrastruktur-Analysen“ das Übersichtsfenster auf der rechten Seite der Seite an.
- Klicken Sie auf das Symbol **Einstellungen**, um das Fenster **Einstellungen** anzuzeigen.
- In beiden Ansichtsformaten zeigt das Übersichtsfenster Details zu allen Instanzen in Ihrem Netzwerk an.

Kreispack-Ansicht

Kreispack-Diagramme zeigen Instanzgruppen als dicht organisierte Kreise. Sie zeigen oft Hierarchien, bei denen kleinere Instanzgruppen entweder ähnlich wie andere in derselben Kategorie gefärbt oder in größere Gruppen verschachtelt sind. Kreispacks stellen hierarchische Datensätze dar und zeigen verschiedene Ebenen in der Hierarchie und wie sie miteinander interagieren.

Instanzkreise

Farbe. Jede Instanz wird im Kreispaket als farbiger Kreis dargestellt. Die Farbe des Kreises gibt den Zustand dieser Instanz an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Grün** – Der Instanz-Score liegt zwischen 100 und 80. Die Instanz ist fehlerfrei.
- **Gelb** – Der Instanz-Score liegt zwischen 80 und 50. Es wurden einige Probleme festgestellt, die überprüft werden müssen.
- **Rot** – Der Instanz-Score liegt unter 50. Die Instanz befindet sich in einem kritischen Zustand, da auf dieser Instanz mehrere Probleme festgestellt wurden.

Größe. Die Größe dieser farbigen Kreise gibt die Anzahl der auf dieser Instanz konfigurierten virtuellen Server an. Ein größerer Kreis weist auf eine größere Anzahl virtueller Server hin.

Sie können den Mauszeiger über jeden der Instanzkreise (farbige Kreise) bewegen, um eine Zusammenfassung anzuzeigen. Der Hover-Tooltip zeigt den Hostnamen der Instanz, die Anzahl der aktiven virtuellen Server und die Anzahl der auf dieser Instanz konfigurierten Anwendungen an.

Gruppierte Instanzkreise

Das Kreispaket umfasst zunächst Instanzkreise, die nach folgenden Kriterien gruppiert, verschachtelt oder in einem anderen Kreis verpackt sind:

- der Standort, an dem sie bereitgestellt werden
- der Typ der bereitgestellten Instanzen – VPX, MPX, SDX und CPX
- das virtuelle oder physische Modell der NetScaler-Instanz
- die auf den Instanzen installierte NetScaler-Image-Version

Die folgende Abbildung zeigt ein Circle Pack, bei dem die Instanzen zuerst nach dem Standort oder Rechenzentrum, in dem sie bereitgestellt werden, und dann weiter nach ihrem Typ, VPX und MPX, gruppiert sind.

Alle diese verschachtelten Kreise werden von zwei äußersten Kreisen begrenzt. Die beiden äußeren Kreise stellen die vier Kategorien von Ereignissen dar, die von der NetScaler Console überwacht werden (Systemressourcen, kritische Ereignisse, SSL-Konfiguration und Konfigurationsabweichung) sowie die beitragenden Gesundheitsindikatoren.

Geclusterte Instanzkreise

NetScaler Console überwacht viele Instanzen. Um die Überwachung und Wartung dieser Instanzen zu erleichtern, ermöglicht Infrastructure Analytics deren Clustering auf zwei Ebenen. Das heißt, die Instanzgruppierungen können in einer anderen Gruppierung verschachtelt sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zum Beispiel verfügt das BLR-Rechenzentrum über zwei Arten von NetScaler-Instanzen – VPX und MPX –, die darin bereitgestellt werden. Sie können die NetScaler-Instanzen zuerst nach ihrem Typ und dann alle Instanzen nach dem Standort gruppieren, an dem sie gruppiert sind. Sie können nun leicht erkennen, wie viele Arten von Instanzen an den von Ihnen verwalteten Standorten bereitgestellt werden.

Einige weitere Beispiele für zweistufiges Clustering sind die folgenden:

Standort und Modell:

Typ und Version:

Standort und Version:

Circle Pack verwenden

Klicken Sie auf jeden der farbigen Kreise, um diese Instanz hervorzuheben.

Je nach den Ereignissen, die in dieser Instanz aufgetreten sind, werden nur diese Gesundheitsindikatoren auf den äußeren Kreisen hervorgehoben. Beispielsweise zeigen die folgenden beiden Bilder des Circle Packs unterschiedliche Sätze von Risikoindikatoren an, obwohl sich beide Instanzen in einem kritischen Zustand befinden.

Sie können auch auf die Gesundheitsindikatoren klicken, um weitere Details zur Anzahl der Instanzen zu erhalten, die diesen Risikoindikator gemeldet haben. Klicken Sie beispielsweise auf `Not recommended Algo`, um den Übersichtsbericht dieses Risikoindikators anzuzeigen.

Tabellarische Ansicht

Die tabellarische Ansicht zeigt die Instanzen und deren Details in einem tabellarischen Format an. Weitere Informationen finden Sie unter Instanzdetails

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Suchleiste

Platzieren Sie den Mauszeiger auf der Suchleiste und wählen Sie die folgenden Suchattribute aus, um die Ergebnisse zu filtern:

- Hostname
- IP-Adresse
- Typ
- Version
- Site

Die Suchergebnisse funktionieren sowohl für die Kreisansicht als auch für die Tabellenansicht.

So verwenden Sie das Übersichtsfenster

Das **Übersichtsfenster** hilft Ihnen, sich effizient und schnell auf die Instanzen zu konzentrieren, die überprüft werden müssen oder sich in einem kritischen Zustand befinden. Das Fenster ist in drei Registerkarten unterteilt: Übersicht, Instanzinformationen und Datenverkehrsprofil. Die Änderungen, die Sie in diesem Fenster vornehmen, ändern die Anzeige sowohl im Kreisdiagramm- als auch im Tabellenansichtsformat. Die folgenden Abschnitte beschreiben diese Registerkarten detaillierter. Die Beispiele in den folgenden Abschnitten helfen Ihnen, die verschiedenen Auswahlkriterien effizient zu nutzen, um die von den Instanzen gemeldeten Probleme zu analysieren.

Übersicht:

Die Registerkarte **Übersicht** ermöglicht es Ihnen, die Instanzen basierend auf Hardwarefehlern, Nutzung, abgelaufenen Zertifikaten und ähnlichen Indikatoren zu überwachen, die in den Instanzen auftreten können. Die Indikatoren, die Sie hier überwachen können, sind folgende:

- CPU-Auslastung
- Speicherauslastung
- Festplattenauslastung
- Systemfehler
- Kritische Ereignisse
- Ablauf von SSL-Zertifikaten

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen zu diesen Indikatoren finden Sie unter *Zustandsindikatoren in NetScaler-Instanzen*.

Die folgenden Beispiele veranschaulichen, wie Sie mit dem **Übersichtsbereich** interagieren können, um die Instanzen zu isolieren, die Fehler melden.

Beispiel 1: Instanzen im Überprüfungsstatus anzeigen:

Wählen Sie das Kontrollkästchen **Überprüfen** aus, um nur die Instanzen anzuzeigen, die keine kritischen Fehler melden, aber dennoch Beachtung erfordern.

Die Histogramme im **Übersichtsbereich** stellen eine aggregierte Anzahl von Instanzen dar, basierend auf Ereignissen mit hoher CPU-Auslastung, hoher Speicherauslastung und hoher Festplattenauslastung. Die Histogramme sind in 10 %, 20 %, 30 %, 40 %, 50 %, 60 %, 70 %, 80 %, 90 % und 100 % gestuft. Fahren Sie mit dem Mauszeiger über eines der Balkendiagramme. Die Legende am unteren Rand des Diagramms zeigt den Nutzungsbereich und die Anzahl der Instanzen in diesem Bereich an. Sie können auch auf das Balkendiagramm klicken, um alle Instanzen in diesem Bereich anzuzeigen.

Beispiel 2: Instanzen anzeigen, die zwischen 10 % und 20 % des zugewiesenen Speichers verbrauchen:

Klicken Sie im Abschnitt zur Speicherauslastung auf das Balkendiagramm. Die Legende zeigt, dass der ausgewählte Bereich 10–20 % beträgt und 29 Instanzen in diesem Bereich betrieben werden.

Sie können in diesen Histogrammen auch mehrere Bereiche auswählen.

Beispiel 3: Instanzen anzeigen, die Festplattenspeicher in mehreren Bereichen verbrauchen:

Um Instanzen anzuzeigen, die zwischen 0 % und 10 % Festplattenspeicher verbraucht haben, ziehen Sie den Mauszeiger über die beiden Bereiche, wie in der folgenden Abbildung gezeigt.

HINWEIS:

Klicken Sie auf „X“, um die Auswahl aufzuheben. Sie können auch auf **Zurücksetzen** klicken, um mehrere Auswahlen aufzuheben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die horizontalen Balkendiagramme im **Übersichtsbereich** zeigen die Anzahl der Instanzen an, die Systemfehler, kritische Ereignisse und den Ablaufstatus der SSL-Zertifikate melden. Aktivieren Sie das Kontrollkästchen, um diese Instanzen anzuzeigen.

Beispiel 4: Instanzen für abgelaufene SSL-Zertifikate anzeigen:

Wählen Sie im Abschnitt **Ablauf von SSL-Zertifikaten** das Kontrollkästchen **Abgelaufen** aus, um die drei Instanzen anzuzeigen.

1 – Klicken Sie auf die Liste **Filter**.

2 – Aktivieren Sie im Abschnitt **Ablauf von SSL-Zertifikaten** das Kontrollkästchen **Abgelaufen**, um die Instanzen anzuzeigen.

Instanzinformationen

Im Bereich **Instanzinformationen** können Sie Instanzen basierend auf dem Bereitstellungstyp, Instanztyp, Modell und der Softwareversion anzeigen. Sie können mehrere Kontrollkästchen aktivieren, um Ihre Auswahl einzugrenzen.

Beispiel 5: NetScaler VPX-Instanzen mit spezifischer Build-Nummer anzeigen:

Wählen Sie die Version aus, die Sie anzeigen möchten.

Traffic-Profil

Die Histogramme im Bereich **Traffic-Profil** stellen eine aggregierte Anzahl von Instanzen dar, basierend auf dem lizenzierten Durchsatz der Instanzen, der Anzahl der Anfragen, Verbindungen und Transaktionen, die von den Instanzen verarbeitet werden. Wählen Sie das Balkendiagramm aus, um Instanzen in diesem Bereich anzuzeigen.

Beispiel 6: Instanzen anzeigen, die TCP-Verbindungen unterstützen:

Die folgende Abbildung zeigt die Anzahl der Instanzen, die TCP-Verbindungen zwischen 23 und 40 unterstützen und auch bis zu 100 SSL-Transaktionen pro Sekunde verarbeiten.

Verwenden des Einstellungsbereichs

Der Bereich **Einstellungen** ermöglicht Ihnen Folgendes:

- Legen Sie die Standardansicht der Infrastruktur-Analysen fest.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Legen Sie die unteren und oberen Schwellenwerte für hohe CPU-Auslastung, hohe Festplattenauslastung und hohe Speicherauslastung fest.
- Wählen Sie die Instanzmetriken aus, konfigurieren Sie Schwellenwerte und weisen Sie diesen Metriken eine Gewichtung zu, um den Instanz-Score zu berechnen.
- Wählen Sie die erforderlichen Probleme aus, aktivieren Sie Benachrichtigungen für Probleme, die die konfigurierten Schwellenwerte überschreiten, und erhalten Sie Benachrichtigungen nur für die ausgewählten Probleme.

Ansicht

- **Standardansicht**. Wählen Sie **Circle Pack** oder das Tabellenformat als Standardansicht auf der Analyseseite. Das von Ihnen ausgewählte Format wird immer angezeigt, wenn Sie die Seite in NetScaler Console aufrufen.
- **Circle Pack – Instanzgröße**. Ermöglichen Sie, dass die Größe des Instanzkreises entweder durch die Anzahl der virtuellen Server oder die Anzahl der aktiven virtuellen Server bestimmt wird.
- **Circle Pack – Gruppieren nach**. Legen Sie die zweistufige Gruppierung der Instanzkreise fest. Weitere Informationen zur Instanzgruppierung finden Sie unter Gruppierte Instanzkreise.

Metriken auswählen und Gewichtung für die Berechnung des Instanz-Scores anpassen

Sie können die Instanzmetriken auswählen, Schwellenwerte konfigurieren und diesen Metriken eine Gewichtung zuweisen, um den Instanz-Score zu berechnen. Standardmäßig sind alle Metriken ausgewählt, und jeder Metrik wird eine Standardgewichtung zugewiesen. Sie können Metriken je nach Ihren Anforderungen auswählen und eine geeignete Gewichtung zuweisen, um die Berechnung des Instanz-Scores zu bestimmen.

Klicken Sie auf das Symbol **Einstellungen** und wählen Sie die Registerkarte **Score-Indikator-Einstellungen**, um:

- Die erforderlichen Metriken auswählen und Schwellenwerte hinzufügen
- Die Gewichtung für Metriken zuweisen.

Nachdem Sie Schwellenwerte konfiguriert und eine Gewichtung zugewiesen haben, klicken Sie auf **Speichern**. Der Instanz-Score wird nur basierend auf den ausgewählten Metriken und deren Gewichtung aktualisiert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benachrichtigungen konfigurieren

Sie können die erforderlichen Probleme auswählen, Benachrichtigungen für Probleme aktivieren, die die konfigurierten Schwellenwerte überschreiten, und Benachrichtigungen nur für die ausgewählten Probleme erhalten. Diese Verbesserung ermöglicht es Ihnen, Benachrichtigungen nur für die ausgewählten Probleme zu erhalten, die Sie überwachen möchten.

HINWEIS:

Standardmäßig sind Probleme in allen Kategorien ausgewählt. Sie können Benachrichtigungen nur für die Probleme aktivieren, für die Sie Schwellenwerte konfigurieren können.

1. Klicken Sie auf das Symbol **Einstellungen** und wählen Sie die Registerkarte **Score Indicator Settings**.
2. Wählen Sie die Probleme aus, für die Sie Benachrichtigungen erhalten möchten.
3. Aktivieren Sie für die Probleme unter den Kategorien **Systemressource** und **Kapazität** die **Benachrichtigung**.

4. Klicken Sie auf **Speichern**.

   HINWEIS:

   Sie müssen sicherstellen, dass Sie mindestens ein Profil auf der Registerkarte **Benachrichtigungen** konfigurieren.

So visualisieren Sie Daten auf dem Dashboard

Mithilfe von Infrastructure Analytics können Netzwerkadministratoren jetzt innerhalb weniger Sekunden die Instanzen identifizieren, die die meiste Aufmerksamkeit benötigen. Um dies genauer zu verstehen, betrachten wir den Fall von Chris, einem Netzwerkadministrator von ExampleCompany.

Chris verwaltet viele NetScaler-Instanzen in seiner Organisation. Einige der Instanzen verarbeiten hohen Datenverkehr, und er muss sie genau überwachen. Er bemerkt, dass einige Instanzen mit hohem Datenverkehr nicht mehr den gesamten durch sie fließenden Datenverkehr verarbeiten. Um diese Reduzierung zu analysieren, musste er früher mehrere Datenberichte aus verschiedenen Quellen lesen. Chris musste mehr Zeit damit verbringen, die Daten manuell zu

© 1997–2026 Citrix Systems, Inc. All rights reserved.

korrelieren und herauszufinden, welche Instanzen sich nicht in einem optimalen Zustand befinden und Aufmerksamkeit benötigen. Er verwendet die Infrastructure Analytics-Funktion, um den Zustand aller Instanzen visuell zu sehen.

Die folgenden zwei Beispiele veranschaulichen, wie Infrastructure Analytics Chris bei Wartungsarbeiten unterstützt:

Beispiel 1 – Zur Überwachung des SSL-Datenverkehrs:

Chris bemerkt auf dem Circle Pack, dass eine Instanz einen niedrigen Instanz-Score hat und sich diese Instanz im Status „Kritisch“ befindet. Er klickt auf die Instanz, um das Problem zu sehen. Die Instanzzusammenfassung zeigt an, dass bei dieser Instanz ein SSL-Kartenfehler vorliegt und diese Instanz daher keinen SSL-Datenverkehr verarbeiten kann (der SSL-Datenverkehr hat sich reduziert). Chris extrahiert diese Informationen und sendet einen Bericht an das Team, um das Problem sofort zu untersuchen.

Beispiel 2 – Zur Überwachung von Konfigurationsänderungen:

Chris bemerkt auch, dass sich eine andere Instanz im Status „Überprüfung“ befindet und dass es kürzlich eine Konfigurationsabweichung gab. Wenn er auf den Risikoindikator für Konfigurationsabweichungen klickt, bemerkt er, dass RC4 Cipher, SSL v3, TLS 1.0 und TLS 1.1 bezogene Konfigurationsänderungen vorgenommen wurden, was auf Sicherheitsbedenken zurückzuführen sein könnte. Er bemerkt auch, dass das SSL-Transaktionsverkehrsprofil für diese Instanz gesunken ist. Er exportiert diesen Bericht und sendet ihn an den Administrator, um weitere Nachforschungen anzustellen.

Instanzdetails in Infrastructure Analytics anzeigen

1. Navigieren Sie zu **Infrastructure > Infrastructure Analytics**.
2. Klicken Sie auf die Kreispackungsansicht und wählen Sie die IP-Adresse aus.

   Sie können auch eine IP-Adresse aus der Tabellenansicht auswählen.

- **Hostname** – Bezeichnet den der NetScaler-Instanz zugewiesenen Hostnamen
- **IP-Adresse** – Bezeichnet die IP-Adresse der NetScaler-Instanz
- **Score** – Bezeichnet den Score der NetScaler-Instanz und den Status wie Kritisch, Gut und Ausreichend.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Verfügbarkeit** – Bezeichnet den aktuellen Status der NetScaler-Instanz, z. B. **Aktiv**, **Inaktiv** oder **Außer Betrieb**.
- **Maximaler Beitrag** – Bezeichnet die Problemkategorie, bei der die NetScaler-Instanz die maximale Fehleranzahl aufweist.
- **CPU-Auslastung** – Bezeichnet die aktuelle CPU-Auslastung in % der Instanz
- **Speichernutzung** – Bezeichnet die aktuelle Speichernutzung in % der Instanz
- **Festplattennutzung** – Bezeichnet die aktuelle Festplattennutzung in % der Instanz
- **Systemfehler** – Bezeichnet die Gesamtzahl der Fehler für das Instanzsystem
- **Kritische Ereignisse** – Bezeichnet die Ereigniskategorie, bei der die NetScaler-Instanz die maximale Anzahl an Ereignissen aufweist
- **SSL-Ablauf** – Bezeichnet den aktuellen Status des auf der NetScaler-Instanz installierten SSL-Zertifikats
- **Typ** – Bezeichnet den NetScaler-Instanztyp, z. B. VPX, SDX, MPX oder CPX
- **Bereitstellung** – Gibt an, ob die NetScaler-Instanz als eigenständige Instanz oder als HA-Paar bereitgestellt wird
- **Modell** – Bezeichnet die Modellnummer der NetScaler-Instanz
- **Version** – Bezeichnet die Version und Build-Nummer der NetScaler-Instanz
- **Durchsatz** – Bezeichnet den aktuellen Netzwerkdurchsatz der NetScaler-Instanz
- **HTTPS-Anfragen/Sek.** – Bezeichnet die aktuellen HTTPS-Anfragen/Sek., die von der NetScaler-Instanz empfangen werden
- **TCP-Verbindung** – Bezeichnet die aktuell hergestellten TCP-Verbindungen
- **SSL-Transaktion** – Bezeichnet die aktuellen SSL-Transaktionen, die von der NetScaler-Instanz verarbeitet werden
- **Site** – Bezeichnet den Namen der Site, auf der die NetScaler-Instanz bereitgestellt wird.

HINWEIS:

Alle 5 Minuten werden die aktuellen Werte für CPU-Auslastung, Speicherauslastung, Festplattenauslastung, Durchsatz usw. aktualisiert.

Klicken Sie auf eine IP-Adresse und auf der angezeigten Seite auf **Instanzdetails**, um die Instanzdetails anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die folgenden Details werden angezeigt:

- **Informationen** – Instanzdetails wie Instanztyp, Bereitstellungstyp, Version, Modell usw.

- **Funktionen** – Standardmäßig werden die nicht lizenzierten Funktionen angezeigt. Klicken Sie auf **Lizenzierte Funktionen**, um die lizenzierten Funktionen anzuzeigen.

- **Modi** – Standardmäßig werden alle auf der Instanz deaktivierten Modi angezeigt. Klicken Sie auf **Aktivierte Modi anzeigen**, um die aktivierten Modi auf der Instanz anzuzeigen.

Das Instanz-Dashboard bietet eine Instanzübersicht, in der Sie die folgenden Details sehen können:

- **Instanzbewertung**

  1 – Zeigt die aktuelle NetScaler-Instanzbewertung für die ausgewählte Zeitdauer an. Die Endbewertung wird als **100 minus Gesamtstrafen** berechnet. Das Diagramm zeigt die Bewertungsbereiche für die ausgewählte Zeitdauer an.

  2 – Zeigt den aktuellen Status der NetScaler-Instanz an, z. B. **Aktiv**, **Inaktiv** und **Außer Betrieb**.

  3 – Zeigt die Dauer an, während der die NetScaler-Instanz aktiv und betriebsbereit ist.

  4 – Zeigt die Gesamtzahl der aktivierten und deaktivierten Netzwerkschnittstellen für die Instanz an. Klicken Sie auf **Aktiviert** oder **Deaktiviert**, um Details wie den Namen der Netzwerkschnittstelle und den Status (aktiviert oder deaktiviert) anzuzeigen.

  5 – Wählen Sie die Zeitdauer aus der Liste aus, um die Instanzdetails anzuzeigen.

  6 – Zeigt die Gesamtanzahl der Probleme und die Problemkategorie der NetScaler-Instanz an.

- **Wichtige Metriken**

  Klicken Sie auf jede Registerkarte, um die Details anzuzeigen. In jeder Metrik können Sie den Durchschnittswert und den Differenzwert für die ausgewählte Zeit anzeigen.

  Die folgende Abbildung ist ein Beispiel für HTTPS-Anfragen/Sek. und die ausgewählte Zeitdauer beträgt 1 Stunde. Der Wert **692** ist der durchschnittliche HTTPS-Anfragen/Sek.-Wert

© 1997–2026 Citrix Systems, Inc. All rights reserved.

für den Zeitraum von 1 Monat, und der Wert **20** ist der Differenzwert. Im Diagramm ist der erste Wert **139** und der letzte Wert **119**. Der Differenzwert ist **139 – 119 = 20**.

Sie können die folgenden Instanzmetriken in einem Diagrammformat für die ausgewählte Zeitdauer anzeigen:

- **CPU-Auslastung** – Die durchschnittliche CPU-Auslastung in % der Instanz für die ausgewählte Dauer (wird sowohl für die Paket-CPU als auch für die Management-CPU angezeigt).
- **Speicherauslastung** – Die durchschnittliche Speicherauslastung in % der Instanz für die ausgewählte Dauer.
- **Festplattenauslastung** – Die durchschnittliche Festplattenauslastung in % der Instanz für die ausgewählte Dauer.
- **Durchsatz** – Der durchschnittliche Netzwerkdurchsatz, der von der Instanz für die ausgewählte Dauer verarbeitet wurde.
- **HTTPS-Anfragen/Sek.** – Die durchschnittlichen HTTPS-Anfragen, die von der Instanz für die ausgewählte Dauer empfangen wurden.
- **TCP-Verbindungen** – Die durchschnittlichen TCP-Verbindungen, die vom Client und Server für die ausgewählte Dauer hergestellt wurden.
- **SSL-Transaktionen** – Die durchschnittlichen SSL-Transaktionen, die von der Instanz für die ausgewählte Dauer verarbeitet wurden.

- **Probleme**

  Sie können die folgenden Probleme anzeigen, die in der NetScaler-Instanz auftreten:

PROBLEMKATEGORIE	BESCHREIBUNG	PROBLEME
Systemressourcen	Zeigt alle Probleme an, die sich auf die NetScaler-Systemressourcen wie CPU, Arbeitsspeicher, Festplattennutzung usw. beziehen.	- Hohe CPU-Auslastung
		- Hohe Speicherauslastung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PROBLEMKATEGORIE	BESCHREIBUNG	PROBLEME
		- Hohe Festplattenauslastung
		- SSL-Kartenfehler
		- Stromausfall
		- Festplattenfehler
		- Flash-Fehler
		- NIC-Verwerfungen
SSL-Konfiguration	Zeigt alle Probleme an, die sich auf die SSL-Konfiguration der NetScaler-Instanz beziehen.	- SSL-Zertifikate abgelaufen
		- Nicht empfohlener Aussteller
		- Nicht empfohlener Algorithmus
		- Nicht empfohlene Schlüsselstärke
Konfigurationsabweichung	Zeigt alle Probleme im Zusammenhang mit den Konfigurationsaufträgen an, die in der NetScaler-Instanz angewendet wurden.	- Konfigurationsdrift
		- Laufend vs. Vorlage
Kritische Ereignisse	Zeigt alle kritischen Ereignisse im Zusammenhang mit NetScaler-Instanzen an, die in einem HA-Paar und in	- Cluster-Propagierungsfehler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PROBLEMKATEGORIE	BESCHREIBUNG	PROBLEME
	einem Cluster konfiguriert sind.	
		- Cluster-Synchronisierungsfehler
		- Cluster-Versionskonflikt
		- HA schlechter Sekundärstatus
		- HA keine Heartbeats
		- HA-Synchronisierungsfehler
		- HA-Versionskonflikt
Kapazitätsprobleme	Zeigt NetScaler-Kapazitätsprobleme an. Die NetScaler Console fragt diese Ereignisse alle fünf Minuten von der NetScaler-Instanz ab und zeigt Paketverluste oder Erhöhungen des Ratenbegrenzungszählers an, falls vorhanden. Die Probleme werden nach den folgenden Kapazitätsparametern kategorisiert.	- Durchsatzlimit erreicht
		- PE-CPU-Limit erreicht
		- PPS-Limit erreicht
		- SSL-Durchsatzratenlimit
		- SSL-TPS-Ratenlimit

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PROBLEMKATEGORIE	BESCHREIBUNG	PROBLEME
Netzwerk	Zeigt die betrieblichen Probleme an, die in den Instanzen auftreten.	Weitere Informationen finden Sie unter Erweiterte Infrastruktur-Analysen mit neuen Indikatoren.

Klicken Sie auf jede Registerkarte, um das Problem zu analysieren und zu beheben. Betrachten Sie beispielsweise, dass eine Instanz für die ausgewählte Zeitdauer die folgenden Fehler aufweist:

- Die Registerkarte **Aktuell** zeigt die Probleme an, die sich derzeit auf den Instanz-Score auswirken.
- Der Tab **Alle** zeigt alle für den ausgewählten Zeitraum erkannten Infrastrukturprobleme an.

Kapazitätsprobleme in einer NetScaler-Instanz anzeigen

Wenn eine NetScaler-Instanz den Großteil ihrer verfügbaren Kapazität verbraucht hat, kann es während der Verarbeitung des Client-Datenverkehrs zu Paketverlusten kommen. Dieses Problem führt zu einer geringen Leistung in einer NetScaler-Instanz. Durch das Verständnis solcher NetScaler-Kapazitätsprobleme können Sie proaktiv zusätzliche Lizenzen zuweisen, um die NetScaler-Leistung zu stabilisieren.

In der **Circle Pack View** können Sie die Kapazitätsprobleme der NetScaler-Instanz anzeigen, falls vorhanden.

So zeigen Sie NetScaler-Kapazitätsprobleme an:

1. Navigieren Sie zu **Infrastructure > Infrastructure Analytics**.
2. Wählen Sie die Circle Pack View.

HINWEIS:

In **Infrastructure Analytics** zeigen die Circle-Pack- und Tabellenansichten die Ereignisse und Probleme an, die in der letzten Stunde aufgetreten sind.

Die folgende Abbildung zeigt, dass in der ausgewählten Instanz Kapazitätsprobleme bestehen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Kapazitätsprobleme in der Circle Pack View anzeigen(/en-us/netscaler-console-service/media/adc-capacity-issues.png)

Die Probleme werden nach den folgenden Kapazitätsparametern kategorisiert:

- **Durchsatzlimit erreicht** – Die Anzahl der in der Instanz verworfenen Pakete, nachdem das Durchsatzlimit erreicht wurde.
- **PE-CPU-Limit erreicht** – Die Anzahl der auf allen NICs verworfenen Pakete, nachdem das PE-CPU-Limit erreicht wurde.
- **PPS-Limit erreicht** – Die Anzahl der in der Instanz verworfenen Pakete, nachdem das PPS-Limit erreicht wurde.
- **SSL-Durchsatzratenlimit** – Die Häufigkeit, zu der das SSL-Durchsatzlimit erreicht wurde.
- **SSL-TPS-Ratenbegrenzung** – Die Häufigkeit, mit der das SSL-TPS-Limit erreicht wurde.

Empfohlene Maßnahmen zur Behebung von Kapazitätsproblemen anzeigen

Die NetScaler Console empfiehlt Maßnahmen, die Kapazitätsprobleme lösen können. Um die empfohlenen Maßnahmen anzuzeigen, führen Sie die folgenden Schritte aus:

1. Wählen Sie unter **Infrastructure > Infrastructure Analytics** die Tabellenansicht aus.
2. Wählen Sie die Instanz mit Kapazitätsproblemen aus und klicken Sie auf **Details**.

   ▢
3. Scrollen Sie auf der Instanzseite zum Abschnitt **Issues**.
4. Wählen Sie jedes Problem aus und zeigen Sie die empfohlenen Maßnahmen zur Behebung von Kapazitätsproblemen an.

   ▢

Die NetScaler Console fragt diese Ereignisse alle fünf Minuten von der NetScaler-Instanz ab und zeigt die Paketverluste oder die Erhöhungen des Ratenbegrenzungszählers an, falls vorhanden.

Die NetScaler Console berechnet den Instanz-Score basierend auf dem definierten Kapazitätsschwellenwert.

- **Niedriger Schwellenwert** – 1 Paketverlust oder Erhöhung des Ratenbegrenzungszählers
- **Hoher Schwellenwert** – 10000 Paketverluste oder Erhöhungen des Ratenbegrenzungszählers

Wenn eine NetScaler-Instanz den Kapazitätsschwellenwert überschreitet, wird der Instanz-Score beeinträchtigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Pakete verloren gehen oder der Ratenbegrenzungszähler erhöht wird, wird ein Ereignis unter der Kategorie `ADCCapacityBreach` generiert. Um diese Ereignisse anzuzeigen, navigieren Sie zu **Settings > System Events**.

Erweiterte Infrastruktur-Analysen mit neuen Indikatoren

Mithilfe der NetScaler Console **Infrastructure Analytics** können Sie:

- Eine neue Reihe von betrieblichen Problemen anzeigen, die in NetScaler-Instanzen auftreten.
- Fehlermeldungen anzeigen und Empfehlungen zur Behebung der Probleme prüfen.

Als Administrator können Sie schnell die Ursachenanalyse von Problemen identifizieren.

HINWEIS:

Regelindikatoren werden nicht unterstützt für:

- NetScaler-Instanzen, die im Cluster-Modus konfiguriert sind.
- NetScaler-Instanzen, die mit Admin-Partitionen konfiguriert sind.

Navigieren Sie in der NetScaler Console zu **Infrastructure > Infrastructure Analytics**, um Indikatoren anzuzeigen für:

INDIKATORNAME IN INFRASTRUCTURE ANALYTICS	BESCHREIBUNG
Portzuweisungsfehler	Erkennt, wenn NetScaler SNIP verwendet, um mit einer neuen Serververbindung zu kommunizieren und die auf diesem SNIP verfügbaren Ports erschöpft sind. Die empfohlene Aktion ist, ein weiteres SNIP im selben Subnetz hinzuzufügen.
Sitzungsaufbau	Erkennt, wenn der NetScaler-Speicher durch SSL-Sitzungen belegt ist.
Keine Standardroutenkonfiguration	Erkennt, wenn der Datenverkehr aufgrund fehlender Routen verworfen wird.
IP-Konflikt	Erkennt, ob dieselbe IP-Adresse auf zwei oder mehr Instanzen in einem Netzwerk konfiguriert oder angewendet wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INDIKATORNAME IN INFRASTRUCTURE ANALYTICS	BESCHREIBUNG
VRID-Konflikt	Erkennt, wenn zeitweilige Zugriffsprobleme für die angegebene VRID auftreten.
VLAN-Fehlübereinstimmung	Erkennt, ob Fehler während der VLAN-Konfiguration auftreten, die an IP-Subnetze gebunden ist.
TCP-Small-Window-Angriff	Erkennt, wenn ein möglicher Small-Window-Angriff im Gange ist. Dieser Alarm dient nur zu Informationszwecken, da NetScaler diesen Angriff bereits abwehrt.
Ratensteuerungsschwelle	Erkennt, wenn Pakete basierend auf der konfigurierten Ratensteuerungsschwelle verworfen werden.
Persistenzlimit	Erkennt, wenn die maximale Anzahl von Zugriffen auf den NetScaler-Speicher angewendet wird.
Nichtübereinstimmung des GSLB-Standortnamens	Erkennt, wenn GSLB-Konfigurationssynchronisierungsfehler aufgrund einer Nichtübereinstimmung des Standortnamens auftreten.
Fehlerhafter IP-Header	Erkennt, wenn Integritätsprüfungen bei IPv4-Paketen fehlschlagen.
Fehlerhafte L4-Prüfsummen	Erkennt, wenn die Prüfsummenvalidierung für TCP-Pakete fehlschlägt.
Erhöhte CPU-Auslastung aufgrund von IP-Verschiebung	Erkennt, ob eine große Anzahl von MAC-Adressen aktualisiert werden muss.
Übermäßige Paketsteuerung	Erkennt hohe Werte der Software-Paketsteuerung aufgrund der Verwendung eines asymmetrischen RSS-Schlüsseltyps.
Layer-2-Schleife	Erkennt das Vorhandensein von Layer-2-Schleifen im Netzwerk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INDIKATORNAME IN INFRASTRUCTURE ANALYTICS	BESCHREIBUNG
Nichtübereinstimmung von getaggtem VLAN	Erkennt, wenn getaggte VLAN-Pakete auf einer ungetaggten Schnittstelle empfangen werden.

Tabellarische Ansicht

Sie können Anomalien auch mithilfe der Option 'Tabellenansicht' in **Infrastructure Analytics** anzeigen. Navigieren Sie zu **Infrastructure > Infrastructure Analytics** und klicken Sie dann auf

, um alle verwalteten Instanzen anzuzeigen. Klicken Sie auf

, um Details zu erweitern.

Details einer Anomalie anzeigen

Wenn Sie beispielsweise Details zu einem **IP-Adresskonflikt** im Netzwerk anzeigen möchten, klicken Sie auf die Anomalie, die für den IP-Adresskonflikt angezeigt wird.

- **Details** – Zeigt an, welche Anomalie erkannt wurde
- **Erkennungsmeldung** – Zeigt die MAC-Adresse an, für die die IP-Adresse den Konflikt aufweist
- **Empfehlungen** – Zeigt das Fehlerbehebungsverfahren zur Behebung dieses IP-Adresskonflikts an

Instanzverwaltung

Instanzen sind Citrix Application Delivery Controller (ADC)-Appliances, die Sie mit NetScaler Console verwalten, überwachen und Fehler beheben können. Fügen Sie Instanzen zu NetScaler Console hinzu, um sie zu überwachen. Instanzen können bei der Einrichtung von NetScaler Console oder auch später hinzugefügt werden. Nachdem Sie Instanzen zu NetScaler Console hinzugefügt haben, werden sie kontinuierlich abgefragt, um Informationen zu sammeln, die später zur Behebung von Problemen oder als Berichtsdaten verwendet werden können.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instanzen können als statische Gruppe oder als privater IP-Block gruppiert werden. Eine statische Gruppe von Instanzen kann nützlich sein, wenn Sie bestimmte Aufgaben wie Konfigurationsaufträge und andere ausführen möchten. Ein privater IP-Block gruppiert Ihre Instanzen basierend auf ihren geografischen Standorten.

Eine Instanz hinzufügen

Sie können Instanzen entweder bei der erstmaligen Einrichtung des NetScaler Console-Servers oder später hinzufügen. Um Instanzen hinzuzufügen, müssen Sie entweder den Hostnamen oder die IP-Adresse jeder NetScaler-Instanz oder einen Bereich von IP-Adressen angeben.

Informationen zum Hinzufügen einer Instanz zu NetScaler Console finden Sie unter Instanzen zu NetScaler Console hinzufügen.

Wenn Sie eine Instanz zum NetScaler Console-Server hinzufügen, fügt sich der Server implizit als Trap-Ziel für die Instanz hinzu und erfasst ein Inventar der Instanz. Weitere Informationen finden Sie unter Wie NetScaler Console Instanzen erkennt.

Nachdem Sie eine Instanz hinzugefügt haben, können Sie diese löschen, indem Sie zu **Infrastruktur > Instanzen** navigieren und die Instanzkategorie auswählen. Wählen Sie dann die zu löschende Instanz aus und klicken Sie auf **Entfernen**.

So verwenden Sie das Instanz-Dashboard

Das Dashboard pro Instanz in NetScaler Console zeigt Daten in tabellarischer und grafischer Form für die ausgewählte Instanz an. Die während des Abfragevorgangs von Ihrer Instanz gesammelten Daten werden im Dashboard angezeigt.

Standardmäßig werden verwaltete Instanzen jede Minute zur Datenerfassung abgefragt. Statistische Informationen wie Status, HTTP-Anfragen pro Sekunde, CPU-Auslastung, Speichernutzung und Durchsatz werden kontinuierlich mithilfe von NITRO-Aufrufen gesammelt. Als Administrator können Sie all diese gesammelten Daten auf einer einzigen Seite anzeigen, Probleme in der Instanz identifizieren und sofort Maßnahmen zur Behebung ergreifen.

Um das Dashboard einer bestimmten Instanz anzuzeigen, navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**. Wählen Sie auf der NetScaler-Seite den Instanztyp und dann die Instanz aus, die Sie anzeigen möchten, und klicken Sie auf **Dashboard**.

- **Übersicht**. Die Registerkarte „Übersicht“ zeigt die CPU- und Speicherauslastung der ausgewählten Instanz an. Sie können auch von der Instanz generierte Ereignisse und die Durchsatzdaten anzeigen. Instanzspezifische Informationen wie die IP-Adresse, Hardware-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

und LOM-Versionen, Profildetails, Seriennummer, Ansprechpartner und andere werden ebenfalls hier angezeigt. Wenn Sie weiter nach unten scrollen, sehen Sie die lizenzierten Funktionen, die auf Ihrer ausgewählten Instanz verfügbar sind, zusammen mit den darauf konfigurierten Modi. Weitere Informationen finden Sie unter Instanzdetails.

- **SSL-Dashboard**. Sie können die Registerkarte „SSL“ im Dashboard pro Instanz verwenden, um die Details der SSL-Zertifikate, SSL-virtuellen Server und SSL-Protokolle Ihrer ausgewählten Instanz anzuzeigen oder zu überwachen. Sie können auf die „Zahlen“ in den Diagrammen klicken, um weitere Details anzuzeigen.
- **Konfigurationsprüfung**. Sie können die Registerkarte „Konfigurationsprüfung“ verwenden, um alle Konfigurationsänderungen anzuzeigen, die an Ihrer ausgewählten Instanz vorgenommen wurden. Die Diagramme **NetScaler-Konfigurationsstatus gespeichert** und **NetScaler-Konfigurationsdrift** im Dashboard zeigen allgemeine Details zu Konfigurationsänderungen in gespeicherten gegenüber nicht gespeicherten Konfigurationen an.
- **Netzwerkfunktionen**. Mithilfe des Dashboards für Netzwerkfunktionen können Sie den Status der auf Ihrer ausgewählten NetScaler-Instanz konfigurierten Entitäten überwachen. Sie können Diagramme für Ihre virtuellen Server anzeigen, die Daten wie Client-Verbindungen, Durchsatz und Server-Verbindungen darstellen.
- **Netzwerknutzung**. Auf der Registerkarte „Netzwerknutzung“ können Sie Netzwerkleistungsdaten für Ihre ausgewählte Instanz anzeigen. Sie können Berichte für eine Stunde, einen Tag, eine Woche oder einen Monat anzeigen. Die Zeitleisten-Schiebereglerfunktion kann verwendet werden, um die Dauer der generierten Netzwerkberichte anzupassen. Standardmäßig werden nur acht Berichte angezeigt, aber Sie können auf das Symbol „Plus“ unten rechts auf dem Bildschirm klicken, um einen weiteren Leistungsbericht hinzuzufügen.

So überwachen Sie global verteilte Standorte

Als Netzwerkadministrator müssen Sie möglicherweise Netzwerkinstanzen überwachen und verwalten, die über geografische Standorte verteilt sind. Es ist jedoch nicht einfach, die Anforderungen des Netzwerks zu beurteilen, wenn Netzwerkinstanzen in geografisch verteilten Rechenzentren verwaltet werden.

Geomaps in NetScaler Console bieten Ihnen eine grafische Darstellung Ihrer Standorte und gliedern Ihre Netzwerküberwachungserfahrung nach Geografie. Mit Geomaps können Sie die Verteilung Ihrer Netzwerkinstanzen nach Standort visualisieren und Netzwerkprobleme überwachen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die folgenden Abschnitte erläutern, wie Sie Rechenzentren in NetScaler Console überwachen können.

Überwachung global verteilter Standorte in NetScaler Console

Ein NetScaler Console-Standort ist eine logische Gruppierung von Citrix Application Delivery Controller (NetScaler)-Instanzen an einem bestimmten geografischen Standort. Zum Beispiel wird ein Standort Amazon Web Services (AWS) zugewiesen, während ein anderer Standort Azure zugewiesen werden könnte. Wieder ein anderer Standort wird auf den Räumlichkeiten des Mandanten gehostet. NetScaler Console verwaltet und überwacht alle NetScaler-Instanzen, die mit allen Standorten verbunden sind. Sie können NetScaler Console verwenden, um Syslog, AppFlow, SNMP und alle ähnlichen Daten, die von den verwalteten Instanzen stammen, zu überwachen und zu erfassen.

Geomaps in NetScaler Console bieten Ihnen eine grafische Darstellung Ihrer Standorte. Geomaps gliedern Ihre Netzwerküberwachungserfahrung auch nach Geografie. Mit Geomaps können Sie die Verteilung Ihrer Netzwerkinstanzen nach Standort visualisieren und alle Netzwerkprobleme überwachen. Sie können im Menü auf **Infrastruktur** klicken, um das **Instanzen-Dashboard** für eine visuelle Darstellung der auf der Weltkarte erstellten Standorte anzuzeigen.

Anwendungsfall

Ein führendes Mobilfunkunternehmen, ExampleCompany, verließ sich auf private Dienstanbieter für das Hosting seiner Ressourcen und Anwendungen. Das Unternehmen hatte bereits zwei Standorte – einen in Minneapolis in den Vereinigten Staaten und einen weiteren in Alice Springs in Australien. In diesem Bild sehen Sie, dass zwei Markierungen die beiden bestehenden Standorte darstellen.

Die Markierungen zeigen auch die Anzahl der folgenden Komponenten am Standort an:

- **Instanzen**: Zeigt die Anzahl der verfügbaren Instanzen an.
- **Anwendungen**: Zeigt die Anzahl der gehosteten Anwendungen an.
- **Virtuelle Server**: Zeigt die Anzahl der verfügbaren virtuellen Server an.
- **Kritische Ereignisse**: Zeigt die Anzahl der auf den Instanzen aufgetretenen kritischen Ereignisse an.
- **Wichtige Ereignisse**: Zeigt die Anzahl der wichtigen Ereignisse an, die auf den Instanzen aufgetreten sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Klicken Sie auf **Anwendungen**, um alle benutzerdefinierten Anwendungen anzuzeigen, die an jedem Standort erstellt wurden.

Klicken Sie auf **Details**, um eine Liste der an jedem Standort hinzugefügten NetScaler-Instanzen anzuzeigen. Klicken Sie auf die Registerkarten, um weitere Informationen anzuzeigen:

- **Instanzen**-Registerkarte: Zeigen Sie auf dieser Registerkarte Folgendes an:
  - IP-Adresse jeder Netzwerkinstanz
  - Typ der NetScaler-Instanz
  - Anzahl kritischer Ereignisse
  - Wichtige Ereignisse und alle auf einer NetScaler-Instanz ausgelösten Ereignisse.
- **Ereignisse**-Registerkarte: Zeigen Sie eine Liste der kritischen und wichtigen Ereignisse an, die auf den Instanzen ausgelöst wurden.
- **Zertifikate**-Registerkarte: Zeigen Sie auf dieser Registerkarte Folgendes an:
  - Liste der Zertifikate aller Instanzen
  - Ablaufstatus
  - Wichtige Informationen und die Top 10 der Instanzen nach Anzahl der verwendeten Zertifikate.
- **Agenten**-Registerkarte: Zeigen Sie eine Liste der Agenten an, an die die Instanzen gebunden sind.

Geomaps konfigurieren

ExampleCompany beschloss, einen dritten Standort in Bangalore, Indien, einzurichten. Das Unternehmen wollte die Cloud testen, indem es einige seiner weniger kritischen, internen IT-Anwendungen in das Büro in Bangalore auslagerte. Das Unternehmen entschied sich für die Nutzung der AWS Cloud-Computing-Dienste.

Als Administrator müssen Sie zuerst einen Standort erstellen und anschließend die NetScaler-Instanzen in der NetScaler Console hinzufügen. Sie müssen die Instanz auch dem Standort hinzufügen, einen Agenten hinzufügen und den Agenten an den Standort binden. Die NetScaler Console erkennt dann den Standort, zu dem die NetScaler-Instanz und der Agent gehören.

Weitere Informationen zum Hinzufügen von NetScaler-Instanzen finden Sie unter Instanzen hinzufügen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Einen Standort erstellen

Erstellen Sie Standorte, bevor Sie Instanzen in der NetScaler Console hinzufügen. Die Angabe von Standortinformationen ermöglicht es Ihnen, den Standort präzise zu lokalisieren.

So erstellen Sie einen Standort:

1. Navigieren Sie zu **Infrastruktur > Instanzen > Standort**. Klicken Sie auf **Hinzufügen**.
2. Wählen Sie auf der Registerkarte **Cloud auswählen** den **Standorttyp** aus. Sie können einen Standort vom Typ **Rechenzentrum** oder **Zweigstelle** erstellen.

   Wählen Sie für den Standorttyp Rechenzentrum den **Typ** aus der Liste aus:

   - Privat
   - AWS
   - Azure
   - Google Cloud
   - VMware vCenter

3. Klicken Sie auf **Weiter**.
4. Geben Sie auf der Registerkarte **Region auswählen** die folgenden Details ein:

   - Standortname
   - Stadt
   - Postleitzahl
   - Region
   - Land
   - Breitengrad
   - Längengrad

   Alternativ können Sie den Standort unter **Standort suchen** eingeben und auf **Standort abrufen** klicken, um den Standort genau zu bestimmen. Die Felder Stadt, Postleitzahl, Region, Land, Breitengrad und Längengrad werden automatisch ausgefüllt.

5. Klicken Sie auf **Fertig stellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEISE:

Die beschriebenen Schritte gelten für:

- Zweigstellen-Standorttyp.
- Rechenzentrums-Standorttyp mit dem Typ „Privat“.
- Wenn die Abrufoption für die Cloud-Anbietertypen nicht ausgewählt ist.

Einen Standort für Cloud-Anbietertypen erstellen

Sie können einen Standort mit einem Cloud-Anbietertyp erstellen und wählen, ob die Option **Abrufen** aktiviert oder deaktiviert werden soll. Standardmäßig ist die Option **Abrufen** nicht ausgewählt.

Die Option **Abrufen** ist nur für AWS-, Azure- und Google Cloud-Plattformen verfügbar.

Detaillierte Anweisungen zum Erstellen eines Standorts für bestimmte Cloud-Anbieter finden Sie in den folgenden Abschnitten:

1. Einen Standort in AWS erstellen
2. Einen Standort in Azure erstellen
3. Einen Standort in Google Cloud erstellen
4. Einen Standort in VMware vCenter erstellen

Einen Standort bearbeiten

So ändern Sie eine vorhandene Site:

1. Wählen Sie die Site aus und klicken Sie auf **Bearbeiten**.
2. Auf der Seite **Site konfigurieren** können Sie den **Sitetyp** aktualisieren. Wenn Sie beispielsweise zuvor **Zweigstelle** ausgewählt haben, können Sie auf **Datencenter** aktualisieren.
3. Je nach Sitetyp können Sie den **Typ** ändern. Sie können beispielsweise den Typ von einem privaten Datencenter in eine öffentliche Cloud aus der Liste ändern.

Site löschen

1. Um eine Site zu löschen, wählen Sie die Site aus und klicken Sie auf **Löschen**.
2. Klicken Sie auf der Bestätigungsseite auf **Ja**.

Instanzen hinzufügen und Sites auswählen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nach dem Erstellen von Sites müssen Sie Instanzen in NetScaler Console hinzufügen. Sie können die zuvor erstellte Site auswählen oder eine Site erstellen und die Instanz zuordnen.

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Instanzen > NetScaler**.
2. Wählen Sie die **VPX** aus und klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Seite **NetScaler VPX hinzufügen** die IP-Adresse ein und wählen Sie das Profil aus der Liste aus.
4. Wählen Sie die Site aus der Liste aus. Sie können auf die Schaltfläche **Hinzufügen** neben dem Feld **Site** klicken, um eine Site zu erstellen, oder auf die Schaltfläche **Bearbeiten** klicken, um die Details der Standardsite zu ändern.
5. Klicken Sie auf den Rechtspfeil und wählen Sie den Agenten aus der angezeigten Liste aus.

6. Nachdem Sie den Agenten ausgewählt haben, müssen Sie den Agenten der Site zuordnen. Dieser Schritt ermöglicht es, den Agenten an die Site zu binden. Wählen Sie den Agenten aus und klicken Sie auf **Site anhängen**.

   a. Wählen Sie die Site aus der Liste aus und klicken Sie auf **Speichern**.
7. Optional können Sie Schlüssel- und Wertfelder für **Tags** eingeben.
8. Klicken Sie auf **OK**.

Sie können einen Agenten auch einer Site zuordnen, indem Sie zu **Infrastructure > Instances > Agents** navigieren.

So ordnen Sie einen Agenten der Site zu:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Instances > Agents**.
2. Wählen Sie den Agenten aus und klicken Sie auf **Site anhängen**.
3. Sie können die Site zuordnen und auf **Speichern** klicken.

NetScaler Console beginnt mit der Überwachung der in der Bangalore-Site hinzugefügten NetScaler-Instanzen sowie der Instanzen an den beiden anderen Sites.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu exportieren, klicken Sie auf das Symbol **Exportieren** oben rechts auf dieser Seite. Auf der Seite **Exportieren** können Sie Folgendes tun:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Wählen Sie die Registerkarte **Jetzt exportieren**. Um den Bericht im PDF-, JPEG-, PNG- oder CSV-Format anzuzeigen und zu speichern.
2. Wählen Sie die Registerkarte **Export planen**. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu senden.

HINWEIS:

- Wenn Sie die **wöchentliche** Wiederholung auswählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie die **monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage, an denen der Bericht geplant werden soll, durch Kommas getrennt eingeben.

So erstellen Sie Tags und weisen sie Instanzen zu

Mit NetScaler Console können Sie Ihre NetScaler-Instanzen jetzt mit Tags verknüpfen. Ein Tag ist ein Schlüsselwort oder ein einwortiger Begriff, den Sie einer Instanz zuweisen können. Die Tags fügen zusätzliche Informationen über die Instanz hinzu. Die Tags können als Metadaten betrachtet werden, die helfen, eine Instanz zu beschreiben. Tags ermöglichen es Ihnen, Instanzen basierend auf diesen spezifischen Schlüsselwörtern zu klassifizieren und zu suchen. Sie können auch mehrere Tags einer einzelnen Instanz zuweisen.

Die folgenden Anwendungsfälle helfen Ihnen zu verstehen, wie die Kennzeichnung von Instanzen Ihnen hilft, diese besser zu überwachen.

- **Anwendungsfall 1**: Sie können ein Tag erstellen, um alle Instanzen zu identifizieren, die sich im Vereinigten Königreich befinden. Hier können Sie ein Tag mit dem Schlüssel „Land“ und dem Wert „UK“ erstellen. Dieses Tag hilft Ihnen, alle Instanzen zu suchen und zu überwachen, die sich in Großbritannien befinden.
- **Anwendungsfall 2**: Sie möchten nach Instanzen suchen, die sich in der Staging-Umgebung befinden. Hier können Sie ein Tag mit dem Schlüssel „Zweck“ und dem Wert „Staging_NS“ erstellen. Dieses Tag hilft Ihnen, alle Instanzen, die in der Staging-Umgebung verwendet werden, von den Instanzen zu trennen, die Client-Anfragen verarbeiten.
- **Anwendungsfall 3**: Stellen Sie sich eine Situation vor, in der Sie die Liste der NetScaler-Instanzen herausfinden möchten, die sich im Gebiet Swindon in Großbritannien befinden und Ihnen, David T., gehören. Sie können Tags für all diese Anforderungen erstellen und diese allen Instanzen zuweisen, die diese Bedingungen erfüllen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So weisen Sie Tags einer NetScaler VPX-Instanz zu:

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Instanzen > NetScaler**.
2. Wählen Sie die Registerkarte **VPX**.
3. Wählen Sie die gewünschte VPX-Instanz aus.
4. Klicken Sie auf **Tags**. Das angezeigte Fenster **Tags** ermöglicht es Ihnen, eigene „Schlüssel-Wert“-Paare zu erstellen, indem Sie jedem von Ihnen erstellten Schlüsselwort Werte zuweisen.

   Die folgenden Abbildungen zeigen beispielsweise einige erstellte Schlüsselwörter und deren Werte. Sie können eigene Schlüsselwörter hinzufügen und für jedes Schlüsselwort einen Wert eingeben.

   Sie können auch mehrere Tags hinzufügen, indem Sie auf „+“ klicken. Das Hinzufügen mehrerer und aussagekräftiger Tags ermöglicht es Ihnen, effizient nach den Instanzen zu suchen.

   Sie können einem Schlüsselwort mehrere Werte hinzufügen, indem Sie sie durch Kommas trennen.

   Zum Beispiel weisen Sie einem anderen Kollegen, Greg T., die Administratorrolle zu. Sie können seinen Namen durch ein Komma getrennt hinzufügen. Das Hinzufügen mehrerer Namen hilft Ihnen, nach einem der Namen oder nach beiden Namen zu suchen. NetScaler Console erkennt die durch Kommas getrennten Werte als zwei verschiedene Werte.

   Weitere Informationen zum Suchen von Instanzen basierend auf Tags finden Sie unter Suchen von Instanzen mithilfe von Tag- und Eigenschaftswerten.
5. Klicken Sie auf **OK**.

HINWEIS

Sie können später neue Tags hinzufügen oder vorhandene Tags löschen. Es gibt keine Beschränkung für die Anzahl der Tags, die Sie erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So suchen Sie Instanzen anhand der Werte von Tags und Eigenschaften

Es kann vorkommen, dass NetScaler Console viele NetScaler-Instanzen verwaltet. Als Administrator möchten Sie möglicherweise die Flexibilität haben, das Instanzinventar basierend auf bestimmten Parametern zu durchsuchen. NetScaler Console bietet jetzt eine verbesserte Suchfunktion, um eine Teilmenge von NetScaler-Instanzen basierend auf den Parametern zu durchsuchen, die Sie im Suchfeld definieren. Sie können die Instanzen anhand von zwei Kriterien suchen – Tags und Eigenschaften.

- **Tags**. Tags sind Begriffe oder Schlüsselwörter, die Sie einer NetScaler-Instanz zuweisen können, um zusätzliche Beschreibungen zur NetScaler-Instanz hinzuzufügen. Sie können Ihre NetScaler-Instanzen jetzt mit Tags verknüpfen. Diese Tags können verwendet werden, um die NetScaler-Instanzen besser zu identifizieren und zu durchsuchen.
- **Eigenschaften**. Jede in NetScaler Console hinzugefügte NetScaler-Instanz verfügt über einige Standardparameter oder Eigenschaften, die dieser Instanz zugeordnet sind. Jede Instanz hat beispielsweise ihren eigenen Hostnamen, ihre IP-Adresse, Version, Host-ID, Hardwaremodell-ID und so weiter. Sie können Instanzen suchen, indem Sie Werte für eine dieser Eigenschaften angeben.

Stellen Sie sich beispielsweise eine Situation vor, in der Sie die Liste der NetScaler-Instanzen finden möchten, die Version 12.0 verwenden und sich im Status „UP“ befinden. Hier werden die Version und der Status der Instanz durch die Standardeigenschaften definiert.

Neben der Version 12.0 und dem UP-Status der Instanzen können Sie auch die Instanzen suchen, die Ihnen gehören. Sie können ein Tag „Owner“ erstellen und diesem Tag den Wert „David T“ zuweisen. Weitere Informationen zum Erstellen und Zuweisen von Tags finden Sie unter So erstellen und weisen Sie Tags Instanzen zu.

Sie können eine Kombination aus Tags und Eigenschaften verwenden, um Ihre eigenen Suchkriterien zu erstellen.

So suchen Sie nach NetScaler VPX-Instanzen

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Instanzen > NetScaler**.
2. Wählen Sie die Registerkarte **VPX** aus.
3. Klicken Sie auf das Suchfeld. Sie können einen Suchausdruck erstellen, indem Sie Tags oder Eigenschaften verwenden oder beides kombinieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die folgenden Beispiele zeigen, wie Sie den Suchausdruck effizient verwenden können, um nach der Instanz zu suchen.

a. Wählen Sie die Option **Tags** und dann **Owner** aus. Wählen Sie „David T“ aus.

NetScaler Console unterstützt reguläre Ausdrücke und Platzhalterzeichen in den Suchausdrücken.

a. Sie können reguläre Ausdrücke verwenden, um die Suchkriterien weiter zu erweiternieren. Beispielsweise möchten Sie Instanzen suchen, die entweder David oder Stephen gehören. In einem solchen Fall können Sie die Werte eingeben, indem Sie sie mit einem "\|"-Ausdruck trennen.

   Besitzer-Tag(/en-us/netscaler-console-service/media/instance-search-tags-properties-3.png)

b. Sie können auch Platzhalterzeichen verwenden, um ein oder mehrere Zeichen zu ersetzen oder darzustellen. Beispielsweise können Sie `Dav*` eingeben, um alle Instanzen zu suchen, die "David" und "Dave P" gehören.

   Reguläre Ausdrücke und Platzhalterzeichen(/en-us/netscaler-console-service/media/instance-search-tags-properties-4.png)

HINWEIS:

Weitere Informationen zu regulären Ausdrücken und Platzhalterzeichen und deren Verwendung finden Sie, indem Sie auf das Symbol "Informationen" in der Suchleiste klicken.

Zentrale GeoIP-DB-Updates über NetScaler® Console

NetScaler Console ermöglicht Administratoren das Hochladen der GeoIP-DB-Datei (Geolocation Database) von MaxMind direkt über die NetScaler Console. Sie können die GeoIP-DB-Datei entweder sofort an verwaltete NetScaler-Instanzen übertragen oder das Update für einen späteren Zeitpunkt planen. Diese Dateien sind für eine genaue IP-zu-Standort-Zuordnung unerlässlich, die häufig in GSLB- und Sicherheitsrichtlinien verwendet wird.

Mit dieser Verbesserung erhalten Sie auch eine Verfolgung des Update-Verlaufs, die es Ihnen ermöglicht, zu sehen, ob ein Update erfolgreich war oder fehlgeschlagen ist. Außerdem können Sie zuvor hochgeladene oder übertragene GeoIP-DB-Versionen von NetScaler Console anzeigen,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

löschen oder herunterladen. Diese Verbesserung führt auch die manuelle Aktualisierung der GeoIP-DB-Datei in NetScaler Console, die Versionskontrolle und automatisierte Update-Workflows ein, die nahtlose GeoIP-DB-Updates ohne Beeinträchtigung der GSLB-Dienste ermöglichen.

Zuvor verfügte NetScaler nicht über einen zentralisierten Mechanismus zur Verwaltung von GeoIP-DB-Updates auf NetScaler. Administratoren mussten die Updates manuell auf jedem Gerät durchführen, was zeitaufwändig, fehleranfällig und in Produktionsumgebungen störend war.

Diese Verbesserung bietet die folgenden Vorteile:

- **Automatisierung**: Der Update-Prozess ist automatisiert und wird ohne geplante Ausfallzeiten durchgeführt, wodurch der Betriebsaufwand reduziert wird.
- **Effektive Skalierbarkeit**: Die Verwaltung von Updates über mehrere NetScaler-Instanzen hinweg ist effizient und einfach zu skalieren.
- **Versionskontrolle**: Wenn ein Problem auftritt, können Sie die historischen Versionen verfolgen, eine ältere GeoIP-DB-Datei hochladen und synchronisieren.

Einschränkungen

- **Unterstützung der Formatkonvertierung beschränkt auf MaxMind**: Die automatische Formatkonvertierung wird nur für MaxMind-Dateien unterstützt. Für andere Anbieter müssen die Dateien bereits im unterstützten Format vorliegen.
- **Einschränkung beim Löschen**: Das Löschen einer aktiv verwendeten Datei ist nicht zulässig. Stellen Sie vor dem Entfernen sicher, dass keine aktive Abhängigkeit besteht.

Konfigurieren zentralisierter GeoIP-DB-Updates über NetScaler Console

Voraussetzungen

- Stellen Sie sicher, dass Sie über eine gültige MaxMind-Lizenz verfügen, die für die Verwendung von GeoIP-DB-Dateien erforderlich ist.
- Wenn Sie das Dateiformat für Dateien anderer Anbieter verwenden, stellen Sie sicher, dass die Dateien im unterstützten Format vorliegen.

Führen Sie die folgenden Schritte aus, um die GeoIP-DB-Datei von MaxMind oder einem anderen Anbieter hochzuladen:

1. Navigieren Sie zu **Infrastructure > GeoIP DB Sync** und klicken Sie auf **Get Started**.

2. Wählen Sie eine der folgenden Optionen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Lokal**: Sie können eine Datei von Ihrem lokalen System hochladen.
- **Appliance**: Sie können eine Datei auswählen, die bereits auf einer NetScaler Console vorhanden ist.

HINWEISE:

- Wenn Sie die GeoIP-DB-Datei zum ersten Mal hochladen, wird die Option **Appliance** nicht angezeigt. Nur wenn die Datei bereits hochgeladen wurde, erscheint die Option **Appliance** bei nachfolgenden Uploads.
- Wenn Sie eine MaxMind-Datei hochladen, konvertiert der NetScaler Console-Dienst die Datei während des Uploads automatisch in das von NetScaler empfohlene Format. Wenn Sie eine Datei von anderen Anbietern hochladen, muss diese im CSV-Format vorliegen und die von NetScaler empfohlene Feldreihenfolge einhalten: IP-Bereich, Ländercode, Region, Stadt.

3. Nach dem Hochladen der Datei wählen Sie eine der folgenden Aktionen aus:

   - **Jetzt synchronisieren:** Fahren Sie sofort mit dem Dialogfeld für die Synchronisierungskonfiguration fort.
   - **Zeitplan erstellen:** Wählen Sie ein zukünftiges Datum und eine zukünftige Uhrzeit aus, um die Datei auf den Zielentitäten bereitzustellen.

4. Wenn Sie auf **Jetzt synchronisieren** klicken, wählen Sie einen der folgenden Bereitstellungsmodi aus:

   - **Alle synchronisieren:** Verteilt die GeoIP-DB-Datei automatisch an alle NetScaler-Instanzen, Agents und NetScaler Console.
   - **Anpassen:** Wählen Sie Ihre Ziele manuell aus:
     - **NetScaler Console auswählen:** Zeigt die NetScaler Console an, bei der Sie aktuell angemeldet sind.
     - **NetScaler-Instanzen auswählen:** Filtert und identifiziert spezifische Instanzen mithilfe des Gruppen-Dropdown-Menüs oder einer Schlüssel-Wert-Suche.
     - **Agenten auswählen:** Zeigt eine Liste der verfügbaren Agenten an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bevor Sie auf **Synchronisierung starten** klicken, beantworten Sie die Frage: *„Enthält die aktuelle Datei IPv6?“*. Wählen Sie *nur* dann **Ja** aus, wenn Ihre GeoIP-Datei IPv6-Adressblöcke enthält. Diese Einstellung bestimmt, wie jede Zielentität die Daten analysiert.

5. Überwachen Sie den Fortschritt und die Ergebnisse auf der Seite **GeoIP DB-Synchronisierung**. Das Panel **Übersicht der letzten Synchronisierung** zeigt die folgenden Metriken an:

   - **Gesamtanzahl ausgewählter Entitäten:** Die kombinierte Anzahl aller Ziel-NetScaler Console-Instanzen und Agenten.
   - **Ausstehende Synchronisierung:** Die Entitäten, die in der Warteschlange stehen, aber noch nicht gestartet wurden.
   - **Synchronisierung läuft:** Die Entitäten, die die Datei aktiv empfangen.
   - **Erfolgreiche Synchronisierung:** Die Entitäten, die fehlerfrei abgeschlossen wurden.
   - **Fehlgeschlagene Synchronisierung:** Die Entitäten, bei denen ein Fehler aufgetreten ist.
   - **Gesamtabschluss der Synchronisierung:** Der Prozentsatz der ausgewählten Entitäten, die erfolgreich abgeschlossen wurden.

   erweitern **Entitätsspezifischer Synchronisierungsstatus**, um eine gerätespezifische Tabelle anzuzeigen, die die IP-Adresse, den Hostnamen, den Typ, den Status, die Version und den Synchronisierungsstatus auflistet. Verwenden Sie die Filterleiste, um die Ergebnisse nach einem beliebigen Feld einzugrenzen, z. B. **Synchronisierungsstatus: Abgeschlossen**.

6. Führen Sie je nach Anforderung eine der folgenden Aktionen von der Seite **GeoIP DB-Synchronisierung** aus:

   - **Neue Datei auswählen:** Laden Sie eine GeoIP-DB-Datei von Ihrem lokalen System hoch oder wählen Sie eine bereits hochgeladene Datei aus NetScaler Console aus.
   - **Dateiinformationen anzeigen:** Überprüfen Sie die zuvor hochgeladenen Dateien. Wenn ein Problem auftritt, können Sie frühere Versionen verfolgen, eine ältere GeoIP-DB-Datei hochladen und synchronisieren.
   - **Aktiver Zeitplan:** Zeigen Sie die bevorstehenden geplanten Synchronisierungsaufträge an, die noch nicht ausgeführt wurden.
   - **Historischer Zeitplan:** Zeigen Sie die abgeschlossenen GeoIP-DB-Synchronisierungsvorgänge an. Jeder Eintrag zeigt den Entitätsbereich (z. B. **2 NetScaler-Instanzen, 1 Agent und NetScaler Console**), den Ausführungszeitstempel und die verwendete GeoIP-Datei. Klicken Sie auf einen beliebigen Eintrag, um die vollständigen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Auftragsdetails anzuzeigen, einschließlich der Synchronisierungsergebnisse pro Entität (Status, Startzeit und Endzeit) für die NetScaler Console-Instanzen und Agenten einzeln.

Verwalten von Administratorpartitionen von NetScaler-Instanzen

Sie können Administratorpartitionen auf Ihren Citrix Application Delivery Controller (NetScaler)-Instanzen konfigurieren, sodass verschiedenen Gruppen in Ihrer Organisation unterschiedliche Partitionen auf derselben NetScaler-Instanz zugewiesen werden. Sie können einem Netzwerkadministrator die Verwaltung mehrerer Partitionen auf mehreren NetScaler-Instanzen zuweisen.

NetScaler Console bietet eine nahtlose Möglichkeit, alle Partitionen, die einem Administrator gehören, über eine einzige Konsole zu verwalten. Sie können diese Partitionen verwalten, ohne andere Partitionskonfigurationen zu stören.

Damit mehrere Benutzer verschiedene Administratorpartitionen verwalten können, müssen Sie Gruppen erstellen und diesen Gruppen dann Benutzer und Partitionen zuweisen. Weitere Informationen zum Erstellen einer Gruppe oder eines Benutzers finden Sie unter und .

Ein Benutzer kann nur die Partitionen in der Gruppe anzeigen und verwalten, zu der der Benutzer gehört. Wenn Sie eine NetScaler-Instanz ermitteln, werden die auf dieser NetScaler-Instanz konfigurierten Administratorpartitionen automatisch dem System hinzugefügt. Jede Administratorpartition wird in NetScaler Console als Instanz betrachtet.

Administratorpartitionen anzeigen

Angenommen, Sie haben zwei NetScaler VPX-Instanzen, und auf jeder Instanz sind zwei Administratorpartitionen konfiguriert. Zum Beispiel hat die NetScaler-Instanz 10.xx.xx.100 partition-1 und partition-2, und die Instanz 10.xx.xx.101 hat first-partition und second-partition.

Führen Sie die folgenden Schritte aus, um Administratorpartitionen anzuzeigen:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**.
2. Klicken Sie auf der Registerkarte **VPX** auf **Partitionen**.

Wenn Sie beispielsweise eine Gruppe mit den folgenden Bedingungen erstellen:

- Unter **Einstellungen > Benutzer & Rollen > Gruppe erstellen > Autorisierungseinstellungen > Instanzen auswählen** wählen Sie die Instanzen „10.xx.xx.100-partition-1“ und „10.xx.xx.101-first-partition“ aus.
- Sie weisen „User1“ der Gruppe zu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User1 kann nur die Partitionen anzeigen und verwalten, die der Gruppe hinzugefügt wurden. Die Partitionen, die der Gruppe nicht hinzugefügt wurden, sind dem Benutzer jedoch eingeschränkt, obwohl sie zu denselben Instanzen gehören.

In diesem Beispiel sind 10.xx.xx.100-partition-2 und 10.xx.xx.101-second-partition eingeschränkt, da die Instanzen nicht der Gruppe hinzugefügt wurden, der der Benutzer zugewiesen ist.

Wenn Sie möchten, dass ein anderer Benutzer die Admin-Partitionen 10.xx.xx.100-partition-2 und 10.xx.xx.101-second-partition verwaltet, erstellen Sie eine Gruppe mit den folgenden Bedingungen:

- Wählen Sie auf der Registerkarte **Autorisierungseinstellungen** die Instanzen 10.xx.xx.100-partition-2 und 10.xx.xx.101-second-partition aus.
- Weisen Sie den erforderlichen Benutzer der Gruppe zu.

Diese Gruppe ermöglicht es dem zugewiesenen Benutzer, die ausgewählten Admin-Partitionen anzuzeigen und zu verwalten.

Revisionsverlaufsunterschied anzeigen

Revisionsverlaufsunterschied für eine Admin-Partition ermöglicht es Ihnen, den Unterschied zwischen den fünf neuesten Konfigurationsdateien für eine partitionierte NetScaler-Instanz anzuzeigen. Sie können die Konfigurationsdateien miteinander vergleichen (Beispiel Konfigurationsrevision - 1 mit Konfigurationsrevision - 2) oder die aktuell ausgeführte/gespeicherte Konfiguration mit der Konfigurationsrevision vergleichen. Neben den Konfigurationsunterschieden werden auch die Korrekturkonfigurationen angezeigt. Sie können alle Korrekturbefehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.

So zeigen Sie den Revisionsverlaufsunterschied an:

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsprüfung**. Das Dashboard für die Konfigurationsprüfung zeigt verschiedene Berichte an. Klicken Sie auf die Zahl, die in der Mitte des Donut-Diagramms angezeigt wird.

   Dashboard für die Konfigurationsprüfung(/en-us/netscaler-console-service/media/admin-partition.png)
2. Wählen Sie die partitionierte NetScaler-Instanz aus.
3. Klicken Sie im Feld „Aktion“ auf **Revisionsverlauf Diff.**

   Revisionsverlaufsunterschied(/en-us/netscaler-console-service/media/admin-partition-1.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Wählen Sie auf der Seite **Revisionsverlauf Diff.** die Dateien aus, die Sie vergleichen möchten. Vergleichen Sie beispielsweise die gespeicherte Konfiguration mit Konfigurationsrevision-2 und klicken Sie dann auf **Konfigurationsunterschied anzeigen**.

   Sie können dann die Unterschiede zwischen den fünf neuesten Konfigurationsdateien für die ausgewählte partitionierte NetScaler-Instanz anzeigen. Im Folgenden sehen Sie ein Beispiel für eine Admin-Partition mit fünf gespeicherten Konfigurationen:

   Gespeicherte Konfigurationen(/en-us/netscaler-console-service/media/admin-partition-3.png)

   Sie können auch die korrigierenden Konfigurationsbefehle anzeigen und diese korrigierenden Befehle in Ihren lokalen Ordner exportieren. Diese korrigierenden Befehle sind die Befehle, die in der Basisdatei ausgeführt werden müssen, um die Konfiguration in den gewünschten Zustand zu versetzen (Konfigurationsdatei, die für den Vergleich verwendet wird).

Die gespeicherten Konfigurationen auf einer Administratorpartition und der Instanz sind unterschiedlich. Im folgenden Beispiel verfügt die Instanz 10.xx.xx.20 über fünf gespeicherte Konfigurationen, während die Administratorpartition dieser Instanz drei verschiedene gespeicherte Konfigurationen aufweist:

Unterschied zwischen Vorlage und laufender Konfiguration anzeigen

Audit-Vorlagen für Partitionen ermöglichen es Ihnen, eine benutzerdefinierte Konfigurationsvorlage zu erstellen und diese einer Partitionsinstanz zuzuordnen. Jede Abweichung in der laufenden Konfiguration der Instanz von der Audit-Vorlage wird in der Spalte „**Template vs Running diff**“ der Seite **Audit Reports** angezeigt. Neben den Konfigurationsunterschieden werden auch die Korrekturkonfigurationen angezeigt. Sie können auch alle korrigierenden Befehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.

1. Navigieren Sie zu **Infrastructure > Configuration > Configuration Audit**. Das Dashboard „Configuration Audit“ zeigt verschiedene Berichte an. Klicken Sie auf die Zahl, die in der Mitte des Donut-Diagramms angezeigt wird.

2. Klicken Sie auf der Seite **Audit Reports** auf den Hyperlink **Diff Exists** unter der Spalte „Template vs Running Diff“.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn es einen Unterschied zwischen der Audit-Vorlage und der laufenden Konfiguration gibt, wird der Unterschied als Hyperlink angezeigt. Klicken Sie auf den Hyperlink, um die Unterschiede anzuzeigen, falls vorhanden. Neben den Konfigurationsunterschieden werden auch die Korrekturkonfigurationen angezeigt. Sie können auch alle korrigierenden Befehle in Ihren lokalen Ordner exportieren und die Konfigurationen korrigieren.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu exportieren, klicken Sie auf das Symbol **Export** oben rechts auf dieser Seite. Auf der Seite **Export** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren**. Um den Bericht im PDF-, JPEG-, PNG- oder CSV-Format anzuzeigen und zu speichern.
2. Wählen Sie die Registerkarte **Export planen**. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu senden.

HINWEIS:

- Wenn Sie die Option **Wöchentliche** Wiederholung auswählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie die Option **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage, an denen der Bericht geplant werden soll, durch Kommas getrennt eingeben.

NetScaler-Instanzen sichern und wiederherstellen

Sie können den aktuellen Zustand einer Citrix Application Delivery Controller (NetScaler)-Instanz sichern und die gesicherten Dateien später verwenden, um die NetScaler-Instanz in denselben Zustand wiederherzustellen. Sie müssen eine Instanz immer sichern, bevor Sie sie aktualisieren oder aus Vorsichtsgründen. Eine Sicherung eines stabilen Systems ermöglicht es Ihnen, es auf einen stabilen Punkt zurückzusetzen, falls es instabil wird. Es gibt mehrere Möglichkeiten, Sicherungen und Wiederherstellungen auf einer NetScaler-Instanz durchzuführen. Sie können NetScaler-Konfigurationen manuell über die GUI, CLI sichern und wiederherstellen, oder Sie können NetScaler Console verwenden, um automatische Sicherungen und manuelle Wiederherstellungen durchzuführen. NetScaler Console sichert den aktuellen Zustand Ihrer verwalteten NetScaler-Instanzen mithilfe von NITRO-Aufrufen und den Protokollen Secure Shell (SSH) und Secure Copy (SCP).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console erstellt eine vollständige Sicherung und stellt die folgenden NetScaler-Instanztypen wieder her:

- NetScaler SDX
- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

Weitere Informationen finden Sie unter Sichern und Wiederherstellen einer NetScaler-Instanz.

HINWEIS:

- Über NetScaler Console können Sie den Sicherungs- und Wiederherstellungsvorgang für einen NetScaler-Cluster nicht durchführen.
- Sie können die Sicherungsdatei einer Instanz nicht verwenden, um eine andere Instanz wiederherzustellen.

Die gesicherten Dateien werden als komprimierte TAR-Datei im folgenden Verzeichnis gespeichert:

```
/var/mps/tenants/root/tenants/<specify-the-tenant-name>/device_backup/
```

Um Probleme aufgrund mangelnden Speicherplatzes zu vermeiden, können Sie maximal drei Sicherungsdateien in diesem Verzeichnis speichern.

Um NetScaler-Instanzen zu sichern und wiederherzustellen, müssen Sie zuerst die Sicherungseinstellungen in NetScaler Console konfigurieren. Nach der Konfiguration der Einstellungen können Sie eine einzelne NetScaler-Instanz oder mehrere Instanzen auswählen und eine Sicherung der Konfigurationsdateien in diesen Instanzen erstellen. Bei Bedarf können Sie die NetScaler-Instanzen auch mithilfe dieser gesicherten Dateien wiederherstellen.

Erstellen einer Sicherung für eine ausgewählte NetScaler-Instanz mithilfe von NetScaler Console

Führen Sie diese Aufgabe aus, wenn Sie eine ausgewählte NetScaler-Instanz oder mehrere Instanzen sichern möchten:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Instances**. Wählen Sie unter **Instances** den Typ der Instanzen (z. B. VPX) aus, die auf dem Bildschirm angezeigt werden sollen.
2. Wählen Sie die Instanz aus, die Sie sichern möchten.
   - Wählen Sie für MPX-, VPX- und BLX-Instanzen **Backup/Restore** aus der Liste **Select Action** aus.
   - Klicken Sie für eine SDX-Instanz auf **Backup/Restore**.
3. Klicken Sie auf der Seite **Backup Files** auf **Back Up**.
4. Geben Sie an, ob Ihre Sicherungsdatei zur Erhöhung der Sicherheit verschlüsselt werden soll. Sie können entweder Ihr Kennwort eingeben oder das globale Kennwort verwenden, das Sie zuvor auf der Seite „Instance Backup Settings“ angegeben haben.
5. Klicken Sie auf **Continue**.

Eine Sicherungsdatei auf ein externes System übertragen

Sie können eine Kopie Ihrer Sicherungsdatei vorsorglich auf ein anderes System übertragen. Wenn Sie die Konfiguration wiederherstellen möchten, müssen Sie die Sicherungsdatei zuerst auf den NetScaler Console-Server hochladen und dann den Wiederherstellungsvorgang durchführen.

So übertragen Sie eine NetScaler Console-Sicherungsdatei:

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler** und wählen Sie dann den Instanztyp aus. Zum Beispiel VPX.
2. Wählen Sie die Instanz aus und wählen Sie aus der Liste **Select Action** die Option **Backup/Restore**.
3. Wählen Sie die Sicherungsdatei aus und klicken Sie dann auf **Transfer**.

   Die Seite **Transfer Backup File** wird angezeigt. Geben Sie die folgenden Parameter an:

   a. **Server** – IP-Adresse des Systems, auf das Sie die Sicherungsdatei übertragen möchten.
   b. **Benutzername** und **Passwort** – Benutzeranmeldeinformationen des neuen Systems, auf das die gesicherten Dateien kopiert werden.
   c. **Port** – Portnummer des Systems, auf das die Dateien übertragen werden.
   d. **Übertragungsprotokoll** – Protokoll, das für die Übertragung der Sicherungsdatei verwendet wird. Sie können SCP-, SFTP- oder FTP-Protokolle zum Übertragen der Sicherungsdatei auswählen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. **Verzeichnispfad** – Der Speicherort, an den die gesicherte Datei auf dem neuen System übertragen wird.

f. Klicken Sie auf **OK**.

HINWEIS:

Die Sicherungsdateien vom NetScaler Console-Dienst werden über einen Agenten an den externen Server gesendet. Wenn es viele Agenten gibt, wird eine NetScaler-Sicherungsdatei über denselben Agenten gesendet, der zum Hinzufügen dieser NetScaler-Instanz verwendet wurde. Um mehr über die mit einem Agenten verbundenen Instanzen zu erfahren, navigieren Sie zu **Infrastructure > NetScaler > Agents**.

Wiederherstellen einer NetScaler-Instanz mit NetScaler Console

HINWEIS:

Wenn Sie NetScaler-Instanzen in einem HA-Paar haben, müssen Sie Folgendes beachten:

- Stellen Sie dieselbe Instanz wieder her, von der die Sicherungsdatei erstellt wurde. Betrachten wir zum Beispiel ein Szenario, in dem eine Sicherung von der primären Instanz des HA-Paares erstellt wurde. Stellen Sie während des Wiederherstellungsprozesses sicher, dass Sie dieselbe Instanz wiederherstellen, auch wenn sie nicht mehr die primäre Instanz ist.
- Wenn Sie den Wiederherstellungsprozess auf der primären NetScaler-Instanz initiieren, können Sie nicht auf die primäre Instanz zugreifen, und die sekundäre Instanz wechselt zu **STAYSECONDARY**. Sobald der Wiederherstellungsprozess auf der primären Instanz abgeschlossen ist, wechselt die sekundäre NetScaler-Instanz von **STAYSECONDARY** in den Modus **ENABLED** und wird wieder Teil des HA-Paares. Sie können eine mögliche Ausfallzeit auf der primären Instanz erwarten, bis der Wiederherstellungsprozess abgeschlossen ist.

Führen Sie diese Aufgabe aus, um eine NetScaler-Instanz mithilfe der zuvor erstellten Sicherungsdatei wiederherzustellen:

1. Navigieren Sie zu **Infrastructure > Instances**, wählen Sie die Instanz aus, die Sie wiederherstellen möchten, und klicken Sie dann auf **View Backup**.
2. Wählen Sie auf der Seite **Backup Files** die Sicherungsdatei aus, die die Einstellungen enthält, die Sie wiederherstellen möchten, und klicken Sie dann auf **Restore**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Um eine extern übertragene Sicherungsdatei hochzuladen, verwenden Sie die Schaltfläche **Upload**.

Wiederherstellen einer NetScaler SDX Appliance mit NetScaler Console

In NetScaler Console umfasst die Sicherung einer NetScaler SDX Appliance Folgendes:

- Auf der Appliance gehostete NetScaler-Instanzen
- SVM-SSL-Zertifikate und -Schlüssel
- Instanz-Pruning-Einstellungen (im XML-Format)
- Instanz-Sicherungseinstellungen (im XML-Format)
- SSL-Zertifikat-Abfrageeinstellungen (im XML-Format)
- SVM-DB-Datei
- NetScaler-Konfigurationsdateien von Geräten, die auf SDX vorhanden sind
- NetScaler-Build-Images
- NetScaler XVA-Images, diese Images werden am folgenden Speicherort gespeichert: `/var/mps/sdx_images/`
- SDX Single Bundle Image (SVM+XS)
- Drittanbieter-Instanz-Images (falls bereitgestellt)

Sie müssen Ihre NetScaler SDX Appliance auf die in der Sicherungsdatei verfügbare Konfiguration wiederherstellen. Während der Appliance-Wiederherstellung wird die gesamte aktuelle Konfiguration gelöscht.

Wenn Sie die NetScaler SDX Appliance mithilfe einer Sicherung einer anderen NetScaler SDX Appliance wiederherstellen, stellen Sie sicher, dass Sie die Lizenzen hinzufügen und die Netzwerkeinstellungen des Management Service der Appliance so konfigurieren, dass sie mit denen in der Sicherungsdatei übereinstimmen, bevor Sie den Wiederherstellungsprozess starten.

Stellen Sie sicher, dass die gesicherte NetScaler SDX Plattformvariante dieselbe ist, auf der Sie die Wiederherstellung versuchen. Sie können nicht von einer anderen Plattformvariante wiederherstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Bevor Sie die SDX RMA Appliance wiederherstellen, stellen Sie sicher, dass die gesicherte Version entweder gleich oder höher als die RMA-Version ist.

So stellen Sie die SDX Appliance aus der gesicherten Datei wieder her:

1. Navigieren Sie in der NetScaler Console GUI zu **Infrastructure > Instances > NetScaler**.
2. Klicken Sie auf **Backup/Restore**.
3. Wählen Sie die Sicherungsdatei derselben Instanz aus, die Sie wiederherstellen möchten.
4. Klicken Sie auf **Repackage Backup**.

   Wenn die SDX Appliance gesichert wird, werden die XVA-Dateien und Images separat gespeichert, um Netzwerkbandbreite und Speicherplatz zu sparen. Daher müssen Sie die gesicherte Datei neu verpacken, bevor Sie die SDX Appliance wiederherstellen.

   Wenn Sie die Sicherungsdatei neu verpacken, enthält sie alle gesicherten Dateien zusammen, um die SDX Appliance wiederherzustellen. Die neu verpackte Sicherungsdatei gewährleistet die erfolgreiche Wiederherstellung der SDX Appliance.
5. Wählen Sie die neu verpackte Sicherungsdatei aus und klicken Sie auf **Restore**.

Bericht dieses Dashboards exportieren

Um den Bericht dieser Seite zu exportieren, klicken Sie auf das Symbol **Exportieren** oben rechts auf dieser Seite. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren**. Um den Bericht im PDF-, JPEG-, PNG- oder CSV-Format anzuzeigen und zu speichern.
2. Wählen Sie die Registerkarte **Export planen**. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu senden.

HINWEIS

- Wenn Sie die Wiederholung **Wöchentlich** auswählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie die Wiederholung **Monatlich** auswählen, stellen Sie sicher, dass Sie alle Tage, an denen der Bericht geplant werden soll, durch Kommas getrennt eingeben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Erzwingen eines Failovers auf die sekundäre NetScaler-Instanz

Möglicherweise möchten Sie ein Failover erzwingen, wenn Sie beispielsweise die primäre Citrix Application Delivery Controller (NetScaler)-Instanz ersetzen oder aktualisieren müssen. Sie können ein Failover entweder von der primären oder von der sekundären Instanz erzwingen. Wenn Sie ein Failover auf der primären Instanz erzwingen, wird die primäre zur sekundären und die sekundäre zur primären. Ein erzwungenes Failover ist nur möglich, wenn die primäre Instanz feststellen kann, dass die sekundäre Instanz UP (aktiv) ist.

Ein erzwungenes Failover wird nicht propagiert oder synchronisiert. Um den Synchronisierungsstatus nach einem erzwungenen Failover anzuzeigen, können Sie den Status der Instanz überprüfen.

Ein erzwungenes Failover schlägt unter den folgenden Umständen fehl:

- Sie erzwingen ein Failover auf einem eigenständigen System.
- Die sekundäre Instanz ist deaktiviert oder inaktiv. Wenn sich die sekundäre Instanz in einem inaktiven Zustand befindet, müssen Sie warten, bis ihr Zustand UP (aktiv) ist, um ein Failover zu erzwingen.
- Die sekundäre Instanz ist so konfiguriert, dass sie sekundär bleibt.

Die NetScaler-Instanz zeigt eine Warnmeldung an, wenn sie ein potenzielles Problem erkennt, während Sie den Befehl zum Erzwingen des Failovers ausführen. Die Meldung enthält die Informationen, die die Warnung ausgelöst haben, und fordert eine Bestätigung an, bevor Sie fortfahren.

Sie können ein Failover auf einer primären Instanz oder auf einer sekundären Instanz erzwingen.

So erzwingen Sie ein Failover auf die sekundäre NetScaler-Instanz mithilfe der NetScaler Console:

1. Navigieren Sie in der NetScaler Console zu **Infrastructure > Instances**. Wechseln Sie zur Registerkarte **VPX** und wählen Sie eine Instanz aus.
2. Wählen Sie Instanzen in einem HA-Setup aus den Instanzen aus, die unter dem ausgewählten Instanztyp aufgeführt sind.
3. Wählen Sie im Feld **Aktion** die Option **Failover erzwingen** aus.
4. Klicken Sie auf **Ja**, um die Aktion zum Erzwingen des Failovers zu bestätigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Eine sekundäre NetScaler-Instanz zwingen, sekundär zu bleiben

In einer Hochverfügbarkeits-(HA)-Einrichtung kann der sekundäre Knoten gezwungen werden, sekundär zu bleiben, unabhängig vom Zustand des primären Knotens.

Angenommen, der primäre Knoten muss aktualisiert werden und der Vorgang dauert einige Sekunden. Während des Upgrades könnte der primäre Knoten für einige Sekunden ausfallen, aber Sie möchten nicht, dass der sekundäre Knoten die Kontrolle übernimmt, und Sie möchten, dass er der sekundäre Knoten bleibt, selbst wenn er einen Fehler im primären Knoten erkennt.

Wenn Sie den sekundären Knoten zwingen, sekundär zu bleiben, bleibt er sekundär, selbst wenn der primäre Knoten ausfällt. Wenn Sie den Status eines Knotens in einem HA-Paar zwingen, sekundär zu bleiben, nimmt er auch nicht an HA-Zustandsautomatenübergängen teil. Der Status des Knotens wird als STAYSECONDARY angezeigt.

HINWEIS

Wenn Sie ein System zwingen, sekundär zu bleiben, wird der Erzwingungsprozess nicht weitergegeben oder synchronisiert. Er betrifft nur den Knoten, auf dem Sie den Befehl ausführen.

So konfigurieren Sie eine sekundäre NetScaler-Instanz, um sekundär zu bleiben, mithilfe von NetScaler Console:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Instances**, und wählen Sie dann eine Instanz unter einem Instanztyp (VPX) aus.
2. Wählen Sie Instanzen in einer HA-Einrichtung aus den Instanzen aus, die unter dem ausgewählten Instanztyp aufgeführt sind.
3. Wählen Sie im Feld **Aktion** die Option **Sekundär bleiben**.
4. Klicken Sie auf **Ja**, um die Ausführung der Aktion „Sekundär bleiben“ zu bestätigen.

Instanzgruppen erstellen

Um eine Instanzgruppe zu erstellen, müssen Sie zuerst alle Ihre NetScaler-Instanzen zur NetScaler Console hinzufügen. Nachdem Sie die Instanzen erfolgreich hinzugefügt haben, erstellen Sie Instanzgruppen basierend auf ihrer Instanzfamilie. Das Erstellen einer Gruppe von Instanzen hilft Ihnen, Upgrades, Sicherungen oder Wiederherstellungen auf den gruppierten Instanzen gleichzeitig durchzuführen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die **Instanzansicht** ermöglicht es Ihnen, alle verwalteten Instanzen zusammen mit ihren zugehörigen Gruppen anzuzeigen, wodurch es einfach wird, nicht zugeordnete Instanzen zu identifizieren. Sie können nicht zugeordnete Instanzen einer Gruppe zuweisen.

So erstellen Sie eine Instanzgruppe mit NetScaler Console

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Instanzen > Instanzgruppen** und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie einen Namen für Ihre Instanzgruppe an und wählen Sie **NetScaler** aus der Liste **Instanzfamilie** aus.
3. Wählen Sie unter **Kategorie** die Option **Standard** aus.
4. Klicken Sie auf **Instanzen auswählen**. Wählen Sie auf der Seite **Instanzen auswählen** die Instanzen aus, die Sie gruppieren möchten, und klicken Sie auf **Auswählen**.

   Die Tabelle listet die ausgewählten Instanzen und deren Details auf. Wenn Sie eine Instanz aus der Gruppe entfernen möchten, wählen Sie die Instanz aus der Tabelle aus und klicken Sie auf **Löschen**.
5. Klicken Sie auf **Erstellen**.

So identifizieren und fügen Sie nicht zugeordnete Instanzen einer Gruppe hinzu

1. Navigieren Sie zu **Infrastruktur > Instanzen > Instanzgruppen > Instanzansicht**.
2. Wählen Sie eine oder mehrere nicht zugeordnete Instanzen aus.
3. Klicken Sie auf **Instanzgruppe hinzufügen**.
4. Wählen Sie die gewünschte **Instanzgruppe** aus der Liste aus. Die Benutzeroberfläche zeigt außerdem an:

   - Verfügbare Instanzgruppen.
   - Instanzen, die bereits jeder Gruppe zugeordnet sind, um doppelte oder falsche Zuweisungen zu verhindern.
5. Klicken Sie auf **Speichern**. Die ausgewählten Instanzen werden der ausgewählten Gruppe zugewiesen.

Global Server Load Balancing-Site-Gruppen

Wenn Sie eine kontinuierliche Verfügbarkeit und Notfallwiederherstellung für Ihre ADC-Instanzen gewährleisten möchten, können Sie eine GSLB-Site-Gruppe konfigurieren. Sie gleicht die Last

© 1997–2026 Citrix Systems, Inc. All rights reserved.

über Sites hinweg aus, indem sie Client-Anfragen an die nächstgelegene oder leistungsstärkste Site oder im Falle eines Ausfalls an die verbleibenden Sites weiterleitet.

Manchmal versuchen in einer GSLB-Site-Gruppe die Konfigurationsobjekte der ADC-Instanzen, sich gegenseitig zu überschreiben. Dies führt zu einer Race Condition. Um solche Probleme zu beheben, müssen Sie die Auswahl des primären Knotens in der GSLB-Site-Gruppe steuern. Die Konfiguration im primären Knoten wird auf die verbleibenden ADC-Instanzen angewendet. In NetScaler Console können Sie eine GSLB-Site-Gruppe erstellen und Folgendes tun:

- Wählen Sie einen primären Knoten aus den ausgewählten ADC-Instanzen aus.
- Legen Sie die Prioritätsreihenfolge für die Auswahl des primären Knotens fest, falls der ausgewählte primäre Knoten ausfällt.

Sie können Ihre GSLB-Site-Gruppen unter **Infrastruktur > Instanzen > GSLB-Site-Gruppe** anzeigen.

Erstellen einer GSLB-Site-Gruppe

Führen Sie die folgenden Schritte aus, um eine GSLB-Site-Gruppe mit ADC-Instanzen zu erstellen:

1. Gehen Sie zu **Infrastruktur > Instanzen > GSLB-Site-Gruppe**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie einen Namen für die GSLB-Site-Gruppe an.
4. Wählen Sie die Instanzen aus, die Sie der GSLB-Site-Gruppe hinzufügen möchten. Diese Instanzen fungieren als Sites in der Gruppe.
5. Wählen Sie mindestens eine Site aus und klicken Sie auf **Site aktiv schalten**.

   Die Instanz, die auf Priorität `1` gesetzt ist, wird zum primären Knoten. Sie können die Priorität der aktiven Sites neu anordnen. Wählen Sie die Instanz mit niedrigerer Priorität aus und klicken Sie auf **Priorität erhöhen**.
6. Klicken Sie auf **Erstellen**.

Unter **Infrastructure > Network Functions > GSLB** zeigt die GUI die Entitäten nur vom primären ADC-Knoten der GSLB-Standortgruppe an.

SNMP-Manager und -Benutzer für NetScaler-Agent erstellen

Sie können den SNMP-Agenten nach systemspezifischen Informationen von einem Remote-Gerät abfragen, das als SNMP-Manager bezeichnet wird. Der Agent durchsucht dann die Management Information Base (MIB) nach angeforderten Daten und sendet die Daten an den SNMP-Manager.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können einen SNMP-Manager hinzufügen, um einen NetScaler-Agenten abzufragen. Der Manager entspricht SNMP V2 und V3. Wenn Sie einen oder mehrere SNMP-Manager angeben, akzeptiert der NetScaler-Agent keine SNMP-Abfragen von Hosts, außer den angegebenen SNMP-Managern.

Einen SNMP v2-Manager hinzufügen

So fügen Sie einen SNMP v2-Manager für den NetScaler-Agenten hinzu:

1. Navigieren Sie zu **Infrastruktur > Instanzen > Agents**, wählen Sie einen NetScaler-Agenten aus und klicken Sie auf **Aktion auswählen > SNMP verwalten**.
2. Klicken Sie auf der Registerkarte **SNMP > SNMP-Manager** auf **Hinzufügen**.
3. Geben Sie auf der Seite **SNMP-Manager erstellen** die folgenden Details an:
   - **SNMP-Manager**. Geben Sie den Namen oder die IP-Adresse des SNMP-Managers ein.
   - **Version**. Wählen Sie v2 aus.
   - **Community**. Geben Sie einen Community-Namen ein. Eine SNMP-Community-Konfiguration authentifiziert SNMP-Abfragen von SNMP-Managern.
   - **Management-Netzwerk aktivieren**: Aktivieren Sie dieses Kontrollkästchen, um die Netzmaske des SNMP-Manager-Netzwerks anzugeben.
   - **Netzmaske**: Geben Sie die Subnetzmaske ein, die einer IP-Adresse zugeordnet ist.
4. Klicken Sie auf **Erstellen**.

Einen SNMP v3 Manager hinzufügen

So fügen Sie einen SNMP v3 Manager für den NetScaler Agent hinzu:

1. Navigieren Sie zu **Infrastructure > Instances > Agents**, wählen Sie einen NetScaler Agent aus und klicken Sie auf **Select Action > Manage SNMP**.
2. Klicken Sie auf der Registerkarte **SNMP > SNMP Manager** auf **Add**.
3. Geben Sie auf der Seite **Create SNMP Manager** die folgenden Details an:
   - **SNMP Manager**. Geben Sie den Namen oder die IP-Adresse des SNMP Managers ein.
   - **Version**. Wählen Sie v3 aus.
   - **Management-Netzwerk aktivieren**: Aktivieren Sie dieses Kontrollkästchen, um die Netzmaske des SNMP-Manager-Netzwerks anzugeben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Netzmaske**: Geben Sie die Subnetzmaske ein, die einer IP-Adresse zugeordnet ist.

4. Klicken Sie auf **Create**.

Ein Dialogfeld wird angezeigt, das bestätigt, dass ein SNMP-Manager erstellt wurde und Sie auffordert, einen SNMP-Benutzer zu konfigurieren.

HINWEIS:

Sie müssen einen SNMP-Benutzer für einen SNMP v3 Manager konfigurieren. Um den SNMP-Benutzer zu konfigurieren, gehen Sie zu **SNMP > SNMP User**.

SNMP-Benutzer hinzufügen

Fügen Sie einen SNMP-Benutzer hinzu, um auf die SNMP v3-Abfragen eines SNMP-Managers zu antworten.

So fügen Sie einen SNMP-Benutzer für den NetScaler-Agent hinzu:

1. Navigieren Sie zu **Infrastructure > Instances > Agents**, wählen Sie einen NetScaler-Agent aus und klicken Sie auf **Select Action > Manage SNMP**.
2. Klicken Sie auf der Registerkarte **SNMP > SNMP User** auf **Add**.
3. Fügen Sie auf der Seite **Create SNMP User** die folgenden Details hinzu:

   - **Name**. Geben Sie den Benutzernamen ein.
   - **Sicherheitsstufe**. Erforderliche Sicherheitsstufe für die Kommunikation zwischen dem NetScaler-Agent und dem SNMP-Manager.

     Wählen Sie eine der folgenden Sicherheitsstufen aus:
   - **noAuthNoPriv**. Erfordert weder Authentifizierung noch Verschlüsselung.

   - **authNoPriv**. Erfordert Authentifizierung, aber keine Verschlüsselung.

   - **authPriv**. Erfordert Authentifizierung und Verschlüsselung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Geben Sie basierend auf der Sicherheitsstufe, die Sie dem Benutzer zugewiesen haben, zusätzliche Authentifizierungsprotokolle wie Authentifizierungsprotokolle und Datenschutzpasswörter an und weisen Sie SNMP-Ansichten zu.

Verwalten von SNMP-Ansichten

SNMP-Ansichten werden verwendet, um die Zugriffssteuerung für einen SNMP-Benutzer zu implementieren. Die SNMP-Ansichten beschränken den Benutzerzugriff auf bestimmte Teile der MIB.

So lassen Sie eine SNMP-OID für den NetScaler-Agenten zu oder schränken sie ein:

1. Navigieren Sie zu **Infrastructure > Instances > Agents**, wählen Sie einen NetScaler-Agenten aus und klicken Sie auf **Select Action > Manage SNMP**.
2. Klicken Sie auf der Registerkarte **SNMP > SNMP User** auf **Add**.
3. Geben Sie unter **Create SNMP View** die folgenden Details ein:
   - **View Name**: Ein Name für die SNMP-Ansicht. Eine Instanz kann viele SNMP-Ansichten mit demselben Namen haben, die sich durch die Parameter der Unterbaum-Einstellungen unterscheiden.
   - **Subtree**: Ein bestimmter Zweig (Unterbaum) des MIB-Baums, den Sie dieser SNMP-Ansicht zuordnen möchten. Sie müssen den Unterbaum als SNMP-OID angeben.
   - **Type**: Dieses Feld ermöglicht es Ihnen, Unterbäume in eine Ansicht aufzunehmen oder auszuschließen.
4. Klicken Sie auf **Create**.

NetScaler VPX-Instanzen auf SDX bereitstellen

Sie können eine oder mehrere NetScaler VPX-Instanzen auf der SDX-Appliance mithilfe von NetScaler Console bereitstellen. Die Anzahl der Instanzen, die Sie bereitstellen können, hängt von der erworbenen Lizenz ab. Wenn die Anzahl der hinzugefügten Instanzen der in der Lizenz angegebenen Anzahl entspricht, erlaubt die NetScaler Console Ihnen nicht, weitere NetScaler-Instanzen bereitzustellen.

Bevor Sie beginnen, stellen Sie sicher, dass Sie eine SDX-Instanz in NetScaler Console hinzufügen, auf der Sie VPX-Instanzen bereitstellen möchten.

Um eine VPX-Instanz bereitzustellen, führen Sie die folgenden Schritte aus:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler**.
2. Wählen Sie auf der Registerkarte **SDX** eine SDX-Instanz aus, auf der Sie eine VPX-Instanz bereitstellen möchten.
3. Wählen Sie unter **Aktion auswählen** die Option **VPX bereitstellen**.

Schritt 1 – Eine VPX-Instanz hinzufügen

Die NetScaler Console verwendet die folgenden Informationen, um VPX-Instanzen in einer SDX-Appliance zu konfigurieren:

- **Name** – Geben Sie einen Namen für eine NetScaler-Instanz an.
- Richten Sie ein Kommunikationsnetzwerk zwischen SDX und VPX ein. Wählen Sie dazu die erforderlichen Optionen aus der Liste aus:
  - **Verwaltung über internes Netzwerk** – Diese Option richtet ein internes Netzwerk für die Kommunikation zwischen der NetScaler Console und einer VPX-Instanz ein.
  - **IP-Adresse** – Sie können eine **IPv4**- oder **IPv6**-Adresse oder beide auswählen, um die NetScaler VPX-Instanz zu verwalten. Eine VPX-Instanz kann nur eine Verwaltungs-IP (auch NetScaler-IP genannt) haben. Sie können die NetScaler-IP-Adresse nicht entfernen.

    Für die ausgewählte Option weisen Sie der NetScaler Console eine Netzmaske, ein Standard-Gateway und einen nächsten Hop für die IP-Adresse zu.
- **XVA-Datei** – Wählen Sie die XVA-Datei aus, von der Sie eine VPX-Instanz bereitstellen möchten. Verwenden Sie eine der folgenden Optionen, um die XVA-Datei auszuwählen.
  - **Lokal** – Wählen Sie die XVA-Datei von Ihrem lokalen Computer aus.
  - **Appliance** – Wählen Sie die XVA-Datei aus einem NetScaler Console-Dateibrowser aus.
- **Admin-Profil** – Dieses Profil bietet Zugriff zum Bereitstellen von VPX-Instanzen. Mit diesem Profil ruft NetScaler Console die Konfigurationsdaten von einer Instanz ab. Wenn Sie ein Profil hinzufügen müssen, klicken Sie auf **Hinzufügen**.
- **Agent** – Wählen Sie den Agenten aus, dem Sie die Instanzen zuordnen möchten.
- **Site** – Wählen Sie die Site aus, an der die Instanz hinzugefügt werden soll.

Schritt 2 – Lizenzen zuweisen

Geben Sie im Abschnitt **Lizenzzuweisung** die VPX-Lizenz an. Sie können Standard-, Advanced- und Premium-Lizenzen verwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Zuweisungsmodus** – Sie können die Modi **Fest** oder **Burstable** für den Bandbreitenpool auswählen.

  Wenn Sie den Modus **Burstable** wählen, können Sie zusätzliche Bandbreite nutzen, wenn die feste Bandbreite erreicht ist.

- **Durchsatz** – Weisen Sie einer Instanz den gesamten Durchsatz (in Mbit/s) zu.

HINWEIS

Kaufen Sie eine separate Lizenz (SDX 2-Instanz-Add-On-Pack für Secure Web Gateway) für Citrix Secure Web Gateway™ (SWG)-Instanzen auf SDX-Appliances. Dieses Instanzpaket unterscheidet sich von der SDX-Plattformlizenz oder dem SDX-Instanzpaket.

Ab der SDX-Version 12.0 57.19 hat sich die Schnittstelle zur Verwaltung der Kryptokapazität geändert. Weitere Informationen finden Sie unter Kryptokapazität verwalten.

Schritt 3 - Ressourcen zuweisen

Im Abschnitt **Ressourcenzuweisung** weisen Sie einer VPX-Instanz Ressourcen zu, um den Datenverkehr aufrechtzuerhalten.

- **Gesamtspeicher (MB)** - Weisen Sie einer Instanz den Gesamtspeicher zu. Der Mindestwert beträgt `2048` MB.
- **Pakete pro Sekunde** - Geben Sie die Anzahl der pro Sekunde zu übertragenden Pakete an.
- **CPU** - Geben Sie die Anzahl der CPU-Kerne für eine Instanz an. Sie können gemeinsam genutzte oder dedizierte CPU-Kerne verwenden.

  Wenn Sie einen gemeinsam genutzten Kern für eine Instanz auswählen, können die anderen Instanzen den gemeinsam genutzten Kern im Falle eines Ressourcenmangels verwenden.

  Starten Sie Instanzen neu, denen CPU-Kerne neu zugewiesen wurden, um Leistungseinbußen zu vermeiden.

  Wenn Sie die SDX 25000xx-Plattform verwenden, können Sie einer Instanz maximal 16 Kerne zuweisen. Wenn Sie die SDX 2500xxx-Plattform verwenden, können Sie einer Instanz maximal 11 Kerne zuweisen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Für eine Instanz beträgt der maximale Durchsatz, den Sie konfigurieren, 180 Gbit/s.

Siehe die Tabelle unter NetScaler-Instanzen bereitstellen, die die unterstützte VPX, die Single-Bundle-Image-Version und die Anzahl der Kerne auflistet, die Sie einer Instanz zuweisen können.

Schritt 4 - Instanzverwaltung hinzufügen

Sie können einen Administratorbenutzer für die VPX-Instanz erstellen. Wählen Sie dazu **Instanzverwaltung hinzufügen** im Abschnitt **Instanzverwaltung**.

Geben Sie die folgenden Details an:

- **Benutzername**: Der Benutzername für den NetScaler-Instanzadministrator. Dieser Benutzer hat Superuser-Zugriff, aber keinen Zugriff auf Netzwerkbefehle zum Konfigurieren von VLANs und Schnittstellen.
- **Passwort**: Geben Sie das Passwort für den Benutzernamen an.
- **Shell-/SFTP-/SCP-Zugriff**: Der dem NetScaler-Instanzadministrator zulässige Zugriff. Diese Option ist standardmäßig ausgewählt.

Schritt 5 – Netzwerkeinstellungen angeben

Wählen Sie die erforderlichen Netzwerkeinstellungen für eine Instanz aus:

- **L2-Modus unter Netzwerkeinstellungen zulassen** – Sie können den L2-Modus auf der NetScaler-Instanz zulassen. Wählen Sie „L2-Modus unter Netzwerkeinstellungen zulassen“ aus. Bevor Sie sich bei der Instanz anmelden und den L2-Modus aktivieren. Weitere Informationen finden Sie unter L2-Modus auf einer NetScaler-Instanz zulassen.

  HINWEIS

  Wenn Sie den L2-Modus für eine Instanz deaktivieren, müssen Sie sich bei der Instanz anmelden und den L2-Modus von dieser Instanz aus deaktivieren. Andernfalls könnten alle anderen NetScaler-Modi nach dem Neustart der Instanz deaktiviert werden.

- **0/1** – Geben Sie unter **VLAN-Tag** eine VLAN-ID für die Verwaltungsschnittstelle an.
- **0/2** – Geben Sie unter **VLAN-Tag** eine VLAN-ID für die Verwaltungsschnittstelle an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Standardmäßig sind die Schnittstellen **0/1** und **0/2** ausgewählt.

Klicken Sie unter **Datenschnittstellen** auf **Hinzufügen**, um Datenschnittstellen hinzuzufügen und Folgendes anzugeben:

- **Schnittstellen** – Wählen Sie die Schnittstelle aus der Liste aus.

  HINWEIS

  Die Schnittstellen-IDs der Schnittstellen, die Sie einer Instanz hinzufügen, entsprechen nicht unbedingt der physischen Schnittstellennummerierung auf der SDX-Appliance.

  Wenn beispielsweise die erste Schnittstelle, die Sie Instanz-1 zuordnen, die SDX-Schnittstelle 1/4 ist, wird sie als Schnittstelle 1/1 angezeigt, wenn Sie die Schnittstelleneinstellungen in dieser Instanz anzeigen. Diese Schnittstelle zeigt an, dass es die erste Schnittstelle ist, die Sie Instanz-1 zugeordnet haben.
- **Zulässige VLANs** – Geben Sie eine Liste von VLAN-IDs an, die einer NetScaler-Instanz zugeordnet werden können.
- **MAC-Adressmodus** – Weisen Sie einer Instanz eine MAC-Adresse zu. Wählen Sie eine der folgenden Optionen:
  - **Standard** – Citrix Workspace weist eine MAC-Adresse zu.
  - **Benutzerdefiniert** – Wählen Sie diesen Modus, um eine MAC-Adresse anzugeben, die die generierte MAC-Adresse überschreibt.
  - **Generiert** – Generieren Sie eine MAC-Adresse unter Verwendung der zuvor festgelegten Basis-MAC-Adresse. Informationen zum Festlegen einer Basis-MAC-Adresse finden Sie unter Zuweisen einer MAC-Adresse zu einer Schnittstelle.
- **VMAC-Einstellungen (IPv4- und IPv6-VRIDs zur Konfiguration der virtuellen MAC)**
  - **VRID IPV4** – Die IPv4-VRID, die die VMAC identifiziert. Mögliche Werte: 1–255. Weitere Informationen finden Sie unter Konfigurieren von VMACs auf einer Schnittstelle.
  - VRID IPV6 – Die IPv6-VRID, die die VMAC identifiziert. Mögliche Werte: 1–255. Weitere Informationen finden Sie unter Konfigurieren von VMACs auf einer Schnittstelle.

Klicken Sie auf **Hinzufügen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schritt 6 – Management-VLAN-Einstellungen angeben

Der Management-Dienst und die Management-Adresse (NSIP) der VPX-Instanz befinden sich im selben Subnetz, und die Kommunikation erfolgt über eine Management-Schnittstelle.

Wenn sich der Management Service und die Instanz in verschiedenen Subnetzen befinden, geben Sie beim Bereitstellen einer VPX-Instanz eine VLAN-ID an. Dadurch ist die Instanz über das Netzwerk erreichbar, wenn sie aktiv ist.

Wenn Ihre Bereitstellung erfordert, dass die NSIP nur über die ausgewählte Schnittstelle zugänglich ist, während die VPX-Instanz bereitgestellt wird, wählen Sie **NSVLAN** aus. Die NSIP wird dann über andere Schnittstellen unzugänglich.

- HA-Heartbeats werden nur über die Schnittstellen gesendet, die Teil des NSVLAN sind.
- Sie können ein NSVLAN erst ab dem VPX XVA Build `9.3-53.4` konfigurieren.

WICHTIG

- Sie können diese Einstellung nach der Bereitstellung der VPX-Instanz nicht mehr ändern.
- Der Befehl `clear config full` auf der VPX-Instanz löscht die VLAN-Konfiguration, wenn **NSVLAN** nicht ausgewählt ist.

☐ Klicken Sie auf **Fertig**, um eine VPX-Instanz bereitzustellen.

Bereitgestellte VPX-Instanz anzeigen

Um die neu bereitgestellte Instanz anzuzeigen, gehen Sie wie folgt vor:

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler**.
2. Suchen Sie auf der Registerkarte **VPX** eine Instanz nach der Eigenschaft **Host IP address** und weisen Sie ihr die SDX-Instanz-IP zu.

☐

Mehrere NetScaler-Instanzen neu erkennen

Sie können mehrere Citrix Application Delivery Controller (NetScaler)-Instanzen (VPX, MPX, SDX, BLX und CPX) in Ihrer NetScaler Console-Einrichtung neu erkennen. Nachdem Sie die Instanzen neu erkannt haben, können Sie die neuesten Zustände und Konfigurationen dieser Instanzen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

anzeigen. Der NetScaler Console-Server erkennt alle ADC-Instanzen neu und prüft, ob die Instanzen erreichbar sind.

So erkennen Sie mehrere NetScaler VPX-Instanzen neu:

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler**. Wählen Sie die Registerkarte für die Instanz (VPX, MPX, SDX, BLX und CPX) aus und wählen Sie die Instanzen aus, die Sie neu erkennen möchten.
2. Klicken Sie im Feld **Aktion** auf **Neu erkennen**. Sie können auch mehrere VPX-Instanzen neu erkennen.
3. Wenn die Bestätigungsmeldung zum Ausführen des Dienstprogramms „Neu erkennen“ angezeigt wird, klicken Sie auf **Ja**.

   Der Bildschirm zeigt den Fortschritt der Neuerkennung jeder Instanz an.

Polling-Übersicht

Polling ist ein Prozess, bei dem NetScaler Console bestimmte Informationen von NetScaler-Instanzen sammelt. Möglicherweise haben Sie mehrere NetScaler-Instanzen für Ihr Unternehmen weltweit konfiguriert. Um Ihre Instanzen über NetScaler Console zu überwachen, muss NetScaler Console bestimmte Informationen wie CPU-Auslastung, Speichernutzung, SSL-Zertifikate, lizenzierte Funktionen und Lizenztypen von allen verwalteten NetScaler-Instanzen erfassen. Im Folgenden sind die verschiedenen Arten des Pollings aufgeführt, die zwischen NetScaler Console und den verwalteten Instanzen stattfinden:

- Instanz-Polling
- Inventar-Polling
- Leistungsdatenerfassung
- Instanz-Backup-Polling
- Konfigurationsprüfungs-Polling
- SSL-Zertifikat-Polling
- Entitäts-Polling

NetScaler Console verwendet Protokolle wie NITRO-Aufruf, Secure Shell (SSH) und Secure Copy (SCP), um Informationen von NetScaler-Instanzen abzufragen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wie NetScaler Console verwaltete Instanzen und Entitäten abfragt

NetScaler Console fragt standardmäßig automatisch in regelmäßigen Intervallen ab. NetScaler Console ermöglicht es Ihnen auch, Polling-Intervalle für einige Polling-Typen zu konfigurieren und bei Bedarf manuell abzufragen.

Die folgende Tabelle beschreibt die Details zu Polling-Typen, Polling-Intervall, verwendetem Protokoll und so weiter:

POLLING-TYP	POLLING-INTERVALL	ABGERUFENE INFORMATIONEN	VERWENDETES PROTOKOLL	KONFIGURATION DES ABRUFINTERVALLS
Instanz-Abruf	Alle 5 Minuten (standardmäßig)	Statistische Informationen wie Status, HTTP-Anfragen pro Sekunde, CPU-Auslastung, Speichernutzung und Durchsatz.	NITRO-Aufruf	Nein
Bestandsabruf	Alle 60 Minuten (standardmäßig)	Bestandsdetails wie Build-Version, Systeminformationen, lizenzierte Funktionen und Modi.	NITRO-Aufruf und SSH	Nein
Leistungsdatenerfassung	Alle 5 Minuten (standardmäßig)	Informationen zur Netzwerkberichterstattung	NITRO-Aufruf	Nein
Abfrage von Instanz-Backups	Alle 12 Stunden (standardmäßig)	Die Sicherungsdatei des aktuellen Zustands der verwalteten	NITRO-Aufruf, SSH und SCP	Ja. Navigieren Sie zu **Infrastructure > Instances > NetScaler**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLLING-TYP	POLLING-INTERVALL	ABGERUFENE INFORMATIONEN	VERWENDETES PROTOKOLL	KONFIGURATION DES ABRUFINTERVALLS
		NetScaler-Instanzen		Wählen Sie die Instanz aus und klicken Sie in der Liste **Aktion auswählen** auf **Sichern/ Wiederherstellen**.
Konfigurationsaudit-Abfrage	Alle 10 Stunden (standardmäßig)	Konfigurationsänderungen, die auf NetScaler-Instanzen auftreten (z. B. laufende vs. gespeicherte Konfiguration)	SSH, SCP und NITRO-Aufruf	Ja. Navigieren Sie zu **Infrastructure > Configuration > Configuration Audit**. Klicken Sie auf der Seite „Konfigurationsprüfung“ auf **Einstellungen** und konfigurieren Sie das Abfrageintervall für die Konfigurationsaudit-Abfrage.
				Sie können Konfigurationsprüfungen manuell abfragen und alle Konfigurationsprüfungen der

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLLING-TYP	POLLING-INTERVALL	ABGERUFENE INFORMATIONEN	VERWENDETES PROTOKOLL	KONFIGURATION DES ABRUFINTERVALLS
				Instanzen sofort zur NetScaler Console hinzufügen. Navigieren Sie dazu zu **Infrastructure > Configuration > Configuration Audit** und klicken Sie auf **Jetzt abfragen**. Auf der Seite **Jetzt abfragen** können Sie alle oder ausgewählte Instanzen im Netzwerk abfragen.
SSL-Zertifikatsabfrage	Alle 24 Stunden (standardmäßig)	SSL-Zertifikate, die auf NetScaler-Instanzen installiert sind.	NITRO-Aufruf und SCP	Ja. Navigieren Sie zu **Infrastructure > SSL Dashboard**. Klicken Sie auf der Seite SSL Dashboard auf **Settings**, um das Abfrageintervall zu konfigurieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLLING-TYP	POLLING-INTERVALL	ABGERUFENE INFORMATIONEN	VERWENDETES PROTOKOLL	KONFIGURATION DES ABRUFINTERVALLS
				Sie können SSL-Zertifikate manuell abfragen und alle Zertifikate der Instanzen sofort zur NetScaler Console hinzufügen. Navigieren Sie dazu zu **Infrastructure > SSL Dashboard** und klicken Sie auf **Poll Now**. Auf der Seite **Poll Now** können Sie alle oder ausgewählte Instanzen im Netzwerk abfragen.
Entitätsabfrage				
Alle Instanzen	Alle 720 Minuten (standardmäßig)	Alle Entitäten, die auf den Instanzen konfiguriert sind. Eine Entität ist entweder eine Richtlinie, ein virtueller	NITRO-Aufruf	Ja. Es kann zwischen 30 Minuten und 1440 Minuten eingestellt werden. Navigieren Sie zur Konfiguration

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLLING-TYP	POLLING-INTERVALL	ABGERUFENE INFORMATIONEN	VERWENDETES PROTOKOLL	KONFIGURATION DES ABRUFINTERVALLS
		Server, ein Dienst oder eine Aktion, die an eine NetScaler-Instanz angehängt ist. Um die Entitätsabfrage zu aktivieren, siehe NetScaler Console-Funktionen aktivieren oder deaktivieren.		zu **Infrastructure > Network Functions**. Klicken Sie auf der Seite Networks Function auf **Settings**, um das Abfrageintervall zu konfigurieren.
				Sie können Entitäten manuell abfragen und alle Entitäten der Instanzen sofort zur NetScaler Console hinzufügen. Navigieren Sie dazu zu **Infrastructure > Network Functions** und klicken Sie auf **Poll Now**. Auf der Seite **Poll Now** können Sie alle oder ausgewählte Instanzen im

© 1997–2026 Citrix Systems, Inc. All rights reserved.

POLLING-TYP	POLLING-INTERVALL	ABGERUFENE INFORMATIONEN	VERWENDETES PROTOKOLL	KONFIGURATION DES ABRUFINTERVALLS
				Netzwerk abfragen.
Ausgewählte NetScaler-Instanzen	Alle 15 Minuten (standardmäßig)	Fragen Sie nur die NetScaler-Instanzen ab, bei denen Änderungen vorgenommen wurden, bevor der Standardabfragezyklus ausgelöst wird.	NITRO-Aufruf	Ja. Sie kann zwischen 5 und 60 Minuten eingestellt werden. Navigieren Sie zu **Infrastructure > Network Functions**, klicken Sie auf **Settings**, und geben Sie die Zeit in das Textfeld **Delay time for Network Functions** ein.

HINWEIS:

Zusätzlich zum Polling werden von verwalteten NetScaler-Instanzen generierte Ereignisse von NetScaler Console über SNMP-Traps empfangen, die an die Instanzen gesendet werden. Ein Ereignis wird beispielsweise generiert, wenn ein Systemfehler oder eine Konfigurationsänderung auftritt.

Während der Instanzsicherung werden SSL-Dateien, CA-Zertifikatsdateien, NetScaler-Vorlagen, Datenbankinformationen usw. auf die NetScaler Console heruntergeladen. Während eines Konfigurationsaudits werden ns.conf-Dateien heruntergeladen und im Dateisystem gespeichert. Alle von verwalteten NetScaler-Instanzen gesammelten Informationen werden intern in der Datenbank gespeichert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verschiedene Arten des Polling von Instanzen

Im Folgenden sind die verschiedenen Arten des Polling aufgeführt, die NetScaler Console für die verwalteten Instanzen durchführt:

- Globales Polling von Instanzen
- Manuelles Polling von Instanzen
- Manuelles Polling von Entitäten

Globales Polling von Instanzen

NetScaler Console fragt automatisch alle verwalteten Instanzen im Netzwerk ab, abhängig vom von Ihnen konfigurierten Intervall. Obwohl das Standard-Polling-Intervall 60 Minuten beträgt, können Sie das Intervall je nach Ihren Anforderungen festlegen, indem Sie zu **Infrastructure > Network Functions > Settings** navigieren.

Manuelles Polling von Instanzen

Wenn NetScaler Console viele Entitäten verwaltet, dauert der Polling-Zyklus länger, um den Bericht zu generieren, was zu einem leeren Bildschirm führen oder das System möglicherweise noch frühere Daten anzeigen könnte.

In NetScaler Console gibt es einen minimalen Polling-Intervallzeitraum, in dem kein automatisches Polling stattfindet. Wenn Sie eine neue NetScaler-Instanz hinzufügen oder eine Entität aktualisiert wird, erkennt NetScaler Console die neue Instanz oder die an einer Entität vorgenommenen Aktualisierungen erst beim nächsten Polling. Und es gibt keine Möglichkeit, sofort eine Liste der virtuellen IP-Adressen für weitere Operationen zu erhalten. Sie müssen warten, bis der minimale Polling-Intervallzeitraum abgelaufen ist. Obwohl Sie ein manuelles Polling durchführen können, um neu hinzugefügte Instanzen zu erkennen, führt dies dazu, dass das gesamte NetScaler-Netzwerk abgefragt wird, was eine hohe Last auf dem Netzwerk erzeugt. Anstatt das gesamte Netzwerk abzufragen, ermöglicht NetScaler Console Ihnen jetzt, jederzeit nur ausgewählte Instanzen und Entitäten abzufragen.

NetScaler Console fragt verwaltete Instanzen automatisch ab, um Informationen zu festgelegten Zeiten am Tag zu sammeln. Die ausgewählte Abfrage reduziert die Aktualisierungszeit, die NetScaler Console benötigt, um den aktuellsten Status der an diese ausgewählten Instanzen gebundenen Entitäten anzuzeigen.

So fragen Sie bestimmte Instanzen in NetScaler Console ab:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Network Functions**.
2. Klicken Sie auf der Seite **Network Functions** oben rechts auf **Poll Now**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Die Pop-up-Seite **Poll Now** bietet Ihnen die Möglichkeit, alle NetScaler-Instanzen im Netzwerk abzufragen oder die ausgewählten Instanzen abzufragen.
    a. **All Instances**-Registerkarte – klicken Sie auf **Start Polling**, um alle Instanzen abzufragen.
    b. **Select Instances**-Registerkarte – wählen Sie die Instanzen aus der Liste aus.
4. Klicken Sie auf **Start Polling**.

    NetScaler Console leitet die manuelle Abfrage ein und fügt alle Entitäten hinzu.

Manuelle Abfrage von Entitäten

NetScaler Console ermöglicht es Ihnen auch, nur einige ausgewählte Entitäten abzufragen, die an eine Instanz gebunden sind. Sie können diese Option beispielsweise verwenden, um den neuesten Status einer bestimmten Entität in einer Instanz zu erfahren. In diesem Fall müssen Sie die Instanz nicht als Ganzes abfragen, um den Status einer aktualisierten Entität zu erfahren. Wenn Sie eine Entität auswählen und abfragen, fragt NetScaler Console nur diese Entität ab und aktualisiert den Status in der NetScaler Console GUI.

Betrachten Sie ein Beispiel, bei dem ein virtueller Server den Status **DOWN** hat. Der Status dieses virtuellen Servers könnte sich auf **UP** geändert haben, bevor die nächste automatische Abfrage erfolgt. Um den geänderten Status des virtuellen Servers anzuzeigen, möchten Sie möglicherweise nur diesen virtuellen Server abfragen, damit der korrekte Status sofort in der GUI angezeigt wird.

Sie können jetzt die folgenden Entitäten auf Aktualisierungen ihres Status abfragen: Dienste, Dienstgruppen, Lastausgleichs-Virtual-Server, Cache-Reduktions-Virtual-Server, Content-Switching-Virtual-Server, Authentifizierungs-Virtual-Server, VPN-Virtual-Server, GSLB-Virtual-Server und Anwendungsserver.

HINWEIS:

Wenn Sie einen virtuellen Server abfragen, wird nur dieser virtuelle Server abgefragt. Die zugehörigen Entitäten wie Dienste, Dienstgruppen und Server werden nicht abgefragt. Wenn Sie alle zugehörigen Entitäten abfragen müssen, müssen Sie die Entitäten manuell abfragen oder die Instanz abfragen.

So fragen Sie bestimmte Entitäten in NetScaler Console ab:

Als Beispiel hilft Ihnen diese Aufgabe, Lastausgleichs-virtuelle Server abzufragen. Ebenso können Sie auch andere Netzwerkfunktionsentitäten abfragen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Network Functions > Load Balancing > Virtual Servers**.
2. Wählen Sie den virtuellen Server aus, dessen Status als **DOWN** angezeigt wird, und klicken Sie dann auf **Jetzt abfragen**. Der Status des virtuellen Servers ändert sich nun in **UP**.

Instanz entwalten

Wenn Sie den Informationsaustausch zwischen NetScaler Console und den Instanzen in Ihrem Netzwerk beenden möchten, können Sie die Instanzen entwalten.

So entwalten Sie eine Instanz:

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler**.
2. Wählen Sie die Registerkarte der NetScaler-Instanz (z. B. VPX).
3. Klicken Sie in der Liste der Instanzen entweder mit der rechten Maustaste auf eine Instanz und wählen Sie dann **Entwalten**, oder wählen Sie die Instanz aus und wählen Sie in der Liste **Aktion** die Option **Entwalten**.

   Der Status der ausgewählten Instanz ändert sich in **Außer Betrieb**.

   Die Instanz wird nicht mehr von NetScaler Console verwaltet und tauscht keine Daten mehr mit NetScaler Console aus.

Route zu einer Instanz verfolgen

Durch die Verfolgung der Route eines Pakets von der NetScaler Console zu einer Instanz können Sie Informationen wie die Anzahl der Hops ermitteln, die zum Erreichen der Instanz erforderlich sind. Der Traceroute verfolgt den Pfad des Pakets von der Quelle zum Ziel. Er zeigt die Liste der Netzwerk-Hops zusammen mit dem Hostnamen und der IP-Adresse jeder Entität in der Route an.

Traceroute zeichnet auch die Zeit auf, die ein Paket benötigt, um von einem Hop zum nächsten zu gelangen. Wenn es zu einer Unterbrechung der Paketübertragung kommt, zeigt der Traceroute an, wo das Problem liegt.

So verfolgen Sie die Route einer Instanz:

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler**.
2. Wählen Sie die Registerkarte der NetScaler-Instanz (z. B. VPX).
3. Klicken Sie in der Liste der Instanzen entweder mit der rechten Maustaste auf eine Instanz und wählen Sie dann **TraceRoute**, oder wählen Sie die Instanz aus und klicken Sie in der Liste **Action** auf **TraceRoute**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Das TraceRoute-Meldungsfeld zeigt die Route zur Instanz und die von jedem Hop verbrauchte Zeit in Millisekunden an.

NetScaler-eigene IP-Adressen anzeigen

Sie können die auf NetScaler-Instanzen konfigurierten IP-Adressen direkt über die NetScaler Console GUI anzeigen. Bitte beachten Sie, dass Konfigurationsänderungen und andere Vorgänge nur auf NetScaler-Instanzen durchgeführt werden können.

Um die NetScaler-eigenen IP-Adressen anzuzeigen, navigieren Sie zu **Infrastructure > Instances > NetScaler Owned IPs**.

Diese Funktion zeigt sowohl IPv4- als auch IPv6-Adressen an, die auf NetScaler-Instanzen konfiguriert sind. Die Typen von IP-Adressen umfassen:

- NetScaler IP-Adresse
- Subnetz-IP-Adresse
- Virtuelle IP-Adresse
- ADNS-Dienst-IP-Adresse
- GSLB-IP-Adresse
- Cluster-IP-Adresse
- Zugeordnete IP-Adresse

NetScaler-eigene IP-Adressen exportieren

Um NetScaler-eigene IP-Adressen zu exportieren, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler Owned IPs**.
2. Klicken Sie auf der Seite **NetScaler-eigene IPs** auf das Exportsymbol in der oberen rechten Ecke.
3. Klicken Sie auf der Seite **Berichte exportieren** auf **Jetzt exportieren**.
4. Wählen Sie auf der Seite **Jetzt exportieren** die Exportoption aus:

   Für den **Snapshot**-Export:

   a. Wählen Sie das Exportdateiformat aus: PDF, JPG oder PNG.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Für den **tabellarischen** Export:

a. Wählen Sie das Exportdateiformat aus: PDF oder CSV.
b. Wählen Sie die Anzahl der zu exportierenden Datensätze aus der Liste aus.

5. Klicken Sie auf **Exportieren**.

Export von NetScaler-eigenen IP-Adressen planen

Um den Export von NetScaler-eigenen IP-Adressen zu planen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler Owned IPs**.
2. Klicken Sie auf der Seite **NetScaler-eigene IPs** auf das Exportsymbol in der oberen rechten Ecke.
3. Klicken Sie auf der Seite **Exportberichte** auf **Export planen**.
4. Geben Sie auf der Seite **Export planen** die folgenden Details ein:

   a. Geben Sie den Betreff und die Beschreibung ein.
   b. Wählen Sie den Exporttyp aus.

      Für den Exporttyp **Snapshot**:

      - Wählen Sie das Exportdateiformat: PDF, JPG oder PNG.

      Für den Exporttyp **Tabellarisch**:

      - Wählen Sie das Exportdateiformat: PDF oder CSV.
      - Wählen Sie die Anzahl der zu exportierenden Datensätze aus der Liste aus.

   c. Wählen Sie die Wiederholung: Täglich, Wöchentlich oder Monatlich.
   d. Wählen Sie die Exportzeit aus.
   e. Wählen Sie aus, wie die exportierten IP-Adressen gesendet werden sollen: E-Mail, Slack oder beides.

      Für E-Mail:

      - Wählen Sie **E-Mail** aus und wählen Sie die E-Mail-Verteilerliste aus, um die Liste der NetScaler-eigenen IP-Adressen zu senden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Um eine E-Mail-Verteilerliste hinzuzufügen, klicken Sie auf **Hinzufügen** und geben Sie die E-Mail-Serverdetails an.
- Um eine E-Mail-Verteilerliste zu bearbeiten, klicken Sie auf **Bearbeiten**.
- Um zu überprüfen, ob die E-Mail-Verteilerliste funktioniert, klicken Sie auf **Testen**. Dadurch wird eine Test-E-Mail an die ausgewählte E-Mail-Verteilerliste gesendet.

Für Slack:

- Wählen Sie **Slack** aus und wählen Sie die Slack-Profilliste aus, um die Liste der NetScaler-eigenen IP-Adressen zu senden.
  - Um ein Slack-Profil hinzuzufügen, klicken Sie auf **Hinzufügen** und geben Sie den **Profilnamen**, den **Kanalnamen** und das **Token** des Slack-Kanals an.
  - Um einen vorhandenen Slack-Kanal zu bearbeiten, klicken Sie auf **Bearbeiten**.

5. Klicken Sie auf **Planen**, um den Export zu planen.

   Export planen(/en-us/netscaler-console-service/media/schedule-export.png)

Nach der Planung wird Ihr Exportzeitplan auf der Seite **Exportberichte** angezeigt, und Sie können den Zeitplan auswählen, um den Bearbeitungs- oder Löschvorgang durchzuführen.

Exportvorgänge planen(/en-us/netscaler-console-service/media/schedule-export-operations.png)

So ändern Sie das NetScaler MPX- oder VPX-Root-Passwort

Gelegentlich müssen Sie das Root-Passwort der NetScaler Appliance aus Sicherheitsgründen oder zur Einhaltung der Passwortrotationsrichtlinie ändern.

Dieses Dokument beschreibt die Schritte, die erforderlich sind, um das Root-Passwort der NetScaler MPX- und VPX-Appliances zu ändern, die über die NetScaler Console Cloud verwaltet werden.

Wenn Sie das NetScaler-Passwort ändern, müssen Sie das NetScaler Console-Administratorprofil ändern, das mit dem NetScaler verknüpft ist. Ein NetScaler Console-Administratorprofil verwaltet die NetScaler-Anmeldeinformationen für die REST-API-, SSH-, SCP- oder SNMP-basierte Kommunikation mit der NetScaler Appliance. Über Administratorprofile verwaltet NetScaler Console NetScaler MPX- und VPX-Appliances.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Passwort mit der Funktion „Konfigurationsaufträge“ ändern

Mit der Funktion „Konfigurationsaufträge“ von NetScaler Console können Sie den wiederholten Passwortänderungsprozess vereinfachen und die Änderungen auf die NetScaler Appliances anwenden, ohne auf die einzelnen Instanzen zugreifen zu müssen.

Führen Sie die folgenden Schritte aus, um das Passwort zu ändern:

- Schritt 1. Erstellen Sie eine Konfigurationsvorlage.
- Schritt 2. Erstellen Sie einen Konfigurationsauftrag.
- Schritt 3. Erstellen Sie ein Administratorprofil und ändern Sie es.

Hinweis:

> Wenn die NetScaler Appliances auch von anderen Tools verwaltet werden, müssen Sie die Anmeldeinformationen auch in diesen Tools ändern.

Konfigurationsvorlage erstellen

1. Navigieren Sie in der NetScaler Console-GUI zu **Infrastructure > Configuration > Configuration Templates**.
2. Wählen Sie **Hinzufügen**. Erstellen Sie eine Konfigurationsvorlage, indem Sie den SSH-Befehl `set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$` eingeben.

3. Wählen Sie die Variable $ROOT_USER_NAME$ aus, und wählen Sie **Textfeld als Typ** aus.
4. Geben Sie optional den Standardwert für den Root-Benutzernamen an. Wählen Sie **Fertig** aus, um die Variableneinstellungen zu speichern.

5. Wählen Sie die Variable $ROOT_USER_PASSWORD$ aus, und wählen Sie **Passwortfeld als Typ** aus. Wählen Sie **Fertig** aus, um die Variableneinstellungen zu speichern.
6. Wählen Sie **OK** aus, um die Konfigurationsvorlage zu speichern.
7. Die neue Konfigurationsvorlage wird unter **Konfigurationsvorlagen** angezeigt.

Konfigurationsauftrag erstellen

1. Navigieren Sie in der NetScaler Console-GUI zu **Infrastruktur > Konfigurationsaufträge**.
2. Wählen Sie **Auftrag erstellen** aus und klicken Sie auf das „+“-Symbol der neuen Konfigurationsvorlage. Wählen Sie **Weiter** aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Wählen Sie die NetScaler-Instanz oder -Instanzen aus, für die das Kennwort geändert werden muss.

4. Wählen Sie im Bereich **Instanzen auswählen** die Instanzen aus und klicken Sie auf **Weiter**.
5. Geben Sie im Bereich **Variablenwerte angeben** Werte für Benutzername und Kennwort an und klicken Sie auf **Weiter**.
6. Überprüfen Sie unter **Job Preview** die tatsächlichen CLI-Befehle, die die NetScaler Console auf den NetScaler-Instanzen ausführen wird. Wenn die Vorschau in Ordnung ist, klicken Sie auf **Next**.

7. Im Bereich **Execute** haben Sie die Wahl, den Job sofort auszuführen oder für später zu planen. Sie können den Job auch parallel auf allen ausgewählten Instanzen ausführen oder nacheinander. Wählen Sie „Finish“, nachdem Sie die Ausführungsdetails angegeben haben.
8. Der Konfigurations-Job zeigt an, ob die Ausführung erfolgreich war oder fehlgeschlagen ist.
9. Wählen Sie den **Job** aus und klicken Sie auf **Details**. Die Ausführungsdetails zeigen den Status auf individueller Instanzebene an.

Administratorprofil ändern

Nachdem Sie die NetScaler-Passwörter geändert haben, müssen Sie die Administratorprofile der Instanzen hinzufügen und ändern. Gehen Sie wie folgt vor:

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler**.
2. Klicken Sie auf **Profiles**, um alle Administratorprofile anzuzeigen.
3. Wählen Sie **Add**, um ein Administratorprofil zu erstellen und neue NetScaler-Anmeldeinformationen anzugeben.

4. Das neu erstellte Profil wird unter **Admin Profiles** angezeigt.
5. Gehen Sie zu **Network > Instances > NetScaler**. Wählen Sie die NetScaler-Instanz aus, für die das Passwort geändert wurde, und wählen Sie dann **Edit**.
6. Wählen Sie den neu erstellten Profilnamen aus und klicken Sie auf **OK**.

7. Wählen Sie die Instanz erneut aus, klicken Sie mit der rechten Maustaste und wählen Sie **Rediscover** aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instanz erneut erkennen(/en-us/netscaler-console-service/media/change-adc-root-password-16a.png)

Sie haben das Kennwort erfolgreich geändert.

Informationen zum Ändern des Kennworts einer SDX-Appliance finden Sie unter So ändern Sie ein NetScaler SDX-Root-Kennwort.

So ändern Sie ein NetScaler SDX nsroot-Passwort

Gelegentlich müssen Sie das nsroot-Passwort der NetScaler Appliance aus Sicherheitsgründen oder zur Einhaltung der Richtlinie zur Passwortrotation ändern.

Dieses Dokument beschreibt die erforderlichen Schritte zum Ändern des nsroot-Passworts einer NetScaler SDX Appliance, die über NetScaler Console Cloud verwaltet wird.

Wenn Sie das NetScaler-Passwort ändern, müssen Sie das NetScaler Console-Administratorprofil anpassen, das mit dem NetScaler verknüpft ist. Ein NetScaler Console-Administratorprofil verwaltet die NetScaler-Anmeldeinformationen für die REST-API-, SSH-, SCP- oder SNMP-basierte Kommunikation mit der NetScaler Appliance. Über Administratorprofile verwaltet NetScaler Console NetScaler SDX Appliances.

Passwort ändern

Führen Sie die folgenden Schritte aus, um das Passwort zu ändern:

- Schritt 1. Ändern Sie das SDX-Passwort über die SDX Management Service-GUI.
- Schritt 2. Ändern Sie das NetScaler Console-Administratorprofil, das mit der SDX verknüpft ist.

Hinweis:

> Wenn die SDX Appliance auch von anderen Tools verwaltet wird, müssen Sie die Anmeldeinformationen auch in diesen Tools ändern.

Ändern Sie das SDX-Passwort über die SDX Management Service-GUI

1. Navigieren Sie im SDX Management Service zu **System > Benutzerverwaltung > Benutzer**.
2. Wählen Sie den Benutzernamen aus, für den Sie das Passwort ändern möchten, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie **Passwort ändern**.
4. Geben Sie ein neues Passwort ein und klicken Sie auf **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Das SDX-Passwort wurde geändert.

NetScaler Console-Administratorprofil ändern

Nachdem Sie die SDX-Passwörter geändert haben, müssen Sie die Administratorprofile der Instanzen ändern. Gehen Sie wie folgt vor:

1. Navigieren Sie zu **Infrastructure > Instances Dashboard > NetScaler > SDX**.
2. Wählen Sie **Profile** aus, um alle Administratorprofile anzuzeigen.
3. Wählen Sie **Hinzufügen** aus, um ein Administratorprofil zu erstellen.
4. Geben Sie neue NetScaler-Anmeldeinformationen ein und klicken Sie auf **Erstellen**.

5. Das neu erstellte Profil wird unter **Administratorprofile** angezeigt.
6. Gehen Sie zu **Network > Instances > NetScaler > SDX**. Wählen Sie die Instanz aus, für die das Passwort geändert wurde, und wählen Sie dann **Bearbeiten**.
7. Wählen Sie den neu erstellten Profilnamen aus und klicken Sie auf **OK**.

8. Wählen Sie die Instanz erneut aus, klicken Sie mit der rechten Maustaste und dann auf **Neu erkennen**.

Sie haben das Passwort erfolgreich geändert.

Informationen zum Ändern des Passworts einer SDX-Appliance finden Sie unter So ändern Sie ein NetScaler MPX- oder VPX-Root-Passwort.

So generieren Sie ein technisches Support-Bundle für eine NetScaler®-Instanz

Um Probleme mit einer NetScaler-Instanz zu analysieren und zu beheben, können Sie auf der Instanz ein technisches Support-Bundle generieren und das Bundle an den technischen Support von Citrix senden. Das technische Support-Bundle ist ein gezipptes Tar-Archiv mit Systemkonfigurationsdaten und Statistiken. Das technische Support-Bundle sammelt die folgenden Daten von der NetScaler-Instanz, auf der Sie das Bundle generieren:

- Konfigurationsdateien. Alle Dateien im Verzeichnis /flash/nsconfig.
- `newnslog`-Dateien. Die aktuell ausgeführte `newnslog` und einige frühere Dateien. Um die Archivdateigröße zu minimieren, ist die `newnslog`-Sammlung auf 500 MB, 6 Dateien oder 7

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tage beschränkt, je nachdem, was zuerst eintritt. Wenn ältere Daten benötigt werden, kann eine manuelle Erfassung erforderlich sein.

- Protokolldateien. Dateien in /var/log/messages, /var/log/ns.log und andere Dateien unter /var/log und /var/nslog.
- Anwendungskern-Dateien. Dateien, die in der letzten Woche im Verzeichnis /var/core erstellt wurden, falls vorhanden.
- Ausgabe einiger CLI-Show-Befehle.
- Ausgabe einiger CLI-Stat-Befehle.
- Ausgabe von BSD-Shell-Befehlen.

Es ist obligatorisch, die Zeit für die Generierung von technischen Support-Dateien anzugeben. Sie müssen explizit einen Zeitbezug wählen, wenn Sie eine technische Support-Datei generieren. Sie können entweder die Option `custom` auswählen und ein benutzerdefiniertes Datum und eine Uhrzeit angeben oder die Option `Now` verwenden. Die Angabe der Zeit stellt sicher, dass der genaue Zeitkontext explizit definiert ist.

Der Zeitparameter gibt die Referenzzeit im Common Log Format an, die verwendet wird, um `newnslog`-Dateien zu finden. Das Format ist: `DD/MMM/YYYY:HH:MM:SS`.

Wenn die Zeit angegeben wird, werden bis zu vier `newnslog`-Protokolldateien gesammelt:

- Die `newnslog`-Datei entsprechend dem angegebenen Zeitbereich
- Die Protokolldatei, die unmittelbar vor der ersten Datei erstellt wurde (falls verfügbar)
- Die Protokolldatei, die unmittelbar nach der ersten Datei erstellt wurde (falls verfügbar)
- Das neueste `newnslog` Verzeichnis

HINWEIS:

Wenn der Bereich auf Cluster eingestellt ist, werden die zweite und dritte Protokolldatei auf keinem Knoten gesammelt.

Sie können das technische Support-Paket auch sicher auf den Citrix Technical Support Server hochladen. Ab NetScaler 14.1 Release 8.x Build müssen Sie ein Authentifizierungstoken generieren, bevor Sie das technische Support-Paket hochladen. In früheren Builds konnten Sie das technische Support-Paket mit Citrix Benutzernamen und Passwort hochladen.

So generieren Sie das Authentifizierungstoken:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Starten Sie einen Browser und geben Sie die folgende URL ein - `<https://cis.citrix.com/auth/api/create_identity_v2/?expiration=3600>`.
2. Melden Sie sich mit der Multi-Faktor-Authentifizierung an.

   HINWEIS:

   Informationen zur Registrierung für die Multi-Faktor-Authentifizierung finden Sie unter So registrieren Sie sich für die Multi-Faktor-Authentifizierung (MFA).

3. Klicken Sie auf **Kopieren**, um das auf dem Bildschirm angezeigte Authentifizierungstoken zu kopieren. Das Token ist 3600 Sekunden (1 Stunde) gültig. Die maximal zulässige Länge für das Token beträgt 1023 Zeichen.

Nach dem Kopieren des Authentifizierungstokens verwenden Sie die GUI, um die Datei hochzuladen.

So laden Sie das technische Support-Paket über die GUI hoch:

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler**.
2. Wählen Sie eine NetScaler-Instanz aus.
3. Wählen Sie **Generate Technical Support File** aus **Select Actions**.
4. Klicken Sie auf **Technische Supportdatei generieren**.
5. Verwenden Sie die Option **Bereich**, um anzugeben, ob Sie Daten auf dem aktuellen Knoten, allen Clusterknoten oder für die angegebenen Partitionen erfassen möchten.
6. Wählen Sie eine der folgenden Optionen aus **Zeitoption für technische Supportdaten auswählen**:
   - **Jetzt** – Verwendet die aktuelle Systemzeit und bewahrt das Verhalten früherer Versionen.
   - **Benutzerdefiniert** – Verwendet das angegebene Datum und die angegebene Uhrzeit.
7. Wählen Sie **Collector-Archiv hochladen**.
8. Geben Sie im Abschnitt **Mein Citrix-Konto** das Authentifizierungstoken in das Feld **Citrix-Authentifizierungstoken** ein.
9. Klicken Sie auf **Technischen Support erstellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ereignisse

Wenn die IP-Adresse einer Citrix Application Delivery Controller (NetScaler)-Instanz zu NetScaler Console hinzugefügt wird, sendet NetScaler Console einen NITRO-Aufruf und fügt sich implizit als Trap-Ziel für die Instanz hinzu, um deren Traps oder Ereignisse zu empfangen.

Ereignisse stellen das Auftreten von Ereignissen oder Fehlern auf einer verwalteten NetScaler-Instanz dar. Wenn beispielsweise ein Systemausfall oder eine Konfigurationsänderung auftritt, wird ein Ereignis generiert und auf dem NetScaler Console-Server aufgezeichnet. In NetScaler Console empfangene Ereignisse werden auf der Seite „Ereignisübersicht“ (**Infrastruktur > Ereignisse**) angezeigt, und alle aktiven Ereignisse werden auf der Seite „Ereignismeldungen“ (**Infrastruktur > Ereignisse > Ereignismeldungen**) angezeigt.

NetScaler Console prüft auch die auf Instanzen generierten Ereignisse, um Alarme unterschiedlicher Schweregrade zu bilden und diese als Meldungen anzuzeigen, von denen einige sofortige Aufmerksamkeit erfordern könnten. Beispielsweise kann ein Systemausfall als „kritisches“ Ereignis eingestuft und sofort behoben werden.

Sie können Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Regeln erleichtern die Überwachung verschiedener Ereignisse, die in Ihrer NetScaler-Infrastruktur generiert werden.

Sie können eine Reihe von Ereignissen filtern, indem Sie Regeln mit bestimmten Bedingungen konfigurieren und den Regeln Aktionen zuweisen. Wenn die generierten Ereignisse die Filterkriterien in der Regel erfüllen, wird die mit der Regel verknüpfte Aktion ausgeführt. Die Bedingungen, für die Sie Filter erstellen können, sind: Schweregrad, NetScaler-Instanzen, Kategorie, Fehlerobjekte, Konfigurationsbefehle und Meldungen.

Sie können auch sicherstellen, dass für ein Ereignis über ein bestimmtes Zeitintervall hinweg mehrere Benachrichtigungen ausgelöst werden, bis das Ereignis gelöscht ist. Als zusätzliche Maßnahme möchten Sie Ihre E-Mail möglicherweise mit einer bestimmten Betreffzeile und Benutzernachricht anpassen und einen Anhang hochladen.

Ereignis-Dashboard verwenden

Als Netzwerkadministrator können Sie Details wie Konfigurationsänderungen, Anmeldebedingungen, Hardwarefehler, Schwellenwertverletzungen und Entitätsstatusänderungen auf Ihren Citrix Application Delivery Controller (NetScaler)-Instanzen sowie Ereignisse und deren Schweregrad auf bestimmten Instanzen anzeigen. Sie können das Ereignis-Dashboard von NetScaler Console verwenden, um Berichte anzuzeigen, die für kritische Ereignisschweregrad-Details auf all Ihren NetScaler-Instanzen generiert wurden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So zeigen Sie die Details im Ereignis-Dashboard an:

Navigieren Sie zu **Infrastructure > Events > Reports**.

Das Diagramm „Top 10 Geräte“ auf dem Dashboard zeigt einen Bericht der Top-10-Instanzen nach der Anzahl der auf ihnen generierten Ereignisse an. Sie können auf eine Instanz im Diagramm klicken, um weitere Details zum Schweregrad des Ereignisses anzuzeigen.

Sie können weitere Details anzeigen, indem Sie zum NetScaler-Instanztyp navigieren (**Infrastructure > Events > Reports** > **NetScaler/ NetScaler SDX/ NetScaler**), um Folgendes anzuzeigen:

- Top 10 Geräte nach Hardwarefehler
- Top 10 Geräte nach Konfigurationsänderung
- Top 10 Geräte nach Authentifizierungsfehler
- Top 10 Geräte nach Entitätsstatusänderungen
- Top 10 Geräte nach Schwellenwertverletzung

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu exportieren, klicken Sie auf das Symbol **Exportieren** oben rechts auf dieser Seite. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren**. Um den Bericht im PDF-, JPEG-, PNG- oder CSV-Format anzuzeigen und zu speichern.
2. Wählen Sie die Registerkarte **Export planen**. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu versenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Wenn Sie die Wiederholung **Wöchentlich** auswählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie die Wiederholung **Monatlich** auswählen, stellen Sie sicher, dass Sie alle Tage, an denen der Bericht geplant werden soll, durch Kommas getrennt eingeben.

Ereignisregeln erstellen

Sie können Regeln konfigurieren, um bestimmte Ereignisse zu überwachen. Regeln erleichtern das Filtern der in Ihrer Infrastruktur generierten Ereignisse.

Sie können eine Reihe von Ereignissen filtern, indem Sie Regeln mit bestimmten Bedingungen konfigurieren und den Regeln Aktionen zuweisen. Wenn die generierten Ereignisse die Filterkriterien in der Regel erfüllen, wird die mit der Regel verknüpfte Aktion ausgeführt.

Sie können Filter für die folgenden Bedingungen erstellen:

- Schweregrad
- Citrix Application Delivery Controller (NetScaler)-Instanzen
- Kategorie
- Fehlerobjekte
- Konfigurationsbefehle
- Nachrichten

Nachdem Sie Ereignisse erstellt haben, können Sie den Ereignissen Aktionen zuweisen. Weitere Informationen finden Sie unter Ereignisregelaktionen hinzufügen.

Als Administrator möchten Sie beispielsweise Ereignisse mit „hoher CPU-Auslastung“ auf NetScaler-Instanzen überwachen, die zu einem Ausfall führen könnten. Sie können eine der folgenden Aktionen ausführen, um Benachrichtigungen zu erhalten:

- Erstellen Sie eine Regel zur Überwachung von Instanzen und fügen Sie der Regel eine Aktion hinzu, um Benachrichtigungen zu erhalten, wenn solche Ereignisse auftreten.
- Planen Sie eine Regel, um Instanzen in einem bestimmten Intervall zu überwachen. So erhalten Sie Benachrichtigungen, wenn solche Ereignisse innerhalb dieses Intervalls auftreten.

Die folgende Abbildung erläutert den Workflow, wie Ereignisregeln funktionieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ereignisregel konfigurieren

Um eine Ereignisregel zu konfigurieren, navigieren Sie zu **Infrastructure > Events > Rules** und klicken Sie auf **Add**. Führen Sie auf der Seite **Create Rule** die folgenden Aufgaben aus:

1. Namen und Instanzfamilie angeben
2. Ereignisalter konfigurieren
3. Schweregrad des Ereignisses auswählen, das die Regel erkennt
4. Kategorie des Ereignisses angeben
5. NetScaler®-Instanzen angeben, für die die Regel gilt
6. Fehlerobjekte auswählen
7. Erweiterte Filter angeben
8. Aktionen angeben, die ausgeführt werden sollen, wenn die Regel ein Ereignis erkennt

Schritt 1 — Namen und Instanzfamilie angeben

1. **Name**. Geben Sie einen Namen für die Ereignisregel ein.
2. **Instanzfamilie**. Wählen Sie eine Instanzfamilie aus der Dropdown-Liste **Instanzfamilie** aus.

   Sie können Ereignisregeln nach **Instanzfamilie** filtern, um die NetScaler-Instanz zu verfolgen, von der NetScaler Console ein Ereignis empfängt.

Schritt 2 – Ereignisalter konfigurieren

1. **Ereignisalter**. Geben Sie das Zeitintervall (in Sekunden) an, nach dem NetScaler Console eine Ereignisregel aktualisiert.

   Sie möchten beispielsweise, dass jedes Mal eine E-Mail gesendet wird, wenn Ihre NetScaler-Instanz 60 Sekunden oder länger ein Ereignis mit „hoher CPU-Auslastung“ aufweist. Sie können das Ereignisalter auf 60 Sekunden einstellen. Immer wenn Ihre NetScaler-Instanz 60 Sekunden oder länger ein Ereignis mit „hoher CPU-Auslastung“ aufweist, erhalten Sie eine E-Mail-Benachrichtigung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Ereignisalter ist ein Pflichtfeld. Der Mindestwert für das Ereignisalter beträgt 60 Sekunden. Wenn Sie das Feld **Ereignisalter** leer lassen, wird die Ereignisregel sofort nach dem Auftreten des Ereignisses angewendet.

2. Wählen Sie eine der folgenden Optionen, um Ihre Ereignisse zu verfolgen:

   - **Ereignisprotokollierung überspringen, bis das Ereignisalter erreicht ist**. Ereignisse, die vor dem angegebenen Ereignisalter auftreten, werden nicht in der NetScaler Console-Serverdatenbank protokolliert. Wenn das Ereignisalter erreicht ist, werden Ereignisse in der Datenbank protokolliert und konfigurierte Ereignisaktionen ausgelöst.
   - **Ereignisse sofort protokollieren, unabhängig von der Dauer des Ereignisalters**. Alle Ereignisse werden unabhängig vom angegebenen Ereignisalter in der NetScaler Console-Serverdatenbank protokolliert. Nachdem das Ereignisalter erreicht ist, werden konfigurierte Ereignisaktionen ausgelöst.

3. **Erweiterten Filter mit Regex-Matching aktivieren**. Wählen Sie diese Option, um einen regulären Ausdruck außer dem Sternchen-Musterabgleich (*) einzuschließen. Diese Option ist für Fehlerobjekte, Konfigurationsbefehle und Nachrichten anwendbar.

Schritt 3 – Schweregrad des Ereignisses auswählen

- Wählen Sie im Abschnitt **Schweregrad** einen Schweregrad für Ihre Ereignisregel aus.

  Sie können die folgenden Schweregrade definieren: Kritisch, Schwerwiegend, Geringfügig, Warnung, Gelöscht und Information.

  HINWEIS:

  Sie können die Schwere für generische und Advanced-spezifische Ereignisse konfigurieren. Um die Ereignisschwere für NetScaler-Instanzen zu ändern, die auf NetScaler Console verwaltet werden, navigieren Sie zu **Infrastructure > Events > Event Settings**. Wählen Sie die **Kategorie** aus, für die Sie die Ereignisschwere konfigurieren möchten, und klicken Sie auf **Configure Severity**. Weisen Sie eine neue Schweregradstufe zu und klicken Sie auf **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schritt 4 – Ereigniskategorie angeben

Sie können die Kategorie oder Kategorien der von Ihren NetScaler-Instanzen generierten Ereignisse angeben. Alle Kategorien werden auf NetScaler-Instanzen erstellt. Diese Kategorien werden dann der NetScaler Console zugeordnet, die zur Definition von Ereignisregeln verwendet werden kann.

- Wählen Sie die Kategorie aus, die Sie berücksichtigen möchten, und verschieben Sie sie von der Tabelle **Verfügbar** in die Tabelle **Konfiguriert**.

  Im Beispiel müssen Sie „cpuUtilization“ als Ereigniskategorie aus der angezeigten Tabelle auswählen.

Schritt 5 – NetScaler-Instanzen angeben

Führen Sie im Abschnitt **Instanzen** folgende Schritte aus:

1. Klicken Sie auf **Instanzen auswählen**. Wählen Sie auf der Seite **Instanzen auswählen** die IP-Adressen der NetScaler-Instanzen aus, für die Sie die Ereignisregel definieren möchten.
2. Klicken Sie auf **Auswählen**.

Schritt 6 – Fehlerobjekte auswählen

Fehlerobjekte sind Entitätsinstanzen oder Zähler, für die ein Ereignis generiert wurde.

1. Klicken Sie auf **Fehlerobjekte auswählen**.
2. Wählen Sie auf der Seite **Fehlerobjekte** ein Fehlerobjekt aus der Liste aus. Klicken Sie auf **Auswählen**.
3. Um ein Fehlerobjekt hinzuzufügen, geben Sie einen regulären Ausdruck unter **Fehlerobjekte hinzufügen** ein. Abhängig vom angegebenen regulären Ausdruck werden die Fehlerobjekte automatisch zur Liste hinzugefügt.

   WICHTIG:

   Um Fehlerobjekte mithilfe eines regulären Ausdrucks aufzulisten, wählen Sie in Schritt 1 die Option **Erweiterten Filter mit Regex-Abgleich aktivieren**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Der erweiterte Filter ermöglicht es Ihnen, Probleme bei den Fehlerobjekten schnell zu verfolgen und die Ursache für ein Problem zu identifizieren. Wenn ein Benutzer beispielsweise Anmeldeprobleme hat, ist das Fehlerobjekt der Benutzername oder das Kennwort, wie z. B. `nsroot`.

4. Um Entitäten hinzuzufügen, wählen Sie eine Entität aus **Entitäten auswählen**.

   Diese Liste kann Zählernamen für alle schwellenwertbezogenen Ereignisse, Entitätsnamen für alle entitätsbezogenen Ereignisse, Zertifikatsnamen für zertifikatsbezogene Ereignisse usw. enthalten.

Schritt 7 – Erweiterte Filter angeben

Sie können eine Ereignisregel mit erweiterten Filtern weiter filtern. Wählen Sie einen der folgenden Filter aus:

- **Konfigurationsbefehle** – Geben Sie den vollständigen Konfigurationsbefehl an oder geben Sie einen regulären Ausdruck an, um Ereignisse zu filtern.

  Sie können die Ereignisregeln auch nach dem Authentifizierungsstatus des Befehls und dessen Ausführungsstatus filtern. Geben Sie beispielsweise für einen `NetscalerConfigChange event` Folgendes ein: `[.]*bind system global policy_name[.]*`.

- **Meldungen** – Geben Sie die vollständige Meldungsbeschreibung an oder geben Sie einen regulären Ausdruck an, um die Ereignisse zu filtern.

  Geben Sie beispielsweise für ein `NetscalerConfigChange` Ereignis Folgendes ein: `[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress : \^([.]*10.122.132.142[.]*)`.

WICHTIG:

Um Konfigurationsbefehle und -meldungen mithilfe regulärer Ausdrücke zu filtern, die nicht der Sternchen-(*)-Musterübereinstimmung entsprechen, wählen Sie **Erweiterten Filter mit Regex-Abgleich aktivieren** in Schritt 1.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schritt 8 - Ereignisregelaktionen hinzufügen

Sie können Ereignisregelaktionen hinzufügen, um Benachrichtigungsaktionen für ein Ereignis zuzuweisen. Diese Benachrichtigungen werden gesendet oder ausgeführt, wenn ein Ereignis die definierten Filterkriterien erfüllt, die Sie in Schritt 7 festgelegt haben.

1. Klicken Sie auf **Aktion hinzufügen**.
2. Auf der Seite **Ereignisaktion hinzufügen** können Sie die folgenden Ereignisaktionen hinzufügen:

- E-Mail-Aktion senden
- Trap-Aktion senden
- Befehlsaktion ausführen
- Job-Aktion ausführen
- Aktion unterdrücken
- Slack-Benachrichtigungen senden
- PagerDuty-Benachrichtigungen senden
- ServiceNow-Benachrichtigungen senden

Aktion: E-Mail senden

Wenn Sie **E-Mail senden-Aktion** auswählen, wird eine E-Mail ausgelöst, wenn die Ereignisse die definierten Filterkriterien erfüllen.

1. **E-Mail-Verteilerliste**. Wählen Sie eine E-Mail-Verteilerliste aus. Um eine Verteilerliste hinzuzufügen, klicken Sie auf Hinzufügen.
    a. Führen Sie auf der Seite **E-Mail-Verteilerliste erstellen** die folgenden Schritte aus:
        i. **Name**. Fügen Sie einen Namen für die Verteilerliste hinzu.
        ii. **E-Mail-Server**. Wählen Sie einen E-Mail-Server aus. Sie können auch einen Server hinzufügen oder einen vorhandenen bearbeiten.
        iii. **Von**. Fügen Sie die E-Mail-Adresse des Absenders hinzu.
        iv. **An**. Fügen Sie die E-Mail-Adressen der Empfänger hinzu. Sie können auch angeben, dass die E-Mail-Adressen in die CC- und Bcc-Liste aufgenommen werden sollen.
        v. Klicken Sie auf **Erstellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **Betreff**. Fügen Sie eine Betreffzeile für Ihre E-Mails hinzu, z. B. den Namen der betroffenen Entität, d. h. den Namen des Fehlerobjekts. Diese Betreffzeile enthält Informationen über den virtuellen Server, auf dem diese Ereignisse auftreten.

   HINWEIS:

   Wenn Sie keine Betreffzeile hinzufügen, wird eine Standardbetreffzeile angezeigt. Die Standardbetreffzeile enthält nur Informationen über den Schweregrad des Ereignisses, die Kategorie des Ereignisses und das Fehlerobjekt. Der Name des virtuellen Servers, auf dem das Ereignis aufgetreten ist, ist nicht verfügbar.

3. **Anhang**. Laden Sie einen Anhang zu Ihrer E-Mail hoch. Dieser Anhang wird gesendet, wenn ein eingehendes Ereignis der konfigurierten Regel entspricht.
4. **Test**. Klicken Sie auf diese Schaltfläche, um eine Test-E-Mail zu senden, nachdem Sie einen E-Mail-Server, zugehörige Verteilerlisten und andere Einstellungen konfiguriert haben. Diese Option ermöglicht es Ihnen, die konfigurierten Einstellungen zu testen.
5. **E-Mail-Benachrichtigung wiederholen, bis das Ereignis behoben ist**. Wählen Sie diese Option, um sicherzustellen, dass E-Mail-Benachrichtigungen für kritische Ereignisse nicht übersehen werden. Diese Option sendet wiederholte E-Mails für Ereignisregeln, die die von Ihnen ausgewählten Kriterien erfüllen. Wenn Sie beispielsweise eine Ereignisregel für Instanzen erstellt haben, die Festplattenfehler betreffen, und Sie benachrichtigt werden möchten, bis das Problem behoben ist, wählen Sie die Option, wiederholte E-Mail-Benachrichtigungen zu diesen Ereignissen zu erhalten.

6. Klicken Sie auf **OK**.

HINWEIS:

Sie können die E-Mail-Verteilerlisten auch hinzufügen, indem Sie zu **Settings** > **Notifications** > **Email** navigieren. Klicken Sie auf **Add** und erstellen Sie die Liste.

Trap-Aktion senden

Wenn Sie den Ereignisaktionstyp **Trap-Aktion senden** auswählen, werden SNMP-Traps an ein externes Trap-Ziel gesendet oder weitergeleitet. Die Trap-Nachrichten werden an den spezifischen Trap-Listener gesendet, wenn Ereignisse die definierten Filterkriterien erfüllen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **Trap-Verteilerliste**. Wählen Sie eine Trap-Verteilerliste (oder ein Trap-Ziel und Trap-Profildetails) aus. Um eine Trap-Verteilerliste zu erstellen, klicken Sie auf **Hinzufügen**.
2. Auf der Seite **Trap-Verteilerliste erstellen** führen Sie die folgenden Schritte aus:
   a. **Profilname**. Geben Sie den Profilnamen ein.
   b. **Trap-Ziel**. Geben Sie den Namen oder die IP-Adresse der Instanz ein, die die Trap-Nachrichten empfangen soll.
   c. **Portnummer des SNMP-Traps**. Geben Sie die Portnummer ein.
   d. **Trap-Community**. Geben Sie die Gruppe ein, zu der die Instanz gehört.

   e. Klicken Sie auf **Erstellen**.
3. Klicken Sie auf **OK**.

Aktion „Befehl ausführen“

Wenn Sie die Ereignisaktion **Befehl ausführen** wählen, können Sie einen Befehl oder ein Skript erstellen, das auf NetScaler Console für Ereignisse ausgeführt werden kann, die einem bestimmten Filterkriterium entsprechen.

Sie können auch die folgenden Parameter für das Skript **Befehl ausführen** festlegen:

Parameter	Beschreibung
$Quelle	Dieser Parameter entspricht der Quell-IP-Adresse des empfangenen Ereignisses.
$Kategorie	Dieser Parameter entspricht dem Typ der Traps, die unter der Kategorie des Filters definiert sind.
$Entität	Dieser Parameter entspricht den Entitätsinstanzen oder Zählern, für die ein Ereignis generiert wurde. Er kann die Zählernamen für alle schwellenwertbezogenen Ereignisse, Entitätsnamen für alle entitätsbezogenen Ereignisse und Zertifikatsnamen für alle zertifikatsbezogenen Ereignisse enthalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

$Schweregrad	Dieser Parameter entspricht dem Schweregrad des Ereignisses.
$Fehlerobjekt	Das Fehlerobjekt beeinflusst die Verarbeitung eines Ereignisses und stellt sicher, dass das Fehlerobjekt das genaue Problem wie gemeldet anzeigt. Dies kann verwendet werden, um Probleme schnell zu verfolgen und den Grund für den Fehler zu identifizieren, anstatt nur Rohereignisse zu melden.

HINWEIS:

Während der Befehlsausführung werden diese Parameter durch tatsächliche Werte ersetzt.

Angenommen, Sie möchten eine Ausführungsbefehlsaktion festlegen, wenn der Status eines Lastausgleichs-Virtual-Servers **Down** ist. Als Administrator möchten Sie möglicherweise eine schnelle Problemumgehung bereitstellen, indem Sie einen weiteren virtuellen Server hinzufügen. In NetScaler Console können Sie:

- Eine Skriptdatei (.sh) schreiben.

  Das Folgende ist eine Beispielskriptdatei (.sh):

```
#!/bin/sh

source=$1

failureobj=$2

payload='{"params":{"warning":"YES"},"lbvserver":
{"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","port":"
80","td":"","m":"IP","state":"ENABLED","rhistate":"PASSIVE","appflowlog
":"ENABLED","

bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":""}}'

url="http://$source/nitro/v1/config/lbvserver"

curl --insecure -basic -u nsroot:nsroot -H "Content-type: application/
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
json" -X POST -d $payload $url
```

- Speichern Sie die .sh-Datei an einem beliebigen persistenten Speicherort auf dem Agenten. Zum Beispiel: `/var`.
- Geben Sie den Speicherort der .sh-Datei in NetScaler Console an, die ausgeführt werden soll, wenn die Regelkriterien erfüllt sind.

1. Klicken Sie unter **Befehlsausführungsliste** auf **Hinzufügen**.

   Die Seite „Befehlsverteilungsliste erstellen“ wird angezeigt.

   a. **Profilname**. Geben Sie einen Namen Ihrer Wahl an.

   b. **Befehl ausführen**. Geben Sie den Speicherort des Agenten an, an dem das Skript ausgeführt werden soll. Zum Beispiel: `sh/var/demo.sh $source $failureobj`.

   c. Wählen Sie **Ausgabe anhängen** und **Fehler anhängen** aus.

   HINWEIS:

   Sie können die Optionen **Ausgabe anhängen** und **Fehler anhängen** aktivieren, wenn Sie die generierte Ausgabe und Fehler (falls vorhanden) speichern möchten, wenn Sie ein Befehlsskript in den NetScaler Console-Serverprotokolldateien ausführen. Wenn Sie diese Optionen nicht aktivieren, verwirft NetScaler Console alle Ausgaben und Fehler, die während der Ausführung des Befehlsskripts generiert werden.

   d. Klicken Sie auf **Erstellen**.

2. Klicken Sie auf der Seite **Ereignisaktion hinzufügen** auf **OK**.

HINWEIS:

Sie können die Optionen **Ausgabe anhängen** und **Fehler anhängen** aktivieren, wenn Sie die generierten Ausgaben und Fehler (falls vorhanden) speichern möchten, wenn Sie ein Befehlsskript in den NetScaler Console Server-Protokolldateien ausführen. Wenn Sie diese Optionen nicht aktivieren, verwirft NetScaler Console alle Ausgaben und Fehler, die während der Ausführung des Befehlsskripts generiert werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Auftragsaktion ausführen

Wenn Sie ein Profil mit Konfigurationsaufträgen erstellen, wird ein Auftrag als integrierter Auftrag oder als benutzerdefinierter Auftrag für NetScaler- und NetScaler SDX-Instanzen für Ereignisse und Alarme ausgeführt, die den von Ihnen angegebenen Filterkriterien entsprechen.

1. Wählen Sie in der **Auftragsprofilliste** ein Auftragsprofil aus. Um eine Liste hinzuzufügen, klicken Sie auf **Hinzufügen**.
2. Führen Sie auf der Seite **Auftrag erstellen** die folgenden Schritte aus:

   a. **Auftrag auswählen**. Erstellen Sie ein Profil mit einem Auftrag, den Sie ausführen möchten, wenn die Ereignisse die definierten Filterkriterien erfüllen. Geben Sie einen Profilnamen, den Instanztyp, die Konfigurationsvorlage und die auszuführende Aktion an, falls die Befehle des Auftrags fehlschlagen.

   b. **Variablenwerte angeben**. Geben Sie basierend auf dem ausgewählten Instanztyp und der gewählten Konfigurationsvorlage Ihre Variablenwerte an.

   c. Klicken Sie auf **Fertig stellen**, um den Auftrag zu erstellen.

3. Klicken Sie auf **OK**.

Aktion unterdrücken

- Geben Sie unter **Unterdrückungszeit** einen Zeitraum in Minuten ein, für den ein Ereignis unterdrückt oder verworfen wird. Sie können das Ereignis für mindestens 1 Minute unterdrücken.

  HINWEIS:

  Sie können die Unterdrückungszeit auch auf 0 Minuten konfigurieren, was unendlich bedeutet. Wenn Sie keine Zeitdauer angeben, betrachtet NetScaler Console die Unterdrückungszeit als Null, und sie läuft nie ab.

Slack-Benachrichtigungen senden

Wenn Sie einen Slack-Kanal konfigurieren, werden die Ereignisbenachrichtigungen an diesen Kanal gesendet. Sie können viele Slack-Kanäle konfigurieren, um diese Benachrichtigungen zu erhalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Wählen Sie in **Slack-Profilliste** ein Slack-Profil aus. Um ein Slack-Profil hinzuzufügen, klicken Sie auf **Hinzufügen**.
2. Führen Sie auf der Seite **Slack-Profil erstellen** die folgenden Schritte aus:
    a. **Profilname**. Geben Sie einen Namen für die Profilliste ein, die in NetScaler Console konfiguriert werden soll.
    b. **Kanalname**. Geben Sie den Namen des Slack-Kanals ein, an den die Ereignisbenachrichtigungen gesendet werden sollen.
    c. **Webhook-URL**. Geben Sie die Webhook-URL des von Ihnen eingegebenen Kanals ein. Eingehende Webhooks sind eine einfache Möglichkeit, Nachrichten von externen Quellen in Slack zu posten. Die URL ist intern mit dem Kanalnamen verknüpft. Alle Ereignisbenachrichtigungen werden an diese URL gesendet und dann an den ausgewählten Slack-Kanal gepostet. Ein Beispiel für einen Webhook ist wie folgt: `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`
    d. Klicken Sie auf **Erstellen**.
3. Klicken Sie auf **OK**.

HINWEIS:

Sie können die Slack-Profile auch hinzufügen, indem Sie zu **Einstellungen** > **Benachrichtigungen** > **Slack-Profile** navigieren. Klicken Sie auf **Hinzufügen** und erstellen Sie das Profil.

PagerDuty-Benachrichtigungen senden

Sie können ein PagerDuty-Profil als Option in NetScaler Console hinzufügen, um die Benachrichtigungen über Vorfälle basierend auf Ihren PagerDuty-Konfigurationen zu überwachen. PagerDuty ermöglicht es Ihnen, Benachrichtigungen per E-Mail, SMS, Push-Benachrichtigung und Telefonanruf an eine registrierte Nummer zu konfigurieren.

1. Wählen Sie in der **PagerDuty-Profilliste** ein PagerDuty-Profil aus. Um ein Profil hinzuzufügen, klicken Sie auf **Hinzufügen**.
2. Auf der Seite **PagerDuty-Profil erstellen**:
    a. **Profilname**. Geben Sie einen Profilnamen Ihrer Wahl ein.
    b. **Integrationsschlüssel**. Geben Sie den Integrationsschlüssel ein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie erhalten den Integrationsschlüssel über Ihr PagerDuty-Portal.

c. Klicken Sie auf **Erstellen**.

Bevor Sie ein PagerDuty-Profil in NetScaler Console hinzufügen, stellen Sie sicher, dass Sie die erforderlichen Konfigurationen in PagerDuty abgeschlossen haben. Weitere Informationen finden Sie in der PagerDuty-Dokumentation.

Sie können Ihr PagerDuty-Profil als eine der Optionen auswählen, um Benachrichtigungen für die folgenden Funktionen zu erhalten:

- **Ereignisse** – Liste der Ereignisse, die für NetScaler-Instanzen generiert werden.
- **Lizenzen** – Liste der Lizenzen, die derzeit aktiv sind, bald ablaufen usw.
- **SSL-Zertifikate** – Liste der SSL-Zertifikate, die zu NetScaler-Instanzen hinzugefügt werden.

Anwendungsfall:

Betrachten Sie ein Szenario, in dem Sie Folgendes tun möchten:

- Benachrichtigungen an Ihr PagerDuty-Profil senden.
- Konfigurieren Sie einen Telefonanruf als Option in PagerDuty, um Benachrichtigungen zu erhalten.
- Telefonanruf-Benachrichtigungen für NetScaler-Ereignisse erhalten.

Erstellen Sie die PagerDuty-Konfiguration. Nachdem die Konfiguration abgeschlossen ist, erhalten Sie immer dann einen Telefonanruf, wenn ein neues Ereignis für die NetScaler-Instanz generiert wird. Über den Telefonanruf können Sie entscheiden, ob Sie:

- Das Ereignis bestätigen
- Es als gelöst markieren
- An ein anderes Teammitglied eskalieren

ServiceNow-Benachrichtigungen senden

Sie können ServiceNow-Vorfälle für NetScaler Console-Ereignisse automatisch generieren, indem Sie das ServiceNow-Profil in der NetScaler Console-GUI auswählen. Sie müssen das **ServiceNow**-Profil in NetScaler Console auswählen, um eine Ereignisregel zu konfigurieren.

Bevor Sie eine Ereignisregel konfigurieren, um ServiceNow-Vorfälle automatisch zu generieren, integrieren Sie die NetScaler Console in die ServiceNow-Instanz. Weitere Informationen finden Sie unter ITSM-Adapter für ServiceNow konfigurieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Wählen Sie unter **ServiceNow-Profil** das Profil **Citrix_Workspace_SN** aus der Liste aus.
2. Klicken Sie auf **OK**.

Einen Ereignisfilter planen

Nachdem Sie einen Filter für Ihre Regel erstellt haben, können Sie den Filter so planen, dass er nur in bestimmten Zeitintervallen wie täglich, wöchentlich oder monatlich ausgelöst wird, wenn die NetScaler Console nicht jedes Mal eine Benachrichtigung senden soll, wenn das generierte Ereignis die Filterkriterien erfüllt.

Wenn Sie beispielsweise eine Systemwartungsaktivität für verschiedene Anwendungen auf Ihren Instanzen zu unterschiedlichen Zeiten geplant haben, können die Instanzen mehrere Alarme generieren.

Wenn Sie einen Filter für diese Alarme konfiguriert und E-Mail-Benachrichtigungen für diese Filter aktiviert haben, sendet der Server viele E-Mail-Benachrichtigungen, wenn die NetScaler Console diese Traps empfängt. Wenn Sie möchten, dass der Server diese E-Mail-Benachrichtigungen nur während eines bestimmten Zeitraums sendet, können Sie dies durch die Planung eines Filters tun.

So planen Sie einen Filter mit NetScaler Console:

1. Navigieren Sie in der NetScaler Console zu **Infrastructure > Events > Rules**.
2. Wählen Sie die Regel aus, für die Sie einen Filter planen möchten, und klicken Sie auf **View Schedule**.
3. Klicken Sie auf der Seite **Scheduled Rule** auf **Schedule** und geben Sie die folgenden Parameter an:
    - **Regel aktivieren** – Aktivieren Sie dieses Kontrollkästchen, um die geplante Ereignisregel zu aktivieren.
    - **Wiederholung** – Intervall, in dem die Regel geplant werden soll.
    - **Geplantes Zeitintervall (Stunden)** – Stunden, zu denen die Regel geplant werden soll (verwenden Sie das 24-Stunden-Format).
4. Klicken Sie auf **Schedule**.

Berichtete Schweregrade von Ereignissen, die auf NetScaler-Instanzen auftreten, ändern

Sie können die Berichterstellung von Ereignissen verwalten, die auf all Ihren Geräten generiert werden, sodass Sie Ereignisdetails zu einem bestimmten Ereignis auf einer Instanz anzeigen und

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Berichte basierend auf dem Ereignisschweregrad anzeigen können. Außerdem können Sie Ereignisregeln erstellen, die die Standard-Schweregradeinstellungen verwenden, und Sie können die Schweregradeinstellungen ändern. Sie können den Schweregrad sowohl für generische als auch für unternehmensspezifische Ereignisse konfigurieren.

Sie können die folgenden Schweregrade definieren: Kritisch, Schwerwiegend, Geringfügig, Warnung und Gelöscht.

So ändern Sie den Ereignisschweregrad:

1. Navigieren Sie zu **Infrastructure > Events > Event Settings**.
2. Klicken Sie auf die Registerkarte für den NetScaler-Instanztyp, den Sie ändern möchten. Wählen Sie dann die Kategorie aus der Liste aus und klicken Sie auf **Configure Severity**.
3. Wählen Sie unter **Configure Event Severity** den Schweregrad aus der Dropdown-Liste aus.
4. Klicken Sie auf **OK**.

Ereignisübersicht anzeigen

Sie können jetzt eine Seite mit der Ereignisübersicht anzeigen, um die auf Ihrer NetScaler Console empfangenen Ereignisse und Traps zu überwachen. Navigieren Sie zu **Infrastruktur > Ereignisse**. Die Seite „Ereignisübersicht“ zeigt die folgenden Informationen in Tabellenform an:

- **Zusammenfassung aller von NetScaler Console empfangenen Ereignisse**. Die Ereignisse sind nach Kategorie aufgelistet, und die verschiedenen Schweregrade werden in unterschiedlichen Spalten angezeigt: Kritisch, Schwerwiegend, Geringfügig, Warnung, Gelöscht und Information. Beispielsweise tritt ein kritisches Ereignis auf, wenn eine Citrix Application Delivery Controller (NetScaler)-Instanz ausfällt und keine Informationen mehr an die NetScaler Console sendet. Während des Ereignisses wird eine Benachrichtigung an einen Administrator gesendet, die den Grund für den Ausfall der Instanz, die Dauer des Ausfalls usw. erläutert. Das Ereignis wird dann auf der Seite „Ereignisübersicht“ aufgezeichnet, auf der Sie die Zusammenfassung anzeigen und auf die Details des Ereignisses zugreifen können.

- **Anzahl der für jede Kategorie empfangenen Traps**. Die Anzahl der empfangenen Traps, nach Schweregrad kategorisiert. Standardmäßig hat jeder von NetScaler-Instanzen an NetScaler Console gesendete Trap einen zugewiesenen Schweregrad, aber als Netzwerkadministrator können Sie dessen Schweregrad in der NetScaler Console-GUI festlegen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Sie auf einen Kategorietyp oder einen Trap klicken, gelangen Sie zur Seite **Ereignisse**, auf der Filter wie Kategorie und Schweregrad vorausgewählt sind. Diese Seite zeigt weitere Informationen zum Ereignis an, wie z. B. die IP-Adresse und den Hostnamen einer NetScaler-Instanz, das Datum des Trap-Empfangs, die Kategorie, Fehlerobjekte, den ausgeführten Konfigurationsbefehl und die Nachrichtenbenachrichtigung.

Sie können die Anzahl der Tage zwischen 1 und 40 konfigurieren, für die Sie die Ereignisse in NetScaler Console anzeigen möchten. Wenn Sie beispielsweise 30 Tage auswählen, zeigt NetScaler Console die Ereignisse für 30 Tage an, und nach 30 Tagen werden die Ereignisse gelöscht. Um diese Ereigniseinstellung zu konfigurieren, navigieren Sie zu **Einstellungen > Globale Einstellungen > Datenaufbewahrungsrichtlinie**. Weitere Informationen finden Sie unter Datenaufbewahrungsrichtlinie.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu exportieren, klicken Sie auf das Symbol **Exportieren** oben rechts auf dieser Seite. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren**. Um den Bericht im PDF-, JPEG-, PNG- oder CSV-Format anzuzeigen und zu speichern.
2. Wählen Sie die Registerkarte **Export planen**. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu senden.

HINWEIS:

- Wenn Sie die Option **Wöchentlich** für die Wiederholung auswählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie die Option **Monatlich** für die Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage, an denen der Bericht geplant werden soll, durch Kommas getrennt eingeben.

Ereignismeldungen

Alle aktiven Ereignisse, die in NetScaler® Console empfangen werden, werden auf der Seite **Infrastruktur > Ereignisse > Ereignismeldungen** angezeigt.

Auf der Seite **Ereignismeldungen** können Sie die Liste der Instanzen und die Details der Ereignisse anzeigen, z. B. Schweregrad, Kategorie, Datum des Ereignisses und das Fehlerobjekt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können die Ereignisse nach dem Zeitpunkt filtern, zu dem sie aufgetreten sind, z. B. in den letzten 30 Minuten, 1 Stunde, 1 Tag. Sie können auch eine benutzerdefinierte Zeit nach Ihren Wünschen auswählen.

NetScaler Console unterstützt benutzerdefinierte SNMP-Traps, die unter **Ereignismeldungen** als **benutzerdefiniert** gekennzeichnet sind. Das Tag **benutzerdefiniert** hilft Ihnen, sie von den Standard-SNMP-Warnungen zu unterscheiden.

Ereignisschweregrade und SNMP-Trap-Details anzeigen

Wenn Sie ein Ereignis und dessen Einstellungen in NetScaler Console erstellen, können Sie das Ereignis sofort auf der Seite „Ereignisübersicht“ anzeigen. Ebenso können Sie den Zustand, die Betriebszeit, die Modelle und die Versionen aller Citrix Application Delivery Controller (NetScaler)-Instanzen, die Ihrem NetScaler Console-Server hinzugefügt wurden, im Detail auf dem Infrastruktur-Dashboard anzeigen und überwachen.

Auf dem Infrastruktur-Dashboard können Sie jetzt irrelevante Werte maskieren, damit Sie Informationen wie Ereignisse nach Schweregraden, Zustand, Betriebszeit, Modelle und Version von NetScaler-Instanzen im Detail leichter anzeigen und überwachen können.

Zum Beispiel treten Ereignisse mit dem Schweregrad **Kritisch** möglicherweise selten auf. Wenn diese kritischen Ereignisse jedoch in Ihrem Netzwerk auftreten, möchten Sie möglicherweise weiter untersuchen, Fehler beheben und überwachen, wo und wann das Ereignis aufgetreten ist. Wenn Sie alle Schweregrade außer Kritisch auswählen, zeigt das Diagramm nur das Auftreten kritischer Ereignisse an. Wenn Sie auf das Diagramm klicken, gelangen Sie zur Seite **Schweregradbasierte Ereignisse**, wo Sie alle Details dazu sehen können, wann ein kritisches Ereignis für die von Ihnen ausgewählte Dauer aufgetreten ist: die Instanzquelle, das Datum, die Kategorie und die Benachrichtigung, die gesendet wurde, als das kritische Ereignis aufgetreten ist.

Ebenso können Sie den Zustand einer NetScaler VPX-Instanz auf dem Dashboard anzeigen. Sie können die Zeit maskieren, in der die Instanz in Betrieb war, und nur die Zeiten anzeigen, in denen die Instanz außer Betrieb war. Wenn Sie auf das Diagramm klicken, gelangen Sie zur Seite dieser Instanz, wo der Filter *außer Betrieb* bereits angewendet ist, und können Details wie Hostname, die Anzahl der pro Sekunde empfangenen HTTP-Anfragen, CPU-Auslastung und andere sehen. Sie können die Instanz auch auswählen und das Instanz-Dashboard für weitere Details anzeigen.

So wählen Sie bestimmte Ereignisse nach Schweregrad in NetScaler Console aus:

1. Melden Sie sich mit Ihren Administratoranmeldeinformationen bei NetScaler Console an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Navigieren Sie zu **Infrastruktur > Instanzen**.

   Oder,

   Navigieren Sie zu **Infrastruktur > Ereignisse > Berichte**.

3. Wählen Sie aus der Dropdown-Liste in der oberen rechten Ecke der Seite die Dauer aus, für die Sie Ereignisse nach Schweregrad anzeigen möchten.

4. Das Donut-Diagramm **Ereignisse nach Schweregrad** zeigt eine visuelle Darstellung aller Ereignisse nach ihrem Schweregrad an. Verschiedene Ereignistypen werden als unterschiedlich farbige Abschnitte dargestellt, und die Länge jedes Abschnitts entspricht der Gesamtzahl der Ereignisse dieses Schweregradtyps.
5. Sie können auf jeden Abschnitt des Donut-Diagramms klicken, um die entsprechende Seite **Schweregradbasierte Ereignisse** anzuzeigen, die die folgenden Details für den ausgewählten Schweregrad für die ausgewählte Dauer anzeigt:

   - Instanzquelle
   - Daten des Ereignisses
   - Kategorie der von der NetScaler-Instanz generierten Ereignisse
   - Gesendete Nachrichtenbenachrichtigung

HINWEIS:

Unterhalb des Donut-Diagramms sehen Sie eine Liste der im Diagramm dargestellten Schweregrade. Standardmäßig zeigt ein Donut-Diagramm alle Ereignisse aller Schweregradtypen an, und daher sind alle Schweregradtypen in der Liste hervorgehoben. Fahren Sie mit der Maus über die Schweregradtypen, um den von Ihnen gewählten Schweregrad einfacher anzuzeigen und zu überwachen.

So zeigen Sie NetScaler SNMP-Trap-Details in NetScaler Console an:

Sie können jetzt die Details jedes SNMP-Traps, der von den verwalteten NetScaler-Instanzen empfangen wurde, in der NetScaler Console auf der Seite **Ereigniseinstellungen** anzeigen. Navigieren Sie zu **Infrastruktur > Ereignisse > Ereigniseinstellungen**. Für einen bestimmten Trap, der von Ihrer Instanz empfangen wurde, können Sie die folgenden Details in Tabellenform anzeigen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Kategorie** – Gibt die Kategorie der Instanz an, zu der das Ereignis gehört.
- **Schweregrad** – Der Schweregrad des Ereignisses wird durch Farben und seinen Schweregradtyp angezeigt.
- **Beschreibung** – Gibt die mit dem Ereignis verbundenen Meldungen an.

Beispielsweise wird bei einem Ereignis mit der Trap-Kategorie **aggregateBWUseNormal** die Beschreibung des Traps als „Dieser Trap wird gesendet, wenn die aggregierte Bandbreitennutzung des Systems wieder normal ist.“ angezeigt.

Syslog-Meldungen anzeigen und exportieren

Sie können Syslog-Meldungen anzeigen, ohne sich bei NetScaler Console anzumelden, indem Sie einen Export aller auf dem Server empfangenen Syslog-Meldungen planen. Sie können Syslog-Meldungen, die auf Ihren Citrix Application Delivery Controller (NetScaler)-Instanzen generiert werden, in den Formaten PDF, CSV, PNG und JPEG exportieren. Außerdem können Sie den Export dieser Berichte in bestimmten Intervallen an angegebene E-Mail-Adressen planen.

Syslog-Meldungen anzeigen

Sie können alle Ihre Syslog-Meldungen anzeigen, die auf Ihren verwalteten NetScaler-Instanzen generiert wurden. Um die Meldungen anzuzeigen, müssen Sie die Instanzen so konfigurieren, dass die Syslog-Meldungen an den NetScaler Console-Server umgeleitet werden. Die Syslog-Meldungen werden zentral in der Datenbank gespeichert und stehen im Syslog Viewer für Prüfzwecke zur Verfügung. Sie können diese Protokollinformationen kombinieren und Berichte für Analysen aus den gesammelten Daten ableiten.

Sie können Syslog auch so konfigurieren, dass verschiedene Arten von Ereignissen protokolliert werden.

Um den Syslog Viewer anzuzeigen, navigieren Sie zu **Infrastruktur > Ereignisse > Syslog-Meldungen**. Wählen Sie die entsprechenden Filter aus, um Ihre Systemprotokollmeldungen anzuzeigen.

Syslog-Meldungen suchen

Sie können Filter verwenden, um Syslog-Meldungen und Audit-Log-Meldungen zu durchsuchen, um Ihre Ergebnisse einzugrenzen und genau das zu finden, wonach Sie suchen, und das in Echtzeit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Um Syslog-Meldungen für alle in der NetScaler Console-Software vorhandenen NetScaler-Instanzen zu suchen, navigieren Sie in der NetScaler Console-GUI zu **Infrastruktur > Ereignisse > Syslog-Meldungen**. Die neuen Filterkategorien sind Instanz, Modul, Ereignis, Schweregrad und Meldung.

Um alle NetScaler Console-System-Audit-Log-Meldungen in der NetScaler Console-Software zu suchen, navigieren Sie in der NetScaler Console-GUI zu **Einstellungen > Audit-Log-Meldungen**. Die neuen Filterkategorien sind Instanz, Modul, Ereignis, Schweregrad und Meldung.

Um Audit-Log-Meldungen für alle in der NetScaler Console vorhandenen Anwendungen zu suchen, navigieren Sie in der NetScaler Console-GUI zu **Infrastruktur > Netzwerkfunktionen > Überwachung**.

Um die Audit-Log-Meldungen für eine bestimmte Anwendung in der NetScaler Console zu suchen, navigieren Sie in der NetScaler Console-GUI zu **Anwendung > Dashboard** und wählen Sie den virtuellen Server aus, für den Sie die Audit-Log-Meldungen suchen möchten. Klicken Sie anschließend auf die Registerkarte **Audit-Log**.

Nachdem Sie eine Filterkategorie ausgewählt haben, geben Sie an, ob sie dem Suchbegriff entspricht oder ihn enthält.

Fügen Sie als Nächstes den Suchbegriff hinzu. Für einige Kategorien wird eine vorab ausgefüllte Liste von Suchbegriffen angezeigt. Standardmäßig beträgt die Suchzeit 1 Tag. Sie können den Zeit- und Datumsbereich ändern, indem Sie auf den Abwärtspfeil klicken. Sie können Ihre Suche weiter eingrenzen, indem Sie Optionen aus dem Bereich **Syslog-Zusammenfassung** oder **Audit-Log-Zusammenfassung** auswählen.

Syslog-Meldungen exportieren

So exportieren Sie einen Syslog-Meldungsbericht mit NetScaler Console:

1. Navigieren Sie zu **Infrastructure > Events > Syslog Messages**.
2. Klicken Sie im rechten Bereich oben rechts auf der Seite „Syslog-Meldungen“ auf die Schaltfläche zum Exportieren.
3. Wählen Sie unter **Jetzt exportieren** das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.

So planen Sie den Export eines Syslog-Meldungsberichts mit NetScaler Console:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie zu **Infrastructure > Events > Syslog Messages**.
2. Klicken Sie auf der Seite **Syslog-Meldungen** im rechten Bereich auf **Exportieren**.
3. Legen Sie auf der Registerkarte **Bericht planen** die folgenden Parameter fest:

    - **Beschreibung**: Meldung, die den Grund für den Export des Berichts beschreibt.
    - **Format**: Format, in dem der Bericht exportiert werden soll.
    - **Wiederholung**: Intervall, in dem der Bericht exportiert werden soll.
    - **Exportzeit**: Zeitpunkt, zu dem der Bericht exportiert werden soll. Geben Sie die Zeit im 24-Stunden-Format für Ihre lokale Zeitzone ein.
    - **E-Mail-Verteilerliste**: Liste der Empfänger, die den Bericht per E-Mail erhalten sollen. Wählen Sie eine E-Mail-Verteilerliste aus der bereitgestellten Liste aus. Eine E-Mail wird ausgelöst, wenn der Bericht generiert wird und die geplanten Zeitkriterien erfüllt sind. Wenn Sie eine E-Mail-Verteilerliste erstellen möchten, klicken Sie auf **+** und geben Sie die Details zum Mailserver und Mailprofil an.

Syslog-Meldungen unterdrücken

Wenn als Syslog-Server konfiguriert, empfängt NetScaler Console alle Syslog-Meldungen von den konfigurierten Citrix Application Delivery Controller (NetScaler)-Instanzen. Es kann viele Meldungen geben, die Sie möglicherweise nicht sehen möchten. Beispielsweise sind Sie möglicherweise nicht daran interessiert, alle Meldungen auf Informationsebene zu sehen. Sie können nun einige der Syslog-Meldungen verwerfen, die Sie nicht interessieren. Sie können einige der in NetScaler Console eingehenden Syslog-Meldungen unterdrücken, indem Sie Filter einrichten. NetScaler Console verwirft alle Meldungen, die den Kriterien entsprechen. Diese verworfenen Meldungen werden nicht in der NetScaler Console-GUI angezeigt und diese Meldungen werden auch nicht in der NetScaler Console-Datenbank des Kunden gespeichert.

Sie können einige der protokollierten Syslog-Meldungen, die in NetScaler Console eingehen, unterdrücken, indem Sie Filter einrichten. Die beiden Filter, die zum Unterdrücken von Syslog-Meldungen verwendet werden können, sind Schweregrad und Einrichtung (Facility). Sie können auch Meldungen unterdrücken, die von einer bestimmten NetScaler-Instanz oder mehreren Instanzen stammen. Sie können auch ein Textmuster angeben, nach dem NetScaler Console Meldungen suchen und unterdrücken soll. NetScaler Console verwirft alle Meldungen, die den Kriterien entsprechen. Diese verworfenen Meldungen werden nicht in der NetScaler Console-GUI angezeigt und diese Meldungen werden auch nicht in der Kundendatenbank gespeichert. Daher wird eine beträchtliche Menge Speicherplatz auf dem Speicherserver gespart.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Einige Anwendungsfälle zum Unterdrücken von Syslog-Meldungen sind die folgenden:

- Wenn Sie alle Meldungen auf Informationsebene ignorieren möchten, unterdrücken Sie Stufe 6 (Information).
- Wenn Sie nur Firewall-Fehlerbedingungen aufzeichnen möchten, unterdrücken Sie alle Stufen außer Stufe 3 (Fehler).

Syslog-Meldungen durch Erstellen von Filtern unterdrücken

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Events > Syslog Messages**.
2. Klicken Sie auf das Zahnradsymbol, um die Seite **Filter unterdrücken** anzuzeigen.

3. Klicken Sie auf der Seite **Filter unterdrücken** auf **Hinzufügen**.
4. Aktualisieren Sie unter **Filter unterdrücken erstellen** die folgenden Informationen:

   a. **Name** – Geben Sie einen Namen für den Filter ein.

   HINWEIS:

   Wenn verschiedene Benutzer unterschiedlichen Zugriff auf mehrere NetScaler-Instanzen haben, müssen unterschiedliche Filter für verschiedene Instanzen erstellt werden, da Benutzer nur die Filter sehen können, für die sie Zugriff auf alle Instanzen haben.

   b. **Schweregrad** – Wählen Sie die Protokollebenen aus, für die Sie die Meldungen unterdrücken möchten, und fügen Sie sie hinzu.Wenn Sie beispielsweise keine Informationsmeldungen anzeigen möchten, können Sie **Informationen** auswählen, um diese Meldungen zu unterdrücken.

   c. **Instanzen** – Wählen Sie die NetScaler-Instanzen aus, auf denen die Syslog-Meldungen konfiguriert wurden.

   d. **Einrichtungen** – Wählen Sie die Einrichtung aus, um Meldungen basierend auf der Quelle zu unterdrücken, die sie generiert.

   e. **Muster für Meldungen** – Sie können auch ein Textmuster eingeben, das von Sternchen (*) umgeben ist, um die Meldungen zu unterdrücken. Die Meldungen werden nach der Textmusterzeichenfolge durchsucht, und die Meldungen, die dieses Muster enthalten, werden unterdrückt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deaktivieren des Filters

Damit die Meldungen in der NetScaler Console angezeigt werden können, müssen Sie den Filter deaktivieren.

1. Navigieren Sie zu **Infrastruktur > Ereignisse > Syslog-Meldungen**.
2. Klicken Sie auf das Zahnradsymbol, um die Seite **Filter unterdrücken** anzuzeigen.
3. Wählen Sie auf der Seite **Filter unterdrücken** den Filter aus und klicken Sie auf **Bearbeiten**.
4. Deaktivieren Sie auf der Seite **Unterdrückungsfilter konfigurieren** das Kontrollkästchen **Filter aktivieren**, um den Filter zu deaktivieren.

SSL-Dashboard

NetScaler Console optimiert jetzt jeden Aspekt der Zertifikatsverwaltung für Sie. Über eine einzige Konsole können Sie automatisierte Richtlinien einrichten, um den richtigen Aussteller, die richtige Schlüsselstärke und die richtigen Algorithmen sicherzustellen und gleichzeitig ungenutzte oder bald ablaufende Zertifikate genau im Auge zu behalten. Bevor Sie das SSL-Dashboard von NetScaler Console und seine Funktionen nutzen können, müssen Sie verstehen, was ein SSL-Zertifikat ist und wie Sie NetScaler Console verwenden können, um Ihre SSL-Zertifikate zu verfolgen.

Ein Secure Socket Layer (SSL)-Zertifikat, das Teil jeder SSL-Transaktion ist, ist eine digitale Datenform (X509), die ein Unternehmen (Domäne) oder eine Einzelperson identifiziert. Das Zertifikat verfügt über eine öffentliche Schlüsselkomponente, die für jeden Client sichtbar ist, der eine sichere Transaktion mit dem Server initiieren möchte. Der entsprechende private Schlüssel, der sicher auf der NetScaler Appliance gespeichert ist, wird verwendet, um die asymmetrische Schlüssel-(oder Public-Key-)Verschlüsselung und -Entschlüsselung abzuschließen.

Sie können ein SSL-Zertifikat und einen Schlüssel auf eine der folgenden Arten erhalten:

- Von einer autorisierten Zertifizierungsstelle (CA)
- Durch Generieren eines neuen SSL-Zertifikats und Schlüssels auf der NetScaler Appliance

NetScaler Console bietet eine zentralisierte Ansicht der SSL-Zertifikate, die auf allen verwalteten NetScaler-Instanzen installiert sind. Auf dem SSL-Dashboard können Sie Diagramme anzeigen, die Ihnen helfen, Zertifikatsaussteller, Schlüsselstärken, Signaturalgorithmen, abgelaufene oder ungenutzte Zertifikate usw. zu verfolgen. Sie können auch die Verteilung der SSL-Protokolle

© 1997–2026 Citrix Systems, Inc. All rights reserved.

sehen, die auf Ihren virtuellen Servern ausgeführt werden, und die Schlüssel, die auf ihnen aktiviert sind.

Sie können auch Benachrichtigungen einrichten, die Sie informieren, wenn Zertifikate ablaufen, und Informationen darüber enthalten, welche NetScaler-Instanzen diese Zertifikate verwenden.

Sie können ein NetScaler-Instanzzertifikat mit einem CA-Zertifikat verknüpfen. Stellen Sie jedoch sicher, dass die Zertifikate, die Sie mit demselben CA-Zertifikat verknüpfen, dieselbe Quelle und denselben Aussteller haben. Nachdem Sie ein oder mehrere Zertifikate mit einem CA-Zertifikat verknüpft haben, können Sie diese wieder trennen.

HINWEIS:

Sie können auch einen Venafi Trust Protection Platform-Server mit NetScaler Console verwenden, um die Verwaltung des gesamten Lebenszyklus von SSL-Zertifikaten zu automatisieren. Weitere Informationen finden Sie unter Automatisieren der SSL-Zertifikatsverwaltung.

Automatisierte Zertifikatserneuerung mit dem ACME-Protokoll

NetScaler Console unterstützt die Automated Certificate Management Environment (ACME), ein offenes Protokoll, das zur Automatisierung der Erneuerung von SSL/TLS-Zertifikaten entwickelt wurde.

Zuvor mussten Netzwerkadministratoren den arbeitsintensiven, mehrstufigen manuellen Prozess der Zertifikatserneuerung durchlaufen. Die ACME-Unterstützung mindert diese Herausforderungen, indem sie ein robustes Framework für die automatisierte Zertifikatserneuerung bereitstellt, um die folgenden Aktionen auszuführen:

- Neue Zertifikate von vertrauenswürdigen Zertifizierungsstellen (CAs) anfordern.
- Domain-Inhaberschaft mit automatisierten Methoden validieren (Derzeit unterstützt NetScaler Console nur die DNS-01-Challenge).
- Zertifikate vor Ablauf automatisch erneuern.

ACME-Unterstützung in NetScaler® Console

NetScaler Console verwendet den `acme.sh` Client und unterstützt die folgenden Zertifizierungsstellen:

- Let’s Encrypt

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- DigiCert Inc
- Sectigo Limited
- Entrust, Inc
- GlobalSign
- GoDaddy.com, Inc
- ZeroSSL
- Google Trust Services
- Google Public CA
- BuyPass Go SSL
- Actalis
- SSL.com
- HashiCorp Vault
- Smallstep
- Pebble
- HARICA
- EJBCA

Die folgenden Schritte erklären, wie die automatisierte Zertifikatserneuerung in NetScaler Console abläuft:

1. Wenn NetScaler Console eine Zertifikatsanfrage für eine Domäne über den `acme.sh` Client initiiert, verbindet sich der Client mit der ausgewählten Zertifizierungsstelle (z. B. Let's Encrypt oder DigiCert).
2. Die Zertifizierungsstelle stellt eine Herausforderung aus, um den Domänenbesitz zu beweisen, was in diesem Fall eine DNS-01-Herausforderung ist.
3. NetScaler Console aktualisiert mithilfe vorkonfigurierter Anmeldeinformationen automatisch den DNS-TXT-Eintrag für die Domäne mit dem von der Zertifizierungsstelle bereitgestellten Wert.
4. Die Zertifizierungsstelle validiert den TXT-Eintrag und bestätigt damit den Domänenbesitz.
5. Nach erfolgreicher Validierung stellt die CA das SSL/TLS-Zertifikat für NetScaler Console aus.
6. NetScaler Console speichert das Zertifikat im jeweiligen Speicher (Zertifikatsspeicher/Zero-Touch-Speicher).
7. Basierend auf dem von Ihnen angegebenen Verlängerungszeitraum wiederholt NetScaler Console diesen Vorgang automatisch zur Verlängerung vor dem Ablaufdatum des Zertifikats.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mit der ACME-Unterstützung in NetScaler Console können Sie die folgenden Aktionen ausführen:

- Zertifikate automatisch erneuern, bevor sie ablaufen
- Während der Verlängerung von einer CA zu einer anderen wechseln
- CSR generieren oder hochladen und ein neues Zertifikat anfordern

Die wichtigsten Vorteile sind:

- Vollständig automatisierter Lebenszyklus ohne manuellen Eingriff bei der Zertifikatsausstellung oder -verlängerung.
- Anpassbarer Verlängerungszeitplan, der den organisatorischen Anforderungen entspricht (z. B. Verlängerung 7 Tage vor Ablauf).
- Eliminiert Ausfallzeiten aufgrund abgelaufener Zertifikate.
- Reduzierter Betriebsaufwand durch Automatisierung der Ablaufverfolgung und Verlängerungen.
- Verbesserte Sicherheitslage durch stets gültige, CA-Best-Practice-konforme Zertifikate.

Konfigurationsschritte für die ACME-Integration

Die Integration von ACME ist ein einmaliger Prozess und umfasst die folgenden Schritte:

- Schritt 1: Konfigurieren Sie die Zertifizierungsstelle (CA).
- Schritt 2: Wählen Sie Zertifikate für die Verlängerung aus.
- Schritt 3: Fügen Sie einen DNS-Anbieter hinzu und ordnen Sie die entsprechenden Domänen zu.

Voraussetzungen

- Stellen Sie sicher, dass Sie ein gültiges Konto für Ihre Zertifizierungsstelle (CA) und eine Lizenz dafür besitzen.
- Stellen Sie sicher, dass Sie über Zugangsdaten für den DNS-Anbieter verfügen.

Schritt 1: Zertifizierungsstelle (CA) konfigurieren

Führen Sie die folgenden Schritte aus, um die für Verlängerungen verwendete Zertifizierungsstelle (CA) zu registrieren:

1. Navigieren Sie zu **Infrastructure > SSL Dashboard**. Wenn Sie ACME zum ersten Mal konfigurieren, wird ein Banner mit „Automatisierte Verlängerungen für SSL-Zertifikate“ angezeigt. Klicken Sie auf **Erste Schritte**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

oder

Navigieren Sie zu **Infrastructure > SSL Dashboard > Third-party Integration > CA Vendors** und klicken Sie auf **Add**.

2. Geben Sie einen Namen ein und wählen Sie den CA-Anbieter aus.
3. Geben Sie die weiteren Details wie E-Mail-Adresse und ACME-Verzeichnis-URL an.
4. Geben Sie die Anzahl der Tage ein, bevor die NetScaler Console die Zertifikate automatisch erneuern muss.
5. Klicken Sie auf **Speichern und fortfahren**. Die NetScaler Console versucht, eine Verbindung zur CA herzustellen. Wenn die Verbindung fehlschlägt, überprüfen Sie die angegebenen Details, korrigieren Sie die Konfigurationsdetails und versuchen Sie es dann erneut.

Schritt 2: Zertifikate zur Erneuerung auswählen

Nachdem die CA-Details hinzugefügt wurden, scannt die NetScaler Console automatisch alle Zertifikate (sowohl aus dem Zertifikatsspeicher als auch aus dem Zero-Touch-Speicher) und listet die von der konfigurierten CA ausgestellten Zertifikate separat auf. Überprüfen Sie die aufgelisteten Zertifikate.

1. Wählen Sie die Zertifikate aus, die Sie automatisch erneuern möchten. Wenn Sie beispielsweise Let’s Encrypt als CA konfigurieren und 2 Zertifikate von Let’s Encrypt und 2 von einem anderen Anbieter haben, zeigt das Dashboard Folgendes an: `Let’s Encrypt: 2 and Other CA: 2`.
2. Sie können auf **Hinzufügen** klicken, um auch von einer anderen CA ausgestellte Zertifikate hinzuzufügen, oder auf **Entfernen**, um Zertifikate zu entfernen, die Sie nicht automatisch erneuern möchten. Wenn Sie Zertifikate von einem anderen Anbieter auswählen, werden Sie aufgefordert, die Anbieteränderung zu bestätigen. Sobald Sie dies bestätigen, werden diese Zertifikate über die neu konfigurierte CA erneuert, wenn ihr Erneuerungszeitraum erreicht ist.

HINWEIS:

Stellen Sie sicher, dass Sie keine doppelten Zertifikate im Zertifikatsspeicher und im Zero-Touch-Zertifikatsspeicher haben. Wenn doppelte Zertifikate vorhanden sind, erfolgt der Erneuerungsprozess für jeden Speicher zweimal.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Klicken Sie auf **Speichern und fortfahren**.

   HINWEIS:

   Zertifikate verbleiben nach der Erneuerung in ihren jeweiligen Speichern. Wenn ein Zertifikat beispielsweise im Zertifikatsspeicher gespeichert ist, wird seine erneuerte Version ebenfalls im Zertifikatsspeicher abgelegt. Wenn das Zertifikat im Zero-Touch-Speicher gespeichert ist, wird seine erneuerte Version ebenfalls im Zero-Touch-Speicher abgelegt.

   Das Verhalten der Zertifikatsbereitstellung hängt vom Speichertyp ab.

   - Wenn die Zertifikate im Zertifikatsspeicher gespeichert sind, müssen sie manuell auf NetScaler bereitgestellt werden.
   - Wenn die Zertifikate im Zero-Touch-Speicher gespeichert sind, werden die Zertifikate automatisch und ohne Eingreifen des Administrators auf NetScaler bereitgestellt. Wir empfehlen Ihnen, Zero-Touch-Zertifikatsverwaltung für eine nahtlose, vollautomatische Bereitstellung erneuerter Zertifikate zu verwenden. Weitere Informationen finden Sie unter Zero-Touch-Zertifikatsverwaltung.

Schritt 3: DNS-Anbieter hinzufügen und Domänen zuordnen

1. Klicken Sie auf der Seite **DNS-Anbieter & Domänenzuordnung** auf **Hinzufügen**.
2. Wählen Sie die DNS-Anbieter aus der Dropdown-Liste **DNS-Anbieter auswählen** aus. Die von `acme.sh` unterstützten DNS-Anbieter sind in der Dropdown-Liste aufgeführt. Wenn Ihr DNS-Anbieter nicht in der Liste angezeigt wird, bedeutet dies, dass er nicht unterstützt wird.
3. Geben Sie Anbieterdetails wie Zugriffs-ID, geheimen Zugriffsschlüssel ein und klicken Sie auf **Speichern**, um die Konfiguration zu speichern.
4. Klicken Sie unter **Domänenzuordnung** auf **Domäne hinzufügen**.
5. Wählen Sie die Domänen aus, die vom konfigurierten DNS-Anbieter bereitgestellt werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

Stellen Sie sicher, dass jede Domäne mit dem richtigen DNS-Anbieter verknüpft ist. NetScaler Console verwendet diese Zuordnungen, um die DNS-01-Challenge automatisch durchzuführen. Während der Ausstellung oder Verlängerung erstellt NetScaler Console die erforderlichen TXT-Einträge im zugeordneten DNS-Anbieter. Sobald die Validierung erfolgreich ist, stellt die CA das Zertifikat aus oder erneuert es. Zertifikate werden nur erneuert, wenn alle zugehörigen Domänen korrekt ihren DNS-Anbietern zugeordnet sind.

Wenn Ihre Organisation beispielsweise Amazon Route53 als DNS-Anbieter verwendet. Fügen Sie zuerst die Amazon Route53-Anmeldeinformationen (Zugriffsschlüssel-ID und geheimer Schlüssel) unter DNS-Anbieterdetails hinzu. Ordnen Sie dann die von Amazon Route53 verwalteten Domänen zu (z. B. example.com, app.example.com). Wenn ein Zertifikat für diese Domänen ausgestellt oder erneuert wird, erstellt NetScaler Console automatisch die erforderlichen TXT-Einträge in Amazon Route53. Sobald die Validierung erfolgreich ist, stellt die CA die Zertifikate aus oder erneuert sie.
Die folgenden öffentlichen DNS-Anbieter werden unterstützt:

- 1984.hosting
- ACME DNS
- AcmeProxy Server API
- Active24
- Akamai.com Edge DNS
- Aliyun
- All-inkl Kas Server
- Alviy.com
- Amazon Route53
- Anexia.com CloudDNS
- ArtFiles.de
- ArvanCloud.ir
- autoDNS-InternetX
- Azure DNS
- Azion.om

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Beget.com
- BookMyName.com
- Bunny.net
- CloudFlare
- ClouDNS.net
- ConoHa
- Constellix.com
- Core-Networks
- cPanel Server API
- Curanet.dk
- cyon.ch
- DDNSS.de
- deSEC.io
- DigitalOcean
- DirectAdmin
- DNS.Services
- DNSExit.com
- dns.la
- DNSMadeEasy
- DNSimple
- dnsHome.de
- DNSPod.cn
- DNSPod.com
- Domain-Offensive do.de
- DomeneShop.no
- DreamHost
- DuckDNS.org
- durabledns.com
- Dyn.com
- DynDnsFree.de

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Dynu.com
- DynV6.com
- easyDNS.net
- edgecenter DNS-API
- EUserv.com
- Exoscale
- Fornex.com
- FreeDNS
- FreeMyIP.com
- Gandi LiveDNS
- Gcore.com
- GeoScaling.com
- GoDaddy.com
- Google Cloud DNS
- Google Domains
- Hetzner.com
- Hexonet.com
- hosting.de
- HuaweiCloud.com
- Hurricane Electric
- Hurricane Electric HE.net DDNS
- Infoblox
- Infomaniak.com
- INWX
- IONOS Cloud DNS
- IONOS.de
- InternetBS.net
- ISPConfig 3.1
- jdcloud.com
- Joker.com

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- kapper.net
- King.host
- Knot DNS
- Leaseweb.com
- Lexicon DNS-Client
- lima-city.de
- Linode
- Linode.com-Old
- Loopia
- LuaDNS
- MailinaBox
- MaraDNS
- mijn.host
- Misaka.io
- MyDNS.JP
- Mythic-Beasts.com
- Name.com
- Namecheap
- NameMaster.de
- Namesilo
- Nanelo.com
- NederHost.nl
- Neodigit.net
- Netcup
- Netlify.com
- nic.ru
- Njalla
- NLnetLabs NSD
- NS1.com
- Nexcess

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- one.com
- Online.net
- omg.lol
- OpenProvider
- OpenStack Designate API
- OPNsense
- Oracle Cloud Infrastructure-OCI
- OVH.com
- Plesk XML
- PointHQ
- Porkbun.com
- PowerDNS
- RackCorp.com
- RackSpace.com
- rage4.com
- RcodeZero
- reg.ru
- ScaleWay.com
- Schlundtech
- Selectel
- SelfHost.de
- ServerCow.de
- Simply.com
- Technitium DNS Server
- tele3.cz
- Tencent.com
- Timeweb.Cloud
- TransIP.nl
- UltraDNS
- united-domains Reselling

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- unoeuro.com
- variomedia.de
- Vercel.com
- veesp.com
- versio.nl AuroraDNS
- VSCALE
- vshosting.cz CloudDNS
- Vultr
- Websupport.sk
- West.cn
- World4You.com
- Yandex 360 für Unternehmen DNS API.
- Yandex Cloud DNS
- Zilore
- Zone.eu
- ZoneEdit.com
- Zonomi

Sobald alle drei Schritte abgeschlossen sind, konfiguriert NetScaler Console den ACME CA-Server. Die ausgewählten Zertifikate werden für die zugeordneten Domänen erneuert. NetScaler Console überprüft regelmäßig die Gültigkeit von Zertifikaten und erneuert sie, bevor sie ablaufen (basierend auf dem konfigurierten Fenster). Da kein manueller Eingriff erforderlich ist, bleiben Zertifikate immer gültig und aktuell.

Ausstellung und Verlängerungen

Navigieren Sie zu **Infrastructure > SSL Dashboard > Issuance & Renewals**, um alle Verlängerungsaktivitäten und die neuen Anfragen zur Zertifikatsausstellung zu überprüfen.

Automatische Verlängerungen

Die Registerkarte **Automatische Verlängerungen** listet die Zertifikate auf, die für die automatische Verlängerung registriert sind. Wenn das konfigurierte Verlängerungsfenster erreicht ist, erneuert NetScaler Console sie automatisch.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können auch eine bedarfsgesteuerte Verlängerung vor dem geplanten Verlängerungsfenster auslösen. Wählen Sie für die bedarfsgesteuerte Verlängerung das gewünschte Zertifikat aus und klicken Sie auf **Jetzt verlängern**.

Wenn Sie nicht möchten, dass bestimmte Zertifikate automatisch verlängert werden, können Sie zu manuellen Verlängerungen wechseln. Um die Zertifikate von der automatischen zur manuellen Verlängerung zu übertragen, wählen Sie die gewünschten Zertifikate aus und klicken Sie auf **Zu manueller Verlängerung migrieren**.

Manuelle Verlängerungen

Die Registerkarte **Manuelle Verlängerungen** listet alle Zertifikate auf, die manuell verlängert werden müssen. Diese Zertifikate müssen manuell aktualisiert werden, entweder durch Offline-Verlängerung des Zertifikats und Hochladen des neuen Zertifikats in den entsprechenden Speicher oder durch Verwendung der Option **Jetzt verlängern**.

Um ein Zertifikat zu verlängern, wählen Sie ein Zertifikat aus und klicken Sie auf **Jetzt verlängern**. Wenn das Zertifikat von einer registrierten CA ausgestellt wurde und der DNS-Anbieter der Domäne konfiguriert ist, können Sie es bei Bedarf mit ACME verlängern, ohne es in die automatischen Verlängerungen zu verschieben.

Sie können ein Zertifikat auch auf automatische Verlängerung umstellen. Um die Zertifikate von der manuellen zur automatischen Verlängerung zu übertragen, wählen Sie die gewünschten Zertifikate aus und klicken Sie auf **Zu automatischer Verlängerung migrieren**.

HINWEIS:

Sie können immer nur ein Zertifikat gleichzeitig verlängern oder migrieren.

Ausstellungs- und Verlängerungsprotokolle

Die Registerkarte **Ausstellungs- und Verlängerungsprotokolle** enthält die Liste der Zertifikatsanfragen, die ACME verwenden, einschließlich Ausstellungen und Verlängerungen. Bei einem fehlgeschlagenen Ereignis können Sie auf das Info-Symbol klicken, um detaillierte Fehlerinformationen anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zertifikat ausstellen

Die ACME-Integration in NetScaler Console unterstützt die direkte Anforderung neuer Zertifikate mithilfe des ACME-Protokolls. Sie können entweder eine CSR in NetScaler Console erstellen oder eine vorhandene CSR hochladen, um neue Zertifikate anzufordern.

Navigieren Sie zu **Infrastructure > SSL dashboard > Issuances & Renewal**, klicken Sie auf **Issue Certificate** und wählen Sie je nach Szenario eine der folgenden Optionen aus:

- **Ich habe keine CSR**: Wenn Sie noch keine CSR haben, können Sie mit NetScaler Console eine generieren und ein neues Zertifikat ausstellen.
- **Ich habe eine CSR**: Wenn Sie bereits eine offline generierte CSR haben, können Sie diese hochladen, um ein Zertifikat auszustellen.

Zertifikat ohne CSR ausstellen

Führen Sie die folgenden Schritte aus, um eine CSR zu generieren und ein neues Zertifikat auszustellen:

1. Navigieren Sie zu **Infrastructure > SSL dashboard > Issuances & Renewal**, klicken Sie auf **Issue Certificate** und wählen Sie **Ich habe keine CSR**.

2. Auf der Seite **Zertifikatsschlüssel** laden Sie entweder einen vorhandenen Schlüssel hoch, indem Sie **Ich habe einen Schlüssel** auswählen, oder generieren Sie einen neuen, indem Sie **Ich habe keinen Schlüssel** auswählen.

3. Geben Sie die erforderlichen CSR-Informationen ein.

4. Wählen Sie die CA, den DNS-Anbieter und den Zertifikatbereitstellungsmodus für die ACME-Anfrage aus. Wählen Sie **Cert Store** für die manuelle Bereitstellung oder **Zero Touch Store** für die automatische Bereitstellung auf NetScaler.
5. Wählen Sie **Zertifikat automatisch erneuern**, wenn das Zertifikat zukünftig automatisch erneuert werden soll.

6. Klicken Sie auf **Speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zertifikat mit CSR ausstellen

Führen Sie die folgenden Schritte aus, wenn Sie bereits eine offline generierte CSR haben und diese hochladen möchten, um ein Zertifikat auszustellen:

1. Navigieren Sie zu **Infrastructure > SSL dashboard > Issuances & Renewal** und klicken Sie auf **Zertifikat ausstellen** und wählen Sie **Ich habe CSR**.

2. Wählen Sie die CSR-Datei und die zugehörige Schlüsseldatei von Ihrem lokalen System aus.

3. Wählen Sie die CA, den DNS-Anbieter und den Zertifikatbereitstellungsmodus für die ACME-Anfrage aus. Wählen Sie **Cert Store** für die manuelle Bereitstellung oder **Zero Touch Store** für die automatische Bereitstellung auf NetScaler.
4. Wählen Sie **Zertifikat automatisch erneuern**, wenn das Zertifikat zukünftig automatisch erneuert werden soll.

5. Klicken Sie auf **Speichern**.

Drittanbieter-Integration

Sie können mehr als einen CA-Anbieter und DNS-Anbieter hinzufügen und verwalten.

Sie können die folgenden Aktionen von der Seite **Drittanbieter-Integration** ausführen:

- Einen CA-Anbieter hinzufügen oder bearbeiten
- Die Einstellungen für die automatische Verlängerung ändern
- Das Zertifikat von einer bestehenden konfigurierten CA hinzufügen oder bearbeiten
- Einen DNS-Anbieter hinzufügen oder bearbeiten
- Domänenzuordnungen ändern

Einen CA-Anbieter hinzufügen oder bearbeiten

Sie können mehr als einen CA-Anbieter registrieren, um Zertifikate zu verwalten, die von verschiedenen Anbietern ausgestellt wurden. Sie können auch die Details des bestehenden CA-Anbieters bearbeiten.

1. Navigieren Sie zu **SSL-Dashboard > Drittanbieter-Integration > ACME > CA-Anbieter**. Klicken Sie auf **Hinzufügen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Um einen CA-Anbieter hinzuzufügen, geben Sie einen Namen für den CA-Anbieter an und wählen Sie die CA aus.
3. Um die Details eines bestehenden CA-Anbieters zu bearbeiten, wählen Sie den CA-Anbieter aus und klicken Sie auf **Bearbeiten**.
4. Fügen Sie die erforderlichen Details hinzu oder aktualisieren Sie sie.
5. Klicken Sie auf **Speichern**.

Einstellungen für die automatische Verlängerung ändern

Führen Sie die folgenden Schritte aus, um die Einstellungen für die automatische Verlängerung zu ändern:

1. Navigieren Sie zu **SSL-Dashboard > Drittanbieterintegration > ACME > CA-Anbieter**.
2. Wählen Sie einen CA-Anbieter aus und klicken Sie auf **Bearbeiten**.
3. Ändern Sie im Abschnitt **CA-Anbieter konfigurieren** die Anzahl der Tage gemäß Ihren Anforderungen im Abschnitt **Einstellungen für die automatische Verlängerung**.
4. Klicken Sie auf **Speichern und fortfahren**.
5. Schließen Sie den Workflow ab.

Zertifikat von einer vorhandenen konfigurierten CA hinzufügen oder bearbeiten

Führen Sie die folgenden Schritte aus, um das Zertifikat von einer vorhandenen konfigurierten CA hinzuzufügen oder zu bearbeiten:

1. Navigieren Sie zu **SSL-Dashboard > Drittanbieterintegration > ACME > CA-Anbieter**.
2. Wählen Sie einen CA-Anbieter aus und klicken Sie auf **Bearbeiten**.
3. Navigieren Sie zu **Schritt 2 Zertifikate auswählen** und fügen Sie die erforderlichen Zertifikate hinzu oder entfernen Sie sie.
4. Klicken Sie auf **Speichern und fortfahren**.
5. Schließen Sie den Workflow ab.

HINWEIS:

Wenn das Zertifikat nicht von der ursprünglichen Zertifizierungsstelle (CA) entkoppelt wurde, wird es nicht in der Auswahlliste für die neue CA angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DNS-Anbieter hinzufügen oder bearbeiten

Führen Sie die folgenden Schritte aus, um einen neuen DNS-Anbieter hinzuzufügen oder vorhandene Domänenzuordnungen bestehender DNS-Anbieter zu bearbeiten:

1. Navigieren Sie zu **SSL-Dashboard > Drittanbieterintegration > ACME > DNS-Anbieter**.
2. Um einen DNS-Anbieter hinzuzufügen, klicken Sie auf **Hinzufügen**. Wählen Sie den DNS-Anbieter aus und klicken Sie auf **Speichern**.
3. Um einen vorhandenen DNS-Anbieter zu bearbeiten, wählen Sie einen DNS-Anbieter aus und klicken Sie auf **Bearbeiten**.
4. Fügen Sie die erforderlichen Details hinzu oder aktualisieren Sie sie.
5. Klicken Sie auf **Speichern**.

Domänenzuordnungen ändern

Führen Sie die folgenden Schritte aus, um die Domänenzuordnungen bestehender DNS-Anbieter zu bearbeiten:

1. Navigieren Sie zu **SSL-Dashboard > Drittanbieterintegration > ACME > DNS-Anbieter**.
2. Wählen Sie einen DNS-Anbieter aus und klicken Sie auf **Bearbeiten**.
3. Navigieren Sie zu **Domänenzuordnung**, und fügen Sie Domänen nach Bedarf hinzu oder entfernen Sie sie.
4. Klicken Sie auf **Speichern**.

WICHTIG:

Wenn eine Domäne nicht zugeordnet ist, wird die Zertifikatsverlängerung beendet. Ordnen Sie Domänen immer einem gültigen DNS-Anbieter neu zu, um sicherzustellen, dass die Verlängerungen fortgesetzt werden.

Einschränkungen

- Die Zertifikatsverlängerung erfolgt nur für die von `acme.sh` unterstützten DNS-Anbieter.

Beheben von Problemen im Zusammenhang mit der automatischen Zertifikatsverlängerung

Einige häufige Fehlermeldungen, die auftreten können, und ihre zugehörigen Ursachen sind in diesem Abschnitt aufgeführt:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Der Fehler **Certificate has invalid domain - ADCD** wird gemeldet, wenn der Domänenname im Zertifikat gemäß den ACME-Anforderungen nicht gültig ist.
- Der Fehler **Invalid identifiers requested :: Cannot issue for "testdomain": Domain name needs at least one dot** wird gemeldet, wenn dem angeforderten Domänennamen ein Punkt fehlt (z. B. „example“ anstelle von „example.com“).
- Der Fehler **Could not get nonce from the CA server. Please check the CA server configuration.** wird gemeldet, wenn der ACME-Client keine Nonce von der CA abrufen kann, oft aufgrund von Netzwerk- oder Serverproblemen.
- Der Fehler **Cannot initialize API for the CA server. Please check the CA server configuration.** wird gemeldet, wenn der ACME-Client die Kommunikation mit dem CA-Server nicht initialisieren kann, möglicherweise aufgrund einer Fehlkonfiguration.
- Der Fehler **Invalid domain name provided. Please check the domain name and try again.** wird gemeldet, wenn das Domänennamenformat ungültig oder vom ACME-Protokoll nicht zugelassen ist.
- Der Fehler **Domains not changed. Certificate with same configuration already exists.** wird gemeldet, wenn eine Zertifikatsanforderung ohne Änderungen an der Domänenliste gestellt wird und das Zertifikat bereits vorhanden ist.
- Der Fehler **Error adding TXT record for domain validation. Please check the DNS configuration and try again.** wird gemeldet, wenn der ACME-Client den erforderlichen DNS-TXT-Eintrag für die Domänenvalidierung nicht hinzufügen kann.
- Der Fehler **Signature does not match. Please check the server time as it may not be in sync.** wird gemeldet, wenn eine Signatur nicht übereinstimmt, oft aufgrund von Zeitsynchronisationsproblemen zwischen Client und Server.
- Der Fehler **Certificate is missing a DNS provider name.** wird gemeldet, wenn kein DNS-Anbieter für die DNS-basierte Domänenvalidierung angegeben ist.
- **Verlängerung übersprungen, da keine aktiven DNS-Anbieter konfiguriert sind.** wird gemeldet, wenn eine Zertifikatsverlängerung versucht wird, aber keine aktiven DNS-Anbieter konfiguriert sind.
- **Fehler beim Validieren des/der Kontakts/Kontakte :: E-Mail-Adresse kann nicht analysiert werden** wird gemeldet, wenn die angegebene Kontakt-E-Mail-Adresse ungültig ist oder nicht analysiert werden kann.
- **Anfrage zur Auftragsfinalisierung kann nicht verarbeitet werden. (Für ungültige ACME-Verzeichnis-URL)** wird gemeldet, wenn der ACME-Client den Auftrag nicht abschließen kann, oft aufgrund einer ungültigen oder nicht erreichbaren ACME-Verzeichnis-URL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **DNS-Anbieter - TestDNS existiert nicht oder ist nicht aktiv.** wird gemeldet, wenn der angegebene DNS-Anbieter im System nicht gefunden wird oder inaktiv ist.
- **Konfigurations-CA-ID ist leer/existiert nicht.** wird gemeldet, wenn die CA-Konfigurations-ID fehlt oder keiner vorhandenen Konfiguration entspricht.

Zero-Touch-Zertifikatsverwaltung

In NetScaler Console können Sie die Zero-Touch-Zertifikatsverwaltung auf den verwalteten NetScaler-Instanzen konfigurieren, die Build **14.1-43.x** und höher ausführen. Mit der Zero-Touch-Zertifikatsverwaltung eliminieren Sie manuelle Eingriffe und erstellen einen In-Memory-Zero-Touch-Zertifikatsspeicher, um die Anwendungsanforderungen zu bedienen. Navigieren Sie zu **Infrastructure > SSL Dashboard > Zero-Touch Certificate Management**, um alle Zertifikate und Schlüssel in NetScaler Console hochzuladen und auf den verwalteten NetScaler-Instanzen zu aktivieren. NetScaler fragt das Zertifikatsrepository regelmäßig ab und liefert die erforderlichen Zertifikate nach Bedarf.

Mit der Zero-Touch-Zertifikatsverwaltung werden die folgenden Prozesse von NetScaler automatisch ausgeführt:

- Hinzufügen, Binden und Verknüpfen der Zertifikate
- Bereitstellen der Zertifikate und Schlüssel in einer bestimmten Reihenfolge oder zusammen
- Installieren und Verwenden der geeigneten Zertifikate basierend auf den Anforderungen
- Löschen abgelaufener Zertifikate während des periodischen Abfragezyklus

Weitere Informationen zur Funktionsweise des Zero-Touch-Zertifikats auf NetScaler-Instanzen finden Sie unter NetScaler Zero-Touch-Zertifikatsverwaltung.

Als Administrator müssen Sie in NetScaler Console Folgendes sicherstellen:

- NetScaler-Instanzen führen Build 14.1-43.x oder höher aus und werden in NetScaler Console verwaltet.
- Laden Sie die Zertifikate (in beliebigem Format) und Schlüssel hoch. Aktivieren Sie dann Zero-Touch auf den verwalteten NetScaler-Instanzen.
- Stellen Sie sicher, dass ein gültiges CA-Zertifikat in NetScaler Console vorhanden ist. Wenn Sie ein aktualisiertes Konsolen-CA-Zertifikat haben, laden Sie das Zertifikat hoch, bevor Sie Zero-Touch auf den verwalteten NetScaler-Instanzen aktivieren. Die folgende Fehlermeldung wird angezeigt, wenn kein CA-Zertifikat in NetScaler Console vorhanden ist:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zertifikate hochladen

1. Navigieren Sie zu **Infrastructure > SSL Dashboard > Zero-Touch Certificate Management**.
2. Klicken Sie auf **Erste Schritte**.

3. NetScaler-Instanzen, die Build 14.1-43.x oder höher ausführen, werden aufgelistet. Sie können entweder auf **Zero-Touch konfigurieren** klicken, um Zero-Touch zu aktivieren, oder auf **Überspringen** klicken, um mit dem nächsten Schritt fortzufahren.
4. Klicken Sie auf **Hochladen**, um alle Zertifikate hochzuladen (können in jedem Format vorliegen, z. B. .pem, .cer und .crt).

   HINWEISE:

   - Die Zertifikats- oder Schlüsseldatei muss kleiner als 8192 Byte sein.
   - Wenn Sie mehrere Zertifikate oder Schlüsseldateien hochladen, beträgt die maximal unterstützte Größe 50000 Byte.
   - Wenn die Zertifikate oder Schlüsseldateien passwortgeschützt sind, stellen Sie sicher, dass Sie das Passwort angeben. Wenn das Passwort nicht angegeben wird, wird das Zertifikat oder die Schlüsseldatei nicht hochgeladen.

Zero-Touch-Zertifikatsverwaltung aktivieren

Nachdem Sie die Zertifikate hochgeladen haben, müssen Sie Zero-Touch auf den verwalteten NetScaler-Instanzen aktivieren.

1. Klicken Sie auf der Seite **Zero-Touch-Zertifikatsverwaltung** auf **Zero-Touch konfigurieren**.

2. Klicken Sie auf **Instanzen hinzufügen**, wählen Sie die Instanzen aus und klicken Sie dann auf **Aktivieren**.

NetScaler Console verwendet das Standard-Abfrageintervall, um alle Zertifikate von den NetScaler-Instanzen abzufragen. Sie können die Option **Jetzt abfragen** verwenden, um sofort abzufragen.

Im **SSL-Dashboard** können Sie auch die Zero-Touch-Zertifikatsnutzung anzeigen, die Details zu den aktiven und inaktiven Zertifikaten zeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unterstützung des SSL-Filtermodus

Eine NetScaler®-Instanz ruft die Metadaten spezifischer SSL-Zertifikate und privater Schlüssel ab. Die Implementierung dieses Prinzips der geringsten Rechte stellt sicher, dass Instanzen nur auf die benötigten Assets zugreifen, wodurch verhindert wird, dass eine Kompromittierung auf einer Instanz Ihre gesamte Zertifikatsinfrastruktur offenlegt. Diese Funktion ist besonders nützlich für Umgebungen mit mehreren Administratoren, die eine Gruppe von NetScaler-Instanzen für unterschiedliche Zwecke verwalten.

Einige der Vorteile sind:

- **Sicherheitssegmentierung** – Beschränkt den Metadatenzugriff auf NetScaler-Ebene, um die Angriffsfläche zu minimieren und die Sicherheitsrichtlinien des Unternehmens einzuhalten.
- **Optimiertes Administratorerlebnis** – Reduziert die Komplexität in Multi-Tenant- oder Abteilungsbereitstellungen, indem Administratoren nur die Assets angezeigt werden, die für ihre Gruppe von NetScaler-Instanzen relevant sind.
- **Optimierte Ressourcennutzung** – Verhindert eine Überlastung des Systemspeichers, indem nur die Metadaten der erforderlichen SSL-Zertifikate und privaten Schlüssel abgerufen werden.

Die Filtermoduskonfiguration definiert, wie NetScaler-Instanzen und SSL-Dateien über bestimmte Synchronisierungstypen interagieren. Sie können diese Einstellungen über die NetScaler Console verwalten, um sicherzustellen, dass jede Instanz nur die erforderlichen Metadaten abruft.

KOMPONENTE	SYNCHRONISIERUNGSTYP	BESCHREIBUNG
NetScaler-Instanz	Angepasste Sync	NetScaler-Instanzen in diesem Modus rufen nur die Metadaten für Zertifikate und Schlüssel ab, die speziell der Instanz zugeordnet sind.
NetScaler-Instanz	Globale Synchronisierung	NetScaler-Instanzen in diesem Modus rufen die Metadaten für alle hochgeladenen Zertifikate und privaten Schlüssel ab.
SSL-Dateien	Benutzerdefinierte Dateien	Diese Dateien sind speziell NetScaler-Instanzen im Modus „Benutzerdefinierte

© 1997–2026 Citrix Systems, Inc. All rights reserved.

KOMPONENTE	SYNCHRONISIERUNGSTYP	BESCHREIBUNG
		Synchronisierung“ zugeordnet.
SSL-Dateien	Globale Dateien	Metadaten für diese Dateien werden von allen NetScaler-Instanzen im Modus „Globale Synchronisierung“ abgerufen.

Filtermoduseinstellungen konfigurieren

Um den Filtermodus zu konfigurieren, definieren Sie Synchronisierungstypen für Ihre Instanzen und Dateien. Dies gewährleistet eine sichere und optimierte Verteilung sensibler Metadaten.

Sie können Zertifikate und private Schlüssel jetzt direkt über die Schaltfläche „Hochladen“ in den Abschnitten „Zertifikatsdateien“ und „NetScaler-Instanzen“ hochladen.

So konfigurieren Sie über die GUI:

1. **Neue Dateien hochladen (Tag Null)** – Navigieren Sie zu Zertifikatsdateien und NetScaler-Instanzen > Hochladen, um neue Assets hinzuzufügen. Wählen Sie einen der folgenden Synchronisierungstypen aus:
   - **GLOBAL** – Wählen Sie die Verwendung des globalen Synchronisierungsmodus aus und schließen Sie den Upload ab.
   - **BENUTZERDEFINIERT** – Wählen Sie die Verwendung des benutzerdefinierten Synchronisierungsmodus aus, wählen Sie die spezifischen Instanzen für die Zuordnung aus und laden Sie dann die Dateien hoch.
2. **Vorhandene Dateien verschieben (Tag N)** – Um Zertifikate und Schlüssel vom globalen Synchronisierungsmodus in den benutzerdefinierten Synchronisierungsmodus zu verschieben, wählen Sie die Ziel-NetScaler-Instanzen aus und klicken Sie auf „Vorhandene Dateien hinzufügen“.
3. **Domänen auswählen** – Sobald Instanzen ausgewählt wurden, wählen Sie die relevanten Domänen aus, um die Verschiebung auszulösen. NetScaler Console erkennt und verschiebt die entsprechenden Zertifikate und privaten Schlüsseldateien automatisch in den benutzerdefinierten Synchronisierungsmodus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. **Assets anzeigen** – Navigieren Sie zur Landingpage, um alle Zertifikate und privaten Schlüsseldateien anzuzeigen, die jeder NetScaler-Instanz im benutzerdefinierten Synchronisierungsmodus zugeordnet sind.
5. **Synchronisierungsmodus wechseln** – Um Instanzen in den globalen Synchronisierungsmodus zurückzuversetzen, klicken Sie auf der Landingpage auf „Zu globaler Synchronisierung wechseln“.

Verwenden Sie das SSL-Dashboard

Sie können das SSL-Zertifikats-Dashboard in NetScaler Console verwenden, um Diagramme anzuzeigen, die Ihnen helfen, den Überblick über Zertifikatsaussteller, Schlüsselstärken und Signaturalgorithmen zu behalten. Das SSL-Zertifikats-Dashboard zeigt auch Diagramme an, die Folgendes anzeigen:

- Anzahl der Tage, nach denen Zertifikate ablaufen
- Anzahl der verwendeten und ungenutzten Zertifikate
- Anzahl der selbstsignierten und von einer Zertifizierungsstelle signierten Zertifikate
- Anzahl der Aussteller
- Signaturalgorithmen
- SSL-Protokolle
- Top 10 Instanzen nach Anzahl der verwendeten Zertifikate

SSL-Zertifikate überwachen

Verwenden Sie das SSL-Dashboard in NetScaler Console, um Ihre Zertifikate zu überwachen, wenn Ihr Unternehmen eine SSL-Richtlinie hat, in der Sie bestimmte Anforderungen an SSL-Zertifikate definiert haben, z. B. dass alle Zertifikate eine minimale Schlüsselstärke von 2048 Bit haben müssen und von einer vertrauenswürdigen Zertifizierungsstelle autorisiert werden müssen.

In einem anderen Beispiel haben Sie möglicherweise ein neues Zertifikat hochgeladen, aber vergessen, es an einen virtuellen Server zu binden. Das SSL-Dashboard hebt die verwendeten oder nicht verwendeten SSL-Zertifikate hervor. Im Abschnitt **Nutzung** sehen Sie die Anzahl der installierten Zertifikate und die Anzahl der verwendeten Zertifikate. Sie können das Diagramm anklicken, um den Namen des Zertifikats, die Instanz, auf der es verwendet wird, seine Gültigkeit, seinen Signaturalgorithmus usw. anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Um SSL-Zertifikate in NetScaler Console zu überwachen, navigieren Sie zu **Infrastructure > SSL Dashboard**.

NetScaler Console ermöglicht es Ihnen, SSL-Zertifikate abzufragen und alle SSL-Zertifikate der Instanzen sofort zu NetScaler Console hinzuzufügen. Navigieren Sie dazu zu **Infrastructure > SSL Dashboard** und klicken Sie auf **Jetzt abfragen**. Die Seite **Jetzt abfragen** wird angezeigt und bietet die Möglichkeit, alle NetScaler-Instanzen im Netzwerk oder ausgewählte Instanzen abzufragen.

Sie können das NetScaler Console SSL-Dashboard verwenden, um die Details von SSL-Zertifikaten, SSL Virtual Servern und SSL-Protokollen anzuzeigen oder zu überwachen. Die Zahlen sind Hyperlinks, die Sie anklicken können, um Details zu SSL-Zertifikaten, SSL Virtual Servern oder SSL-Protokollen anzuzeigen.

Wenn ein Benutzer beispielsweise in der obigen Abbildung auf die Zahl 30 unter **Selbstsigniert vs. CA-signiert** klickt, wird ein neues Fenster angezeigt, das Details zu den 30 SSL-Zertifikaten auf den NetScaler-Instanzen zeigt.

Das NetScaler Console SSL-Dashboard zeigt auch die Verteilung der SSL-Protokolle an, die auf Ihren virtuellen Servern ausgeführt werden. Als Administrator können Sie die Protokolle, die Sie überwachen möchten, über die SSL-Richtlinie festlegen. Weitere Informationen finden Sie unter Konfigurieren von SSL-Richtlinien. Die unterstützten Protokolle sind SSLv2, SSLv3, TLS1.0, TLS1.1 und TLS1.2. Die auf virtuellen Servern verwendeten SSL-Protokolle werden in einem Balkendiagrammformat angezeigt. Durch Klicken auf ein bestimmtes Protokoll wird eine Liste der virtuellen Server angezeigt, die dieses Protokoll verwenden.

Ein Donut-Diagramm wird angezeigt, nachdem Diffie-Hellman (DH)- oder Ephemeral RSA-Schlüssel auf dem SSL-Dashboard aktiviert oder deaktiviert wurden. Diese Schlüssel ermöglichen eine sichere Kommunikation mit Export-Clients, selbst wenn das Serverzertifikat keine Export-Clients unterstützt, wie im Fall eines 1024-Bit-Zertifikats. Durch Klicken auf das entsprechende Diagramm wird eine Liste der virtuellen Server angezeigt, auf denen DH- oder Ephemeral RSA-Schlüssel aktiviert sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Audit-Protokolle für SSL-Zertifikate anzeigen

Sie können jetzt Protokolldetails von SSL-Zertifikaten in der NetScaler Console anzeigen. Die Protokolldetails zeigen Vorgänge an, die mit SSL-Zertifikaten in der NetScaler Console durchgeführt wurden, wie z. B.: Installieren von SSL-Zertifikaten, Verknüpfen und Entknüpfen von SSL-Zertifikaten, Aktualisieren von SSL-Zertifikaten und Löschen von SSL-Zertifikaten. Audit-Protokollinformationen sind nützlich bei der Überwachung von SSL-Zertifikatsänderungen, die an einer Anwendung mit mehreren Besitzern vorgenommen wurden.

Um ein Audit-Protokoll für einen bestimmten Vorgang anzuzeigen, der in der NetScaler Console mit SSL-Zertifikaten durchgeführt wurde, navigieren Sie zu **Infrastructure > SSL Dashboard** und wählen Sie **Audit Logs**.

Für einen bestimmten Vorgang, der mit dem SSL-Zertifikat durchgeführt wurde, können Sie dessen Status, Startzeit und Endzeit anzeigen. Darüber hinaus können Sie die Instanz anzeigen, auf der der Vorgang durchgeführt wurde, und die auf dieser Instanz ausgeführten Befehle.

Standard-NetScaler-Zertifikate im SSL-Dashboard ausschließen

Mit NetScaler Console können Sie Standardzertifikate, die in den SSL-Dashboard-Diagrammen angezeigt werden, nach Ihren Präferenzen ein- oder ausblenden. Standardmäßig werden alle Zertifikate im SSL-Dashboard angezeigt, einschließlich der Standardzertifikate.

So blenden Sie Standardzertifikate im SSL-Dashboard ein oder aus:

1. Navigieren Sie in der NetScaler Console GUI zu **Infrastructure > SSL Dashboard**.
2. Klicken Sie auf der Seite **SSL-Dashboard** auf **Einstellungen**.
3. Wählen Sie auf der Seite **Einstellungen** die Option **Allgemein**.
4. Deaktivieren Sie im Abschnitt **Zertifikatsfilter** die Option **Standardzertifikate anzeigen** und wählen Sie **Speichern und Beenden**.

SSL-Zertifikate herunterladen

SSL-Zertifikate müssen pro Instanz individuell verwaltet werden. NetScaler Console bietet Einblick in alle Zertifikate, die über mehrere Instanzen hinweg bereitgestellt werden.

- Sie können auswählen, welche Zertifikate ablaufen, und die Zertifikatserneuerungen automatisieren.
- Richtlinien können bezüglich der zulässigen Zertifikatstypen und Signaturbehörden festgelegt und durchgesetzt werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Sie können die SSL-Zertifikate auch zur Erneuerung herunterladen und sie später hochladen.

So laden Sie SSL-Zertifikate herunter:

1. Navigieren Sie in der NetScaler Console GUI zu **Infrastruktur > SSL-Dashboard**.
2. Klicken Sie auf der Seite **SSL-Dashboard** auf die Gesamtzahl der SSL-Zertifikate in einem der Diagramme.

1. Klicken Sie auf der Seite **SSL-Zertifikate** auf das Zertifikat, das Sie herunterladen möchten. Sie möchten beispielsweise das Zertifikat herunterladen, das in der nächsten Woche abläuft.
2. Wählen Sie im Listenfeld **Aktion auswählen** die Option **Herunterladen**. Das Zertifikat wird auf Ihr System heruntergeladen.

So exportieren Sie den Bericht dieses Dashboards:

Um den Bericht dieser Seite zu exportieren, klicken Sie auf das Symbol **Exportieren** oben rechts auf dieser Seite. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren**. Um den Bericht im PDF-, JPEG-, PNG- oder CSV-Format anzuzeigen und zu speichern.
2. Wählen Sie die Registerkarte **Export planen**. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu senden.

HINWEIS

- Wenn Sie die Wiederholung **Wöchentlich** auswählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie die Wiederholung **Monatlich** auswählen, stellen Sie sicher, dass Sie alle Tage, an denen der Bericht geplant werden soll, durch Kommas getrennt eingeben.

So löschen Sie das SSL-Zertifikat im SSL-Dashboard

NetScaler 14.1-38.x und höher bietet die Möglichkeit, die zugehörigen SSL-Zertifikatsdateien von NetScaler zu löschen, während das ausgewählte SSL-Zertifikat gelöscht wird. So löschen Sie ein SSL-Zertifikat:

1. Navigieren Sie zu **Infrastruktur > SSL-Dashboard**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Klicken Sie im Abschnitt **SSL-Zertifikate**, in dem die Details der SSL-Zertifikate angezeigt werden, auf den Link auf der Bezeichnung **Nicht verwendet**. Eine Seite mit einer Liste der nicht verwendeten Zertifikate wird angezeigt.
3. Wählen Sie ein oder mehrere ungenutzte Zertifikate zum Löschen aus.

4. Klicken Sie auf **Löschen**.
5. Ein Dialogfeld **Bestätigen** wird angezeigt, das die folgenden Optionen zum Löschen der Zertifikatsdateien auch von NetScaler® bietet:

   - **Nicht löschen**: Überspringt das Löschen von Zertifikatsdateien von NetScaler.
   - **Löschen**: Löscht die Zertifikatsdateien von NetScaler für abgelaufene und nicht abgelaufene Zertifikate.
   - **Löschen, wenn abgelaufen**: Löscht die Zertifikatsdateien von NetScaler nur für abgelaufene Zertifikate.

   HINWEIS:

   - Für NetScaler-Versionen vor 14.1-38.x wird das Löschen der Zertifikatsdatei(en) für alle drei Optionen übersprungen.
   - Die Option zum Löschen der Zertifikatsdatei zusammen mit der Konfiguration ist nur für NetScaler 14.1-38.x und höher anwendbar.

6. Wählen Sie die entsprechende Option basierend auf Ihren Anforderungen aus.
7. Klicken Sie auf **Ja**, um das Zertifikat zu löschen, oder auf **Nein**, um den Workflow ohne Änderungen zu beenden.

SSL-Zertifikatskette anzeigen

Sie können die vollständige Kette von Links für ein Zertifikat anzeigen, einschließlich der Zwischenzertifikate bis zum Root-CA-Zertifikat.

So zeigen Sie eine Zertifikatskette an:

1. Navigieren Sie zu **Infrastructure > SSL Dashboard** und klicken Sie auf die SSL-Zertifikate in einer beliebigen Kachel.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Wählen Sie auf der Seite **SSL Certificates** ein Zertifikat aus und klicken Sie auf **Details**. Die Zertifikatskette wird unter **Links** angezeigt.

Benachrichtigungen für den Ablauf von SSL-Zertifikaten einrichten

Als Sicherheitsadministrator können Sie Benachrichtigungen konfigurieren, wenn Zertifikate kurz vor dem Ablauf stehen, und Informationen darüber einschließen, welche NetScaler-Instanzen diese Zertifikate verwenden. Durch die Aktivierung von Benachrichtigungen können Sie Ihre SSL-Zertifikate rechtzeitig erneuern.

Sie können beispielsweise eine E-Mail-Benachrichtigung einrichten, die 30 Tage vor Ablauf Ihres Zertifikats an eine E-Mail-Verteilerliste gesendet wird.

So richten Sie Benachrichtigungen über die NetScaler Console ein:

1. Navigieren Sie in der NetScaler Console zu **Infrastructure > SSL Dashboard**.
2. Klicken Sie auf der Seite **SSL Dashboard** auf **Settings**.
3. Klicken Sie auf der Seite **Settings** auf **General**.
4. Geben Sie im Abschnitt **Notification Settings** an, wann die Benachrichtigung in Tagen vor dem Ablaufdatum gesendet werden soll.
5. Wählen Sie den Typ der Benachrichtigung aus, die Sie senden möchten. Wählen Sie den Benachrichtigungstyp und die Verteilerliste aus dem Menü aus. Die Benachrichtigungstypen sind wie folgt:

    - **E-Mail** – Geben Sie einen Mailserver und Profildetails an. Eine E-Mail wird ausgelöst, wenn Ihre Zertifikate kurz vor dem Ablauf stehen.
    - **Slack** – Geben Sie ein Slack-Profil an. Eine Benachrichtigung wird gesendet, wenn Ihre Zertifikate kurz vor dem Ablauf stehen.
    - **PagerDuty** – Geben Sie ein PagerDuty-Profil an. Basierend auf den in Ihrem PagerDuty-Portal konfigurierten Benachrichtigungseinstellungen wird eine Benachrichtigung gesendet, wenn Ihre Zertifikate kurz vor dem Ablauf stehen.
    - **ServiceNow** – Eine Benachrichtigung wird an das Standard-ServiceNow-Profil gesendet, wenn Ihre Zertifikate kurz vor dem Ablauf stehen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG

Stellen Sie sicher, dass der Citrix Cloud ITSM Adapter für ServiceNow konfiguriert und in die NetScaler Console integriert ist. Weitere Informationen finden Sie unter NetScaler Console in ServiceNow-Instanz integrieren.

6. Klicken Sie auf **Speichern und Beenden**.

Installiertes Zertifikat aktualisieren

Nachdem Sie ein erneuertes Zertifikat von der Zertifizierungsstelle (CA) erhalten haben, müssen Sie sich nicht bei einzelnen NetScaler-Instanzen anmelden, um die Zertifikate zu aktualisieren. Sie können die vorhandenen Zertifikate in der NetScaler Console mit Zertifikaten aus dem Zertifikatsspeicher aktualisieren.

So aktualisieren Sie ein SSL-Zertifikat über die NetScaler Console:

1. Navigieren Sie in der NetScaler Console zu **Infrastructure > SSL Dashboard**.
2. Klicken Sie auf eines der Diagramme, um die Liste der SSL-Zertifikate anzuzeigen.
3. Wählen Sie auf der Seite **SSL-Zertifikate** ein Zertifikat aus und klicken Sie auf **Aktualisieren**. Alternativ können Sie auf das SSL-Zertifikat klicken, um dessen Details anzuzeigen, und klicken Sie dann oben rechts auf der Seite **SSL-Zertifikat** auf **Aktualisieren**.
4. Wählen Sie auf der Seite **SSL-Zertifikat aktualisieren** die Option **Zertifikat** aus, um die Seite **Zertifikatsspeicher** anzuzeigen.

5. Wählen Sie auf der Seite **Zertifikatsspeicher** die Zertifikatsdatei aus, die Sie hinzufügen möchten. Klicken Sie auf **Auswählen**.

6. Wenn der Domänenname des neuen Zertifikats nicht mit dem alten Zertifikat übereinstimmt und Sie möchten, dass der Server die neue Domäne hostet, wählen Sie **Keine Domänenprüfung** aus.

   Klicken Sie auf **OK**. Alle SSL-virtuellen Server, an die dieses Zertifikat gebunden ist, werden automatisch aktualisiert.

   Wenn Sie ein vorhandenes SSL-Zertifikat mit einer Zertifikatskette aus dem Zertifikatsspeicher aktualisieren, wird das vorhandene Zertifikat mit den verknüpften Zertifikaten aktualisiert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wählen Sie das Zertifikat aus und klicken Sie auf **Details**, um die Zertifikatskette anzuzeigen.

Installieren von SSL-Zertifikaten auf einer NetScaler-Instanz

Bevor Sie SSL-Zertifikate auf NetScaler-Instanzen installieren, stellen Sie sicher, dass die Zertifikate von vertrauenswürdigen CAs ausgestellt wurden. Stellen Sie außerdem sicher, dass die Schlüssellänge der Zertifikatsschlüssel 2.048 Bit oder höher ist und dass die Schlüssel mit sicheren Signaturalgorithmen signiert sind.

So installieren Sie ein SSL-Zertifikat von einer anderen NetScaler-Instanz:

Sie können ein Zertifikat auch von einer ausgewählten NetScaler-Instanz importieren und über die NetScaler Console-GUI auf andere Ziel-NetScaler-Instanzen anwenden.

1. Navigieren Sie zu **Infrastructure > SSL Dashboard**.
2. Klicken Sie in der oberen rechten Ecke des SSL-Dashboards auf **Installieren**.
3. Geben Sie auf der Seite **SSL-Zertifikat auf NetScaler-Instanzen installieren** die folgenden Parameter an:

   a. Zertifikatsquelle

      Wählen Sie die Option **Von Instanz importieren**.

      - Wählen Sie die **Instanz** aus, von der Sie das Zertifikat importieren möchten.
      - Wählen Sie das **Zertifikat** aus der Liste aller SSL-Zertifikatsdateien auf der Instanz aus.

   b. Zertifikatsdetails

      - **Zertifikatsname**. Geben Sie einen Namen für den Zertifikatsschlüssel an.
      - **Passwort**. Passwort zur Verschlüsselung des privaten Schlüssels. Sie können diese Option verwenden, um verschlüsselte private Schlüssel hochzuladen.

4. Klicken Sie auf **Instanzen auswählen**, um die NetScaler-Instanzen auszuwählen, auf denen Sie Ihre Zertifikate installieren möchten.
5. Klicken Sie auf OK.

So installieren Sie ein SSL-Zertifikat von NetScaler Console:

1. Navigieren Sie zu **Infrastructure > SSL Dashboard**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Klicken Sie in der oberen rechten Ecke des Dashboards auf **Zertifikat installieren**.
3. Geben Sie auf der Seite **SSL-Zertifikat auf NetScaler-Instanz installieren** die folgenden Parameter an:
    - **Zertifikatsdatei** – Laden Sie eine SSL-Zertifikatsdatei hoch, indem Sie entweder **Lokal** (Ihr lokaler Computer) oder **Appliance** (die Zertifikatsdatei muss auf der NetScaler-Instanz vorhanden sein) auswählen.
    - **Schlüsseldatei** – Laden Sie die Schlüsseldatei hoch.
    - **Zertifikatsname** – Geben Sie einen Namen für den Zertifikatsschlüssel an.
    - **Passwort** – Passwort zur Verschlüsselung des privaten Schlüssels. Sie können diese Option verwenden, um verschlüsselte private Schlüssel hochzuladen.
    - **Instanzen auswählen** – Wählen Sie die NetScaler-Instanzen aus, auf denen Sie Ihre Zertifikate installieren möchten.
4. Um die Konfiguration für die zukünftige Verwendung zu speichern, aktivieren Sie das Kontrollkästchen **Konfiguration speichern**.
5. Klicken Sie auf **OK**.

Eine Zertifikatsignieranforderung (CSR) erstellen

Eine Zertifikatsignieranforderung (CSR) ist ein Block verschlüsselten Textes, der auf dem Server generiert wird, auf dem das Zertifikat verwendet werden soll. Sie enthält Informationen, die im Zertifikat enthalten sind, wie den Namen Ihrer Organisation, den allgemeinen Namen (Domänennamen), den Ort und das Land.

So erstellen Sie eine CSR mit NetScaler Console:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > SSL Dashboard**.
2. Klicken Sie auf eines der Diagramme, um die Liste der installierten SSL-Zertifikate anzuzeigen, wählen Sie dann das Zertifikat aus, für das Sie eine CSR erstellen möchten, und wählen Sie **Create CSR** aus der Dropdown-Liste **Select Action**.
3. Geben Sie auf der Seite **Create Certificate Signing Request (CSR)** einen Namen für die CSR an.
4. Führen Sie einen der folgenden Schritte aus:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Schlüssel hochladen** – Wählen Sie die Option **I have a Key**. Um Ihre Schlüsseldatei hochzuladen, wählen Sie entweder **Local** (Ihr lokaler Computer) oder **Appliance** (die Schlüsseldatei muss auf der virtuellen Instanz der NetScaler Console vorhanden sein).
- **Schlüssel erstellen** – Wählen Sie die Option **I do not have a Key** und geben Sie dann die folgenden Parameter an:

OPTIONEN	BESCHREIBUNG
Verschlüsselungsalgorithmus	Schlüsseltyp. Zum Beispiel RSA.
Schlüsseldateiname	Name für Ihre Datei, in der der RSA-Schlüssel gespeichert ist.
Schlüsselgröße	Schlüsselgröße in Bit.
Wert des öffentlichen Exponenten	Wählen Sie entweder **3** oder **F4** aus der bereitgestellten Dropdown-Liste. Dieser Wert ist Teil des Chiffrieralgorithmus, der zum Erstellen Ihres RSA-Schlüssels erforderlich ist.
Schlüsselformat	Standardmäßig ist PEM ausgewählt. PEM ist das empfohlene Schlüsselformat für Ihr SSL-Zertifikat.
PEM-Kodierungsalgorithmus	Wählen Sie in der Dropdown-Liste den Algorithmus (**DES** oder **DES3**) aus, den Sie zum Verschlüsseln des generierten RSA-Schlüssels verwenden möchten. Wenn Sie diesen Algorithmus auswählen, müssen Sie eine PEM-Passphrase angeben.
PEM-Passphrase	Wenn Sie den PEM-Kodierungsalgorithmus gewählt haben, geben Sie eine Passphrase ein.
PEM-Passphrase bestätigen	Bestätigen Sie Ihre PEM-Passphrase.

Ein neuer Schlüssel wird erstellt. Navigieren Sie zu **Infrastructure > SSL Dashboard**, wählen Sie **View Files on NetScaler Console** aus der Liste und dann die Registerkarte **SSL Keys**, um den Schlüssel anzuzeigen.

5. Klicken Sie auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Geben Sie auf der folgenden Seite weitere Details an.

   Die meisten Felder haben Standardwerte, die aus dem Betreff des ausgewählten Zertifikats extrahiert werden. Der Betreff enthält Details wie den allgemeinen Namen, den Organisationsnamen, den Bundesstaat und das Land.

   Im Feld **Subject Alternative Name** können Sie mehrere Werte angeben, z. B. Domänennamen und IP-Adressen mit einem einzigen Zertifikat. Die alternativen Antragstellernamen helfen Ihnen, mehrere Domänen mit einem einzigen Zertifikat zu sichern.

   Geben Sie die Domänennamen und IP-Adressen im folgenden Format an:

   ```
   DNS:<Domain name>, IP:<IP address>
   ```

   Zum Beispiel ist `10.0.0.1` eine IP-Adresse und `www.example.com` ein Domänenname.

   Überprüfen Sie die Felder und klicken Sie auf **Weiter**.

HINWEIS

Die meisten CAs akzeptieren Zertifikatseinreichungen per E-Mail. Die CA sendet ein gültiges Zertifikat an die E-Mail-Adresse zurück, von der aus Sie die CSR übermitteln.

SSL-Zertifikate verknüpfen und Verknüpfung aufheben

Sie erstellen ein Zertifikatspaket, indem Sie mehrere Zertifikate miteinander verknüpfen. Um ein Zertifikat mit einem anderen Zertifikat zu verknüpfen, muss der Aussteller des ersten Zertifikats mit der Domäne des zweiten Zertifikats übereinstimmen. Wenn Sie beispielsweise Zertifikat A mit Zertifikat B verknüpfen möchten, muss der „Aussteller“ von Zertifikat A mit der „Domäne“ von Zertifikat B übereinstimmen.

So verknüpfen Sie ein SSL-Zertifikat mit einem anderen Zertifikat mithilfe von NetScaler Console:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > SSL Dashboard**.
2. Klicken Sie auf eines der Diagramme, um die Liste der SSL-Zertifikate anzuzeigen.
3. Wählen Sie das Zertifikat aus, das Sie verknüpfen möchten, und wählen Sie dann **Link** aus der Dropdown-Liste **Select Action**.
4. Wählen Sie aus der Liste der übereinstimmenden Zertifikate das Zertifikat aus, mit dem Sie verknüpfen möchten, und klicken Sie dann auf **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Wenn kein übereinstimmendes Zertifikat gefunden wird, wird die folgende Meldung angezeigt: Es wurde kein Zertifikat zum Verknüpfen gefunden.

So heben Sie die Verknüpfung eines SSL-Zertifikats mithilfe von NetScaler Console auf:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > SSL Dashboard**.
2. Klicken Sie auf eines der Diagramme, um die Liste der SSL-Zertifikate anzuzeigen.
3. Wählen Sie eines der verknüpften Zertifikate aus, und wählen Sie dann **Unlink** aus der Dropdown-Liste **Select Action**.
4. Klicken Sie auf **OK**.

HINWEIS

Wenn das ausgewählte Zertifikat nicht mit einem anderen Zertifikat verknüpft ist, wird die folgende Meldung angezeigt: Zertifikat hat keine CA-Verknüpfung.

Eine Unternehmensrichtlinie konfigurieren

Sie können eine Unternehmensrichtlinie konfigurieren und alle vertrauenswürdigen CAs und sicheren Signaturalgorithmen hinzufügen sowie die empfohlene Schlüssellänge für Ihre Zertifikatsschlüssel in NetScaler Console auswählen. Wenn eines der auf Ihrer NetScaler-Instanz installierten Zertifikate nicht zur Unternehmensrichtlinie hinzugefügt wurde, zeigt das SSL-Zertifikats-Dashboard den Aussteller dieser Zertifikate als Nicht empfohlen an.

Wenn die Schlüssellänge des Zertifikats nicht der empfohlenen Schlüssellänge in der Unternehmensrichtlinie entspricht, zeigt das SSL-Zertifikats-Dashboard die Stärken dieser Schlüssel als Nicht empfohlen an.

So konfigurieren Sie eine Unternehmensrichtlinie in NetScaler Console:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > SSL Dashboard**, und klicken Sie dann auf **Settings**.
2. Klicken Sie auf der Seite **Settings** auf das Symbol **Enterprise Policy**, um alle vertrauenswürdigen CAs und sicheren Signaturalgorithmen hinzuzufügen und die empfohlene Schlüssellänge für Ihre Zertifikate und Schlüssel auszuwählen. Unterstützte Schlüssellängen sind 512, 1024, 2048, 3072 und 4096 Bit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Empfohlene Schlüssellängen** – Bezeichnet die Algorithmus-Sicherheit und die Anzahl der Bits in einem Schlüssel.
- **Empfohlene Signaturalgorithmen** – Bezeichnet die signierten Token, die für die Anwendungen ausgegeben werden.
- **Empfohlene vertrauenswürdige CA** – Bezeichnet die vertrauenswürdige Entität, die die digitalen Zertifikate ausstellt. Klicken Sie auf das Symbol **+**, um weitere Entitäten hinzuzufügen.
- **Empfohlene SSL-Protokolle** – Bezeichnet die TLS/SSL-Versionen.

3. Klicken Sie auf **Finish** oder **Save and Exit**, um Ihre Unternehmensrichtlinie zu speichern.

HINWEIS

Das SSL-Dashboard zeigt nur die **Signaturalgorithmen** an, die über die Option **Settings** ausgewählt wurden, und andere werden als **Nicht empfohlen** angezeigt.

SSL-Zertifikate von NetScaler-Instanzen abrufen

NetScaler Console ruft SSL-Zertifikate automatisch alle 24 Stunden mithilfe von NITRO-Aufrufen und dem Secure Copy (SCP)-Protokoll ab. Sie können die SSL-Zertifikate auch manuell abrufen, um neu hinzugefügte SSL-Zertifikate auf den NetScaler-Instanzen zu erkennen. Das Abrufen aller SSL-Zertifikate der NetScaler-Instanzen belastet das Netzwerk stark.

Anstatt alle SSL-Zertifikate der NetScaler-Instanzen abzurufen, können Sie manuell nur die SSL-Zertifikate einer oder mehrerer ausgewählter Instanzen abrufen.

So rufen Sie SSL-Zertifikate auf NetScaler-Instanzen ab:

1. Navigieren Sie zu **Infrastructure > SSL Dashboard**.
2. Klicken Sie auf der Seite **SSL Dashboard** oben rechts auf **Poll Now**.
3. Das Fenster **Poll Now** wird eingeblendet und bietet Ihnen die Möglichkeit, alle NetScaler-Instanzen im Netzwerk oder ausgewählte Instanzen abzurufen.
    a. Um die SSL-Zertifikate aller NetScaler-Instanzen abzurufen, wählen Sie die Registerkarte **All Instances** und klicken Sie auf **Start Polling**.
4. Um bestimmte Instanzen abzurufen, wählen Sie die Registerkarte **Select Instances**, wählen Sie die Instanzen aus der Liste aus und klicken Sie auf **Poll Now**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verwenden Sie den NetScaler Console Zertifikatsspeicher zur Verwaltung von SSL-Zertifikaten

Der NetScaler Console Zertifikatsspeicher hilft Ihnen, Ihre SSL-Zertifikate an einem Ort zu speichern und zu verwalten. Sie können die gespeicherten Zertifikate später verwenden, um NetScaler-Einstellungen zu konfigurieren.

Der Zertifikatsspeicher ermöglicht es Ihnen, SSL-Zertifikate hinzuzufügen, zu aktualisieren und zu löschen. Sie können den Zertifikatsspeicher auch verwenden, um ein Zertifikat von einer NetScaler-Instanz zu importieren und es auf andere Ziel-NetScaler-Instanzen anzuwenden.

SSL-Zertifikate zum Zertifikatsspeicher hinzufügen

1. Navigieren Sie zu **Infrastructure > SSL Dashboard > Certificate Store**. Klicken Sie auf **Add**.
2. Geben Sie auf der Seite **Add Certificate** die folgenden Details ein:

    - **Zertifikatsschlüsselname** – Geben Sie einen Namen für das Zertifikat ein. Der Name darf nur alphanumerische ASCII-Zeichen, Unterstriche und Bindestriche enthalten und muss weniger als 30 Zeichen lang sein. Sie können den Namen nach der Erstellung des Zertifikats nicht mehr ändern.
    - **Zertifikatsdatei** – Navigieren Sie zu Ihrem lokalen Laufwerk und laden Sie die Zertifikatsdatei hoch.
    - **Schlüsseldatei** – Laden Sie die Schlüsseldatei von Ihrem lokalen Computer hoch.
    - **Passwort** – Wenn Sie einen verschlüsselten privaten Schlüssel im PEM-Format haben, geben Sie die Passphrase ein, die zum Verschlüsseln des privaten Schlüssels verwendet wurde.
    - **Zertifikatskette hinzufügen** – Wählen Sie diese Option, um das Zertifikat in einer Zertifikatskette hinzuzufügen.
    - **Zertifikatskette** – Navigieren Sie zu Ihrem lokalen Laufwerk und laden Sie die Zertifikatsdatei hoch.
    - Klicken Sie auf **Create**.

SSL-Zertifikate im Zertifikatsspeicher aktualisieren

1. Navigieren Sie zu **Infrastructure > SSL Dashboard > Certificate Store**. Wählen Sie das Zertifikat aus, das Sie aktualisieren möchten, und klicken Sie auf **Update**.
2. Geben Sie auf der Seite **Zertifikat aktualisieren** die folgenden Details ein:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Zertifikatschlüsselname** – Zeigt den Namen des Zertifikats an, das Sie zum Aktualisieren ausgewählt haben.
- **Zertifikatdatei** – Um die Zertifikatdatei zu aktualisieren, laden Sie eine Zertifikatdatei hoch.
- **Schlüsseldatei** – Um die Schlüsseldatei zu aktualisieren, laden Sie eine Schlüsseldatei von Ihrem lokalen Computer hoch.
- **Passwort** – Wenn Sie einen verschlüsselten privaten Schlüssel im PEM-Format haben, geben Sie die Passphrase ein, die zum Verschlüsseln des privaten Schlüssels verwendet wurde.
- **Zertifikatskette hinzufügen** – Wählen Sie diese Option, um das Zertifikat in einer Zertifikatskette hinzuzufügen.
- **Zertifikatskette** – Navigieren Sie zu Ihrem lokalen Laufwerk und laden Sie die Zertifikatdatei hoch.
- Klicken Sie auf **OK**.

SSL-Zertifikate aus dem Zertifikatsspeicher löschen

1. Navigieren Sie zu **Infrastructure > SSL Dashboard > Certificate Store**. Klicken Sie auf **Löschen**.
2. Klicken Sie auf **Ja**, wenn Sie dazu aufgefordert werden, um das Zertifikat zu löschen.

SSL-Zertifikate auf NetScaler®-Instanzen installieren

1. Navigieren Sie zu **Infrastructure > SSL Dashboard > Certificate Store**. Wählen Sie das Zertifikat aus, das Sie auf einer NetScaler-Instanz installieren möchten.
2. Geben Sie auf der Seite **SSL-Zertifikat auf NetScaler-Instanzen installieren** die folgenden Details ein:

   a. **Zertifikatsquelle**

   - **Zertifikat** – Zeigt den Namen des von Ihnen ausgewählten Zertifikats an.

   b. **Zertifikatdetails**

   - **Zertifikatname** – Zeigt den Namen des Zertifikats an.
   - **Konfiguration speichern** – Wählen Sie diese Option, um die NetScaler-Konfiguration zu speichern. Die NetScaler-Konfiguration wird nach der Installation des Zertifikats gespeichert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Klicken Sie auf **Instanzen auswählen**, um die NetScaler-Instanzen auszuwählen, auf denen Sie Ihre Zertifikate installieren möchten.

Klicken Sie auf **OK**.

Zertifikate von NetScaler-Instanzen importieren

1. Navigieren Sie zu **Infrastructure > SSL Dashboard > Certificate Store**. Klicken Sie auf **NetScaler-Zertifikate importieren**.
2. Auf der Seite **NetScaler-Zertifikate importieren** können Sie eine der folgenden Registerkarten auswählen:

   - **NetScaler-Zertifikate importieren** – Klicken Sie auf **Polling starten**, um alle SSL-Zertifikate auf allen NetScaler-Instanzen abzufragen.
   - **Instanzen auswählen** – Wählen Sie eine NetScaler-Instanz aus und klicken Sie auf **NetScaler-Zertifikate importieren**, um SSL-Zertifikate nur auf der ausgewählten NetScaler-Instanz abzufragen.

   Nach dem Polling werden die SSL-Zertifikate und Schlüsseldateien heruntergeladen und dem Zertifikatsspeicher hinzugefügt.

   HINWEIS:

   Der Importvorgang schlägt für Zertifikate fehl, wenn identische Zertifikatnamen im Speicher vorhanden sind. Der Importvorgang setzt jedoch das Polling der verbleibenden Zertifikate fort und fügt NetScaler-Zertifikate, falls verfügbar, dem Speicher hinzu.

Serverzertifikate ohne Zwischen-Uploads aktualisieren

Sie können Zertifikate erneuern, ohne die sich wiederholende Aufgabe des erneuten Hochladens von Zwischenzertifikaten. Diese Verbesserung reduziert den manuellen Arbeitsaufwand und minimiert das Risiko von Konfigurationsfehlern.

Mühelose Erneuerungen:

NetScaler Console bewahrt die vorhandene Zertifikatskette während eines Updates standardmäßig. Dies stellt sicher, dass Ihre Kette intakt und gültig bleibt, selbst wenn Sie nur ein neues Zertifikat auf Serverebene hochladen.

Wichtige Verbesserungen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Reduzierte Komplexität**: Eliminiert obligatorische Zwischen-Uploads bei Standard-Serverzertifikats-Updates.
- **Sicherheit geht vor**: Die automatische Kettenkonservierung verhindert „Kettenbrüche“, eine häufige Ursache für SSL-Handshake-Fehler.

So aktualisieren Sie Serverzertifikate ohne Zwischen-Uploads

1. Navigieren Sie zu **Infrastructure > SSL Dashboard > Certificate Store**.
2. Wählen Sie das Zertifikat aus, das Sie aktualisieren möchten, und klicken Sie auf **Update**.
3. **Vorhandene Zertifikatskette überschreiben** – Wählen Sie diese Option, wenn Ihre Erneuerung Änderungen an der Zwischenkette erfordert:
    - **Mit einem Bundle**: Ersetzt die vorhandene Kette durch das neu hochgeladene Bundle.
    - **Ohne Bundle**: Entfernt die aktuelle Zertifikatskette vollständig.
4. **Zertifikatskette hinzufügen** – Wählen Sie diese Option, um Zwischenzertifikate manuell hochzuladen und anzuhängen, falls diese nicht in Ihrer primären Serverzertifikatsdatei enthalten sind.

Beispiele

Die endgültige Zertifikatsstruktur hängt vom Kettenstatus Ihres vorhandenen Zertifikats und den Optionen ab, die Sie während des Updates auswählen:

SZENARIO A: VORHANDENES ZERTIFIKAT HAT KEINE KETTE

UPDATE-AKTION	ERGEBNIS
Neu hochgeladenes Zertifikat enthält keine Kette	Das Serverzertifikat wird aktualisiert. Es wird keine Zwischenkette hinzugefügt.
Neu hochgeladenes Zertifikat enthält eine Kette	Das Serverzertifikat wird aktualisiert und die neue Zwischenkette wird angehängt.

SZENARIO B: VORHANDENES ZERTIFIKAT HAT EINE KETTE

UPDATE-AKTION	ERGEBNIS
Neu hochgeladenes Zertifikat enthält eine Kette (Vorhandene Zertifikatskette überschreiben ist aktiviert)	Das Serverzertifikat wird aktualisiert und die vorhandene Zwischenkette wird durch die neue Kette ersetzt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

UPDATE-AKTION	ERGEBNIS
Neu hochgeladenes Zertifikat enthält keine Kette (Vorhandene Zertifikatskette überschreiben ist aktiviert)	Das Serverzertifikat wird aktualisiert und die vorhandene Zwischenkette wird explizit entfernt.

Konfigurationsjobs

Der Konfigurationsverwaltungsprozess der NetScaler Console gewährleistet die ordnungsgemäße Replikation von Konfigurationsänderungen, System-Upgrades und anderen Wartungsaktivitäten über mehrere NetScaler-Instanzen im Netzwerk hinweg.

Mit NetScaler Console können Sie Konfigurationsjobs erstellen, die Ihnen helfen, all diese Aktivitäten auf mehreren Geräten als einzelne Aufgabe mit Leichtigkeit auszuführen. Konfigurationsjobs und -vorlagen vereinfachen die meisten sich wiederholenden administrativen Aufgaben zu einer einzigen Aufgabe in NetScaler Console. Ein Konfigurationsjob enthält eine Reihe von Konfigurationsbefehlen, die Sie auf einem oder mehreren verwalteten Geräten ausführen können.

Konfigurationsjobs können entweder SSH-Befehle für Konfigurationsbefehle verwenden oder SCP für das Kopieren von Dateien entweder lokal oder auf eine andere Appliance nutzen. Zum Beispiel können wir ein HA-Failover oder ein HA-Upgrade planen.

Sie können einen Konfigurationsjob mit einer der folgenden vier Optionen in NetScaler Console erstellen. Verwenden Sie eine davon, um eine wiederverwendbare Quelle von Befehlen und Anweisungen für das System zu erstellen, um einen Konfigurationsjob auszuführen.

1. Konfigurationsvorlage
2. Instanz
3. Datei
4. Aufzeichnen und Abspielen

Konfigurationsvorlage

Sie können Konfigurationsvorlagen erstellen, während Sie einen Job erstellen und eine Reihe von Konfigurationsbefehlen als Vorlage speichern. Wenn Sie diese Vorlagen auf der Seite „Jobs erstellen“ speichern, werden sie automatisch auf der Seite „Vorlage erstellen“ angezeigt. Weitere Informationen finden Sie unter So verwenden Sie die Master-Konfigurationsvorlage in NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Die Option **Umbenennen** ist für die Standard-Konfigurationsvorlagen deaktiviert. Sie können jedoch benutzerdefinierte Konfigurationsvorlagen umbenennen.

Sie können eine der folgenden Vorlagen verwenden:

Konfigurationseditor: Sie können den Konfigurationseditor verwenden, um CLI-Befehle einzugeben, die Konfiguration als Vorlage zu speichern und sie zum Konfigurieren von Jobs zu verwenden.

Integrierte Vorlage: Sie können aus einer Liste von Konfigurationsvorlagen wählen. Diese Vorlagen stellen die Syntax der CLI-Befehle bereit und ermöglichen es Ihnen, Werte für die Variablen anzugeben. Die integrierten Vorlagen sind mit ihren Beschreibungen in der folgenden Tabelle aufgeführt. Sie können einen Auftrag mithilfe der Option für integrierte Vorlagen planen. Ein Auftrag ist eine Reihe von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen ausführen können. Sie können beispielsweise die Option für integrierte Vorlagen verwenden, um einen Auftrag zur Konfiguration von Syslog-Servern zu planen. Sie können den Auftrag auch sofort ausführen oder für einen späteren Zeitpunkt planen.

Weitere Informationen finden Sie unter Verwenden von Konfigurationsvorlagen zum Erstellen von Auditvorlagen

Instanz

Sie können ein Single-Bundle-Upgrade Ihrer NetScaler SDX-Instanzen durchführen, die NetScaler Release 11.0 und höher ausführen. Um ein Single-Bundle-Upgrade durchzuführen, verwenden Sie eine integrierte Aufgabe in NetScaler Console. Sie können eine NetScaler-Instanz auch aktualisieren, indem Sie die laufende Konfiguration oder eine gespeicherte Konfiguration extrahieren und die Befehle auf einer anderen NetScaler-Instanz desselben Typs ausführen. Dieses Upgrade ermöglicht es Ihnen, die Konfiguration einer Instanz auf die andere zu replizieren.

Datei

Sie können eine Konfigurationsdatei von Ihrem lokalen Computer hochladen und Aufträge erstellen.

Vorteile der Verwendung einer Datei

- Sie können jede Textdatei verwenden, um eine wiederverwendbare Quelle für Konfigurationsbefehle zu erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Es ist keine Formatierung erforderlich.
- Die Datei kann auf Ihrem lokalen Computer gespeichert werden.

Sie können entweder eine neue Datei erstellen und speichern oder eine vorhandene Datei importieren und die Befehle ausführen.

Aufzeichnen und Abspielen

Mit „Auftrag erstellen“ können Sie entweder eigene CLI-Befehle eingeben oder die Schaltfläche „Aufzeichnen und Abspielen“ verwenden, um Befehle aus einer NetScaler-Sitzung abzurufen. Wenn Sie den Auftrag ausführen, werden Änderungen in der ns.conf auf der ausgewählten Instanz aufgezeichnet und in die NetScaler Console kopiert. Siehe Verwenden von Aufzeichnen und Abspielen zum Erstellen von Konfigurationsaufträgen.

Bericht dieses Dashboards exportieren

Um den Bericht dieser Seite zu exportieren, klicken Sie auf das Symbol **Exportieren** oben rechts auf dieser Seite. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren**. Um den Bericht im PDF-, JPEG-, PNG- oder CSV-Format anzuzeigen und zu speichern.
2. Wählen Sie die Registerkarte **Export planen**. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu versenden.

HINWEIS

- Wenn Sie die **wöchentliche** Wiederholung auswählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie die **monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage, an denen der Bericht geplant werden soll, durch Kommas getrennt eingeben.

Verwandte Artikel

- Verwenden des SCP-(put)-Befehls in Konfigurationsaufträgen
- Verwenden von Variablen in Konfigurationsaufträgen
- Erstellen von Konfigurationsaufträgen aus Korrekturbefehlen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfigurationsauftrag erstellen

Ein Auftrag ist ein Satz von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen erstellen und ausführen können.

Sie können Aufträge erstellen, um Konfigurationsänderungen über Instanzen hinweg vorzunehmen. Sie können Konfigurationen auf mehreren Instanzen replizieren in Ihrem Netzwerk und Konfigurationsaufgaben aufzeichnen und wiedergeben mithilfe der NetScaler Console GUI und diese in CLI-Befehle umwandeln.

Sie können die Funktion „Konfigurationsaufträge“ der NetScaler Console verwenden, um einen Konfigurationsauftrag zu erstellen, E-Mail-Benachrichtigungen zu senden und Ausführungsprotokolle der erstellten Aufträge zu überprüfen.

So erstellen Sie einen Konfigurationsauftrag in NetScaler Console:

1. Navigieren Sie zu **Infrastructure > Configuration > Configuration Jobs**.
2. Klicken Sie auf **Create Job**.
3. Geben Sie auf der Seite **Create Job** unter der Registerkarte **Select Configuration** den Auftragsnamen ein und wählen Sie den **Instance Type** aus der Liste aus.
4. Wählen Sie in der Liste **Configuration Source** die Konfigurationsauftragsvorlage aus, die Sie erstellen möchten. Fügen Sie die Befehle für die ausgewählte Vorlage hinzu.

    - Sie können die Befehle entweder eingeben oder die vorhandenen Befehle aus den gespeicherten Konfigurationsvorlagen importieren.
    - Sie können auch mehrere Vorlagen unterschiedlicher Typen im Konfigurationseditor hinzufügen, während Sie einen Auftrag in den Konfigurationsaufträgen erstellen.
    - Wählen Sie aus der Liste **Configuration Source** die verschiedenen Vorlagen aus und ziehen Sie die Vorlagen dann in den Konfigurationseditor. Die Vorlagentypen können **Configuration Template**, **In built Template**, **Master Configuration**, **Record and Play**, **Instance** und **File** sein.

HINWEIS

Wenn Sie die Vorlage „Deploy Master Configuration Job“ zum ersten Mal hinzufügen und dann eine Vorlage eines anderen Typs hinzufügen, wird die gesamte Auftragsvorlage zu einem Master-Konfigurationstyp.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können die Befehle im Konfigurationseditor auch neu anordnen und umsortieren. Sie können den Befehl von einer Zeile in eine andere verschieben, indem Sie die Befehlszeile ziehen und ablegen. Sie können die Befehlszeile auch von einer Zeile zu einer beliebigen Zielzeile verschieben oder neu anordnen, indem Sie einfach die Befehlszeilennummer im Textfeld ändern. Sie können die Befehlszeile auch neu anordnen und umsortieren, während Sie den Konfigurationsauftrag bearbeiten.

Sie können Variablen definieren, die es Ihnen ermöglichen, diesen Parametern unterschiedliche Werte zuzuweisen oder einen Job über mehrere Instanzen hinweg auszuführen. Sie können alle Variablen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsjobs definiert haben, in einer einzigen konsolidierten Ansicht überprüfen. Klicken Sie auf die Registerkarte **Variablenvorschau**, um die Variablen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsjobs definiert haben, in einer einzigen konsolidierten Ansicht anzuzeigen.

Sie können Rollback-Befehle für jeden Befehl im Konfigurationseditor anpassen. Um Ihre angepassten Befehle anzugeben, aktivieren Sie die Option für benutzerdefiniertes Rollback.

WICHTIG

Damit das benutzerdefinierte Rollback wirksam wird, schließen Sie den Assistenten **Job erstellen** ab. Wählen Sie auf der Registerkarte **Ausführen** die Option **Erfolgreiche Befehle zurücksetzen** aus der Liste **Bei Befehlsfehler** aus.

5. Wählen Sie auf der Registerkarte **Instanzen auswählen** die Instanzen aus, auf denen Sie die Konfigurationsprüfung ausführen möchten.

   a. In einem NetScaler Hochverfügbarkeitspaar können Sie einen Konfigurationsjob lokal auf einem primären oder einem sekundären Knoten ausführen. Wählen Sie aus, auf welchem Knoten Sie den Job ausführen möchten.

      - **Auf primären Knoten ausführen** – Wählen Sie diese Option, um den Job nur auf primären Knoten auszuführen.
      - **Auf sekundären Knoten ausführen** – Wählen Sie diese Option, um den Job nur auf sekundären Knoten auszuführen.

      Sie können auch sowohl den primären als auch den sekundären Knoten auswählen, um denselben Konfigurationsjob auszuführen. Wenn Sie weder den primären noch den

© 1997–2026 Citrix Systems, Inc. All rights reserved.

sekundären Knoten auswählen, wird der Konfigurationsjob automatisch auf dem primären Knoten ausgeführt.

b. Klicken Sie auf **Instanzen hinzufügen** und wählen Sie die Instanzen aus der Liste aus. Klicken Sie auf **OK**.

c. Klicken Sie auf **Weiter**.

6. Auf der Registerkarte **Variablenwerte angeben** haben Sie zwei Optionen:

   a. Laden Sie die Eingabedatei herunter, um die Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den NetScaler Console-Server hoch.

   b. Geben Sie gemeinsame Werte für die Variablen ein, die Sie für alle Instanzen definiert haben.

   c. Klicken Sie auf **Weiter**.

7. Bewerten und überprüfen Sie die Befehle, die auf jeder Instanz auf der Registerkarte **Auftragsvorschau** ausgeführt werden sollen. Diese Registerkarte zeigt auch die Rollback-Befehle an, falls sie auf der Registerkarte **Konfiguration auswählen** angegeben wurden.
8. Auf der Registerkarte **Ausführen** wählen Sie, ob Sie Ihren Auftrag jetzt ausführen oder die Ausführung des Auftrags für später planen möchten.

   Wählen Sie außerdem eine der folgenden Aktionen aus der Liste **Bei Befehlsfehler** aus, die NetScaler Console ausführen soll, wenn der Befehl fehlschlägt:

   - **Fehler ignorieren und fortfahren**: NetScaler Console ignoriert den fehlgeschlagenen Befehl und führt die verbleibenden Befehle für die ausgewählte Instanz aus.

     HINWEIS

     Diese Aktion erlaubt es Ihnen nicht, einen Konfigurationsauftrag abzubrechen, der gerade ausgeführt wird.

   - **Weitere Ausführung stoppen**: NetScaler Console stoppt die verbleibenden Befehle, wenn ein Befehl während der Ausführung fehlschlägt.
   - **Erfolgreiche Befehle zurücksetzen**: NetScaler Console stellt die erfolgreich ausgeführten Befehle wieder her, wenn ein Befehl während der Ausführung fehlschlägt.

     Wenn das benutzerdefinierte Rollback aktiviert ist, führt die NetScaler Console die entsprechenden Rollback-Befehle für die fehlgeschlagenen Befehle aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Klicken Sie auf **Fertig stellen**.

So senden Sie eine E-Mail- und Slack-Benachrichtigung für einen Auftrag:

Eine E-Mail- und Slack-Benachrichtigung wird jetzt jedes Mal gesendet, wenn ein Auftrag ausgeführt oder geplant wird. Die Benachrichtigung enthält Details wie den Erfolg oder Misserfolg des Auftrags zusammen mit den relevanten Details.

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsaufträge**.
2. Wählen Sie den Auftrag aus, für den Sie E-Mail- und Slack-Benachrichtigungen aktivieren möchten, und klicken Sie auf **Bearbeiten**.
3. Auf der Registerkarte **Ausführen** gehen Sie zum Bereich **Ausführungsbericht empfangen über**:

   - Aktivieren Sie das Kontrollkästchen **E-Mail**, und wählen Sie die E-Mail-Verteilerliste aus, an die Sie den Ausführungsbericht senden möchten.

     Wenn Sie eine E-Mail-Verteilerliste hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie die Details des E-Mail-Servers an.
   - Aktivieren Sie das Kontrollkästchen **Slack**, und wählen Sie den Slack-Kanal aus, an den Sie den Ausführungsbericht senden möchten.

     Wenn Sie ein Slack-Profil hinzufügen möchten, klicken Sie auf **Hinzufügen** und geben Sie den **Profilnamen**, den **Kanalnamen** und das **Token** des erforderlichen Slack-Kanals an.

   ▢
4. Klicken Sie auf **Fertig stellen**.

So zeigen Sie die Details der Ausführungszusammenfassung an:

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsaufträge**.
2. Wählen Sie den Auftrag aus, für den Sie die Ausführungszusammenfassung anzeigen möchten, und klicken Sie auf **Details**.
3. Klicken Sie auf **Ausführungszusammenfassung**, um Folgendes anzuzeigen:

   - Den Status der Instanz für den ausgeführten Auftrag
   - Die für den Auftrag ausgeführten Befehle
   - Die Start- und Endzeit des Auftrags und
   - Den Namen des Instanzbenutzers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verwenden Sie „Aufzeichnen und Wiedergeben“, um Konfigurationsaufträge zu erstellen

Wenn Sie es gewohnt sind, die NetScaler-GUI zur Konfiguration einer NetScaler-Instanz zu verwenden, kann es manchmal schwierig sein, sich an die genauen CLI-Befehle zu erinnern, um eine Konfigurationsaufgabe zu erstellen und diese auf mehreren NetScaler-Instanzen auszuführen.

NetScaler Console ermöglicht es Ihnen, die über die GUI einer NetScaler-Instanz durchgeführten Konfigurationsaufgaben aufzuzeichnen und in CLI-Befehle umzuwandeln. Sie können dann aus diesen CLI-Befehlen eine Konfigurationsaufgabe erstellen und diese Aufgabe auf mehreren Instanzen ausführen.

So zeichnen Sie die GUI-Konfiguration auf und wandeln sie in eine Konfigurationsaufgabe um:

1. Navigieren Sie zu **Infrastructure > Configuration > Configuration Jobs**, und klicken Sie dann auf **Create Job**.
2. Geben Sie den Auftragsnamen und den Instanztyp an.
3. Wählen Sie aus der Liste **Configuration Source** die Option **Record and Play** aus, und wählen Sie dann die Quellinstanz aus, von der Sie die Konfiguration aufzeichnen möchten. Klicken Sie auf **Record**.

4. Die **NetScaler GUI** wird geöffnet. Konfigurieren Sie die Funktionen und Einstellungen, die die Konfigurationsaufgabe enthalten soll. Schließen Sie dann das NetScaler GUI-Fenster und klicken Sie im **Configuration Editor** auf **Stop**. Die Befehle werden als Link im linken Bereich angezeigt. Ziehen Sie die Befehle in den rechten Bereich und klicken Sie dann auf **Next**.

   Sie können die Befehle im Konfigurationseditor dann nach Bedarf neu anordnen und umsortieren. Sie können den Befehl von einer Zeile in eine andere verschieben, indem Sie die Befehlszeile ziehen und ablegen. Sie können die Befehlszeile auch von einer Zeile in eine beliebige Zielzeile verschieben oder neu anordnen, indem Sie einfach die Befehlszeilennummer im Textfeld ändern.
5. Sie können alle Variablen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben, in einer einzigen konsolidierten Ansicht überprüfen.
6. Führen Sie einen der folgenden Schritte aus, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Navigieren Sie beim Erstellen eines Konfigurationsauftrags zu **Infrastructure > Configuration Jobs**, wählen Sie **Create Job**. Auf der Seite **Create Job** können Sie alle Variablen überprüfen, die Sie beim Erstellen des Konfigurationsauftrags hinzugefügt haben.
- Navigieren Sie beim Bearbeiten eines Konfigurationsauftrags zu **Infrastructure > Configuration > Configuration Jobs**, wählen Sie den Jobnamen aus und klicken Sie auf **Edit**. Auf der Seite **Configure Job** können Sie alle Variablen überprüfen, die beim Erstellen des Konfigurationsauftrags hinzugefügt wurden.

7. Sie können dann auf die Registerkarte **Preview Variables** klicken, um die Variablen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben, in einer einzigen konsolidierten Ansicht anzuzeigen.
8. Ein neues Pop-up-Fenster wird angezeigt und zeigt alle Parameter von Variablen wie Name, Anzeigename, Typ und Standardwert in einem Tabellenformat an. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf die Schaltfläche **Fertig**, nachdem Sie Parameter bearbeitet oder geändert haben.

9. Klicken Sie auf **Instanzen hinzufügen** und wählen Sie die Instanzen aus, auf denen Sie den Konfigurationsauftrag ausführen möchten. Klicken Sie auf **OK** und dann auf **Weiter**.

10. Wenn Sie Variablen in den Befehlen angegeben haben, wählen Sie auf der Registerkarte **Variablenwerte angeben** eine der folgenden Optionen aus, um Variablen für Ihre Instanzen anzugeben:

    - **Eingabedatei für Variablenwerte hochladen**: Klicken Sie auf **Eingabeschlüsseldatei herunterladen**, um eine Eingabedatei herunterzuladen. Geben Sie in der Eingabedatei Werte für die Variablen ein, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den NetScaler Console-Server hoch.
    - **Gemeinsame Variablenwerte für alle Instanzen**: Geben Sie Werte für die Variablen ein. Die Variablen variieren je nach ausgewählter Vorlage.

    Die Eingabedateien, die die Variablenwerte enthalten, werden (mit demselben Dateinamen) in den Konfigurationsaufträgen gespeichert. Sie können diese Eingabedateien, die Sie zuvor beim Erstellen oder Bearbeiten der Konfigurationsaufträge verwendet und hochgeladen haben, anzeigen und bearbeiten.

    Um die ausgeführten Konfigurationsaufträge beim Erstellen eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk** > **Konfigurationsaufträge** und klicken Sie auf

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Auftrag erstellen. Wählen Sie auf der Seite **Auftrag erstellen** auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien dann hoch (wobei der Dateiname beibehalten wird).

Um die bereits ausgeführten Konfigurationsaufträge beim Bearbeiten eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk** > **Konfigurationsaufträge**, wählen Sie den Auftragsnamen aus und klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite **Auftrag konfigurieren** auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter und bearbeiten und laden Sie die Dateien dann hoch (wobei der Dateiname beibehalten wird).10. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle, die auf jeder Instanz oder Instanzgruppe ausgeführt werden sollen, auswerten und überprüfen.

11. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle, die auf jeder Instanz oder Instanzgruppe ausgeführt werden sollen, auswerten und überprüfen.
12. Auf der Registerkarte **Ausführen** können Sie wählen, ob Sie Ihren Auftrag jetzt ausführen oder für einen späteren Zeitpunkt planen möchten. Sie können auch auswählen, welche Aktion NetScaler Console ausführen soll, wenn der Befehl fehlschlägt.

    Sie können auch autorisierten Benutzern erlauben, Aufträge auf Ihren verwalteten Instanzen auszuführen, und Sie können wählen, ob eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Auftrags zusammen mit anderen Details gesendet werden soll.

13. Auf der Seite **Aufträge** können Sie dann den Fortschritt der Ausführung Ihrer Konfigurationsaufgabe auf allen Instanzen anzeigen.

Konfigurationsaufträge verwenden, um die Konfiguration von einer Instanz auf mehrere Instanzen zu replizieren

Möglicherweise haben Sie sowohl Lastausgleich als auch AppFlow auf einer NetScaler-Instanz für Ihre Bereitstellung konfiguriert. Jetzt möchten Sie jedoch nur die AppFlow-Konfiguration auf andere NetScaler-Instanzen replizieren.

Sie können die Funktion Konfigurationsaufträge von NetScaler Console verwenden, um die AppFlow-Konfiguration von einer NetScaler-Instanz zu extrahieren und auf mehreren Instanzen zu replizieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So rufen Sie die Konfiguration von einer Instanz ab und replizieren sie auf andere NetScaler-Instanzen:

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsaufträge**, und klicken Sie dann auf **Auftrag erstellen**.
2. Geben Sie den Auftragsnamen und den Instanztyp an.
3. Wählen Sie **Instanz** als **Konfigurationsquelle** und wählen Sie die Quellinstanz aus, deren Konfiguration Sie replizieren möchten. Wählen Sie den Typ der Konfiguration aus, die Sie extrahieren möchten. Wenn Sie „Konfiguration nach Zeitdauer“ auswählen, legen Sie den Zeitraum fest, in dem Sie diese Konfiguration ausgeführt haben, und klicken Sie dann auf **Extrahieren**.

   Die Anzahl der Befehle, die in dem von Ihnen ausgewählten Zeitraum auf dieser Instanz ausgeführt wurden, wird auf dem Bildschirm angezeigt, wie in der Abbildung unten hervorgehoben.

4. Ziehen Sie die Befehle in das Feld **Befehle** im rechten Bereich.

   Behalten Sie nur die Befehle bei, die sich auf FEO beziehen, und löschen Sie manuell die Befehle, die sich auf den Lastausgleich oder andere Konfigurationen beziehen, und klicken Sie dann auf **Weiter**.
5. Klicken Sie auf **Instanzen hinzufügen** und fügen Sie die Instanzen hinzu, auf die Sie die FEO-Konfiguration anwenden möchten. Klicken Sie auf **OK** und dann auf **Weiter**.

   Wenn Sie Variablen in den Befehlen angegeben haben, klicken Sie auf der Registerkarte Variablenwerte angeben auf **Eingabeschlüsseldatei herunterladen**. Geben Sie in der heruntergeladenen Datei Werte für die Variablen an und laden Sie die Datei dann in NetScaler Console hoch.

Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle, die auf jeder Instanz oder Instanzgruppe ausgeführt werden sollen, auswerten und überprüfen.

Klicken Sie auf der Registerkarte **Ausführen** auf **Fertig stellen**, um den Auftrag auf den ausgewählten NetScaler-Instanzen auszuführen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Variablen in Konfigurationsaufträgen verwenden

Ein Konfigurationsauftrag ist eine Reihe von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen ausführen können. Wenn Sie dieselbe Konfiguration auf mehreren Instanzen ausführen, möchten Sie möglicherweise unterschiedliche Werte für die in Ihrer Konfiguration verwendeten Parameter verwenden. Sie können Variablen definieren, die es Ihnen ermöglichen, diesen Parametern unterschiedliche Werte zuzuweisen oder einen Auftrag über mehrere Instanzen hinweg auszuführen.

Betrachten Sie beispielsweise eine grundlegende Lastenausgleichskonfiguration, bei der Sie einen virtuellen Lastenausgleichsserver hinzufügen, zwei Dienste hinzufügen und die Dienste an den virtuellen Server binden. Nun möchten Sie möglicherweise dieselbe Konfiguration auf zwei Instanzen haben, jedoch mit unterschiedlichen Werten für die Namen und IP-Adressen des virtuellen Servers und der Dienste. Sie können die Funktion für Konfigurationsaufträge verwenden, um dies zu erreichen, indem Sie Variablen verwenden, um die Namen und IP-Adressen des virtuellen Servers und der Dienste zu definieren.

In diesem Beispiel werden die folgenden Befehle und Variablen verwendet:

```
add lb vserver **servername** HTTP **ipaddress portnumber**


add service **servicename1** **ipaddress1** HTTP 80


add service **servicename2** **ipaddress2** HTTP 80


bind lb vserver **servername** **servicename1**


bind lb vserver **servername** **servicename2**
```

So erstellen Sie einen Konfigurationsauftrag, indem Sie Variablen in NetScaler Console definieren:

1. Navigieren Sie zu **Infrastructure > Configuration > Configuration Jobs**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Klicken Sie auf **Create Job**.
3. Wählen Sie auf der Seite **Create Job** die benutzerdefinierten Auftragsparameter wie den Namen des Auftrags, den Instanztyp und den Konfigurationstyp aus.
4. Geben Sie im Konfigurationseditor die Befehle ein, um einen virtuellen Lastenausgleichsserver und zwei Dienste hinzuzufügen und die Dienste an den virtuellen Server zu binden. Doppelklicken Sie, um die Werte auszuwählen, die Sie in eine Variable umwandeln möchten, und klicken Sie dann auf **Convert to Variable**. Wählen Sie beispielsweise die IP-Adresse des Lastenausgleichsservers `ipaddress` aus und klicken Sie auf **Convert to Variable**.
5. Sobald Sie sehen, dass Dollarzeichen den Wert der Variablen umschließen, klicken Sie auf die Variable, um die Details der Variablen wie Name, Anzeigename und Typ weiter anzugeben. Sie können auch auf die Option **Advanced** klicken, wenn Sie einen Standardwert für Ihre Variable weiter angeben möchten. Klicken Sie auf **Save** und dann auf **Next**.
6. Sie können alle Variablen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben, in einer einzigen konsolidierten Ansicht überprüfen.
7. Führen Sie einen der folgenden Schritte aus, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:

   - Navigieren Sie beim Erstellen eines Konfigurationsauftrags zu **Infrastructure > Configuration > Configuration Jobs**, wählen Sie **Create Job**. Auf der Seite **Create Job** können Sie alle Variablen überprüfen, die Sie beim Erstellen des Konfigurationsauftrags hinzugefügt haben.
   - Navigieren Sie beim Bearbeiten eines Konfigurationsauftrags zu **Network** > **Configuration Jobs**, wählen Sie den Jobnamen aus und klicken Sie auf **Edit**. Auf der Seite **Configure Job** können Sie alle Variablen überprüfen, die beim Erstellen des Konfigurationsauftrags hinzugefügt wurden.

8. Sie können dann auf die Registerkarte **Preview Variables** klicken, um die Variablen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben, in einer einzigen konsolidierten Ansicht anzuzeigen.
9. Ein neues Pop-up-Fenster wird angezeigt und zeigt alle Parameter der Variablen wie Name, Anzeigename, Typ und Standardwert in einem Tabellenformat an. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf die Schaltfläche **Fertig**, nachdem Sie einen der Parameter bearbeitet oder geändert haben.

10. Sie können die Befehle im Konfigurationseditor dann nach Bedarf neu anordnen und umsortieren. Sie können den Befehl von einer Zeile in eine andere verschieben, indem Sie die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Befehlszeile ziehen und ablegen. Sie können die Befehlszeile auch von einer Zeile zu einer beliebigen Zielzeile verschieben oder neu anordnen, indem Sie einfach die Befehlszeilennummer im Textfeld ändern.

11. Wählen Sie die Instanzen aus, auf denen Sie den Konfigurationsauftrag ausführen möchten.
12. Wählen Sie auf der Registerkarte **Variablenwerte angeben** die Option **Eingabedatei für Variablenwerte hochladen** aus und klicken Sie dann auf **Eingabeschlüsseldatei herunterladen**. In unserem Beispiel müssen Sie den Servernamen auf jeder Instanz, die IP-Adressen des Servers und der Dienste, Portnummern und die Dienstnamen angeben. Speichern Sie die Datei und laden Sie sie hoch. Wenn Ihre Werte nicht genau definiert sind, kann das System einen Fehler ausgeben.
13. Die Eingabeschlüsseldatei wird auf Ihr lokales System heruntergeladen, und Sie können sie bearbeiten, indem Sie die Variablenwerte für jede zuvor ausgewählte NetScaler-Instanz angeben und auf **Hochladen** klicken, um die Eingabeschlüsseldatei in die NetScaler Console hochzuladen. Klicken Sie auf **Weiter**. Die Eingabeschlüsseldatei wird auf Ihr lokales System heruntergeladen, und Sie können sie bearbeiten, indem Sie die Variablenwerte für jede zuvor ausgewählte NetScaler-Instanz angeben.

HINWEIS

In der Eingabeschlüsseldatei werden die Variablen auf drei Ebenen definiert:

- Globale Ebene
- Instanzgruppenebene
- Instanzebene

Globale Variablen sind Variablenwerte, die auf alle Instanzen angewendet werden. Variablenwerte auf Instanzgruppenebene werden auf alle Instanzen angewendet, die in einer Gruppe definiert sind. Variablenwerte auf Instanzebene werden nur auf eine bestimmte Instanz angewendet.

NetScaler Console gibt den Werten auf Instanzebene die höchste Priorität. Wenn für die Variablen einzelner Instanzen keine Werte angegeben sind, verwendet NetScaler Console den auf Gruppenebene angegebenen Wert. Wenn auf Gruppenebene keine Werte angegeben sind, verwendet NetScaler Console den auf globaler Ebene angegebenen Variablenwert. Wenn Sie eine Eingabe für eine Variable auf allen drei Ebenen bereitstellen, verwendet NetScaler Console den Wert auf Instanzebene als Standardwert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

14. Klicken Sie auf **Hochladen**, um die Eingabeschlüsseldatei in die NetScaler Console hochzuladen. Klicken Sie auf **Weiter**.

    WICHTIG

    Wenn Sie eine CSV-Datei von einem Mac hochladen, speichert Mac die CSV-Datei mit Semikolons anstelle von Kommas. Dies führt dazu, dass die Konfiguration fehlschlägt, wenn Sie die Eingabedatei hochladen und den Auftrag ausführen. Wenn Sie einen Mac verwenden, verwenden Sie einen Texteditor, um die erforderlichen Änderungen vorzunehmen, und laden Sie dann die Datei hoch.

15. Sie können auch gemeinsame Variablenwerte für alle Instanzen angeben und auf **Hochladen** klicken, um die Eingabeschlüsseldatei in NetScaler Console hochzuladen.

    Die Eingabeschlüsseldateien, die die Variablenwerte enthalten, werden (mit demselben Dateinamen) in den Konfigurationsaufträgen gespeichert. Sie können diese Eingabedateien, die Sie zuvor beim Erstellen oder Bearbeiten der Konfigurationsaufträge verwendet und hochgeladen haben, anzeigen und bearbeiten.

    Um die ausgeführten Konfigurationsaufträge beim Erstellen eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk** > **Konfigurationsaufträge** und klicken Sie auf **Auftrag erstellen**. Auf der Seite **Auftrag erstellen**. Wählen Sie auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen**, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter, bearbeiten und laden Sie die Dateien dann hoch (unter Beibehaltung desselben Dateinamens).

    Um die bereits ausgeführten Konfigurationsaufträge beim Bearbeiten eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Netzwerk** > **Konfigurationsaufträge**, wählen Sie den Auftragsnamen aus und klicken Sie auf **Bearbeiten**. Wählen Sie auf der Seite **Auftrag konfigurieren** auf der Registerkarte **Variablenwerte angeben** die Option **Gemeinsame Variablenwerte für alle Instanzen**, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter, bearbeiten und laden Sie die Dateien dann hoch (unter Beibehaltung desselben Dateinamens).

16. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle, die auf jeder Instanz oder Instanzgruppe ausgeführt werden sollen, auswerten und überprüfen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

17. Auf der Registerkarte **Ausführen** können Sie wählen, ob Sie Ihren Auftrag jetzt ausführen oder für einen späteren Zeitpunkt planen möchten. Sie können auch auswählen, welche Aktion NetScaler Console ergreifen soll, wenn der Befehl fehlschlägt, und ob Sie eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Auftrags zusammen mit weiteren Details senden möchten.

Nachdem Sie Ihre Aufträge konfiguriert und ausgeführt haben, können Sie die Auftragsdetails anzeigen, indem Sie zu **Infrastruktur > Konfiguration > Konfigurationsaufträge** navigieren und den von Ihnen konfigurierten Auftrag auswählen. Klicken Sie auf **Details** und dann auf **Variablendetails**, um die Liste der zu Ihrem Auftrag hinzugefügten Variablen anzuzeigen.

HINWEIS

Die Werte, die Sie für die Variablen in **Schritt 5** angegeben haben, werden von NetScaler Console beibehalten, wenn Sie den Auftrag speichern und beenden oder wenn Sie einen Auftrag für einen späteren Zeitpunkt planen.

Konfigurationsaufträge aus Korrekturbefehlen erstellen

Sie können die Audit-Vorlagenfunktion in NetScaler Console verwenden, um Konfigurationsänderungen über verwaltete NetScaler-Instanzen hinweg zu überwachen und Konfigurationsfehler zu beheben.

Der typische Arbeitsablauf zur Überprüfung von Konfigurationsänderungen mithilfe von Audit-Vorlagen besteht aus den folgenden Schritten.

1. Erstellen Sie eine Audit-Vorlage mit einer Reihe gültiger/erwarteter NetScaler-Befehle zur Überprüfung von Instanzkonfigurationen.
2. Wählen Sie die NetScaler-Instanzen aus, für die Sie die Audit-Vorlage ausführen möchten, um Unterschiede zwischen der laufenden Konfiguration und den erwarteten Konfigurationen zu überprüfen.
3. Verstehen Sie die differenziellen/korrigierenden Befehle und nutzen Sie die Funktion „Create Job“, um die Konfigurationen der Instanz in den gewünschten Zustand zu versetzen.

Stellen Sie sich ein Szenario vor, in dem mehrere Administratoren fünf NetScaler-Instanzen verwalten. Alle diese Administratoren aktualisieren die vorhandene Instanzkonfiguration, sobald Änderungen erforderlich sind. Der Superadministrator möchte sicherstellen, dass eine bestimmte Reihe wichtiger Konfigurationen unberührt bleibt, unabhängig von den Änderungen, die von

© 1997–2026 Citrix Systems, Inc. All rights reserved.

anderen Administratoren vorgenommen werden. Für diesen Anwendungsfall erstellt der Superadministrator eine Vorlage der Konfiguration, die auf den NetScaler-Instanzen vorhanden sein soll, und führt sie für die Instanzen aus. NetScaler Console vergleicht die Audit-Vorlagenkonfiguration mit der laufenden Konfiguration und meldet jede Nichtübereinstimmung im Dashboard **Konfigurationsprüfung**.

Wenn Sie feststellen, dass sich die Konfiguration einiger Instanzen geändert hat, können Sie die Funktion für Korrekturbefehle von NetScaler Console verwenden, um einen Konfigurationsauftrag mit den geänderten und korrigierten Konfigurationsbefehlen für bestimmte NetScaler-Instanzen zu erstellen.

Wenn ein Unterschied zwischen der Audit-Vorlagenkonfiguration und der laufenden Konfiguration besteht, wird auf der Seite **Audit-Bericht** die Statusmeldung **Diff Exists** angezeigt. Durch Klicken auf den Link **Diff Exists** gelangen Sie zur Seite **Konfigurationsunterschied**, wo Sie den Korrekturbefehl anzeigen können. Sie können diese Korrekturbefehle auch verwenden, um einen Konfigurationsauftrag zu erstellen und diesen auf den spezifischen NetScaler-Instanzen auszuführen, um sie wieder in die gewünschte Konfiguration zu versetzen.

So erstellen Sie einen Konfigurationsauftrag aus Korrekturbefehlen in NetScaler Console:

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsprüfung**.
2. Klicken Sie auf der Seite **Konfigurationsprüfung** in eines der beiden Donut-Diagramme, um auf die Seite **Audit-Berichte** zuzugreifen.
3. Klicken Sie auf den Link **Diff Exists** (unter der Spalte **Gespeicherter vs. laufender Unterschied** in der Tabelle) für die Instanz, für die Sie die Konfigurationsbefehle korrigieren möchten. Die Seite **Konfigurationsunterschied** wird angezeigt, die die Unterschiede zwischen der gespeicherten Konfiguration, der laufenden Konfiguration und der Korrekturkonfiguration für diese Instanz auflistet.

   Konfigurationsunterschied anzeigen(/en-us/netscaler-console-service/media/auditreports.png)
4. Klicken Sie auf **Auftrag erstellen**, um zur Seite **Auftrag erstellen** zu gelangen, auf der die Korrekturbefehle vorab ausgefüllt sind. Anweisungen zum Erstellen eines Konfigurationsauftrags finden Sie unter So erstellen Sie einen Konfigurationsauftrag in NetScaler Console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Laufende und gespeicherte Konfiguration von einer NetScaler-Instanz auf eine andere replizieren

Sie können jetzt die Konfiguration einer NetScaler-Instanz auf andere Instanzen replizieren. Wenn Sie einen Auftrag in NetScaler Console konfigurieren, wählen Sie eine Instanz als Konfigurationsquelle aus und wählen Sie die laufende oder gespeicherte Konfiguration der ausgewählten Instanz.

Wenn Sie beispielsweise **Laufende Konfiguration** auswählen und auf **Extrahieren** klicken, sendet NetScaler Console eine Anforderung an die ausgewählte NetScaler-Instanz, um die laufende Konfiguration zu finden, und zeigt sie als Vorlage an. Sie können die Vorlage in das Feld **Befehle** im rechten Bereich ziehen. Sie können Befehle, Parameter und die Instanzen ändern.

So replizieren Sie laufende und gespeicherte Konfigurationsbefehle einer Instanz auf eine andere Instanz in NetScaler Console:

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsaufträge**, und klicken Sie auf **Auftrag erstellen**.
2. Geben Sie den Auftragsnamen und den Instanztyp an. Geben Sie beispielsweise *NetScaler Running Config1* als Namen Ihres Auftrags und *NetScaler* als Instanztyp an.
3. Wählen Sie **Instanz** als **Konfigurationsquelle** aus, und wählen Sie die Quellinstanz aus, deren Konfiguration Sie auf andere Instanzen replizieren möchten.
4. Sie sehen die folgenden drei Optionen:
   - Laufende Konfiguration
   - Gespeicherte Konfiguration
   - Konfiguration nach Zeitdauer
5. Wählen Sie **Laufende Konfiguration** aus, und klicken Sie auf **Extrahieren**. Die Anzahl der auf dieser Instanz ausgeführten laufenden Konfigurationsbefehle wird angezeigt.

6. Ziehen Sie die Befehle in das Feld **Befehle** im rechten Bereich.
7. Sie können die Befehle im Feld Befehle bearbeiten. Zum Beispiel, wenn die extrahierten Befehle zum Einrichten einer NetScaler-Instanz dienen. Dies könnte das Hinzufügen von Partitionen, das Einrichten des Lastausgleichs, das Binden des Lastausgleichsservers an Dienste usw. umfassen. Möglicherweise möchten Sie Ihre Befehle bearbeiten, um Ihre neuen NetScaler-Instanzen ohne Partitionen einzurichten. Um Partitionen zu entfernen, löschen Sie

© 1997–2026 Citrix Systems, Inc. All rights reserved.

daher manuell Befehle, die sich auf die Erstellung von Partitionen beziehen, und klicken Sie auf **Weiter**.

8. Klicken Sie auf **Instanzen hinzufügen** und fügen Sie die Instanzen hinzu, auf die Sie die laufenden Konfigurationsbefehle anwenden möchten. Klicken Sie auf **OK** und klicken Sie dann auf **Weiter**.
9. Wenn Sie Variablen in den Befehlen angegeben haben, klicken Sie auf der Registerkarte **Variablenwerte angeben** auf **Eingabeschlüsseldatei herunterladen**. Geben Sie in der heruntergeladenen Datei Werte für die Variablen an und laden Sie die Datei dann in die NetScaler Console hoch.
10. Auf der Registerkarte **Auftragsvorschau** können Sie die Befehle, die auf jeder Instanz oder Instanzgruppe ausgeführt werden sollen, auswerten und überprüfen.
11. Auf der Registerkarte **Ausführen** können Sie wählen, ob Sie Ihren Auftrag jetzt ausführen oder für eine spätere Ausführung planen möchten. Sie können auch wählen, welche Aktion die NetScaler Console ausführen soll, wenn der Befehl fehlschlägt, und ob Sie eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Auftrags zusammen mit weiteren Details senden möchten.

Ausgeführte Konfigurationsaufträge wiederverwenden

Konfigurationsaufträge ermöglichen es Ihnen, einen Satz von Konfigurationsbefehlen zu erstellen, die Sie auf einer oder mehreren verwalteten Instanzen ausführen können. Sie können denselben Satz gespeicherter Konfigurationsaufträge auch nach dem Ändern der Befehle, der Parameter, der Konfigurationsquelle und der Instanzen im Auftrag erneut ausführen. Diese Funktion ist nützlich, wenn derselbe Satz von Befehlen auf einer anderen Instanz ausgeführt werden muss oder wenn der Auftrag auf einen Fehler stößt und die weitere Ausführung stoppt.

NetScaler Console bietet eine Funktion, um die abgeschlossenen Aufträge erneut auszuführen. Mit dieser Funktion können vollständig ausgeführte Aufträge erneut ausgeführt werden, ohne den Auftragsnamen zu ändern.

HINWEIS

Sie können nur die Aufträge erneut ausführen, die ausgeführt werden, wenn der Ausführungsmodus „Jetzt“ ist.

So bearbeiten Sie abgeschlossene Aufträge:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie auf der Startseite der NetScaler Console zu **Infrastruktur > Konfiguration > Konfigurationsaufträge**.
2. Wählen Sie auf der Seite **Aufträge** einen Auftrag aus, dessen Ausführungsübersicht als „Abgeschlossen“ angezeigt wird, und klicken Sie auf **Bearbeiten**. Sie können auch einen geplanten Konfigurationsauftrag bearbeiten.

3. Auf der Seite **Auftrag konfigurieren** sehen Sie, dass der Auftragsname und der Instanztyp nicht bearbeitbar sind. Sie können andere Felder wie die Konfigurationsquelle ändern, Instanzen hinzufügen, Variablenwerte bearbeiten und Ausführungseinstellungen festlegen.
4. Klicken Sie auf **Fertig stellen**, um den Konfigurationsauftrag erneut auszuführen.

HINWEIS

Sie können den Auftrag auch auswählen und erneut auf **Ausführen** klicken, um den Auftrag auszuführen, ohne Quelle, Instanz und Befehle zu ändern. Diese Option ist nützlich, wenn Sie denselben Satz von Befehlen auf denselben Instanzen ausführen müssen. Manchmal kann der Auftrag auf einen vorübergehenden Fehler von der Serverseite stoßen, und Sie müssen den Auftrag möglicherweise erneut ausführen.

SCP (put)-Befehl in Konfigurationsaufträgen verwenden

Sie können die Funktion **Konfigurationsaufträge** von NetScaler Console verwenden, um Konfigurationsaufträge zu erstellen, E-Mail-Benachrichtigungen zu senden und Ausführungsprotokolle der erstellten Aufträge zu überprüfen. Ein Auftrag ist eine Reihe von Konfigurationsbefehlen, die Sie auf einer einzelnen verwalteten Instanz oder auf mehreren verwalteten Instanzen erstellen und ausführen können. Sie können Konfigurationsaufträge beispielsweise für Geräte-Upgrades verwenden.

Konfigurationsaufträge in NetScaler Console verwenden Secure Shell (SSH)-Befehle zur Konfiguration von Instanzen, und Sie können einen Konfigurationsauftrag so konfigurieren, dass er Secure Copy (SCP) zum sicheren Übertragen von Dateien verwendet. SCP basiert auf dem SSH-Protokoll. Einer der SCP-Befehle, die Sie in einen Konfigurationsauftrag aufnehmen können, ist der „put“-Befehl. Sie können den „put“-Befehl in Konfigurationsaufträgen verwenden, um eine oder mehrere Dateien, die in einem lokalen Verzeichnis auf Ihrem System gespeichert sind, in die NetScaler Console und dann in ein Verzeichnis auf der NetScaler-Instanz oder den Instanzen hochzuladen oder zu übertragen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Die Datei wird in die NetScaler Console hochgeladen und später auf die ausgewählten NetScaler-Instanzen kopiert (put). Die hochgeladene Datei wird in der NetScaler Console gespeichert und erst gelöscht, wenn der Auftrag gelöscht wird. Dies ist für Aufträge erforderlich, die für eine spätere Ausführung geplant sind.

Der Befehl hat die folgende Syntax:

```
put \<local\_filename\> \<remote\_path/remote\_filename\>
```

Dabei gilt:

\<local_filename\> ist der Name der hochzuladenden lokalen Datei.

\<remote_path/ remote_filename\> ist der Pfad zu einem Remote-Verzeichnis und der Name, der der Datei zugewiesen werden soll, wenn sie in dieses Verzeichnis kopiert wird.

Beim Erstellen des Konfigurationsauftrags können Sie die Parameter für den lokalen und Remote-Dateinamen in Variablen umwandeln. Dadurch können Sie denselben NetScaler-Instanzen bei jeder Ausführung des Auftrags unterschiedliche Dateien zuweisen. Wenn Sie eine Datei an mehreren Stellen in einem Auftrag verwenden und die Datei umbenennen möchten, können Sie die Variable neu definieren, anstatt den Dateinamen an allen Stellen zu ändern.

So verwenden Sie den put-Befehl zum Hochladen von Dateien in einem Konfigurationsauftrag:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Configuration > Configuration Jobs**.
2. Klicken Sie auf der Seite **Jobs** auf **Create Job**.
3. Geben Sie auf der Seite **Create Job** den Namen des Auftrags in das Feld Job name ein und geben Sie im Bereich **Configuration Editor** den Befehl „put“ ein.

   Wenn Sie beispielsweise einen Konfigurationsauftrag erstellen möchten, der eine auf Ihrem lokalen System gespeicherte SSL-Zertifikatsdatei auf mehrere NetScaler-Instanzen kopiert, können Sie einen „put“-Befehl hinzufügen, der eine Variable anstelle des Namens einer bestimmten Datei verwendet, und den Variablentyp als „file“ definieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
put ssl-file /nsconfig/ssl-file
```

In diesem Beispiel:

- `ssl-file` – dies ist der Name der Datei, die in die NetScaler-Instanz hochgeladen werden muss.
- `/nsconfig/ssl-file` – dies ist der Zielordner auf der Instanz, in den die `ssl-file` nach Ausführung der Aufgabe abgelegt wird.

4. Wählen Sie in dem von Ihnen eingegebenen Befehl den Dateinamen aus, den Sie in eine Variable konvertieren möchten, und klicken Sie dann auf **In Variable konvertieren**, wie in der folgenden Abbildung gezeigt.

5. Vergewissern Sie sich, dass der Dateiname in Dollarzeichen eingeschlossen ist (was anzeigt, dass es sich jetzt um eine Variable handelt), und klicken Sie dann auf die Variable.
6. Geben Sie die Details der Variable an, z. B. Name, Anzeigename und Typ.
7. Wählen Sie in der Dropdown-Liste **Typ** die Option **Datei** aus. Klicken Sie auf **Speichern**.

   Das Deklarieren der Variable als „Dateityp“ ermöglicht Ihnen das Hochladen von Dateien in NetScaler Console.

8. Klicken Sie auf **Weiter** und wählen Sie die NetScaler-Instanzen aus, auf die die Dateien kopiert werden sollen.
9. Wählen Sie auf der Registerkarte **Variablenwerte angeben** im Abschnitt **Gemeinsame Variablenwerte für alle Instanzen** die Datei aus dem lokalen Speicher Ihres Systems aus, klicken Sie auf **Hochladen**, um die Datei in NetScaler Console hochzuladen, und klicken Sie auf **Weiter**.

10. Auf der Registerkarte **Auftragsvorschau** können Sie die auf jeder Instanz oder Instanzgruppe auszuführenden Befehle auswerten und überprüfen.
11. Auf der Registerkarte **Ausführen** können Sie den Auftrag jetzt ausführen oder für eine spätere Ausführung planen. Sie können auch auswählen, welche Aktion NetScaler Console ausführen soll, wenn der Befehl fehlschlägt. Sie können auch eine E-Mail-Benachrichtigung erstellen, um Benachrichtigungen über den Erfolg oder Misserfolg des Auftrags und andere Details zu erhalten. Klicken Sie auf **Fertig stellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. Sie können die Jobdetails einsehen, indem Sie zu **Infrastructure > Configuration > Configuration Jobs** navigieren und den von Ihnen konfigurierten Job auswählen. Klicken Sie auf **Details** und klicken Sie dann auf **Variablendetails**, um die Ihrem Job hinzugefügten Variablen aufzulisten.

Konfigurationsvorlagen verwenden

Eine Konfigurationsvorlage ist ein wiederverwendbarer Satz von Konfigurationsbefehlen, den Sie in NetScaler Console speichern und beim Erstellen von Konfigurationsaufträgen oder Konfigurationsprüfungen anwenden können. Vorlagen helfen Ihnen, Konfigurationen zu standardisieren, wiederholten Aufwand zu reduzieren und konsistente Einstellungen über mehrere verwaltete NetScaler-Instanzen hinweg bereitzustellen.

Sie können eine Konfigurationsvorlage erstellen, während Sie einen Auftrag erstellen, indem Sie einen Satz von Konfigurationsbefehlen als Vorlage speichern. Sie können auch integrierte Vorlagen, Master-Konfigurationsvorlagen und Audit-Vorlagen verwenden und diese zwischen den Modulen Konfigurationsaufträge und Konfigurationsprüfung teilen.

Die folgenden Themen beschreiben, wie Sie mit Konfigurationsvorlagen in NetScaler Console arbeiten:

- Die Master-Konfigurationsvorlage verwenden
- Aufträge planen, die mit integrierten Vorlagen erstellt wurden
- Einen Auftrag zum Konfigurieren des Exports von Metriken von NetScaler nach Prometheus planen
- Konfigurationsvorlagen verwenden, um Audit-Vorlagen zu erstellen
- Aufträge neu planen, die mit integrierten Vorlagen konfiguriert wurden
- Konfigurations-Audit-Vorlagen in Konfigurationsaufträgen wiederverwenden
- Konfigurationsvorlagen importieren und exportieren

Verwenden der Master-Konfigurationsvorlage

Die Verwendung einer Master-Konfigurationsvorlage ist eine flexible Option zum Erstellen und Bereitstellen einer Master-Konfiguration auf mehreren NetScaler-Instanzen.

Als Administrator möchten Sie möglicherweise Konfigurationsänderungen vornehmen und Lizenzen, Zertifikate und andere Dateien auf einer NetScaler-Instanz speichern. Sie können die neue Konfiguration als Master-Konfigurationsvorlage (.conf-Datei) speichern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Um Ihre Master-Konfigurationsvorlage von einer NetScaler-Instanz zu speichern, können Sie eine der folgenden Aktionen ausführen:

- Geben Sie an der Eingabeaufforderung **save ns config** ein. Die Konfiguration wird im FLASH-Speicher der Instanz in der Datei /nsconfig/ns.conf gespeichert.
- Navigieren Sie in der GUI der NetScaler-Instanz zu **Diagnostics** > **View Configuration**. Wählen Sie die Art der Konfiguration aus, die Sie speichern möchten. Wenn Sie beispielsweise die gespeicherte Konfiguration Ihrer NetScaler-Instanz speichern möchten, wählen Sie **Saved configuration**. Klicken Sie auf den Link **Save text to a file**, um die Datei 'ns.conf' auf Ihrem lokalen Computer zu speichern.

Wenn Sie die Master-Konfigurationsvorlage mithilfe der Konfigurationsvorlage 'DeployMasterConfiguration' beim Erstellen eines Jobs bereitstellen, können Sie diese für jede spezifische NetScaler-Instanz weiter anpassen, indem Sie weitere Befehle hinzufügen, vorhandene Befehle ändern und verschiedene Variablenwerte in der Eingabedatei angeben.

Als Administrator möchten Sie beispielsweise zusätzlich zur ns.conf-Datei Zertifikatsschlüssel auf Ihre NetScaler-Instanzen hochladen und die Master-Konfiguration auch dort bereitstellen.

WICHTIG

Sie können keinen Konfigurationsjob mit der DeployMasterConfiguration-Vorlage auf NetScaler CPX-Instanzen, in einem Cluster konfigurierten NetScaler-Instanzen oder auf partitionierten NetScaler-Instanzen ausführen.

So erstellen Sie einen Konfigurationsjob mithilfe der Master-Konfigurationsvorlage in NetScaler Console:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Configuration > Configuration Jobs**, und klicken Sie dann auf **Create Job**.
2. Geben Sie auf der Seite **Create Job** auf der Registerkarte **Select Configuration** den **Job Name** an und wählen Sie den **Instance Type** aus der Dropdown-Liste aus.
3. Wählen Sie **Master Configuration** aus der Dropdown-Liste **Configuration Source** aus. Ziehen Sie die Befehle der DeployMasterConfiguration-Vorlage in den rechten Bereich. Sie können Befehle im rechten Bereich auch hinzufügen, ändern oder löschen. Klicken Sie auf **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Sie können **put**-Befehle hinzufügen, um Eingabedateien zu Ihrer Vorlage hinzuzufügen. In unserem Beispiel müssen wir Zertifikats- und Schlüsseldateien zusätzlich zur Konfigurationsvorlagendatei und den variablen Eingabedateien hochladen.

Masterkonfiguration(/en-us/netscaler-console-service/media/master-config.png)

4. Sie können alle Variablen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben, in einer einzigen konsolidierten Ansicht überprüfen.
5. Führen Sie einen der folgenden Schritte aus, um alle Variablen in einer einzigen konsolidierten Ansicht anzuzeigen:

   - Navigieren Sie beim Erstellen eines Konfigurationsauftrags zu **Infrastructure > Configuration Jobs**, wählen Sie **Create Job**. Auf der Seite **Create Job** können Sie alle Variablen überprüfen, die Sie beim Erstellen des Konfigurationsauftrags hinzugefügt haben.
   - Navigieren Sie beim Bearbeiten eines Konfigurationsauftrags zu **Infrastructure > Configuration > Configuration Jobs**, wählen Sie den Auftragsnamen aus und klicken Sie auf **Edit**. Auf der Seite **Configure Job** können Sie alle Variablen überprüfen, die beim Erstellen des Konfigurationsauftrags hinzugefügt wurden.

6. Sie können dann auf die Registerkarte **Preview Variables** klicken, um die Variablen, die Sie beim Erstellen oder Bearbeiten eines Konfigurationsauftrags definiert haben, in einer einzigen konsolidierten Ansicht anzuzeigen.

   Beispiel für die Konfigurationsvorschau(/en-us/netscaler-console-service/media/master-config-preview.png)

7. Ein neues Pop-up-Fenster wird angezeigt und zeigt alle Parameter von Variablen wie Name, Anzeigename, Typ und Standardwert in einem Tabellenformat an. Sie können diese Parameter auch bearbeiten und ändern. Klicken Sie auf die Schaltfläche **Done**, nachdem Sie einen der Parameter bearbeitet oder geändert haben.

   Angegebene Variablen(/en-us/netscaler-console-service/media/master-config-preview-1.png)

8. Wählen Sie die Instanzen aus, auf denen Sie den Konfigurationsauftrag ausführen möchten, und klicken Sie dann auf **Next**.
9. Laden Sie auf der Registerkarte **Specify Variable Values** Folgendes hoch:

   - **Konfigurationsvorlagendatei (.conf)** – Laden Sie die .conf-Datei hoch, die Sie aus einer NetScaler-Instanz extrahiert haben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Eingabedatei hochladen (.xml/csv)** – Laden Sie die Eingabedatei mit Werten für die Variablen hoch, die Sie in Ihren Befehlen definiert haben.

Eine Beispiel-XML-Datei wird hier zur Verfügung gestellt. Stellen Sie sicher, dass die XML-Dateien die Details der von Ihnen verwendeten NetScaler-Instanzen enthalten.

```
<?xml version="1.0" encoding="UTF-8" ?>

<properties>

<!--

Provide inputs for all the parameters defined in the master config
file.

-  global. This tag contains all the common parameters and value.

-  devicegroup. This tag contains all the instance group specific
parameters and values.

If the same parameters are defined in global and instance tags, the
instance specific parameters value will take precedence over the
instance group. The instance group specific parameters value will take
precedence over global parameters in the execution.

-  name. This attribute represents the name of the instance group.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-  device. This tag contains all the instance specific parameters and
value.



If the same parameters are defined in global and instance tags, the
instance specific parameters value will take precedence in the
execution.



-  name. This attribute represents the IP Address of the instance. Host
name is not supported for the attibute.



HA pair should be represented as <primaryip>-<secondaryip>. Example
10.102.2.1-10.102.2.2



In the template file, the parameter name must be specified within the
dollar sign,Example: $NSIP$, $CC_Trap_Dest$ and parameters names are
case sensitive.

-->



<global>



</global>

<devicegroup name="BLR_DEVS">

</devicegroup>

<device name="10.106.101.209">

<param name="IP" value="10.106.101.209"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</device>



<!-- HA PAIR-->

<!--<device name="10.102.43.154-10.102.43.155">

<param name="NSIP" value="10.102.43.154"/>

<param name="HostName" value="NS43HA"/>

<param name="LBSERVER" value="haserver43http"/>

<param name="SNMPTrapDest" value="10.102.43.130"/>

</device>-->

</properties>
```

Eine Beispiel-CSV-Datei wird hier für Ihre Verwendung bereitgestellt.

```
#job-s_variable_input_key_file ,,,,

,,,,

#Global,NSIP,HostName,LBSERVER,SNMPTrapDest

Global Values,,,,

#InstanceGroup,NSIP,HostName,LBSERVER,SNMPTrapDest

example_doc,,,,

#Instance(s),NSIP,HostName,LBSERVER,SNMPTrapDest

10.xx.xx.xx,,,,
```

Dieselbe Datei wird in Microsoft Excel angezeigt:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. Klicken Sie auf **Weiter**.

    Die Eingabedateien, die die Variablenwerte enthalten, werden (mit demselben Dateinamen) in den Konfigurationsaufträgen beibehalten. Sie können diese Eingabedateien, die Sie zuvor beim Erstellen oder Bearbeiten der Konfigurationsaufträge verwendet und hochgeladen haben, anzeigen und bearbeiten.

    Um die ausgeführten Konfigurationsaufträge beim Erstellen eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Network** > **Configuration Jobs**, und klicken Sie auf **Create Job**. Auf der Seite **Create Job** wählen Sie auf der Registerkarte **Specify Variable Values** die Option **Common Variable Values for all Instances** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter, bearbeiten und laden Sie die Dateien dann hoch (wobei der Dateiname beibehalten wird).

    Um die bereits ausgeführten Konfigurationsaufträge beim Bearbeiten eines Konfigurationsauftrags anzuzeigen, navigieren Sie zu **Network** > **Configuration Jobs**, wählen Sie den Jobnamen aus und klicken Sie auf **Edit**. Auf der Seite **Configure Job** wählen Sie auf der Registerkarte **Specify Variable Values** die Option **Common Variable Values for all Instances** aus, um die hochgeladenen Dateien anzuzeigen. Um die Eingabedateien zu bearbeiten, laden Sie die Eingabedatei herunter, bearbeiten und laden Sie die Dateien dann hoch (wobei der Dateiname beibehalten wird).

11. Auf der Registerkarte **Job Preview** können Sie die Befehle, die auf jeder Instanz oder Instanzgruppe ausgeführt werden sollen, auswerten und überprüfen und klicken Sie dann auf **Next**.

12. Auf der Registerkarte **Execute** können Sie wählen, ob Sie Ihren Auftrag jetzt ausführen oder für eine spätere Ausführung planen möchten. Sie können auch auswählen, welche Aktion NetScaler Console ausführen soll, wenn der Befehl fehlschlägt.

    Sie können auch autorisierten Benutzern erlauben, Aufträge auf Ihren verwalteten Instanzen auszuführen, und Sie können wählen, ob eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Auftrags zusammen mit weiteren Details gesendet werden soll.

    Nachdem Sie Ihren Auftrag ausgeführt haben, können Sie die Auftragsdetails anzeigen, indem Sie zu **Infrastructure > Configuration > Configuration Jobs** navigieren und den soeben konfigurierten Auftrag auswählen. Klicken Sie auf **Details** und dann auf **Execution Summary**,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

um die Details Ihres Auftrags anzuzeigen. Klicken Sie auf die Instanz, um die **Command Logs** anzuzeigen und die für den Auftrag ausgeführten Befehle zu sehen.

Aufträge planen, die mithilfe integrierter Vorlagen erstellt wurden

Sie können einen Auftrag mithilfe der Option für integrierte Vorlagen planen. Ein Auftrag ist ein Satz von Konfigurationsbefehlen, die Sie auf einer oder mehreren verwalteten Instanzen ausführen können. Zum Beispiel können Sie die Option für integrierte Vorlagen verwenden, um einen Auftrag zur Konfiguration von Syslog-Servern zu planen. Sie können den Auftrag auch sofort ausführen oder für einen späteren Zeitpunkt planen.

So planen Sie einen Auftrag mithilfe integrierter Vorlagen in NetScaler Console:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Configuration > Configuration Jobs**, und klicken Sie dann auf **Create Job**.
2. Geben Sie auf der Seite **Create Job** auf der Registerkarte **Select Configuration** den **Job Name** an und wählen Sie den **Instance Type** aus der Dropdown-Liste aus.
3. Wählen Sie **Inbuilt Template** aus der Dropdown-Liste **Configuration Source** aus. Ziehen Sie den Befehl *NSConfigureSyslogServer* in den rechten Bereich, und klicken Sie dann auf **Next**.

   Integrierte Vorlagen verwenden(/en-us/netscaler-console-service/media/createjobinbuilttemp1.png)
4. Klicken Sie auf der Registerkarte **Select Instances** auf **Add Instances**, wählen Sie die Instanzen aus, auf denen Sie den Auftrag ausführen möchten, und klicken Sie dann auf **OK**.
5. Klicken Sie auf **Next**. Wählen Sie auf der Registerkarte **Specify Variable Values** eine der folgenden Optionen aus, um Variablen für Ihre Instanzen anzugeben:

   - **Variablenwerte aus einer Eingabedatei** – Laden Sie eine Eingabedatei herunter, um Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den NetScaler Console-Server hoch.
   - **Gemeinsame Variablenwerte für alle Instanzen** – Geben Sie die IP-Adresse und den Port des Syslog-Servers an.
6. Auf der Registerkarte **Job Preview** können Sie die Befehle auswerten und überprüfen, die auf jeder Instanz oder Instanzgruppe ausgeführt werden sollen.
7. Klicken Sie auf **Next**.
8. Legen Sie auf der Registerkarte **Execute** die folgenden Bedingungen fest:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Bei Befehlsfehler** – Wenn ein Befehl fehlschlägt, können Sie entweder die Fehler ignorieren und den Auftrag weiter ausführen oder die weitere Ausführung des Auftrags stoppen. Wählen Sie die gewünschte Aktion aus der Dropdown-Liste aus.
- **Ausführungsmodus** – Sie können den Auftrag entweder sofort ausführen oder für eine spätere Ausführung planen. Wenn Sie den Auftrag später planen möchten, müssen Sie die Einstellungen für die Ausführungshäufigkeit für diesen Auftrag angeben. Wählen Sie aus der Dropdown-Liste den Zeitplan aus, dem der Auftrag folgen soll.

9. Sie können einen Auftrag auch auf einer Reihe von Instanzen sequenziell oder parallel ausführen, indem Sie die gewünschte Methode unter **Ausführungseinstellungen** auswählen. Wenn eine Auftragsausführung auf einer Instanz fehlschlägt, wird sie auf den verbleibenden Instanzen nicht fortgesetzt.

   Sie können auch festlegen, dass autorisierte Benutzer Aufträge auf Ihren verwalteten Instanzen ausführen dürfen, und Sie können wählen, ob eine E-Mail-Benachrichtigung über den Erfolg oder Misserfolg des Auftrags zusammen mit weiteren Details gesendet werden soll.
10. Klicken Sie auf **Fertig stellen**.

Einen Auftrag zum Konfigurieren des Exports von Metriken von NetScaler nach Prometheus planen

Mithilfe der `NSConfigurePrometheusAnalyticsProfile`-Vorlage können Sie entweder das Standardschema oder ein benutzerdefiniertes Schema mit geänderten Parametern verwenden und den Auftrag für alle verwalteten Instanzen ausführen.

Voraussetzung

Stellen Sie sicher, dass die verwalteten NetScaler in **13.1 Build 39-27 oder höher** sind.

So planen Sie einen Auftrag:

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Konfiguration > Konfigurationsaufträge**, und klicken Sie dann auf **Auftrag erstellen**.
2. Geben Sie auf der Seite **Auftrag erstellen** einen Namen für den Auftrag an und wählen Sie **NetScaler®** aus der Liste **Instanztyp** aus.
3. Wählen Sie **Integriertes Template** aus der Liste **Konfigurationsquelle** aus. Ziehen Sie den Befehl *NSConfigurePrometheusAnalyticsProfile* in den rechten Bereich, und klicken Sie dann auf **Weiter**. Sie können auch auf **+** klicken, um die Vorlage hinzuzufügen.

4. Wenn Sie mit dem Standardschema fortfahren möchten:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Entfernen Sie Schritt 3 (`put $Schema_file /var/metrics.conf/$schema_filename$`). Platzieren Sie den Mauszeiger auf Schritt 3 und:

- Unter Windows verwenden Sie Strg + A und Entf.
- Unter Mac verwenden Sie Befehl + A und Entf.

b. Klicken Sie nach dem Löschen auf **Weiter**.

c. Klicken Sie auf der Registerkarte **Instanzen auswählen** auf **Instanzen hinzufügen**, wählen Sie die Instanzen aus, auf denen Sie den Auftrag ausführen möchten, und klicken Sie dann auf **Weiter**.

d. Auf der Registerkarte **Variablenwerte angeben** wählen Sie **Gemeinsame Variablenwerte für alle Instanzen** aus.

- **Name des Analytics TimeSeries-Profils** – Geben Sie den Namen des Analyseprofils an. Weitere Informationen finden Sie unter `https://docs.netscaler.com/de-de/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html#configure-the-metrics-collector`.
- **Name der Schemadatei, die auf NetScaler hochgeladen werden soll** – Behalten Sie diesen Dateinamen als `schema.json` bei, da dies die Standarddatei ist.

e. Fahren Sie ab Schritt 6 fort.

5. Wenn Sie mit einem benutzerdefinierten Schemazähler fortfahren möchten:

a. Wählen Sie **Integriertes Template** aus der Liste **Konfigurationsquelle** aus. Ziehen Sie den Befehl `NSConfigurePrometheusAnalyticsProfile` in den rechten Bereich und klicken Sie auf **Weiter**. Sie können auch auf + klicken, um die Vorlage hinzuzufügen.

b. Auf der Registerkarte **Instanzen auswählen** klicken Sie auf **Instanzen hinzufügen**, wählen die Instanzen aus, auf denen Sie den Job ausführen möchten, und klicken dann auf **Weiter**.

c. Auf der Registerkarte **Variablenwerte angeben** wählen Sie **Gemeinsame Variablenwerte für alle Instanzen** aus.

- **NetScaler Zähler-Schemadatei (.json)** – Wählen Sie die Schemadatei aus, die Sie mit den Parametern geändert haben. In NetScaler ist eine Referenzdatei `reference_schema.json` mit allen unterstützten Zählern unter dem Pfad `/var/metrics_conf/` verfügbar.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können einen FTP-Client verwenden, um die Datei lokal zu kopieren, die erforderlichen Parameter zu bearbeiten, zu speichern und dann hochzuladen.

- **Name der Schemadatei, die auf NetScaler hochgeladen werden soll** – Geben Sie den Namen der Schemadatei an, die Sie auf NetScaler hochladen möchten.
- **Name des Analytics TimeSeries-Profils** – Geben Sie den Namen des Analyseprofils an. Weitere Informationen finden Sie unter `https://docs.netscaler.com/de-de/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html#configure-the-metrics-collector`.

6. Auf der Registerkarte **Jobvorschau** können Sie die Befehle auswerten und überprüfen, die auf jeder Instanz oder Instanzgruppe ausgeführt werden sollen.
7. Klicken Sie auf **Weiter**.
8. Legen Sie auf der Registerkarte **Ausführen** die folgenden Bedingungen fest:

   - **Bei Befehlsfehler** – Wenn ein Befehl fehlschlägt, können Sie entweder die Fehler ignorieren und den Job weiter ausführen oder die weitere Ausführung des Jobs stoppen. Wählen Sie die gewünschte Aktion aus der Dropdown-Liste aus.
   - **Ausführungsmodus** – Sie können den Job entweder sofort ausführen oder für eine spätere Ausführung planen. Wenn Sie den Job später planen möchten, müssen Sie die Einstellungen für die Ausführungshäufigkeit für diesen Job angeben. Wählen Sie den Zeitplan, dem der Job folgen soll, aus der Dropdown-Liste aus.

9. Sie können einen Job auch sequenziell oder parallel auf einer Reihe von Instanzen ausführen, indem Sie die erforderliche Methode unter **Ausführungseinstellungen** auswählen. Wenn eine Jobausführung auf einer Instanz fehlschlägt, wird sie auf den verbleibenden Instanzen nicht fortgesetzt.

   Sie können auch autorisierten Benutzern erlauben, Jobs auf Ihren verwalteten Instanzen auszuführen, und Sie können wählen, ob Benachrichtigungen über den Erfolg oder Misserfolg des Jobs zusammen mit anderen Details gesendet werden sollen.

10. Klicken Sie auf **Fertig stellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfigurationsvorlagen zum Erstellen von Audit-Vorlagen verwenden

Sie können jetzt Konfigurationsbefehle, die zuvor als Konfigurationsvorlagen gespeichert wurden, verwenden, um Audit-Vorlagen zu erstellen, die auf bestimmte NetScaler-Instanzen angewendet werden können. Beim Erstellen einer Audit-Vorlage können Sie zuvor gespeicherte Konfigurationsvorlagen in das Feld **Befehle** ziehen und die Vorlage an Ihre Anforderungen anpassen. Sie können die Audit-Vorlage dann auf bestimmte NetScaler-Instanzen anwenden. NetScaler Console vergleicht diese Instanzen mit der Audit-Vorlage und meldet jede Abweichung. Dieser Prozess hilft Ihnen, Fehler zu identifizieren und rechtzeitig zu beheben.

Sie können Konfigurationsvorlagen erstellen, während Sie einen Job erstellen und einen Satz von Konfigurationsbefehlen als Vorlage speichern. Wenn Sie diese Vorlagen auf der Seite **Jobs erstellen** speichern, werden sie automatisch auf der Seite **Vorlage erstellen** angezeigt.

Betrachten Sie zum Beispiel eine grundlegende Lastenausgleichskonfiguration, für die Sie einen virtuellen Lastenausgleichsserver hinzufügen, zwei Dienste hinzufügen und die Dienste an den virtuellen Server binden.

Dieses Beispiel verwendet die folgenden Befehle:

```
add lb vserver **servername** HTTP **ipaddress portnumber**
```

```
add service **servicename1 ipaddress1** HTTP 80
```

```
add service **servicename2 ipaddress2** HTTP 80
```

```
bind lb vserver **servername servicename1**
```

```
bind lb vserver **servername servicename2**
```

So speichern Sie eine Konfigurationsvorlage in NetScaler Console:

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsjobs**, und klicken Sie auf **Job erstellen**.
2. Geben Sie auf der Seite **Job erstellen** den Jobnamen und den Instanztyp an.
3. Wählen Sie **Konfigurationsvorlage** als Konfigurationsquelle und geben Sie im Feld **Befehle** Befehle wie die im vorhergehenden Beispiel ein.
4. Aktivieren Sie das Kontrollkästchen **Als Konfigurationsvorlage speichern** und geben Sie einen Namen für Ihre Vorlage an. Sie können wählen, ob Sie andere Vorlagen mit demselben Namen überschreiben möchten.
5. Klicken Sie auf **Speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So verwenden Sie eine Konfigurationsvorlage zum Erstellen einer Audit-Vorlage in NetScaler Console:

1. Navigieren Sie zu **Infrastructure > Configuration > Configuration Audit > Audit Templates**., und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite **Vorlage erstellen** einen Namen für die Vorlage an und geben Sie eine Beschreibung ein.
3. Wählen Sie aus der Liste **Konfigurationsquelle** die Option **Konfigurationsvorlage** aus, und ziehen Sie die Vorlage dann in das Feld „Befehle“ im rechten Bereich. Sie können die Konfiguration auch bearbeiten und die Vorlage unter einem anderen Namen speichern. Klicken Sie auf **Weiter**.
4. Klicken Sie auf der Registerkarte **Instanzen auswählen** auf **Instanzen hinzufügen** und fügen Sie die Instanzen hinzu, auf denen Sie die Konfiguration ausführen möchten. Klicken Sie auf **OK**.
5. Klicken Sie auf **Fertig stellen**.

Die Audit-Vorlage wird in der Liste der Audit-Vorlagen angezeigt und wird alle 12 Stunden anhand der Konfigurationen der angegebenen Instanzen ausgeführt.

Aufträge neu planen, die mit integrierten Vorlagen konfiguriert wurden

Sie können einen Auftrag neu planen, den Sie mit integrierten Vorlagen in NetScaler Console geplant haben. Sie können beispielsweise die Aktion ändern, die NetScaler Console ausführen soll, wenn ein Befehl fehlschlägt. Wenn Sie zuvor die Option gewählt haben, einen Fehler zu ignorieren und fortzufahren, können Sie dies so ändern, dass alle erfolgreichen Befehle zurückgesetzt werden, wenn ein Befehl fehlschlägt.

So planen Sie einen Auftrag neu, der mit integrierten Vorlagen in NetScaler Console konfiguriert wurde:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Configuration > Configuration Jobs**.
2. Wählen Sie den Auftrag aus, den Sie bearbeiten möchten, fügen Sie Instanzen hinzu oder entfernen Sie sie, geben Sie Variablenwerte an und ändern Sie dann Ausführungsaktionen und -einstellungen.
3. Klicken Sie auf **Fertig stellen**, um den Auftrag neu zu planen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Sie können den Auftrag auch auswählen und erneut auf **Ausführen** klicken, um den Auftrag auszuführen, ohne Quelle, Instanz und Befehle zu ändern. Dies ist nützlich, wenn Sie dieselbe Reihe von Befehlen auf denselben Instanzen ausführen müssen. Manchmal kann der Auftrag einen vorübergehenden Fehler auf der Serverseite aufweisen, und Sie müssen den Auftrag möglicherweise erneut ausführen.

Konfigurationsüberwachungsvorlagen in Konfigurationsaufträgen wiederverwenden

Als Administrator können Sie Konfigurationsbefehle jetzt als Satz wiederverwendbarer Konfigurationsvorlagen speichern, wenn Sie einen Auftrag erstellen und auch wenn Sie eine Konfigurationsüberwachung ausführen. Die im Modul **Konfigurationsaufträge** erstellte und gespeicherte Konfigurationsvorlage ist in der Konfigurationsüberwachung verfügbar, um eine Überwachungsvorlage zu erstellen, die auf bestimmte NetScaler-Instanzen angewendet werden kann. Ebenso ist die im Modul **Konfigurationsüberwachung** erstellte Überwachungsvorlage in Konfigurationsaufträgen verfügbar, sodass Sie die Vorlage als Konfigurationsauftrag ausführen können. Jede an der Vorlage vorgenommene Änderung ist jetzt sowohl in den Modulen Konfigurationsaufträge als auch **Konfigurationsüberwachung** sichtbar.

Zuvor mussten die Konfigurationsauftrags- und Konfigurationsüberwachungsvorlagen für dieselbe Konfiguration separat erstellt und als verschiedene Dateien gespeichert werden. Dies führte zu einer doppelten Anstrengung bei der Erstellung und Pflege der Vorlagen.

NetScaler Console ermöglicht es Ihnen, diese Vorlage im System zu speichern, sodass die Überwachungsvorlage auch in **Konfigurationsaufträgen** verfügbar ist. Jetzt können die Überwachungsvorlagen verwendet werden, um Konfigurationsaufträge zu erstellen. Auf diese Weise können die Vorlagen zwischen den Konfigurationsaufträgen und Konfigurationsüberwachungen austauschbar verwendet werden.

Betrachten Sie beispielsweise eine grundlegende Lastenausgleichskonfiguration, für die Sie einen virtuellen Lastenausgleichsserver hinzufügen, zwei Dienste hinzufügen und die Dienste an den virtuellen Server binden.

Dieses Beispiel verwendet die folgenden Befehle:

```
add lb vserver servername HTTP ipaddress portnumber
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add service servicename1 ipaddress1 HTTP 80

add service servicename2 ipaddress2 HTTP 80

bind lb vserver servername servicename1

bind lb vserver servername servicename2
```

Erstellen einer Vorlage in Konfigurationsüberwachungen und Wiederverwenden in Konfigurationsaufträgen

Führen Sie die folgende Aufgabe aus, um eine Vorlage im Konfigurationsüberwachungsmodul zu erstellen und diese im Konfigurationsauftragsmodul wiederzuverwenden.

So erstellen Sie eine Überwachungsvorlage:

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Konfiguration > Konfigurationsüberwachung** > **Überwachungsvorlage**, und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite **Vorlage erstellen** den Vorlagennamen an. Sie können auch weitere Informationen zur Vorlage im Feld **Beschreibung** hinzufügen.
3. Geben Sie im Bereich **Befehle** Befehle wie die im vorhergehenden Beispiel ein.
4. Aktivieren Sie das Kontrollkästchen **Als Konfigurationsvorlage speichern** und geben Sie einen Namen für Ihre Vorlage an, z. B. können Sie diese Vorlage „LBVariablesTemplate“ nennen. Sie können wählen, ob andere Vorlagen mit demselben Namen überschrieben werden sollen.

   HINWEIS

   Der Name der Überwachungsvorlage kann derselbe sein wie der Name der Konfigurationsvorlage.

5. Klicken Sie auf **Speichern** und dann auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Registerkarte **Instanzen auswählen** die NetScaler-Instanzen aus, auf denen Sie diese Konfigurationsbefehle ausführen möchten, und klicken Sie auf **Fertig stellen**. Die neue Vorlage ist nun in der Liste der Audit-Vorlagen sichtbar.

8. Wenn Sie diese Konfigurationsbefehle ausführen möchten, navigieren Sie zu **Infrastructure > Configuration > Configuration Jobs** und klicken Sie auf **Job erstellen**. Die zuvor erstellte Audit-Vorlage wird als Konfigurationsvorlage aufgeführt.

So verwenden Sie die Audit-Vorlage in Konfigurationsaufträgen wieder:

1. Geben Sie einen Namen für den Job ein, wählen Sie den Instanztyp aus und ziehen Sie die Vorlage in den Befehlsbereich.

   Beim Erstellen des Konfigurationsauftrags können Sie die Parameter für lokale und Remote-Dateinamen in Variablen umwandeln. Dadurch können Sie diesen Parametern jedes Mal, wenn Sie den Job ausführen, verschiedene Dateien für dieselbe Gruppe von NetScaler-Instanzen zuweisen.
2. Wählen Sie in dem von Ihnen eingegebenen Befehl den Dateinamen aus, den Sie in eine Variable umwandeln möchten, und klicken Sie dann auf **In Variable konvertieren**.
3. Wählen Sie auf der Registerkarte **Instanzen auswählen** die Instanzen aus, auf denen Sie diese Befehle ausführen möchten.
4. Wenn Sie Variablen in den Befehlen angegeben haben, wählen Sie auf der Registerkarte **Variablenwerte angeben** eine der folgenden Optionen aus, um Variablen für Ihre Instanzen anzugeben:

   - Variablenwerte aus einer Eingabedatei – Laden Sie eine Eingabedatei herunter, um Werte für die in Ihren Befehlen definierten Variablen einzugeben, und laden Sie die Datei dann auf den NetScaler Console-Server hoch.
   - Gemeinsame Variablenwerte für alle Instanzen – Geben Sie die IP-Adresse und den Port des Syslog-Servers an.
5. Auf der Registerkarte **Job-Vorschau** können Sie die Befehle, die auf jeder Instanz oder Instanzgruppe ausgeführt werden sollen, auswerten und überprüfen und auf **Weiter** klicken.
6. Klicken Sie auf der Registerkarte **Ausführen** auf **Fertig stellen**, um den Konfigurationsauftrag auszuführen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Sie nun einen weiteren Dienst zu diesem Lastenausgleichsserver hinzufügen und den Dienst an den Server binden möchten, können Sie die Befehle auf der Befehlsseite bearbeiten und speichern.

7. Navigieren Sie zu **Überwachungsvorlagen** und klicken Sie auf **Hinzufügen**.
8. Ziehen Sie die Vorlage „LBVariablesTemplate“ in den Befehlsbereich. Sie können sehen, dass die Vorlage mit den neuen Befehlen aktualisiert wurde.

   Die Überwachungsvorlage wird in der Liste der Überwachungsvorlagen angezeigt und wird alle 12 Stunden anhand der Konfigurationen der angegebenen Instanzen ausgeführt. Sie können nun Vorlagen erstellen und diese zwischen Konfigurationsaufträgen und Konfigurationsüberwachungsmodulen wiederverwenden.

Konfigurationsvorlagen importieren und exportieren

Sie können die Konfigurationsvorlagen von jeder NetScaler Console Appliance exportieren und die Datei jederzeit in dieselbe oder eine andere NetScaler Console Appliance importieren. Die Daten der Konfigurationsvorlagen (wie Konfigurationsbefehle, Variablendefinitionen und Parameter) gehen dabei nicht verloren.

Sie können die Konfigurationsvorlagen in ein **.json**-Dateiformat exportieren und im lokalen Ordner speichern. Sie können Konfigurationsvorlagen im **.json**-Dateiformat in NetScaler Console Appliances importieren, die Sie von derselben oder einer anderen NetScaler Console Appliance exportiert oder manuell erstellt haben.

So exportieren Sie die Konfigurationsvorlagen:

1. Navigieren Sie zu **Infrastructure > Configuration > Configuration Templates**.
2. Klicken Sie auf **Add**, um die Konfigurationsvorlage zu erstellen.

3. Auf der Seite **Create Configuration Template** geben Sie den Namen der Konfigurationsvorlage an und wählen Sie den Instanztyp aus. Wählen Sie unter **Configuration Editor** als Konfigurationsquelle „Configuration Template“ aus dem Dropdown-Menü aus. Sie können die vorhandenen Konfigurationsvorlagen in den Konfigurationseditor ziehen. Klicken Sie auf **OK**.

4. Navigieren Sie zu **Infrastructure > Configuration > Configuration Templates**, um die erstellten Vorlagen in der Liste der Konfigurationsvorlagen anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Wählen Sie die neu erstellte Konfigurationsvorlage aus und klicken Sie auf die Schaltfläche **Export**.

   Die entsprechende Konfigurationsvorlage wird in **.json**-Format auf Ihr lokales System heruntergeladen.

So importieren Sie die Konfigurationsvorlagen:

1. Navigieren Sie zu **Infrastructure > Configuration > Configuration Templates** und klicken Sie auf die Schaltfläche **Importieren**. Wählen Sie den Pfad aus, in dem sich die .**json**-Dateien der Konfigurationsvorlage befinden, und laden Sie die .**json**-Dateien hoch. Es wird dringend empfohlen, die .**json**-Dateien hochzuladen, die Sie bereits exportiert haben.

2. Sie können die Konfigurationsvorlage auch über die Option **Datei** im **Konfigurationseditor** importieren. Wählen Sie **Datei** aus dem Dropdown-Menü im **Konfigurationseditor** und **Datei auswählen** (.**json**-Dateien) von Ihrem lokalen System aus und laden Sie die .**json**-Dateien der Konfigurationsvorlage hoch.

   HINWEIS

   Sie können die Konfigurationsvorlagen nur importieren, wenn die Datei im .**json**-Format gespeichert ist. Wenn Sie Konfigurationsvorlagen von Ihrem lokalen System importieren, die keine .**json**-Dateien sind, wird ein Fehler angezeigt und der Import der Dateien schlägt fehl.

Konfigurationsaudit

Dieses Dokument enthält:

- Auditvorlagen erstellen
- Auditberichte anzeigen
- Konfigurationsänderungen über Instanzen hinweg prüfen
- Konfigurationsempfehlungen für die Netzwerkkonfiguration erhalten
- So fragen Sie das Konfigurationsaudit von NetScaler Console-Instanzen ab
- Konfigurationsaudit-Diff für ConfigChange SNMP-Traps generieren

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Audit-Vorlagen erstellen

Sie möchten sicherstellen, dass bestimmte Konfigurationen auf bestimmten Instanzen ausgeführt werden, um die optimale Leistung Ihres Netzwerks zu gewährleisten. Sie möchten auch Konfigurationsänderungen über verwaltete NetScaler-Instanzen hinweg überwachen, Konfigurationsfehler beheben und nicht gespeicherte Konfigurationen nach einem plötzlichen Systemausfall wiederherstellen. Sie können Audit-Vorlagen mit spezifischen Konfigurationen erstellen, die Sie auf bestimmten Instanzen prüfen möchten. NetScaler Console vergleicht diese Instanzen mit der Audit-Vorlage und meldet, wenn eine Diskrepanz in der Konfiguration vorliegt. Bei einer Konfigurationsdiskrepanz generiert NetScaler Console einen Konfigurations-Diff-Bericht, der Ihnen hilft, unerwünschte Konfigurationsänderungen zu beheben und zu korrigieren.

Sie können die Ausführung der Audit-Vorlage automatisieren, indem Sie

- den Zeitpunkt planen, zu dem die Vorlage ausgeführt werden soll
- die Häufigkeit festlegen, mit der NetScaler Console die Vorlage ausführen soll. Sie können die Vorlage täglich, an einem bestimmten Wochentag oder an einem bestimmten Datum im Monat ausführen.

Außerdem haben Sie die Möglichkeit, den von NetScaler Console generierten Diff-Bericht an bestimmte E-Mail-Adressen zu senden, die Sie konfigurieren können. Durch diese Option kann Ihr Benutzer den Bericht als E-Mail-Anhang erhalten, und der Benutzer muss sich nicht bei NetScaler Console anmelden, um die Berichte manuell zu exportieren.

Hinweis Die Option **Umbenennen** ist für die Standardkonfigurationsvorlagen deaktiviert. Sie können jedoch benutzerdefinierte Konfigurationsvorlagen umbenennen.

So erstellen Sie Audit-Vorlagen:

1. Navigieren Sie zu **Infrastructure > Configuration > Configuration Audit > Audit Templates**, und klicken Sie auf **Add**.
2. Geben Sie auf der Seite **Create Template** und auf der Registerkarte **Audit Commands** den Vorlagennamen und dessen Beschreibung an.
3. Geben Sie auf der Seite **Configuration Editor** Ihre Befehle ein und speichern Sie die Befehle als Konfigurationsvorlage. Sie können auch eine vorhandene Vorlage aus dem linken Bereich in den Editor ziehen.
4. Wählen Sie die Werte aus, die Sie in eine Variable umwandeln möchten, und klicken Sie dann auf **Convert to Variable**. Wählen Sie beispielsweise die IP-Adresse des Lastausgleichsservers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

„ipaddress1“ aus und klicken Sie auf **Convert to Variable**. Die Variable ist nun mit „$“ umschlossen, wie in der Abbildung unten gezeigt.

Legen Sie im Fenster **Define Variable** die Eigenschaften für diese Variable fest – Name, Anzeigename und Variablentyp. Klicken Sie auf die Option **Advanced**, wenn Sie einen Standardwert für Ihre Variable genauer angeben möchten.

Sie können die Befehle auch als Konfigurationsvorlage speichern.

5. Klicken Sie auf **Speichern** und dann auf **Weiter**.
6. Wählen Sie auf der Registerkarte **Instanzen auswählen** die Instanzen aus, für die Sie das Konfigurationsaudit ausführen möchten, und klicken Sie auf **Weiter**.

7. Auf der Registerkarte **Variablenwerte angeben** haben Sie zwei Optionen:

   a. Laden Sie die Eingabedatei herunter, um die Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den NetScaler Console-Server hoch.

   b. Geben Sie gemeinsame Werte für die Variablen ein, die Sie für alle Instanzen definiert haben.

8. Klicken Sie auf **Weiter**.

](/en-us/netscaler-console-service/media/nmas-config-audit-template-5.png)

9. Auf der Registerkarte **Vorlagenvorschau** können Sie die Befehle, die auf jeder Instanz oder Instanzgruppe ausgeführt werden sollen, auswerten und überprüfen. Klicken Sie auf **Weiter**.

10. Auf der Registerkarte **Vorlage planen** haben Sie die folgenden Optionen, um die Ausführung der Vorlage zu planen und die E-Mail-Adresse für den Versand des Diff-Berichts zu konfigurieren.

    - **Globales Abfrageintervall verwenden**. Wählen Sie diese Option, um die Vorlage auf den Instanzen zu einem global in NetScaler Console konfigurierten Zeitpunkt auszuführen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Um das globale Abfrageintervall in NetScaler Console zu konfigurieren, navigieren Sie zu **Infrastructure > Configuration > Configuration Audit > Audit Templates**. und klicken Sie auf **Global Polling Interval**. Geben Sie im Feld **Poll Interval** die Minuten ein, in denen NetScaler Console die Instanzen global abfragen soll.

- **Vorlagenzeitplan anpassen**. Verwenden Sie diese Option, um die Uhrzeit und die Häufigkeit zu konfigurieren, mit der die Vorlagen ausgeführt werden sollen.
- **Bericht per E-Mail senden**. Verwenden Sie diese Option, um das E-Mail-Profil zu konfigurieren, an das der Diff-Bericht als E-Mail-Anhang gesendet werden soll.

11. Klicken Sie auf **Fertig stellen**.

    Die Audit-Vorlage wird in der Liste **Audit Templates** angezeigt und zur geplanten Zeit für die Konfigurationen in den angegebenen Instanzen ausgeführt.

Konfigurationsaudit von NetScaler-Instanzen abfragen

NetScaler Console fragt die Konfigurationsaudits automatisch alle 10 Stunden ab, um nach Konfigurationsänderungen zu suchen, die auf NetScaler-Instanzen auftreten. Sie können die Konfigurationsaudits auch manuell abfragen, um aktuelle Änderungen zu ermitteln, aber das Abfragen der Konfiguration aller NetScaler-Instanzen belastet das Netzwerk stark.

Anstatt das gesamte Konfigurationsaudit der NetScaler-Instanzen abzufragen, können Sie manuell nur die Konfigurationsaudits einer oder mehrerer ausgewählter Instanzen abfragen.

So fragen Sie Konfigurationsaudits von NetScaler-Instanzen ab:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Configuration > Configuration Audit**.
2. Klicken Sie auf der Seite **Configuration Audit** in der oberen rechten Ecke auf **Poll Now**.

   Option „Poll Now“(/en-us/netscaler-console-service/media/config-audit-poll-now.png)
3. Die Seite **Poll Now** wird angezeigt und bietet Ihnen die Möglichkeit, alle NetScaler-Instanzen im Netzwerk abzufragen oder ausgewählte Instanzen abzufragen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Um alle NetScaler-Instanzen abzufragen, wählen Sie die Registerkarte **All Instances** aus und klicken Sie auf **Start Polling**.

   Alle Instanzen abfragen(/en-us/netscaler-console-service/media/config-audit-poll-now-1.png)

b. Um bestimmte Instanzen abzufragen, wählen Sie die Registerkarte **Select Instances** aus, wählen Sie die Instanzen aus der Liste aus und klicken Sie auf **Start Polling**.

   Bestimmte Instanzen abfragen(/en-us/netscaler-console-service/media/config-audit-poll-now-2.png)

Auditberichte anzeigen

Mit NetScaler Console können Sie den Konfigurations-Audit-Diff-Bericht im Abschnitt Konfigurations-Audit anzeigen und herunterladen. Der Abschnitt Konfigurations-Audit ermöglicht Ihnen den Export des Zusammenfassungsberichts über alle Instanzen und pro Instanz sowie den Export eines detaillierten Diff-Berichts für jedes Instanz-Vorlagen-Paar.

Die Audit-Vorlagen, die in der Liste der Audit-Vorlagen erscheinen, werden zum geplanten Zeitpunkt mit den Konfigurationen in den angegebenen Instanzen ausgeführt. Das Diagramm **NetScaler Config Drift** auf dem Dashboard **Konfigurations-Audit** zeigt übergeordnete Details zu Konfigurationsänderungen in gespeicherten gegenüber nicht gespeicherten Konfigurationen an. Wenn Sie auf das Diagramm **NetScaler Config Drift** klicken, zeigt die folgende Seite **Auditberichte** eine Liste von Instanzen an, die sowohl „Diff Exists“ als auch „No Diff“ aufweisen. Sie können die von NetScaler Console angezeigten Diff-Berichte herunterladen.

NetScaler Console bietet auch die Möglichkeit, den automatischen Export von Diff-Berichten als E-Mail-Anhang zu planen. Weitere Informationen zum Planen des Exports von Berichten finden Sie unter Audit-Vorlagen erstellen.

Konfigurations-Auditberichte exportieren

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Konfiguration > Konfigurations-Audit**.
2. Klicken Sie auf der Seite **Konfigurations-Audit** in das Diagramm **NetScaler Config Drift**.
3. Die Seite **Auditberichte** listet Instanzen auf, die eine Abweichung aufweisen. Die Seite zeigt auch eine Liste von Instanzen an, die keine Abweichung in ihren laufenden Konfigurationen aufweisen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Im Bild sehen Sie, dass für einige Instanzen ein Diff nur in **Gespeicherte vs. Laufende Diff** vorhanden ist und für einige Instanzen ein Diff nur in **Vorlage vs. Laufende Diff** vorhanden ist. Für einige Instanzen bestehen Unterschiede sowohl in **Gespeicherte vs. Laufende Diff** als auch in **Vorlage vs. Laufende Diff**.

Gespeicherte vs. Laufende Diff:

Sie können einen Bericht über die Abweichung zwischen der auf der Instanz gespeicherten Konfiguration und der aktuell auf dieser Instanz ausgeführten Konfiguration anzeigen. Klicken Sie beispielsweise auf **Diff Exists** für eine Instanz unter **Gespeicherte vs. Laufende Diff**.

Hier sehen Sie einen Bericht über die gespeicherte Konfiguration im Vergleich zur laufenden Konfigurationsabweichung für diese Instanz.

Klicken Sie auf **Diff-Bericht exportieren**, um eine .csv-Datei des Diff-Berichts herunterzuladen. Sie können auch auf **Korrekturbefehle exportieren** klicken, um die Befehle in eine .txt-Datei zu exportieren. Anschließend können Sie die Befehle über Konfigurationsaufträge auf der zugehörigen NetScaler-Instanz ausführen, um die Konfiguration in dieser Instanz zu korrigieren.

Vorlagen- vs. Laufzeit-Diff:

Der **Vorlagen- vs. Laufzeit-Diff** umfasst alle Vorlagen außer **Gespeicherter vs. Laufzeit-Diff**, die die Standardvorlage ist. Sie können den Unterschied zwischen der Vorlage und der laufenden Konfiguration anzeigen. Klicken Sie beispielsweise auf **Diff vorhanden** für eine der Instanzen unter **Vorlagen- vs. Laufzeit-Diff**.

Jetzt sehen Sie, dass zwei Vorlagen einen Unterschied aufweisen und die NetScaler-Instanz eine andere Konfiguration hat, als die Vorlage erwartet.

Klicken Sie erneut auf **Diff vorhanden**. Die folgende Abbildung zeigt die Konfiguration, die die Vorlage erwartet, und die leere laufende Konfiguration, da keine solchen Befehle konfiguriert oder entfernt wurden. Sie können auch die Korrekturkonfigurationen oder die auszuführenden Befehle zur Korrektur der Konfiguration sehen.

Sie können auch die Einstellung „Vorlage vs. Laufzeit“ und „Laufzeit vs. Vorlagenabweichung“ verwenden, um die Konfiguration auf beide Arten zu vergleichen:

- Vergleicht die Audit-Vorlagenkonfiguration mit der laufenden Konfiguration auf der Instanz.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Vergleicht die laufende Konfiguration auf der Instanz mit der Audit-Vorlage.

Standardmäßig ist die Einstellung „Vorlage vs. Laufzeitabweichung“ ausgewählt. Um die Abweichungseinstellung zu ändern, wählen Sie in der NetScaler Console GUI auf der Seite **Konfigurationsprüfung** die Option **Einstellungen** aus.

Klicken Sie auf **Diff-Bericht exportieren**, um eine .csv-Datei des Diff-Berichts herunterzuladen. Sie können auch auf **Korrekturbefehle exportieren** klicken, um die Befehle in eine .txt-Datei zu exportieren. Anschließend können Sie die Befehle in der CLI ausführen, um die Konfiguration in dieser Instanz zu korrigieren.

Die folgende Abbildung zeigt eine Beispiel-Diff-Datei im .csv-Format, die auf Ihr System heruntergeladen wird:

Dateistatus-Auditberichte anzeigen

Mithilfe des Diagramms **NetScaler-Dateistatus** können Sie überwachen, ob Dateien im Ordner `nsconfig` hinzugefügt, geändert oder entfernt wurden. Beispiel: Wenn die Lizenzdatei auf einer NetScaler-Instanz aktualisiert wird, können Sie überprüfen, wann diese Datei zuletzt aktualisiert wurde, und entsprechende Maßnahmen ergreifen.

So exportieren Sie die Dateistatus-Auditberichte für die NetScaler-Instanzen:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Configuration > Configuration Audit**.
2. Klicken Sie auf der Seite **Configuration Audit** in das Diagramm **NetScaler-Dateistatus**.

   Auf der Seite **Audit Reports** werden Instanzen mit dem Diff-Status aufgelistet.

   Der **Diff-Status** wird für das Intervall zwischen der **Previous Polled Time** und der **Latest Polled Time** berechnet. Der **Diff-Status** kann einer der folgenden sein:

   - **Diff vorhanden** – Dieser Status zeigt an, dass sich die Dateien im Ordner `nsconfig` einer Instanz seit der **Previous Polled Time** geändert haben. Um anzuzeigen, was sich an der Datei geändert hat, klicken Sie auf **Diff vorhanden**.

   - **Kein Diff** – Dieser Status zeigt an, dass sich die Dateien im Ordner `nsconfig` seit der vorherigen Abfragezeit nicht geändert haben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **N/A** – Dieser Status zeigt an, dass die Überwachung des Dateistatus nicht zutreffend ist. Dieser Status wird angezeigt, wenn die NetScaler Console die Instanz nicht abfragt. Beispiel: Wenn eine Instanz neu hinzugefügt wird oder der Instanzstatus inaktiv ist, erfolgt keine Abfrage der Instanz.

Bericht dieses Dashboards exportieren

Um den Bericht dieser Seite zu exportieren, klicken Sie auf das Symbol **Exportieren** oben rechts auf dieser Seite. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Export Now**. Um den Bericht im PDF-, JPEG-, PNG- oder CSV-Format anzuzeigen und zu speichern.
2. Wählen Sie die Registerkarte **Schedule Export**. Um den Bericht täglich, wöchentlich oder monatlich zu planen und per E-Mail oder Slack-Nachricht zu versenden.

HINWEIS

- Wenn Sie die **Wöchentliche** Wiederholung auswählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie die **Monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie alle Tage, an denen der Bericht geplant werden soll, durch Kommas getrennt eingeben.

Dateien vom Config Audit ausschließen

Sie können bestimmte Dateien vom Config Audit ausschließen, damit sie nicht auf Änderungen überwacht werden. Verwenden Sie Ausschlüsse für systemgenerierte oder häufig aktualisierte Dateien (z. B. täglich geänderte Dateien), um Rauschen zu reduzieren und Fehlalarme in den Auditergebnissen zu vermeiden.

Beispiele für Dateinamen (oder relativen Pfad), die vom Config Audit-Dateivergleich ausgeschlossen werden sollen:

- Gültiger Dateiname (oder relativer Pfad)
  - `ns.conf`, `ssl/ns.cert`
- Ungültiger Dateiname (oder relativer Pfad)
  - `/ns.txt`, `\nsconfig\ns.conf` (Der ausgeschlossene Dateiname muss ein relativer Pfad sein)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `ñs.conf` (Der ausgeschlossene Dateiname darf nur ASCII-Zeichen enthalten)
- `C:/nsconfig/ns.conf` (Der ausgeschlossene Dateiname darf keine Laufwerksbuchstabenpfade verwenden)
- `ssl/../../ns.conf` (Der ausgeschlossene Dateiname darf keine Traversierung über das übergeordnete Verzeichnis `..` enthalten)

HINWEISE:

- Alle Dateien unter `/nsconfig/license/` sind standardmäßig vom Konfigurationsaudit ausgeschlossen. NetScaler Console schreibt alle 8 Stunden während der Token-Aktualisierungszyklen LAS-Dateien in dieses Verzeichnis. Da diese Dateien vollständig von NetScaler Console verwaltet werden und nicht Teil der NetScaler-Konfiguration des Kunden sind, lösen sie falsch-positive **Diff Exists**-Warnungen aus. Das Verzeichnis `license/` ist jetzt als Standardausschluss voreingestellt, um diese falsch-positive Meldung zu verhindern. Sie können diesen Ausschluss bei Bedarf entfernen.
- Der Dateidifferenzvergleich ist nur auf Dateien unter dem Verzeichnis `/nsconfig` anwendbar.
- Beim Ausschließen von Dateien aus dem Konfigurationsaudit müssen Benutzer relative Pfade unter `/nsconfig` angeben. Wenn sich beispielsweise ein Ordner `ssl` unter `/nsconfig` befindet, können Ausschlüsse wie folgt angegeben werden: `ssl/abc.pem`
- Dateidifferenzen außerhalb von `/nsconfig` werden nicht als Teil des Konfigurationsaudit-Diffs berücksichtigt.

Um Dateien vom Konfigurationsaudit auszuschließen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsaudit**.
2. Wählen Sie **Einstellungen**.
3. Unter **NetScaler-Konfigurationsdateieinstellungen** fügen Sie die Dateipfade hinzu, die Sie vom Audit ausschließen möchten.
4. Klicken Sie auf **Speichern**.

Konfigurationsaudit-Diff für ConfigChange SNMP-Traps generieren

Immer wenn eine Konfigurationsänderung in einer NetScaler-Instanz im Netzwerk vorliegt, wird die Konfigurationsdatei aktualisiert. Die Instanz sendet einen ConfigChange SNMP-Trap an NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Console. Sie können NetScaler Console aktivieren, um eine Konfigurationsprüfung für diese Instanz durchzuführen, wenn die Instanz einen ConfigChange SNMP-Trap sendet.

Wenn eine Differenz zwischen der Audit-Vorlagenkonfiguration und der laufenden Konfiguration besteht, wird eine Statusmeldung „Diff Exists“ auf der Seite „Audit Report“ angezeigt. Durch Klicken auf den Link „Diff Exits“ gelangen Sie zur Seite „Configuration Diff“, wo Sie den Korrekturbefehl anzeigen können. Sie können diese Korrekturbefehle verwenden, um einen Konfigurationsauftrag zu erstellen und diesen auf den spezifischen NetScaler-Instanzen auszuführen. Wenn Sie den Konfigurationsauftrag ausführen, werden die Instanzen auf die gewünschte Konfiguration zurückgesetzt. Weitere Informationen zum Erstellen von Konfigurationsaufträgen aus Korrekturbefehlen finden Sie unter So erstellen Sie Konfigurationsaufträge aus Korrekturbefehlen in NetScaler Console.

So führen Sie Konfigurationsaudit-Vorlagen beim Empfang eines ConfigChange SNMP-Traps aus:

NetScaler Console ermöglicht es Ihnen, die Option zum Ausführen der Konfigurationsaudit-Vorlage in NetScaler Console zu aktivieren.

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Konfiguration > Konfigurationsaudit**.
2. Klicken Sie auf der Seite **Konfigurationsaudit** auf **Einstellungen**.
3. Klicken Sie im Abschnitt **Einstellungen für Konfigurationsänderungs-Audit** auf das Bearbeitungssymbol.
4. Aktivieren Sie das Kontrollkästchen **Konfigurationsaudit durchführen, wenn ein netScalerConfigChange-Ereignis empfangen wird**.

   HINWEIS

   Dies ist eine globale Einstellung für alle Instanzen. NetScaler Console führt ein Konfigurationsaudit für jede Instanz durch, für die es in Zukunft die netScalerConfigChange SNMP-Traps empfängt.

5. Geben Sie im Feld **Zeitverzögerung zum Ausführen der Audit-Vorlage (in Minuten)** die Minuten ein. NetScaler Console führt die Konfigurationsaudit-Vorlage auf der NetScaler-Instanz nach dieser Zeitverzögerung aus, wenn es den ConfigChange SNMP-Trap von dieser Instanz empfängt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfigurationsänderungen über Instanzen hinweg prüfen

Sie möchten sicherstellen, dass bestimmte Konfigurationen auf bestimmten Instanzen ausgeführt werden, um die optimale Leistung Ihres Netzwerks zu gewährleisten. Sie möchten auch Konfigurationsänderungen über verwaltete NetScaler-Instanzen hinweg überwachen, Konfigurationsfehler beheben und nicht gespeicherte Konfigurationen nach einem plötzlichen Systemausfall wiederherstellen. Sie können Audit-Vorlagen mit spezifischen Konfigurationen erstellen, die Sie auf bestimmten Instanzen ausführen möchten. Die NetScaler Console vergleicht diese Instanzen mit der Audit-Vorlage und meldet, wenn eine Konfigurationsabweichung vorliegt. Dieser Vergleich ermöglicht es Ihnen, die Fehler zu beheben und zu korrigieren.

Sie können die Ausführung der Audit-Vorlage automatisieren, indem Sie die Zeit planen, zu der die Vorlage ausgeführt werden soll. Sie können auch die Häufigkeit festlegen, mit der die NetScaler Console die Vorlage ausführen soll. Sie können die Vorlage täglich, an einem bestimmten Wochentag oder an einem bestimmten Datum im Monat ausführen. Sie können den von der NetScaler Console generierten Diff-Bericht auch an angegebene E-Mail-Adressen senden, die Sie konfigurieren können. Durch diese Option erhält Ihr Benutzer den Bericht als E-Mail-Anhang, und der Benutzer muss sich nicht bei der NetScaler Console anmelden, um die Berichte manuell zu überprüfen.

So erstellen Sie Audit-Vorlagen:

1. Navigieren Sie zu **Infrastructure > Configuration > Configuration Audit > Audit Templates** und klicken Sie auf **Add**.
2. Geben Sie auf der Seite **Create Template** und auf der Registerkarte **Audit Commands** den Vorlagennamen und dessen Beschreibung an.
3. Geben Sie im **Configuration Editor** Ihre Befehle ein und speichern Sie die Befehle als Konfigurationsvorlage. Sie können auch eine vorhandene Vorlage aus dem linken Bereich in den Editor ziehen.
4. Wählen Sie die Werte aus, die Sie in eine Variable umwandeln möchten, und klicken Sie dann auf **Convert to Variable**. Wählen Sie beispielsweise die IP-Adresse des Lastausgleichsservers `ipaddress` aus und klicken Sie auf **Convert to Variable**, wie in der folgenden Abbildung gezeigt.

   Klicken Sie auf die Option **Advanced**, wenn Sie einen Standardwert für Ihre Variable genauer angeben möchten.

   Sie können die Befehle auch als Konfigurationsvorlage speichern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Klicken Sie auf **Save** und dann auf **Next**.
6. Wählen Sie auf der Registerkarte **Select Instances** die Instanzen aus, für die Sie das Konfigurationsaudit ausführen möchten.
7. Auf der Registerkarte **Specify Variable Values** haben Sie zwei Optionen:
   a. Laden Sie die Eingabedatei herunter, um die Werte für die Variablen einzugeben, die Sie in Ihren Befehlen definiert haben, und laden Sie die Datei dann auf den NetScaler Console-Server hoch
   b. Geben Sie gemeinsame Werte für die Variablen ein, die Sie für alle Instanzen definiert haben
8. Klicken Sie auf **Weiter**.

9. Auf der Registerkarte **Vorlagenvorschau** können Sie die Befehle, die auf jeder Instanz oder Instanzgruppe ausgeführt werden sollen, auswerten und überprüfen. Klicken Sie auf **Weiter**.
10. Auf der Registerkarte **Vorlage planen** haben Sie drei Optionen, um die Ausführung der Vorlage und die E-Mail-Adresse, an die der Diff-Bericht gesendet werden soll, zu automatisieren.
    - **Globales Abfrageintervall verwenden**. Wählen Sie diese Option, um die Vorlage zu einem global in NetScaler Console konfigurierten Zeitpunkt auf den Instanzen auszuführen
    - **Vorlagenzeitplan anpassen**. Verwenden Sie diese Option, um die Uhrzeit und die Häufigkeit zu konfigurieren, mit der die Vorlagen ausgeführt werden sollen
    - **Bericht per E-Mail senden**. Verwenden Sie diese Option, um das E-Mail-Profil zu konfigurieren, an das der Diff-Bericht als E-Mail-Anhang gesendet werden soll.
11. Klicken Sie auf **Fertig stellen**.

Die Audit-Vorlage wird in der Liste der Audit-Vorlagen angezeigt und zum geplanten Zeitpunkt anhand der Konfigurationen in den angegebenen Instanzen ausgeführt.

Details zu Konfigurationsänderungen anzeigen

Sie können auch das Konfigurationsaudit-Dashboard verwenden, um übergeordnete Details zu Konfigurationsänderungen anzuzeigen, wie zum Beispiel:

- Die Top 10 Instanzen nach Konfigurationsänderung
- Die Anzahl der gespeicherten und ungespeicherten Konfigurationen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die im Ordner `nsconfig` hinzugefügte, entfernte oder geänderte Datei

Mit NetScaler Console können Sie Konfigurationsprüfungen auch manuell abfragen und alle Konfigurationsprüfungen der Instanzen sofort zur NetScaler Console hinzufügen. Navigieren Sie dazu zu **Infrastructure > Configuration > Configuration Audit**, klicken Sie auf **Jetzt abfragen**. Die Pop-up-Seite **Jetzt abfragen** bietet Ihnen die Möglichkeit, alle NetScaler-Instanzen im Netzwerk abzufragen oder die ausgewählten Instanzen abzufragen.

Sie können auch eine Prüfung für eine Instanz erzwingen. Klicken Sie dazu auf eines der folgenden Diagramme:

- **NetScaler Konfigurations-Speicherstatus**
- **NetScaler Konfigurationsabweichung**

Wählen Sie auf der Seite **Audit Reports** die Instanz aus und wählen Sie in der Liste **Action** die Option **Poll Now**.

Das Diagramm **NetScaler Config File Status** zeigt Ihnen den Status der NetScaler-Dateien im Ordner `nsconfig` an. Die NetScaler Console zeichnet Änderungen in Dateien im Ordner `nsconfig` auf, vergleicht sie und zeigt die Unterschiede an. Siehe Berichte zur Überprüfung des Dateistatus anzeigen.

Benachrichtigungen zur Konfigurationsprüfung einrichten

1. Navigieren Sie zu **Infrastructure > Configuration > Configuration Audit**.
2. Klicken Sie auf der Seite **Configuration Audit** auf **Settings**.
3. Auf der Seite **Settings**:
   a. Aktivieren Sie das Kontrollkästchen **Perform Audit on receiving "netScalerConfigChange event**, um die Benachrichtigungseinstellungen zu aktivieren.
   b. Legen Sie die Verzögerungszeit für das Audit fest.
4. Legen Sie unter **Konfigurationsaudit-Abfrage** das **Abfrageintervall** fest.

   Die NetScaler Console fragt die Konfigurationsaudit-Ereignisse für das angegebene Abfrageintervall ab.
5. Wählen Sie unter **Benachrichtigung über Konfigurationsdateidifferenzen** die Plattform aus, auf der Sie die Benachrichtigungen erhalten möchten:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **E-Mail** – Wählen Sie die E-Mail-Verteilerliste aus. Klicken Sie auf Hinzufügen, um eine E-Mail-Verteilerliste hinzuzufügen, um Benachrichtigungen zu erhalten.
- **Slack** – Wählen Sie den Slack-Kanal aus der Liste aus. Klicken Sie auf Hinzufügen, um einen Kanal hinzuzufügen, um Benachrichtigungen zu erhalten.

Konfigurationsempfehlungen für die Netzwerkkonfiguration erhalten

Sie richten Ihre NetScaler-Instanzen mit optimalen Konfigurationen ein, um eine optimale Leistung Ihrer Anwendungen zu erzielen. Es ist jedoch möglich, dass einige Konfigurationen keine Standardkonfigurationen sind, was die Leistung Ihrer Anwendungen beeinträchtigen kann.

Um Sie bei der Optimierung Ihrer Anwendungsleistung zu unterstützen, analysiert NetScaler Console die NetScaler-Instanzkonfiguration und gibt Ihnen Empfehlungen. Sie können die empfohlenen Konfigurationen über NetScaler Console anwenden.

So analysieren Sie die NetScaler-Instanz:

1. Navigieren Sie zu **Infrastruktur > Konfiguration > Konfigurationsprüfung > Konfigurationsempfehlungen**.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Konfigurationsdatei hochladen** und laden Sie die Konfigurationsdatei Ihrer Netzwerkinstanz hoch.
   - Klicken Sie auf **Gerät auswählen** und wählen Sie die NetScaler-Instanz aus, die Sie analysieren möchten.

NetScaler Console analysiert die Konfiguration Ihrer Instanz und stellt eine Liste von Konfigurationsempfehlungen bereit, wie in der folgenden Abbildung gezeigt. Klicken Sie auf das Kontrollkästchen neben einer Konfigurationsempfehlung, um die Korrekturbefehle anzuzeigen.

Wenn Sie Ihre Konfiguration aktualisieren möchten, geben Sie die Werte für die Variablen in den Korrekturbefehlen an und klicken Sie auf **Jetzt anwenden**, wie in der folgenden Abbildung gezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Die hier aufgeführten Befehle sind nur Empfehlungen. Ein Benutzer mit Lese- und Schreibzugriff kann möglicherweise jeden Befehl mit dieser Funktion bearbeiten. Stellen Sie sicher, dass Sie Benutzern, die die Befehle nicht bearbeiten dürfen, nur eingeschränkte Berechtigungen erteilen.

Wenn der Befehl erfolgreich auf der Netzwerkinstanz ausgeführt wurde, verschwindet das Kontrollkästchen neben der Empfehlung.

Benutzerverwaltung einrichten(/en-us/netscaler-console-service/media/mas-configuration-advice-6.png)

Wenn Sie die Details der auf Ihrer Netzwerkinstanz ausgeführten Befehle anzeigen möchten, navigieren Sie zu **Infrastruktur > Instanzen > \<Instance_Type>**, wählen Sie die IP-Adresse der Instanz aus und klicken Sie dann in der Dropdown-Liste **Aktionen auswählen** auf **Ereignisse anzeigen**.

Ereignisse anzeigen(/en-us/netscaler-console-service/media/config-advice4.png)

Auf der Seite **Ereignisse** können Sie die Details der Konfigurationsänderung anzeigen.

Konfigurationsänderung anzeigen(/en-us/netscaler-console-service/media/config-advice5.png)

Upgrade-Aufträge

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der Lizenzaktivierungsdienst (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Citrix Produktpalette. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, und unterstützt NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed Term Bandwidth-Lizenzen. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die mindestens erforderlichen NetScaler®-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 für Console on-prem-Versionen ab 14.1-51.x und ab 13.1-60.x eingestellt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch vor 15th April 2026 auf Console on-prem Version 14.1-51.x oder höher aktualisieren und zu LAS wechseln, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, unbefristet werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden nach dem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies gesetzlich oder durch Vorschriften untersagt ist.
Wenn Sie Fragen oder Bedenken haben, wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix-Wartung bei Nichteinhaltung dieser Anforderungen ohne Haftung zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit zustehen, einschränken oder aussetzen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften untersagt sind.
Mit NetScaler Console können Sie die folgenden Wartungsaufgaben erstellen. Sie können die Wartungsaufgaben dann zu einem bestimmten Datum und einer bestimmten Uhrzeit planen.

- NetScaler-Instanzen aktualisieren
- NetScaler SDX-Instanzen aktualisieren
- NetScaler BLX-Instanzen aktualisieren
- NetScaler-Instanzen in der Autoscale-Gruppe aktualisieren
- HA-Paar von NetScaler-Instanzen konfigurieren
- HA-Paar von Instanzen in Cluster konvertieren

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Während Sie eine beliebige Anzahl von NetScaler-Instanzen für das Upgrade auswählen können, unterstützt der NetScaler Console-Dienst maximal 100 gleichzeitige Upgrade-Threads. Dies bedeutet, dass nur 100 Instanzen gleichzeitig aktualisiert werden können. Dieses Limit ist dynamisch und kann je nach gleichzeitiger Upgrade-Aktivität anderer Mandanten variieren.

Vor-Upgrade-Validierung

NetScaler Console führt die folgenden Prüfungen durch:

- **Verfügbarer Speicherplatz auf `/var`**: Überprüft, ob auf der `/var`-Partition ausreichend freier Speicherplatz vorhanden ist, um die Extraktion von Images und Installationsvorgänge sicher durchzuführen.
- **Verfügbarer Speicherplatz auf /flash**: Überprüft, ob die `/flash`-Partition den mindestens erforderlichen freien Speicherplatz aufweist, um wesentliche Systemoperationen während der Installation zu unterstützen.
- **NSPEPI-Konfigurationsprüfung**: Validiert die NetScaler-Konfigurationsdatei auf nicht unterstützte oder ungültige Richtlinien, um Konfigurationsfehler nach der Installation oder dem Upgrade zu vermeiden.
- **High Availability (HA)-Konfigurationsprüfung**: Überprüft den HA-Status und die Rollenkonsistenz, um eine fehlerfreie und unterstützte HA-Einrichtung zu gewährleisten.
- **SSH-Konnektivitätsprüfung**: Bestätigt die SSH-Zugänglichkeit, Vertrauensvalidierung und Konnektivität zu Zielgeräten, die für Remote-Installations- und Verwaltungsoperationen erforderlich sind.
- **Passende ns.conf für Downgrade**: Stellt sicher, dass eine geeignete und kompatible `ns.conf file` für Downgrade-Szenarien verfügbar ist, um Konfigurationsinkompatibilität zu vermeiden.

Alle Vorabprüfungsergebnisse werden einheitlich wie folgt kategorisiert:

- **Kritisch (Blockierend)**: Das Upgrade ist blockiert. Alle gemeldeten Probleme müssen behoben werden, bevor Sie fortfahren.
- **Warnung**: Das Upgrade kann mit Genehmigung des Administrators fortgesetzt werden.
- **Hinweis**: Das Upgrade kann mit Genehmigung des Administrators fortgesetzt werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Upgrade von NetScaler-Instanzen planen

1. Navigieren Sie in der NetScaler Console zu **Infrastruktur > Upgrade-Aufträge**. Klicken Sie auf **Auftrag erstellen**.

2. Wählen Sie unter **Wartungsaufträge erstellen** die Option **NetScaler aktualisieren (Standalone/Hochverfügbarkeit/Cluster)** aus und klicken Sie auf **Weiter**.

3. Geben Sie unter **Instanz auswählen** einen Namen Ihrer Wahl für **Auftragsname** ein.
4. Klicken Sie auf **Instanzen hinzufügen**, um NetScaler-Instanzen hinzuzufügen, die Sie aktualisieren möchten.

   - Um ein HA-Paar zu aktualisieren, geben Sie die IP-Adresse eines primären oder sekundären Knotens an. Es wird jedoch empfohlen, die primäre Instanz für das Upgrade des HA-Paares zu verwenden.
   - Um einen Cluster zu aktualisieren, geben Sie die Cluster-IP-Adresse an.

5. Klicken Sie auf **Weiter**, um das Image auszuwählen. Wählen Sie eine der folgenden Optionen aus der Liste **Software-Image** aus:

   - **Lokal** – Wählen Sie die Instanz-Upgrade-Datei von Ihrem lokalen Computer aus.
   - **Appliance** – Wählen Sie die Instanz-Upgrade-Datei aus einem NetScaler Console-Dateibrowser aus. Die NetScaler Console-GUI zeigt die Instanzdateien an, die bereits serverseitig hochgeladen wurden.

     - **Bild-Upload auf NetScaler überspringen, wenn das ausgewählte Bild bereits verfügbar ist** – Wählen Sie diese Option, wenn das Bild bereits in der NetScaler-Instanz vorhanden ist.
     - **Software-Image nach erfolgreichem Upgrade von NetScaler entfernen** – Wählen Sie diese Option, um das hochgeladene Image in der NetScaler-Instanz nach dem Instanz-Upgrade zu löschen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Wenn die ausgewählten Instanzen bereits auf dem Ziel-Build sind, wird eine Warnung angezeigt. Diese Warnung hilft, die Auswahl falscher Instanzen während Upgrade-Aufträgen zu verhindern. Wenn Sie die Instanzen erneut aktualisieren möchten, ignorieren Sie die Warnung und fahren Sie mit dem Upgrade fort.

- Wenn für die ausgewählte Instanz bereits ein Upgrade-Auftrag geplant ist, zeigt die NetScaler Console eine Warnmeldung an. Diese Warnmeldung hilft, das unbeabsichtigte Planen doppelter Upgrade-Aufträge auf derselben NetScaler-Instanz zu verhindern.

6. Klicken Sie auf **Weiter**, um die Vor-Upgrade-Validierung für die ausgewählten Instanzen zu starten.

   Die Registerkarte **Vor-Upgrade-Validierung** zeigt die fehlgeschlagenen Instanzen an. Entfernen Sie die fehlgeschlagenen Instanzen und klicken Sie auf **Weiter**. Weitere Informationen finden Sie unter Vor-Upgrade-Validierung.

   WICHTIG

   Wenn Sie die Cluster-IP-Adresse angeben, führt die NetScaler Console die Vor-Upgrade-Validierung nur für die angegebene Instanz durch, nicht für die anderen Cluster-Knoten.

7. Optional können Sie unter **Benutzerdefinierte Skripte** die Skripte angeben, die vor und nach einem Instanz-Upgrade ausgeführt werden sollen. Verwenden Sie eine der folgenden Methoden, um die Befehle auszuführen:

   - **Befehle aus Datei importieren** – Wählen Sie die Befehlseingabedatei von Ihrem lokalen Computer aus.
   - **Befehle eingeben** – Geben Sie Befehle direkt in die GUI ein.

   Sie können benutzerdefinierte Skripte verwenden, um die Änderungen vor und nach einem Instanz-Upgrade zu überprüfen. Zum Beispiel:

   - Die Instanzversion vor und nach dem Upgrade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Der Status von Schnittstellen, Hochverfügbarkeitsknoten, virtuellen Servern und Diensten vor und nach dem Upgrade.
- Die Statistiken der virtuellen Server und Dienste.
- Die dynamischen Routen.

8. Klicken Sie auf **Weiter**. Wählen Sie unter **Aufgabe planen** eine der folgenden Optionen aus:

   - **Jetzt aktualisieren** – Der Upgrade-Auftrag wird sofort ausgeführt.
   - **Später planen** – Wählen Sie diese Option, um diesen Upgrade-Auftrag später auszuführen. Geben Sie das **Ausführungsdatum** und die **Startzeit** an, wann Sie die Instanzen aktualisieren möchten.

     Wenn Sie ein NetScaler HA-Paar in zwei Phasen aktualisieren möchten, wählen Sie **Zweistufiges Upgrade für Knoten in HA durchführen**.

     Geben Sie das **Ausführungsdatum** und die **Startzeit** an, wann Sie eine weitere Instanz im HA-Paar aktualisieren möchten.

9. Klicken Sie auf **Weiter**. Geben Sie unter **Auftrag erstellen** die folgenden Details an:

   a. Geben Sie an, wann Sie das Image auf eine Instanz hochladen möchten:

      - **Jetzt hochladen** – Wählen Sie diese Option, um das Image sofort hochzuladen. Der Upgrade-Auftrag wird jedoch zum geplanten Zeitpunkt ausgeführt.
      - **Zum Zeitpunkt der Ausführung hochladen** – Wählen Sie diese Option, um das Image zum Zeitpunkt der Ausführung des Upgrade-Auftrags hochzuladen.
      - **Sichern Sie die NetScaler-Instanzen, bevor Sie das Upgrade starten.** – Erstellt ein Backup der ausgewählten NetScaler-Instanzen.
      - **NetScaler-Konfiguration vor dem Start des Upgrades speichern** – Speichert die Konfigurationsaufträge, die vor dem Upgrade auf der Instanz konfiguriert sind.
      - **ISSU aktivieren, um Netzwerkausfälle bei NetScaler HA-Paaren zu vermeiden** – Durch die Aktivierung von In-Service Software Upgrade (ISSU) können Sie ein NetScaler Hochverfügbarkeits- (HA-) Paar ohne Netzwerkausfallzeiten aktualisieren. ISSU stellt sicher, dass die bestehenden Verbindungen während des Upgrades berücksichtigt werden, indem die aktiven Sitzungen nahtlos zwischen den Knoten migriert werden. Nach der Aktivierung von ISSU im Upgrade-Workflow kann das System auch den Abschluss der ISSU-Migration nach der vom Kunden definierten Verzögerungszeit auslösen. Die NetScaler Console, die einen vollständigen Abschluss der ISSU-Migration auslöst, stellt sicher, dass das Upgrade auch dann abgeschlossen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

wird, wenn Verbindungen bestehen bleiben. Geben Sie das ISSU-Migrations-Timeout in Minuten an, um die Wartezeit festzulegen, bevor NetScaler Console die Migration abschließt.

- **Console Advisory Connect** – Wenn Sie auf Build **13.0-64 oder höher** und **12.1-58 oder höher** aktualisieren, wird Console Advisory Connect automatisch aktiviert. Weitere Informationen finden Sie unter Low-Touch-Onboarding von NetScaler-Instanzen mit NetScaler Console Service Connect.
- **Ausführungsbericht per E-Mail erhalten** – Sendet den Ausführungsbericht per E-Mail. Um eine E-Mail-Verteilerliste hinzuzufügen, siehe E-Mail-Verteilerliste erstellen.
- **Ausführungsbericht über Slack erhalten** – Sendet den Ausführungsbericht über Slack. Um ein Slack-Profil hinzuzufügen, siehe Slack-Profil erstellen.

10. Klicken Sie auf **Job erstellen**.

Upgrade von NetScaler SDX-Instanzen planen

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Upgrade Jobs**. Klicken Sie auf **Job erstellen**.
2. Wählen Sie **NetScaler SDX aktualisieren** und klicken Sie auf **Weiter**.
3. Auf der Seite **NetScaler SDX aktualisieren**, auf der Registerkarte **Instanzauswahl**:
   a. Fügen Sie einen **Aufgabennamen** hinzu.
   b. Wählen Sie aus der Liste **Software-Image** entweder **Lokal** (Ihr lokaler Computer) oder **Appliance** (die Build-Datei muss auf der virtuellen NetScaler Console Appliance vorhanden sein).

      Der Upload-Vorgang beginnt.
   c. Fügen Sie die NetScaler SDX-Instanzen hinzu, auf denen Sie den Upgrade-Vorgang ausführen möchten.
   d. Klicken Sie auf **Weiter**.
4. Auf der Registerkarte **Aufgabe planen** wählen Sie **Jetzt** aus der Liste **Ausführungsmodus**, um eine NetScaler SDX-Instanz jetzt zu aktualisieren, und klicken Sie auf **Fertig stellen**.
5. Um eine NetScaler SDX-Instanz später zu aktualisieren, wählen Sie **Später** aus der Liste **Ausführungsmodus**. Sie können dann das Ausführungsdatum und die Startzeit für die Aktualisierung der NetScaler-Instanz auswählen und auf **Fertig stellen** klicken.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Sie können auch E-Mail- und Slack-Benachrichtigungen aktivieren, um den Ausführungsbericht der aktualisierten NetScaler SDX-Instanz zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht per E-Mail erhalten** und das Kontrollkästchen **Ausführungsbericht über Slack erhalten**, um die Benachrichtigungen zu aktivieren.

   Weitere Informationen zum Konfigurieren der E-Mail-Verteilerliste und des Slack-Kanals finden Sie unter **Schritt 8** in Planen der Aktualisierung von NetScaler-Instanzen

Planen der Aktualisierung von NetScaler BLX-Instanzen

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Upgrade-Aufträge**. Klicken Sie auf **Auftrag erstellen**.
2. Wählen Sie unter **Wartungsaufträge erstellen** die Option **NetScaler BLX aktualisieren** und klicken Sie auf **Weiter**.
3. Geben Sie unter **Instanz auswählen** einen Namen Ihrer Wahl für **Auftragsname** ein.
4. Klicken Sie auf **Instanzen hinzufügen**, um die BLX-Instanzen hinzuzufügen, die Sie aktualisieren möchten.

   - Um ein HA-Paar zu aktualisieren, geben Sie die IP-Adresse eines primären oder sekundären Knotens an. Es wird jedoch empfohlen, die primäre Instanz für die Aktualisierung des HA-Paares zu verwenden.
   - Um einen Cluster zu aktualisieren, geben Sie die Cluster-IP-Adresse an.

5. Klicken Sie auf **Weiter**, um das Image auszuwählen. Wählen Sie eine der folgenden Optionen aus der Liste **Software-Image**:

   - **Lokal** – Wählen Sie die Instanz-Upgrade-Datei von Ihrem lokalen Computer aus.
   - **Appliance** – Wählen Sie die Instanz-Upgrade-Datei aus einem NetScaler Console-Dateibrowser aus. Die NetScaler Console-GUI zeigt die Instanzdateien an, die sich unter `/var/mps/mps_images` befinden.

     - **Image-Upload auf NetScaler überspringen, wenn das ausgewählte Image bereits verfügbar ist** – Wählen Sie diese Option, wenn das Image bereits in der NetScaler-Instanz vorhanden ist.
     - **Software-Image von NetScaler nach erfolgreichem Upgrade bereinigen** – Wählen Sie diese Option, um das hochgeladene Image in der NetScaler-Instanz nach dem Instanz-Upgrade zu löschen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Klicken Sie auf **Weiter**, um die Vor-Upgrade-Validierung für die ausgewählten Instanzen zu starten.

   Die Registerkarte **Vor-Upgrade-Validierung** zeigt die fehlgeschlagenen Instanzen an. Entfernen Sie die fehlgeschlagenen Instanzen und klicken Sie auf **Weiter**.

   WICHTIG

   Wenn Sie die Cluster-IP-Adresse angeben, führt die NetScaler Console die Vor-Upgrade-Validierung nur für die angegebene Instanz durch, nicht für die anderen Cluster-Knoten.

7. Optional: Geben Sie unter **Benutzerdefinierte Skripte** die Skripte an, die vor und nach einem Instanz-Upgrade ausgeführt werden sollen. Verwenden Sie eine der folgenden Methoden, um die Befehle auszuführen:

   - **Befehle aus Datei importieren** – Wählen Sie die Befehlseingabedatei von Ihrem lokalen Computer aus.
   - **Befehle eingeben** – Geben Sie Befehle direkt in die GUI ein.

   Sie können benutzerdefinierte Skripte verwenden, um die Änderungen vor und nach einem Instanz-Upgrade zu überprüfen. Zum Beispiel:

   - Die Instanzversion vor und nach dem Upgrade.
   - Der Status von Schnittstellen, Hochverfügbarkeitsknoten, virtuellen Servern und Diensten vor und nach dem Upgrade.
   - Die Statistiken von virtuellen Servern und Diensten.
   - Die dynamischen Routen.

8. Klicken Sie auf **Weiter**. Wählen Sie unter **Aufgabe planen** eine der folgenden Optionen aus:

   - **Jetzt aktualisieren** – Der Upgrade-Auftrag wird sofort ausgeführt.
   - **Später planen** – Wählen Sie diese Option, um diesen Upgrade-Auftrag später auszuführen. Geben Sie das **Ausführungsdatum** und die **Startzeit** an, zu der Sie die Instanzen aktualisieren möchten.

     Wenn Sie ein HA-Paar in zwei Phasen aktualisieren möchten, wählen Sie **Zweistufiges Upgrade für Knoten in HA durchführen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Geben Sie das **Ausführungsdatum** und die **Startzeit** an, zu der Sie eine weitere Instanz im HA-Paar aktualisieren möchten.

9. Klicken Sie auf **Weiter**. Geben Sie unter **Auftrag erstellen** die folgenden Details an:

   a. Geben Sie an, wann Sie das Image auf eine Instanz hochladen möchten:

      - **Jetzt hochladen** – Wählen Sie diese Option, um das Image sofort hochzuladen. Der Upgrade-Auftrag wird jedoch zur geplanten Zeit ausgeführt.
      - **Zum Zeitpunkt der Ausführung hochladen** – Wählen Sie diese Option, um das Image zum Zeitpunkt der Ausführung des Upgrade-Auftrags hochzuladen.
      - **NetScaler-Instanzen vor Beginn des Upgrades sichern** – Erstellt eine Sicherung der ausgewählten NetScaler-Instanzen.
      - **NetScaler-Konfiguration vor Beginn des Upgrades speichern** – Speichert die Konfigurationsaufträge, die vor dem Upgrade auf der Instanz konfiguriert wurden.
      - **ISSU aktivieren, um Netzwerkausfälle bei NetScaler HA-Paaren zu vermeiden** – Durch die Aktivierung von In-Service Software Upgrade (ISSU) können Sie ein NetScaler Hochverfügbarkeits- (HA-) Paar aktualisieren, ohne Netzwerkausfallzeiten zu verursachen. ISSU stellt sicher, dass die bestehenden Verbindungen während des Upgrades berücksichtigt werden, indem die aktiven Sitzungen nahtlos zwischen den Knoten migriert werden. Nach der Aktivierung von ISSU im Upgrade-Workflow kann das System auch den Abschluss der ISSU-Migration nach der vom Kunden definierten Verzögerungszeit auslösen. NetScaler Console, das einen vollständigen Abschluss der ISSU-Migration auslöst, stellt sicher, dass das Upgrade auch dann abgeschlossen wird, wenn Verbindungen bestehen bleiben. Geben Sie das ISSU-Migrations-Timeout in Minuten an, um die Wartezeit festzulegen, bevor NetScaler Console die Migration abschließt.

   - **Console Advisory Connect** – Wenn Sie auf Build **13.0-64 oder höher** und **12.1-58 oder höher** aktualisieren, wird Console Advisory Connect automatisch aktiviert. Weitere Informationen finden Sie unter Low-touch-Onboarding von NetScaler-Instanzen mit Console Advisory Connect.
   - **Ausführungsbericht per E-Mail erhalten** – Sendet den Ausführungsbericht per E-Mail. Informationen zum Hinzufügen einer E-Mail-Verteilerliste finden Sie unter Eine E-Mail-Verteilerliste erstellen.
   - **Ausführungsbericht über Slack erhalten** – Sendet den Ausführungsbericht über Slack. Informationen zum Hinzufügen eines Slack-Profils finden Sie unter Ein Slack-Profil erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. Klicken Sie auf **Auftrag erstellen**.

Upgrade der Autoscale™-Gruppe planen

Führen Sie die folgenden Schritte aus, um alle Instanzen in den Cloud-Diensten zu aktualisieren, die Teil der Autoscale-Gruppe sind:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Upgrade Jobs**. Klicken Sie auf **Create Job**.
2. Wählen Sie **Upgrade Autoscale Group** aus und klicken Sie auf **Proceed**.
3. Auf der Registerkarte **Upgrade Settings**:
   a. Wählen Sie die **Autoscale Group** aus, die Sie aktualisieren möchten.
   b. Wählen Sie unter **Image** die NetScaler-Version aus. Dieses Image ist die vorhandene Version der NetScaler-Instanzen in der Autoscale-Gruppe.
   c. Suchen Sie unter **NetScaler Image** die NetScaler-Versionsdatei, auf die Sie aktualisieren möchten.

      Wenn Sie **Graceful Upgrade** aktivieren, wartet die Upgrade-Aufgabe, bis die angegebene Drain-Verbindungsperiode abläuft.
   d. Klicken Sie auf **Next**.
4. Auf der Registerkarte **Schedule Task**:
   a. Wählen Sie eine der folgenden Optionen aus der Liste „Execution Mode“:
      - **Now:** Um das Upgrade der NetScaler-Instanzen sofort zu starten.
      - **Later:** Um das Upgrade der NetScaler-Instanzen zu einem späteren Zeitpunkt zu starten.
   b. Wenn Sie die Option **Later** auswählen, wählen Sie das Ausführungsdatum und die Startzeit aus, zu der Sie die Upgrade-Aufgabe starten möchten.

   Sie können auch E-Mail- und Slack-Benachrichtigungen aktivieren, um den Ausführungsbericht der aktualisierten Autoscale-Gruppe zu erhalten. Aktivieren Sie die Kontrollkästchen **Ausführungsbericht per E-Mail erhalten** und **Ausführungsbericht über Slack erhalten**, um die Benachrichtigungen zu aktivieren.
5. Klicken Sie auf **Fertig stellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfiguration eines HA-Paares von NetScaler-Instanzen planen

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Upgrade-Aufträge**. Klicken Sie auf **Auftrag erstellen**.
2. Wählen Sie **HA-Paar von NetScaler-Instanzen konfigurieren** und klicken Sie auf **Weiter**.
3. Auf der Seite **NetScaler HA-Paar**, im Tab **Instanzauswahl**:
    a. Fügen Sie einen **Aufgabennamen** hinzu.
    b. Geben Sie die primäre IP-Adresse ein.
    c. Geben Sie die sekundäre IP-Adresse ein.
    d. Klicken Sie auf **Weiter**.
    e. Klicken Sie, um den **INC-Modus (Independent Network Configuration) zu aktivieren**, wenn Sie die HA-Paar-Instanzen in zwei Subnetzen haben.
4. Wählen Sie auf der Registerkarte **Aufgabe planen** eine der folgenden Optionen aus:
    - **Jetzt aktualisieren**: Wählen Sie diese Option, um eine NetScaler-Instanz sofort zu aktualisieren. Klicken Sie auf **Fertig stellen**.
    - **Später planen**: Wählen Sie diese Option, um ein NetScaler HA-Paar später zu aktualisieren.
5. Wenn Sie die Option **Später planen** wählen, wählen Sie das **Ausführungsdatum** und die **Startzeit** für das Upgrade der NetScaler-Instanz.
    a. Wählen Sie **Führen Sie das Upgrade der NetScaler HA-Knoten in zwei Phasen durch**. Wenn Sie diese Option auswählen, sind HA-Synchronisierung und HA-Propagation deaktiviert, bis beide Knoten erfolgreich aktualisiert wurden.
    b. Wählen Sie eine der folgenden Optionen, um das Upgrade des sekundären Knotens zu planen. Mit dieser Option wird das Upgrade von Phase 2 erst nach dem erfolgreichen Abschluss von Phase 1 ausgeführt.
        - **Nach einer festgelegten Verzögerung**: Geben Sie eine Verzögerung (in Stunden) an, nachdem das Upgrade des ersten Knotens abgeschlossen ist, bevor das Upgrade des zweiten Knotens beginnt.
        - **Zu einem bestimmten Zeitpunkt**: Wählen Sie ein Datum und eine Uhrzeit für das Upgrade des sekundären Knotens.
6. Wählen Sie **Verzögern Sie das HA-Failover bis zum Beginn des Upgrades des sekundären Knotens**. Klicken Sie auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Sie können auch E-Mail- und Slack-Benachrichtigungen aktivieren, um den Ausführungsbericht der Erstellung des NetScaler HA-Paares zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht per E-Mail erhalten** und das Kontrollkästchen **Ausführungsbericht über Slack erhalten**, um die Benachrichtigungen zu aktivieren.

   Weitere Informationen zum Konfigurieren von E-Mail-Verteilerlisten und Slack-Kanälen finden Sie unter **Schritt 8** in Planen des Upgrades von NetScaler-Instanzen.

Planen der Konvertierung eines HA-Instanzpaares in einen Cluster

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Upgrade Jobs**. Klicken Sie auf **Job erstellen**.
2. Wählen Sie **HA-Instanzpaar in 2-Knoten-Cluster konvertieren** und klicken Sie auf **Weiter**.
3. Auf der Seite **NetScaler HA zu Cluster migrieren** fügen Sie auf der Registerkarte **Instanzauswahl** einen **Aufgabennamen** hinzu. Geben Sie die primäre IP-Adresse, die sekundäre IP-Adresse, die primäre Knoten-ID, die sekundäre Knoten-ID, die Cluster-IP-Adresse, die Cluster-ID und die Backplane an und klicken Sie dann auf **Weiter**.
4. Wählen Sie auf der Registerkarte **Aufgabe planen Jetzt** aus der Liste **Ausführungsmodus** aus, um eine NetScaler-Instanz sofort zu aktualisieren, und klicken Sie auf **Fertig stellen**.
5. Um später ein Upgrade durchzuführen, wählen Sie **Später** aus der Liste **Ausführungsmodus** aus. Sie können dann das **Ausführungsdatum** und die **Startzeit** für das Upgrade der NetScaler HA-Paar-Instanz auswählen und auf **Fertig stellen** klicken.
6. Sie können auch E-Mail- und Slack-Benachrichtigungen aktivieren, um den Ausführungsbericht des Upgrades einer NetScaler SDX-Instanz zu erhalten. Aktivieren Sie das Kontrollkästchen **Ausführungsbericht per E-Mail erhalten** und das Kontrollkästchen **Ausführungsbericht über Slack erhalten**, um die Benachrichtigungen zu aktivieren.

   Weitere Informationen zum Konfigurieren von E-Mail-Verteilerlisten und Slack-Kanälen finden Sie unter **Schritt 8** in Planen des Upgrades von NetScaler-Instanzen.

NetScaler-Instanzen mithilfe von Aufträgen aktualisieren

In NetScaler Console können Sie eine oder mehrere NetScaler-Instanzen aktualisieren. Sie müssen das Lizenzierungs-Framework und die Lizenztypen kennen, bevor Sie eine Instanz aktualisieren.

HINWEIS: Wenn Sie eine Instanz aktualisieren möchten, die klassische Richtlinien hat, empfehlen wir, die klassischen Richtlinien vor dem Upgrade der Instanz mithilfe des NSPEPI-Tools in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

erweiterte Richtlinien zu konvertieren. Dies gilt für die Funktionen, die vom NSPEPI-Tool unterstützt werden. Weitere Informationen finden Sie unter Upgrade-Überlegungen für Konfigurationen mit klassischen Richtlinien.

Voraussetzungen

NetScaler Console führt die folgenden Vorvalidierungsprüfungen für die Instanz durch, die Sie aktualisieren möchten:

1. **Überprüfung des Speicherplatzes** – Geben Sie Speicherplatz frei, um eine ausreichende Festplattenkapazität für ein Instanz-Upgrade zu gewährleisten. Beheben Sie gegebenenfalls Festplattenprobleme.
2. **Überprüfung auf Festplatten-Hardwareprobleme** – Beheben Sie gegebenenfalls Hardwareprobleme.
3. **Überprüfung auf Anpassungen** – Sichern Sie Ihre Anpassungen und löschen Sie diese von den Instanzen. Sie können die gesicherte Anpassung nach dem Instanz-Upgrade erneut anwenden.
4. **Richtlinienprobleme** – NetScaler unterstützt klassische Richtlinien ab Version `13.1` nicht. Bevor Sie eine Instanz auf diese Version aktualisieren, migrieren Sie klassische Richtlinien zu erweiterten Richtlinien.

   Weitere Informationen finden Sie unter Klassische und erweiterte Richtlinien.
5. **Überprüfung auf STAYPRIMARY- und STAYSECONDARY-Knoten** – Bei einer NetScaler HA ist das Upgrade für die Knoten in den Zuständen STAYPRIMARY und STAYSECONDARY blockiert. Diese Knoten werden bei der Vorvalidierungsprüfung identifiziert und unter **Instanzen, die vom Upgrade ausgeschlossen sind** aufgeführt.

Upgrade-Überlegungen für angepasste NetScaler-Konfigurationen

Es ist wichtig, dass sowohl die Upgrade-Änderungen als auch Ihre Anpassungen auf eine aktualisierte NetScaler-Appliance angewendet werden. Wenn Sie also angepasste Konfigurationsdateien im Verzeichnis /etc haben, lesen Sie Upgrade-Überlegungen für angepasste Konfigurationsdateien bevor Sie mit dem Upgrade der NetScaler-Appliance fortfahren. Im Folgenden sind die allgemeinen Schritte aufgeführt, die Sie ausführen müssen:

1. Schritte vor dem Upgrade in NetScaler
   - Angepasste Datei vor dem Upgrade sichern

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Den Symlink der angepassten Datei vor dem Upgrade löschen

2. Führen Sie ein Upgrade von NetScaler mit ADM durch. Befolgen Sie zum Upgrade die Anweisungen, die am Anfang der Seite verfügbar sind.
3. Schritte nach dem Upgrade in NetScaler

   - Anpassungen nach dem Upgrade wiederherstellen

Sowohl die Schritte vor dem Upgrade als auch nach dem Upgrade müssen auf jeder NetScaler-Instanz durchgeführt werden. In Schritt 2 können jedoch zum Upgrade von NetScaler mit ADM alle anfälligen NetScaler-Instanzen ausgewählt und zusammen aktualisiert werden.

NetScaler Hochverfügbarkeitspaar

Wenn Sie ein NetScaler Hochverfügbarkeitspaar aktualisieren, beachten Sie Folgendes:

- Der sekundäre Knoten wird zuerst aktualisiert.
- Synchronisierung und Weitergabe der Knoten sind deaktiviert, bis beide Knoten erfolgreich aktualisiert wurden.
- Nach dem erfolgreichen Upgrade des Hochverfügbarkeitspaares wird eine Fehlermeldung im Ausführungsverlauf angezeigt. Diese Meldung wird angezeigt, wenn Ihre Knoten im Hochverfügbarkeitspaar unterschiedliche Builds oder Versionen aufweisen. Sie weist darauf hin, dass die Synchronisierung zwischen primären und sekundären Knoten deaktiviert ist.

Sie können ein NetScaler Hochverfügbarkeitspaar in zwei Phasen aktualisieren:

1. Erstellen Sie einen Upgrade-Job und führen Sie ihn sofort auf einem der Knoten aus oder planen Sie ihn für später.
2. Planen Sie den Upgrade-Job so, dass er später auf dem verbleibenden Knoten ausgeführt wird. Stellen Sie sicher, dass dieser Job nach dem Upgrade des ursprünglichen Knotens geplant wird.

NetScaler Cluster

Wenn Sie einen NetScaler-Cluster aktualisieren, validiert die NetScaler Console in der Validierungsphase vor dem Upgrade nur die angegebene Instanz. Überprüfen und beheben Sie daher die folgenden Probleme auf den Clusterknoten:

- Anpassung
- Festplattennutzung
- Hardwareprobleme

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler-Upgrade-Job erstellen

Gehen Sie wie folgt vor, um einen NetScaler-Upgrade-Job zu erstellen:

1. Navigieren Sie zu **Infrastructure > Upgrade Jobs**.

2. Wählen Sie unter **Wartungsjobs erstellen** die Option **NetScaler aktualisieren (Standalone/ Hochverfügbarkeit/Cluster)** und klicken Sie auf **Weiter**.

   HINWEIS:

   Informationen zum Upgrade von Autoscale-Gruppen finden Sie unter Upgrade einer Autoscale-Gruppe.

3. Wählen Sie auf der Registerkarte **Instanzen auswählen,**

   a. Geben Sie einen Namen Ihrer Wahl für **Job Name** an.

   b. Klicken Sie auf **Instanzen hinzufügen**, um NetScaler-Instanzen hinzuzufügen, die Sie aktualisieren möchten.

      - Um ein NetScaler Hochverfügbarkeitspaar zu aktualisieren, wählen Sie die IP-Adressen des Hochverfügbarkeitspaares aus (gekennzeichnet durch den hochgestellten Buchstaben 'S' und 'P').
      - Um einen Cluster zu aktualisieren, wählen Sie die Cluster-IP-Adresse aus (gekennzeichnet durch den hochgestellten Buchstaben 'C').

      Instanzen zum Upgrade-Wartungsauftrag hinzufügen(/en-us/netscaler-console-service/media/upgrade-add-instances.png)

   c. Klicken Sie auf **OK**.

4. Wählen Sie auf der Registerkarte **Select Image** ein NetScaler-Image aus der Image-Bibliothek oder lokal oder von der Appliance aus.

   - **Aus Image-Bibliothek auswählen**: Wählen Sie ein NetScaler-Image aus der Liste aus. Diese Option listet alle NetScaler-Images auf, die auf der NetScaler-Download-Website verfügbar sind.

     NetScaler-Images(/en-us/netscaler-console-service/media/adc-images.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die NetScaler-Software-Images zeigen die bevorzugten Builds mit dem Sternsymbol an. Und die am häufigsten heruntergeladenen Builds mit dem Lesezeichensymbol.

- **Lokal oder von Appliance auswählen**: Sie können das Image von Ihrem lokalen Computer oder der NetScaler-Appliance hochladen. Wenn Sie NetScaler-Appliance auswählen, zeigt die NetScaler Console GUI die Instanzdateien an, die sich in `/var/mps/ns_images` befinden. Wählen Sie das Image aus der NetScaler Console GUI aus.
- **Image-Upload auf NetScaler überspringen, wenn das ausgewählte Image bereits verfügbar ist** – Diese Option prüft, ob das ausgewählte Image in NetScaler verfügbar ist. Der Upgrade-Job überspringt das Hochladen eines neuen Images und verwendet das in NetScaler verfügbare Image.
- **Software-Image nach erfolgreichem Upgrade von NetScaler bereinigen** – Diese Option löscht das hochgeladene Image in der NetScaler-Instanz nach dem Instanz-Upgrade.

Klicken Sie auf **Weiter**, um die Vor-Upgrade-Validierung für die ausgewählten Instanzen zu starten.

HINWEIS:

- Die heruntergeladenen NetScaler-Images werden im Agent gespeichert und befinden sich in `/var/mps/adcimages`. Diese zwischengespeicherten Images können für mehrere NetScaler-Upgrades verwendet werden, wodurch das Herunterladen eines Images für jedes Upgrade entfällt.
- NetScaler Console löscht die zwischengespeicherten NetScaler-Images alle drei Tage basierend auf dem Zeitpunkt der letzten Änderung der Images. Es werden jeweils nur die beiden neuesten Image-Dateien im Agent zwischengespeichert.

5. Die Registerkarte **Pre-upgrade validation** (Validierung vor dem Upgrade) zeigt die folgenden Abschnitte an:

   - **Instances ready for upgrade** (Instanzen bereit für das Upgrade). Sie können mit dem Upgrade dieser Instanzen fortfahren.
   - **Instances blocked from upgrade** (Instanzen, die vom Upgrade blockiert sind). Diese NetScaler-Instanzen sind aufgrund von Validierungsfehlern vor dem Upgrade vom Upgrade blockiert.

     Sie können die Fehler überprüfen, beheben und dann auf **Move to ready for upgrade** (Bereit für das Upgrade verschieben) klicken, um sie zu aktualisieren. Wenn Sie auf einer

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instanz nicht genügend Speicherplatz haben, können Sie den Speicherplatz überprüfen und bereinigen. Siehe NetScaler-Festplattenspeicher bereinigen.

- **Policy Check** (Richtlinienprüfung): Wenn NetScaler Console nicht unterstützte klassische Richtlinien findet, können Sie diese Richtlinien entfernen, um einen Upgrade-Job zu erstellen.

WICHTIG:

Wenn Sie eine Cluster-IP-Adresse angeben, führt NetScaler Console die Validierung vor dem Upgrade nur auf der angegebenen Instanz und nicht auf den anderen Clusterknoten durch.

Um Diskrepanzen zwischen primären und sekundären Knoten während eines Upgrades anzuzeigen, wählen Sie den Hochverfügbarkeitsknoten aus und klicken Sie auf **Details**.

- **Configuration discrepancies found in primary node of HA** (Konfigurationsdiskrepanzen im primären HA-Knoten gefunden) – Zeigt alle Konfigurationen an, die im sekundären Knoten des NetScaler®-Hochverfügbarkeitspaares gefunden wurden, aber im primären Knoten fehlen.
- **Configuration discrepancies found in secondary node of HA** (Konfigurationsdiskrepanzen im sekundären HA-Knoten gefunden) – Zeigt alle Konfigurationen an, die im primären Knoten des NetScaler-Hochverfügbarkeitspaares gefunden wurden, aber im sekundären Knoten fehlen.

HINWEIS:

Sie können die folgenden Diskrepanzen ignorieren, die in den Abschnitten zu Konfigurationsdiskrepanzen auftreten können:

- Gerätespezifische Konfigurationen wie IP-Adressen.
- Verschlüsselte Passwörter oder Zertifikate, die sich zwischen den Knoten unterscheiden können, selbst wenn das Passwort dasselbe ist.

Sie können die Abweichungen überprüfen und sie ignorieren, wenn sie nicht relevant sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Geben Sie unter **Validierungsskripte** die Skripte an, die vor und nach einem Instanz-Upgrade ausgeführt werden sollen. Sie können eine der folgenden Optionen wählen:

   - **Standard-Validierungsskripte** – Wählen Sie diese Option, um die vordefinierten Validierungsskripte auszuführen. Diese Skripte werden sowohl vor als auch nach dem Upgrade-Job ausgeführt und generieren einen Diff-Bericht für das Validierungsskript.

     HINWEIS:

     Sie können diese vordefinierten Befehlssätze nicht ändern oder bearbeiten.

   - **Benutzerdefinierte Validierungsskripte** – Wählen Sie diese Option, um Ihr eigenes Validierungsskript auszuführen. Sie können angeben, ob die Skripte vor oder nach dem Upgrade ausgeführt werden sollen. Ein Diff-Bericht wird nur generiert, wenn dieselben Skripte vor und nach dem Upgrade ausgewählt werden.

   Um den Befehlssatz in jeder Konfiguration zu erfahren, klicken Sie auf **Details anzeigen**. Weitere Informationen finden Sie unter Benutzerdefinierte Skripte verwenden.

7. Wählen Sie unter **Aufgabe planen** eine der folgenden Optionen aus:

   - **Jetzt aktualisieren**: Der Upgrade-Job wird sofort ausgeführt.
   - **Später planen**: Wählen Sie diese Option, um diesen Upgrade-Job später auszuführen. Geben Sie das **Ausführungsdatum** und die **Startzeit** an, wann Sie die Instanzen aktualisieren möchten.

   Wenn Sie ein NetScaler Hochverfügbarkeitspaar in zwei Phasen aktualisieren möchten, wählen Sie **Zweistufiges Upgrade für Knoten in Hochverfügbarkeit durchführen**.

   Geben Sie das **Ausführungsdatum** und die **Startzeit** an, wann Sie eine weitere Instanz im Hochverfügbarkeitspaar aktualisieren möchten.

   Weitere Informationen finden Sie unter NetScaler Hochverfügbarkeitspaar.

8. Geben Sie unter **Job erstellen** die folgenden Details an:

   Wenn Sie den Upgrade-Job planen, können Sie angeben, wann das Image auf eine Instanz hochgeladen werden soll:

   - **Jetzt hochladen**: Wählen Sie diese Option, um das Image sofort hochzuladen. Der Upgrade-Job wird jedoch zur geplanten Zeit ausgeführt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Zum Zeitpunkt der Ausführung hochladen**: Wählen Sie diese Option, um das Image zum Zeitpunkt der Ausführung des Upgrade-Jobs hochzuladen.

Für Hochverfügbarkeitspaare können Sie die Knoten angeben, auf die Sie das Image hochladen möchten:

- **Auf primäre und sekundäre Knoten hochladen**: Laden Sie die Build-Imagedatei auf primäre und sekundäre Knoten hoch.
- **Nur auf sekundären Knoten hochladen**: Laden Sie die Build-Imagedatei nur auf den sekundären Knoten hoch. Nachdem der sekundäre Knoten aktualisiert wurde, tritt ein Failover auf, und die Build-Imagedatei wird auf den neuen sekundären Knoten hochgeladen, der zuvor der primäre Knoten war.

Weitere Informationen zu den verfügbaren Planungsszenarien für Hochverfügbarkeitspaare finden Sie unter Planen von Upgrade-Jobs für NetScaler Hochverfügbarkeitspaare.

Weitere Informationen zu anderen Upgrade-Optionen finden Sie unter NetScaler Upgrade-Optionen.

9. Klicken Sie auf **Job erstellen**.

Der Upgrade-Job wird unter **Infrastruktur > Upgrade-Jobs** angezeigt. Wenn Sie einen vorhandenen Job bearbeiten, können Sie zu beliebigen Registerkarten wechseln, wenn die erforderlichen Felder bereits ausgefüllt sind. Wenn Sie sich beispielsweise auf der Registerkarte **Konfiguration auswählen** befinden, können Sie zur Registerkarte **Jobvorschau** wechseln.

Einen geplanten Upgrade-Job anhalten oder fortsetzen

Sie können Ihren geplanten Upgrade-Job auch anhalten.

Um diese Funktion zu nutzen, navigieren Sie zu **Infrastructure > Upgrade Jobs**, wählen Sie einen bestehenden geplanten Upgrade-Job aus und klicken Sie auf **Stop**, um den Job anzuhalten. Um den geplanten Upgrade-Job fortzusetzen, klicken Sie auf **Resume**.

HINWEIS:

Wenn die geplante Zeit für den Upgrade-Job nach Ihrer Entscheidung, ihn fortzusetzen, bereits verstrichen ist, müssen Sie den Upgrade-Job erneut erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fehlgeschlagene Upgrade-Jobs wiederholen

1. Wählen Sie unter **Infrastructure > Upgrade Jobs** den fehlgeschlagenen Upgrade-Job aus und klicken Sie auf **Retry**. Alternativ können Sie auch zu **Select Action > Retry Upgrade Job** gehen, um einen fehlgeschlagenen Job zu wiederholen.

2. Geben Sie unter **Select Instance** die folgenden Details an:

   - **Job Name** – Geben Sie einen Namen für das Upgrade ein.
   - Wählen Sie die NetScaler-Instanzen aus der Liste aus, die Sie aktualisieren möchten. Um Instanzen zu löschen, klicken Sie auf **Remove**.

   Klicken Sie auf **Next**, um den Validierungsprozess zu starten.

3. Die Registerkarte **Pre-upgrade validation** zeigt die folgenden Abschnitte an:

   - **Instances ready for upgrade**. Sie können mit dem Upgrade dieser Instanzen fortfahren.
   - **Instanzen, die vom Upgrade blockiert sind**. Diese NetScaler-Instanzen sind aufgrund von Validierungsfehlern vor dem Upgrade vom Upgrade blockiert.

     Sie können die Fehler überprüfen, beheben und dann auf **Bereit zum Upgrade verschieben** klicken, um sie zu aktualisieren. Wenn auf einer Instanz nicht genügend Speicherplatz vorhanden ist, können Sie den Speicherplatz überprüfen und bereinigen. Siehe, NetScaler-Speicherplatz bereinigen.
   - **Richtlinienprüfung**: Wenn NetScaler Console nicht unterstützte klassische Richtlinien findet, können Sie diese Richtlinien entfernen, um einen Upgrade-Job zu erstellen.

   Klicken Sie auf **Weiter**.

4. Wählen Sie unter **Aufgabe planen** eine der folgenden Optionen aus:

   - **Jetzt aktualisieren**: Der Upgrade-Job wird sofort ausgeführt.
   - **Später planen**: Wählen Sie diese Option, um diesen Upgrade-Job später auszuführen. Geben Sie das **Ausführungsdatum** und die **Startzeit** an, zu der Sie die Instanzen aktualisieren möchten.

   Klicken Sie auf **Wiederholen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bereinigen des NetScaler-Speicherplatzes

Wenn beim Upgrade einer NetScaler-Instanz das Problem mit unzureichendem Speicherplatz auftritt, bereinigen Sie den Speicherplatz direkt über die NetScaler Console GUI.

1. Auf der Registerkarte **Validierung vor dem Upgrade** zeigt der Abschnitt **Instanzen, die vom Upgrade blockiert sind** die Instanzen an, deren Upgrade aufgrund von unzureichendem Speicherplatz fehlgeschlagen ist. Wählen Sie die Instanz aus, die das Speicherplatzproblem aufweist.
2. Klicken Sie auf **Speicherplatz prüfen**.

   Ein Bereich **Details zum Speicherplatz** wird angezeigt. Dieser Bereich zeigt die Instanzen, den belegten Speicher und den verfügbaren Speicher an.

3. Wählen Sie im Bereich **Details zum Speicherplatz** die Instanz aus, die bereinigt werden muss, und führen Sie einen der folgenden Schritte aus:

   a. **Datenträgerbereinigung** – Navigieren Sie zu den erforderlichen Ordnern oder Verzeichnissen und löschen Sie diese, um Speicherplatz freizugeben.

   b. **Schnelle Bereinigung** – Geben Sie schnell Speicherplatz frei, indem Sie mehrere Ordner löschen. Wählen Sie im angezeigten Bereich **Bestätigen** die Ordner aus, die Sie löschen möchten, und klicken Sie auf **Ja**.

   c. Nachdem Sie den Speicherplatz freigegeben haben, können Sie überprüfen, ob nun ausreichend Speicherplatz für das Upgrade der Instanz verfügbar ist. Klicken Sie im Abschnitt **Instanzen, die vom Upgrade blockiert sind** auf **Neu validieren**.

   Im folgenden Beispiel ist Speicherplatz verfügbar. Sie können jetzt auf **Bereit für Upgrade verschieben** klicken, um die Instanz zu aktualisieren, oder auf **Weiter** klicken, um mit dem nächsten Schritt fortzufahren.

Benutzerdefinierte Skripte verwenden

Sie können benutzerdefinierte Skripte angeben, während Sie einen NetScaler-Upgrade-Job erstellen. Die benutzerdefinierten Skripte werden verwendet, um die Änderungen vor und nach einem NetScaler-Instanz-Upgrade zu überprüfen. Zum Beispiel:

- Die Instanzversion vor und nach dem Upgrade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Der Status von Schnittstellen, Hochverfügbarkeitsknoten, virtuellen Servern und Diensten vor und nach dem Upgrade.
- Die Statistiken von virtuellen Servern und Diensten.
- Die dynamischen Routen.

Geben Sie die benutzerdefinierten Skripte an, die in den folgenden Phasen ausgeführt werden sollen:

- **Vor dem Upgrade**: Das angegebene Skript wird vor dem Upgrade einer Instanz ausgeführt.
- **Nach dem Upgrade vor dem Failover (anwendbar für HA)**: Diese Phase gilt nur für die Hochverfügbarkeitsbereitstellung. Das angegebene Skript wird nach dem Upgrade der Knoten, aber vor deren Failover ausgeführt.
- **Nach dem Upgrade (anwendbar für Standalone) / Nach dem Upgrade nach dem Failover (anwendbar für HA)**: Das angegebene Skript wird nach dem Upgrade einer Instanz in der Standalone-Bereitstellung ausgeführt. In der Hochverfügbarkeitsbereitstellung wird das Skript nach dem Upgrade der Knoten und deren Failover ausgeführt.

HINWEIS:

- Stellen Sie sicher, dass die Skript- oder Befehlsausführung in den erforderlichen Phasen aktiviert ist. Andernfalls werden die angegebenen Skripte nicht ausgeführt.
- Der Diff-Bericht wird nur generiert, wenn Sie dasselbe Skript in den Pre-Upgrade- und Post-Upgrade-Phasen angeben. Stellen Sie daher sicher, dass Sie in den Post-Upgrade-Phasen **Dasselbe Skript wie Pre-Upgrade verwenden** auswählen. Siehe, Konsolidierten Diff-Bericht eines NetScaler-Upgrade-Jobs herunterladen.

Sie können eine Skriptdatei importieren oder Befehle direkt in die NetScaler Console-GUI eingeben.

- **Befehle aus Datei importieren**: Wählen Sie die Befehlseingabedatei von Ihrem lokalen Computer aus.
- **Befehle eingeben**: Geben Sie die Befehle direkt in die GUI ein.

In der Post-Upgrade-Phase können Sie dasselbe Skript verwenden, das in der Pre-Upgrade-Phase angegeben wurde.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler-Upgrade-Optionen

Wenn Sie einen NetScaler-Upgrade-Job erstellen, können Sie die folgenden Optionen auf der Registerkarte **Job erstellen** auswählen:

- **NetScaler-Instanzen vor Beginn des Upgrades sichern.**: Erstellt ein Backup der ausgewählten NetScaler-Instanzen.
- **Primären und sekundären Status von Hochverfügbarkeitsknoten nach dem Upgrade beibehalten**: Wählen Sie diese Option, wenn der Upgrade-Job nach dem Upgrade jedes Knotens ein Failover starten soll. Auf diese Weise behält der Upgrade-Job den primären und sekundären Status der Knoten bei.
- **NetScaler-Konfiguration vor Beginn des Upgrades speichern** – Speichert die laufende NetScaler-Konfiguration, bevor die NetScaler-Instanzen aktualisiert werden.
- **ISSU aktivieren, um Netzwerkausfälle bei NetScaler HA-Paaren zu vermeiden** – ISSU gewährleistet das Upgrade ohne Ausfallzeiten bei einem NetScaler-Hochverfügbarkeitspaar. Diese Option bietet eine Migrationsfunktion, die bestehende Verbindungen während des Upgrades berücksichtigt. So können Sie ein NetScaler-Hochverfügbarkeitspaar ohne Ausfallzeiten aktualisieren. Geben Sie das ISSU-Migrations-Timeout in Minuten an.
- **Ausführungsbericht per E-Mail erhalten** – Sendet den Ausführungsbericht per E-Mail. Um eine E-Mail-Verteilerliste hinzuzufügen, siehe E-Mail-Verteilerliste erstellen.
- **Ausführungsbericht über Slack erhalten** – Sendet den Ausführungsbericht über Slack. Um ein Slack-Profil hinzuzufügen, siehe Slack-Profil erstellen.

Upgrade-Jobs für ein NetScaler-Hochverfügbarkeitspaar planen

Die folgende Tabelle listet die verschiedenen Planungsszenarien auf der Seite **Aufgabe planen** und die entsprechenden Upgrade-Optionen auf der Seite **Job erstellen** auf:

WANN MÖCHTEN SIE DEN UPGRADE-JOB AUSFÜHREN?	WANN MÖCHTEN SIE DAS SOFTWARE-IMAGE AUF NETSCALER HOCHLADEN?	WIE MÖCHTEN SIE DAS BUILD-IMAGE AUF HA-KNOTEN HOCHLADEN?
Jetzt aktualisieren	Nicht zutreffend	**Auf primäre und sekundäre Knoten hochladen** (Standardoption)
	Nur auf sekundären Knoten hochladen	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WANN MÖCHTEN SIE DEN UPGRADE-JOB AUSFÜHREN?	WANN MÖCHTEN SIE DAS SOFTWARE-IMAGE AUF NETSCALER HOCHLADEN?	WIE MÖCHTEN SIE DAS BUILD-IMAGE AUF HA-KNOTEN HOCHLADEN?
Später planen	**Upload zum Zeitpunkt der Ausführung** (Standardoption)	**Upload auf primäre und sekundäre Knoten** (Standardoption)
	Upload nur auf sekundären Knoten	
	Jetzt hochladen	Nicht zutreffend
Später planen (wenn **Zweistufiges Upgrade für Knoten in HA durchführen** ausgewählt ist)	**Upload zum Zeitpunkt der Ausführung** (Standardoption)	**Upload nur auf sekundären Knoten** (Standard- und einzige Option)
	Jetzt hochladen	Nicht zutreffend

Konsolidierten Diff-Bericht eines NetScaler-Upgrade-Jobs herunterladen

In NetScaler Console können Sie einen Diff-Bericht eines NetScaler-Upgrade-Jobs herunterladen. Dazu muss der Upgrade-Job benutzerdefinierte Skripte enthalten. Ein Diff-Bericht enthält die Unterschiede zwischen den Ausgaben des Pre-Upgrade- und Post-Upgrade-Skripts. Mit diesem Bericht können Sie feststellen, welche Änderungen an der NetScaler-Instanz nach dem Upgrade vorgenommen wurden.

HINWEIS:

Der Diff-Bericht wird nur generiert, wenn Sie dasselbe Skript in den Pre-Upgrade- und Post-Upgrade-Phasen angeben.

Um einen Diff-Bericht eines Upgrade-Jobs herunterzuladen, gehen Sie wie folgt vor:

1. Navigieren Sie zu **Infrastruktur > Konfigurationsaufträge > Wartungsaufträge**.
2. Wählen Sie den Upgrade-Auftrag aus, für den Sie einen Diff-Bericht herunterladen möchten.
3. Klicken Sie auf **Diff-Berichte**.
4. Laden Sie unter **Diff-Berichte** einen konsolidierten Diff-Bericht des ausgewählten Upgrade-Auftrags herunter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Auf dieser Seite können Sie einen der folgenden Typen von Diff-Berichten herunterladen:

- **Vor vs. Nach Upgrade vor Failover Diff-Bericht**
- **Vor vs. Nach Upgrade Diff-Bericht**

Netzwerkfunktionen

Mit der Funktion „Netzwerkfunktionen“ können Sie den Status der auf Ihren verwalteten Citrix Application Delivery Controller (NetScaler)-Instanzen konfigurierten Entitäten überwachen. Sie können Statistiken wie Transaktionsdetails, Verbindungsdetails und den Durchsatz eines virtuellen Lastausgleichsservers anzeigen. Sie können die Entitäten auch aktivieren oder deaktivieren, wenn Sie eine Wartung planen.

Das Dashboard für Netzwerkfunktionen bietet Ihnen die folgenden Diagramme:

- Top 5 virtuelle Server mit den meisten Client-Verbindungen
- Top 5 virtuelle Server mit den meisten Server-Verbindungen
- Top 5 virtuelle Server mit dem höchsten Durchsatz (MB/Sek.)
- Die 5 virtuellen Server mit dem niedrigsten Durchsatz (MB/Sek.)
- Top 5 Instanzen mit den meisten virtuellen Servern
- Status der virtuellen Server
- Zustand der virtuellen Lastausgleichsserver
- Protokolle
- Lastausgleichsmethode
- Lastausgleichs-Persistenz

Berichte für Lastenausgleichsentitäten generieren

Mit NetScaler Console können Sie die Berichte von Citrix Application Delivery Controller (NetScaler)-Instanzentitäten auf allen Ebenen anzeigen. Es gibt zwei Arten von Berichten, die Sie in **NetScaler Console > Netzwerkfunktionen** herunterladen können – konsolidierte Berichte und individuelle Berichte.

Konsolidierte Berichte: Sie können einen konsolidierten oder zusammenfassenden Bericht für alle Entitäten herunterladen und anzeigen, die auf NetScaler-Instanzen verwaltet werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dieser Bericht ermöglicht Ihnen einen Überblick über die Zuordnung zwischen den NetScaler-Instanzen, Partitionen und den entsprechenden Lastenausgleichsentitäten (virtuelle Server, Dienstgruppen und Dienste), die im Netzwerk vorhanden sind.

Die folgende Abbildung zeigt ein Beispiel für einen zusammenfassenden Bericht.

Der konsolidierte Bericht liegt im CSV-Format vor. Die Einträge in jeder Spalte werden wie folgt beschrieben:

- **NetScaler IP-Adresse**: Die IP-Adresse der NetScaler-Instanz wird im Bericht angezeigt.
- **NetScaler Hostname**: Der Hostname wird im Bericht angezeigt.
- **Partition**: Die IP-Adresse der administrativen Partition wird angezeigt.
- **Virtueller Server**: \<name_of_the_virtual_server\>#virtual_IP_address:port_number
- **Dienste**: \<name_of_the_service\>#service-IP_address:port_number
- **Dienstgruppen**: \<name_of_service_group\>#server_member1_IP_address:port,server_member2_IP_address:port,

HINWEIS

- Wenn kein Hostname verfügbar ist, wird die entsprechende IP-Adresse angezeigt.
- Leere Spalten zeigen an, dass die jeweiligen Entitäten für diese NetScaler-Instanz nicht konfiguriert sind.

Einzelne Berichte: Sie können auch unabhängige Berichte aller Instanzen und Entitäten herunterladen und anzeigen. Sie können beispielsweise einen Bericht nur für Lastausgleichs-Virtual-Server oder Lastausgleichsdienste oder Lastausgleichsdienstgruppen herunterladen.

Mit NetScaler Console können Sie den Bericht sofort herunterladen. Sie können den Bericht auch so planen, dass er einmal täglich, einmal wöchentlich oder einmal monatlich zu einem festen Zeitpunkt generiert wird.

Kombinierten Lastausgleichsbericht generieren

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Netzwerkfunktionen**.
2. Klicken Sie auf **Bericht generieren**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Auf der sich öffnenden Seite **Bericht generieren** haben Sie zwei Optionen, um den Bericht anzuzeigen:

   a. Wählen Sie auf der Registerkarte **Jetzt exportieren** die Option **Lastausgleich** aus und klicken Sie auf **OK**.

      Der konsolidierte Bericht wird auf Ihr System heruntergeladen.

   b. Wählen Sie **Bericht planen**, um einen Zeitplan für die Generierung und den Export von Berichten in regelmäßigen Abständen zu erstellen. Geben Sie die Einstellungen für die Wiederholung der Berichtsgenerierung an und erstellen Sie ein E-Mail-Profil, an das der Bericht exportiert werden soll.

      i. Wählen Sie **Zeitplan aktivieren**.

      ii. **Wiederholung** – wählen Sie **Täglich**, **Wöchentlich** oder **Monatlich** aus der Liste aus.

      HINWEIS

      Wenn Sie die Wiederholung **Wöchentlich** auswählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.

      HINWEIS

      Wenn Sie die **monatliche** Wiederholung auswählen, stellen Sie sicher, dass Sie die Tage des Monats mit Werten zwischen 1 und 31 eingeben.

      iii. **Exportzeit** – Geben Sie die Uhrzeit im Format Stunde:Minute im 24-Stunden-Format ein.

      iv. **E-Mail** – Aktivieren Sie das Kontrollkästchen und wählen Sie dann ein Profil aus der Liste aus, oder klicken Sie auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

      v. **Slack** – Aktivieren Sie das Slack-Kontrollkästchen und wählen Sie dann ein Profil aus der Listenfeld aus, oder klicken Sie auf **Hinzufügen**, um ein Slack-Profil zu erstellen.

      vi. Klicken Sie auf **Planen**, um den Vorgang abzuschließen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Einen individuellen Bericht für Lastausgleichsentitäten generieren

Sie können einen individuellen Bericht für einen bestimmten Entitätstyp, der den Instanzen zugeordnet ist, generieren und exportieren. Betrachten Sie beispielsweise ein Szenario, in dem Sie eine Liste aller Lastausgleichsdienste im Netzwerk sehen möchten.

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Network Functions > Load Balancing > Services**.
2. Klicken Sie auf der Seite **Services** oben rechts auf die Schaltfläche **Exportieren**.

   Wählen Sie die Registerkarte **Jetzt exportieren**, wenn Sie den Bericht sofort generieren und anzeigen möchten.

   HINWEIS

   Sie können die Berichte nur herunterladen oder als E-Mail-Anhänge exportieren. Sie können die Berichte nicht in der NetScaler Console GUI anzeigen.

Berichte zu Netzwerkfunktionen exportieren oder den Export planen

Sie können in NetScaler Console einen umfassenden Bericht für ausgewählte Netzwerkfunktionen wie Lastausgleich (Load Balancing), Inhaltswechsel (Content Switching), Cache-Umleitung (Cache Redirection), Global Server Load Balancing (GSLB), Authentifizierung und NetScaler Gateway erstellen. Dieser Bericht bietet Ihnen einen Überblick über die Zuordnung zwischen den Instanzen, Partitionen und den entsprechenden gebundenen Entitäten (virtuelle Server, Dienstgruppen und Dienste), die im Netzwerk vorhanden sind. Sie können diese Berichte im .csv-Dateiformat exportieren.

Der Bericht zeigt die folgenden Daten des virtuellen Servers an:

- NetScaler IP-Adresse
- Hostname
- Partitionsdaten
- Name des virtuellen Servers
- Typ des virtuellen Servers
- Virtueller Server
- Ziel-LB-Virtual-Server

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Für virtuelle Content Switching- und Cache Redirection-Server listet die Spalte „Ziel-LB-Virtual-Server“ alle LB-Server auf, d. h. sowohl Standardserver als auch richtlinienbasierte Server.

- Dienstname
- Dienstgruppenname

Sie können den Export dieser Berichte in bestimmten Intervallen an angegebene E-Mail-Adressen planen. Informationen zum Einrichten von E-Mail-Benachrichtigungen finden Sie unter Ereignisregeln erstellen.

HINWEIS

- Für GSLB-virtuelle Server zeigt der Netzwerkfunktionsbericht nur GSLB-virtuelle Server und zugehörige Dienste an.
- Für Content Switching- und Cache Redirection-virtuelle Server zeigt der Bericht nur die Bindungen zu den zugehörigen LB-Servern an.
- SSL-virtuelle Server werden in diesem Bericht nicht aufgeführt, da auf NetScaler Console keine separate Liste von SSL-virtuellen Servern geführt wird.
- Wenn ein neuer Bericht generiert wird, werden die älteren Berichte automatisch aus Ihrem Konto gelöscht.

So exportieren und planen Sie Netzwerkfunktionsberichte:

1. Navigieren Sie zu **Infrastructure > Network Functions**.
2. Klicken Sie auf der Seite **Network Functions** im rechten Bereich oben rechts auf der Seite auf **Generate Report**.
3. Auf der Seite **Generate Report** haben Sie die folgenden 2 Optionen:

   a. Wählen Sie die Registerkarte **Export Now** und klicken Sie auf **OK**.

      Der Bericht wird auf Ihr System heruntergeladen.

      Die folgende Abbildung zeigt ein Beispiel für einen Netzwerkfunktionsbericht.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Wählen Sie **Schedule Report**, um einen Zeitplan zum Generieren und Exportieren von Berichten in regelmäßigen Abständen zu erstellen. Geben Sie die Einstellungen für die Wiederholung der Berichtsgenerierung an und erstellen Sie ein E-Mail-Profil, an das der Bericht exportiert werden soll.

   i. **Recurrence** – Wählen Sie **Daily**, **Weekly** oder **Monthly** aus der Dropdown-Liste.

   ii. **Wiederholungszeit** – Geben Sie die Uhrzeit im Format Stunde:Minute im 24-Stunden-Format ein.

   iii. **E-Mail** – Aktivieren Sie das Kontrollkästchen und wählen Sie dann das Profil aus der Dropdown-Liste aus, oder klicken Sie auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

   iv. **Slack** – Aktivieren Sie das Kontrollkästchen und wählen Sie dann das Profil aus der Dropdown-Liste aus, oder klicken Sie auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

   Klicken Sie auf **Zeitplan aktivieren**, um Ihren Bericht zu planen, und klicken Sie dann auf **OK**. Indem Sie das Kontrollkästchen **Zeitplan aktivieren** aktivieren, können Sie die ausgewählten Berichte generieren.

Netzwerkberichterstattung

Sie können die Ressourcennutzung optimieren, indem Sie Ihr Netzwerk-Reporting in NetScaler Console überwachen. Möglicherweise verfügen Sie über eine verteilte Bereitstellung mit vielen Anwendungen, die an mehreren Standorten bereitgestellt werden. Um die optimale Leistung Ihrer Anwendungen zu gewährleisten, haben Sie auch mehrere Citrix Application Delivery Controller (NetScaler)-Instanzen bereitgestellt, um den Datenverkehr auszugleichen (Load Balancing), Inhalte zu wechseln (Content Switching) oder zu komprimieren. Die Netzwerkleistung kann die Anwendungsleistung beeinträchtigen. Um die Leistung Ihrer Anwendungen weiterhin aufrechtzuerhalten, müssen Sie Ihre Netzwerkleistung regelmäßig überwachen und sicherstellen, dass alle Ressourcen optimal genutzt werden.

NetScaler Console ermöglicht es Ihnen, Berichte für Instanzen auf globaler Ebene und für Entitäten wie virtuelle Server und Netzwerkschnittstellen zu generieren. Die virtuellen Server, für die Sie Berichte generieren können, sind die folgenden:

- Lastausgleichsserver, -dienste und -dienstgruppen
- Content-Switching-Server
- Cache-Umleitungsserver
- Globaler Dienstlastenausgleich (GSLB)
- Authentifizierung

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Gateway

Sie können in NetScaler Console mehrere Dashboards für verschiedene Instanzen, virtuelle Server und andere Entitäten erstellen.

Dashboard für Netzwerkberichterstattung

Die folgende Abbildung zeigt die verschiedenen Funktionen im Dashboard:

- Das linke Seitenpanel listet alle benutzerdefinierten Dashboards auf, die in NetScaler Console erstellt wurden. Sie können auf eines davon klicken, um die verschiedenen Berichte anzuzeigen, aus denen das Dashboard besteht. Zum Beispiel enthält ein TCP- und SSL-Dashboard verschiedene Berichte zu TCP- und SSL-Protokollen.
- Sie können jedes Dashboard mit mehreren Widgets anpassen, um verschiedene Berichte anzuzeigen. Ein Widget stellt einen Bericht auf dem Dashboard dar, der eine Sammlung weiterer verwandter Berichte ist. Zum Beispiel enthält ein Bericht zur TCP-Byte-Nutzung (Komprimierung) Berichte über komprimierte TCP-Bytes, die pro Sekunde übertragen und empfangen werden.
- Sie können Berichte für eine Stunde, einen Tag, eine Woche oder einen Monat anzeigen. Sie können die Zeitleisten-Schieberegleroption verwenden, um die Dauer der auf der NetScaler Console generierten Berichte anzupassen.
- Sie können einen Bericht entfernen, indem Sie auf „X“ klicken. Sie können den Bericht auch als .pdf-, .jpeg-, .png- oder .csv-Format auf Ihr System exportieren. Sie können auch einen Zeitpunkt und die Wiederholung für die Generierung des Berichts planen. Sie können auch eine E-Mail-Verteilerliste konfigurieren, an die Sie die Berichte senden möchten.
- Der Abschnitt „Instanzen“ oben im Dashboard listet die IP-Adressen aller Instanzen auf, für die der Bericht generiert wird.
- Sie können Instanzen entweder durch Klicken auf „X“ entfernen oder weitere Instanzen zu den Berichten hinzufügen. Derzeit können Sie mit NetScaler Console jedoch Berichte für 10 Instanzen anzeigen.
- Sie können das gesamte Dashboard auch als .pdf-, .jpeg-, .png- oder .csv-Format auf Ihr System exportieren. Alle am Dashboard vorgenommenen Änderungen müssen gespeichert werden. Klicken Sie auf „Speichern“, um die Änderungen zu speichern.

Der folgende Abschnitt erläutert detailliert die Aufgaben zum Erstellen eines Dashboards, zum Generieren von Berichten und zum Exportieren von Berichten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So zeigen Sie ein Dashboard an oder erstellen es:

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Netzwerkberichterstellung**.

2. Um die vorhandenen Dashboards anzuzeigen, klicken Sie auf **Dashboard anzeigen**. Die Seite „Netzwerkberichterstellung **Dashboard**“ wird geöffnet, auf der Sie alle Ihre Dashboards und Berichtswidgets anzeigen können.
3. Um ein Dashboard zu erstellen, klicken Sie auf **Dashboard erstellen**.

   Die Seite **Dashboard erstellen** wird geöffnet.

4. Geben Sie auf der Registerkarte **Grundeinstellungen** die folgenden Details ein:

   a. **Name**. Geben Sie den Namen des Dashboards ein.

   b. **Instanzfamilie**. Wählen Sie den Instanztyp aus – NetScaler oder NetScaler SDX.

   a. **Typ**. Wählen Sie den Entitätstyp aus, für den Sie Berichte generieren möchten. Wählen Sie in diesem Beispiel virtuelle Lastausgleichsserver aus.

   b. **Beschreibung**. Geben Sie eine aussagekräftige Beschreibung für das Dashboard ein.

5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Registerkarte **Berichte auswählen** die erforderlichen Berichte aus. In diesem Beispiel können Sie Transaktionen, Verbindungen und Durchsatz auswählen. Klicken Sie auf **Weiter**.

7. Klicken Sie auf der Registerkarte **Entitäten auswählen** auf **Hinzufügen**.

   Ein Fenster mit der Entitätenliste wird angezeigt, abhängig vom ausgewählten Entitätstyp auf der Registerkarte **Grundeinstellungen**. In diesem Beispiel wird das Fenster **Virtuelle LB-Server auswählen** angezeigt.
8. Wählen Sie die Entitäten aus, die Sie überwachen möchten.

9. Klicken Sie auf **Erstellen**.

Das Dashboard wird erstellt und zeigt alle von Ihnen ausgewählten Berichte an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Derzeit können Änderungen, die Sie an Legenden oder Filtern vornehmen, nicht gespeichert werden.

Netzwerkberichtsdaten durch Anwenden von Aggregationen anzeigen

Sie können Aggregationen auf die Netzwerk-Leistungsdaten anwenden und die Anwendungsleistung auf dem Dashboard anzeigen. Sie können die Ergebnisse auch nach Ihren Anforderungen exportieren. Mithilfe dieser auf die Daten angewendeten Aggregationen können Sie analysieren und überprüfen, ob alle Ressourcen optimal genutzt werden. Navigieren Sie zu **Netzwerk > Netzwerkberichterstellung** und wählen Sie die Zeitdauer „1 Tag oder später“ aus, um die Option **Anzeigen nach** zu erhalten.

In den vorhandenen Durchschnittsdaten können Sie Aggregationen anwenden, indem Sie die Option aus der Liste **Anzeigen nach** auswählen. Wenn Sie eine Aggregation anwenden, werden die Daten für jede Metrik im Dashboard aktualisiert. Klicken Sie auf **Einstellungen** und wählen Sie **Aggregationsfilter** aus.

Die folgenden Aggregationen können Sie hinzufügen:

- Anzahl
- Maximum
- Minimum
- Summe
- Standardabweichung
- Varianz
- Modus
- Median
- Fünfundzwanzigstes Perzentil
- Fünfundsiebzigstes Perzentil
- Fünfundneunzigstes Perzentil
- Das 99. Perzentil
- Erste

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Letzte

Sie können dem Dashboard bis zu 4 Aggregationsoptionen hinzufügen. Nachdem Sie die Aggregationsoptionen hinzugefügt haben, benötigt NetScaler Console etwa 1 Stunde, um Berichte für die ausgewählten Aggregationsoptionen zu generieren.

Netzwerkberichte exportieren

Während Sie Widget-Berichte in den Formaten .pdf, .png, .jpeg oder .csv exportieren können, können Sie die gesamten Dashboards nur in den Formaten .pdf, .jpeg oder .png exportieren.

HINWEIS

Sie können in NetScaler Console keine Berichte exportieren, wenn Sie nur Leseberechtigungen haben. Sie benötigen eine Bearbeitungsberechtigung, um eine Datei in NetScaler Console zu erstellen und zu exportieren.

So exportieren Sie Dashboard-Berichte:

1. Navigieren Sie zu **Infrastruktur > Netzwerkberichterstellung**
2. Klicken Sie auf **Dashboards anzeigen**, um alle von Ihnen erstellten Dashboards anzuzeigen.
3. Klicken Sie im linken Bereich auf ein Dashboard. Klicken Sie in diesem Beispiel auf **Dashboard 1**.
4. Klicken Sie auf die Export-Schaltfläche oben rechts auf der Seite.
5. Wählen Sie unter der Registerkarte **Jetzt exportieren** das gewünschte Format aus, und klicken Sie dann auf **Exportieren**.

   Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

6. Wählen Sie die Registerkarte **Jetzt exportieren**. Um den Bericht im PDF-, JPEG-, PNG- oder CSV-Format anzuzeigen und zu speichern.
7. Wählen Sie die Registerkarte **Export planen**. Um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu versenden.

   Sie können einen Export der Seite **Netzwerkberichts-Dashboard** regelmäßig planen. Sie können beispielsweise eine Option festlegen, um jede Woche zu einer bestimmten Zeit einen Dashboard-Bericht für die vorherige Stunde zu erstellen. Der Bericht wird dann jede Woche generiert und zeigt den Status des Dashboards an. Der Bericht überschreibt den Zeit- und Datumsstempel, falls vom Benutzer festgelegt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

- Wenn Sie die wöchentliche Wiederholung auswählen, wählen Sie die Wochentage aus, an denen der Bericht geplant werden soll.
- Wenn Sie die monatliche Wiederholung auswählen, geben Sie alle Tage durch Kommas getrennt ein, an denen der Bericht geplant werden soll.

Beim Planen von Netzwerkberichten können Sie die Überschrift des Berichts anpassen, indem Sie eine Textzeichenfolge in das Feld **Betreff** eingeben. Der zum geplanten Zeitpunkt erstellte Bericht trägt diese Zeichenfolge als Namen.

Beispielsweise können Sie für Netzwerkberichte, die von einem bestimmten virtuellen Server stammen, den Betreff als „authentication-reports-10.106.118.120“ eingeben, wobei 10.106.118.120 die IP-Adresse des überwachten virtuellen Servers ist.

HINWEIS

Derzeit ist diese Option nur verfügbar, wenn Sie den Export von Berichten planen. Sie können dem Bericht keine Überschrift hinzufügen, wenn Sie ihn sofort exportieren.

So exportieren Sie Widget-Berichte:

1. Navigieren Sie zu **Infrastruktur > Netzwerkberichterstellung**.
2. Klicken Sie auf **Dashboards anzeigen**, um alle von Ihnen erstellten Dashboards anzuzeigen.
3. Klicken Sie im linken Bereich auf ein Dashboard. Klicken Sie in diesem Beispiel auch auf **Skype for Business**.
4. Wählen Sie ein Widget aus. Wählen Sie beispielsweise **Load Balancing Virtual Server Transactions** aus.
5. Klicken Sie auf die Schaltfläche „Exportieren“ oben rechts auf der Seite.
6. Wählen Sie auf der Registerkarte **Jetzt exportieren** das gewünschte Format aus und klicken Sie dann auf **Exportieren**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schwellenwerte für Netzwerkberichte in NetScaler Console verwalten

Um den Status einer NetScaler-Instanz zu überwachen, können Sie Schwellenwerte für Zähler festlegen und Benachrichtigungen erhalten, wenn ein Schwellenwert überschritten wird. In NetScaler Console können Sie Schwellenwerte konfigurieren, anzeigen, bearbeiten und löschen.

Sie können beispielsweise eine E-Mail-Benachrichtigung erhalten, wenn der Verbindungszähler für einen Content-Switching-virtuellen Server einen bestimmten Wert erreicht. Sie können einen Schwellenwert für einen bestimmten Instanztyp definieren. Sie können auch die Berichte auswählen, die Sie für bestimmte Zählermetriken Ihrer gewählten Instanz generieren möchten.

Wenn der Wert eines Zählers den Schwellenwert überschreitet oder unterschreitet (wie durch die Regel festgelegt), wird ein Ereignis der angegebenen Schwere generiert, um ein leistungsbezogenes Problem anzuzeigen. Wenn der Zählerwert auf einen Wert zurückkehrt, den Sie als normal betrachten, wird das Ereignis gelöscht. Diese Ereignisse können angezeigt werden, indem Sie zu **Infrastruktur > Ereignisse > Berichte** navigieren. Auf der Seite **Berichte** können Sie auf den Donut **Ereignisse nach Schweregrad** klicken, um Ereignisse nach ihrem Schweregrad anzuzeigen.

Sie können einem Schwellenwert auch eine Aktion zuordnen, z. B. das Senden einer E-Mail oder SMS-Nachricht, wenn der Schwellenwert überschritten wird.

So erstellen Sie einen Schwellenwert:

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Netzwerkberichte > Schwellenwerte**. Klicken Sie unter **Schwellenwerte** auf **Hinzufügen**.
2. Geben Sie auf der Seite **Schwellenwert erstellen** die folgenden Details an:
    - **Name**. Name des Schwellenwerts.
    - **Instanztyp**. Eine NetScaler-Instanz.
    - **Berichtsname**. Name des Leistungsberichts, der Informationen zu diesem Schwellenwert bereitstellt.
3. Sie können auch Regeln festlegen, um anzugeben, wann ein Ereignis generiert oder gelöscht werden soll. Sie können die folgenden Details im Abschnitt **Regel konfigurieren** angeben:
    - **Metrik**. Wählen Sie die Metrik aus, für die Sie einen Schwellenwert festlegen möchten.
    - **Vergleichsoperator**. Wählen Sie einen Vergleichsoperator aus, um zu prüfen, ob der überwachte Wert größer oder gleich oder kleiner oder gleich dem Schwellenwert ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Schwellenwert**. Geben Sie den Wert ein, für den der Schweregrad des Ereignisses berechnet wird. Sie möchten beispielsweise ein Ereignis mit kritischem Schweregrad generieren, wenn der überwachte Wert für aktuelle Clientverbindungen 80 Prozent erreicht. Geben Sie in diesem Fall 80 als Schwellenwert ein. Sie können Ereignisse mit „kritischem Schweregrad“ anzeigen, indem Sie zu **Infrastruktur > Ereignisse** > **Berichte** navigieren. Auf der Seite **Berichte** können Sie auf den Donut **Ereignisse nach Schweregrad** klicken, um Ereignisse nach ihrem Schweregrad anzuzeigen.
- **Wert löschen**. Geben Sie den Wert ein, der angibt, wann der Wert gelöscht werden soll. Sie möchten beispielsweise den Schwellenwert für aktuelle Clientverbindungen löschen, wenn der überwachte Wert 50 Prozent erreicht. Geben Sie in diesem Fall 50 als Löschwert ein.
- **Ereignisschweregrad**. Wählen Sie die Sicherheitsstufe aus, die Sie für den Schwellenwert festlegen möchten.

4. Sie können Instanzen und Entitäten auswählen, für die der Schwellenwert festgelegt werden soll. Wählen Sie im Abschnitt **Instanzen** eine der folgenden Optionen aus:

   - **Alle Instanzen**. Der Schwellenwert wird für alle Instanzen festgelegt.
   - **Spezifische Instanzen**. Der Schwellenwert wird für bestimmte Instanzen festgelegt. Verwenden Sie den Rechtspfeil, um Instanzen aus der Liste **Verfügbar** in die Liste **Konfiguriert** zu verschieben. Der Schwellenwert wird für die Instanzen in der Liste **Konfiguriert** festgelegt.
   - **Spezifische Entitäten**. Der Schwellenwert wird für bestimmte Entitäten festgelegt.

     Klicken Sie auf **Hinzufügen**, um die Entitäten auszuwählen.

     Ein Fenster mit der Entitätenliste wird angezeigt, abhängig vom ausgewählten Berichtstyp im Feld **Berichtsname**. In diesem Beispiel wird das Fenster **LB Virtual Servers auswählen** angezeigt.

     Wählen Sie die Entitäten aus, für die Sie einen Schwellenwert festlegen möchten. Klicken Sie auf **Auswählen**. Die ausgewählten Entitäten werden im Abschnitt **Instanzen** angezeigt.

5. Sie können festlegen, dass eine Meldung angezeigt wird, wenn der Schwellenwert erreicht ist. Geben Sie im Abschnitt **Ereignismeldung** die Meldung in das Nachrichtenfeld ein. NetScaler Console hängt den überwachten Wert und den Schwellenwert an diese Meldung an.
6. Wählen Sie im Abschnitt **Benachrichtigungseinstellungen** die Option **Schwellenwert aktivieren**, um den Schwellenwert zum Generieren von Alarmen zu aktivieren. Optional

© 1997–2026 Citrix Systems, Inc. All rights reserved.

können Sie **Per E-Mail benachrichtigen** auswählen, um Benachrichtigungen über verschiedene Kanäle wie E-Mail, Slack, ServiceNow oder PagerDuty zu erhalten, wenn der Schwellenwert erreicht ist.

7. Klicken Sie auf **Erstellen**.

Leistungsabfrageintervall für Netzwerkberichte festlegen

Standardmäßig erfassen NITRO-Aufrufe alle 5 Minuten Leistungsdaten für die Netzwerkberichterstattung. Die NetScaler Console ruft Instanzstatistiken wie Zählerinformationen ab und aggregiert diese pro Minute, pro Stunde, pro Tag oder pro Woche. Sie können diese aggregierten Daten in vordefinierten Berichten anzeigen.

Um das Leistungsabfrageintervall festzulegen, navigieren Sie zu **Infrastructure > Network Reporting** und klicken Sie auf **Configure Polling Interval**. Ihr Abfrageintervall darf nicht weniger als 5 Minuten oder mehr als 60 Minuten betragen.

Konfigurieren der Bereinigungseinstellungen für die Netzwerkberichterstattung

Sie können das Bereinigungsintervall für Netzwerkberichtsdaten in der NetScaler Console konfigurieren. Dieses Intervall begrenzt die Menge der Netzwerkberichtsdaten, die in der Datenbank des NetScaler Console-Servers gespeichert werden. Standardmäßig erfolgt die Bereinigung der historischen Netzwerkberichtsdaten alle 24 Stunden (um 01:00 Uhr).

HINWEIS

Der von Ihnen angegebene Wert darf 90 Tage nicht überschreiten und nicht weniger als 1 Tag betragen.

Bereitstellung

Dieser Abschnitt behandelt die folgenden Themen:

- App-basierte Bereitstellung in AWS
- App-basierte Bereitstellung in Azure
- Bereitstellung von NetScaler VPX-Instanzen
    - AWS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Microsoft Azure
    - Google Cloud
    - VMware vCenter

- NetScaler Global Load Balancing für öffentliche Clouds

App-basiertes Provisioning in AWS

Der NetScaler Console-Dienst führt das „App-basierte“ Provisioning ein, das darauf ausgelegt ist, NetScaler-Bereitstellungen in Cloud-Rechenzentren zu optimieren und zu vereinfachen und Anwendungen von dort bereitzustellen.

Der NetScaler Console-Dienst akzeptiert die Cloud-Anmeldeinformationen des Kunden und richtet die für die Anwendungsbereitstellung erforderliche Infrastruktur ein, indem er den Start von NetScaler, Agenten und den notwendigen Cloud-Entitäten in AWS orchestriert. NetScaler-Administratoren können sowohl Flexed- als auch Cloud-Marketplace-Lizenzen für ihre NetScaler nutzen, was Flexibilität bei den Lizenzierungsoptionen gewährleistet.

Administratoren können dann Anwendungen in ihrer Cloud bereitstellen, indem sie die Bereitstellungseinstellungen auf einfache, anwendungszentrierte Weise über den NetScaler Console-Dienst definieren. Dieser kümmert sich dann um die Konfiguration sowohl der ADCs als auch der AWS-Infrastruktur, um ihre Anwendungen bereitzustellen. Sobald die Anwendungen bereitgestellt sind, erhalten NetScaler-Administratoren Zugriff auf die umfangreichen Analyse- und Überwachungsfunktionen des NetScaler Console-Dienstes, um ihre Anwendungen effektiv zu verwalten und zu überwachen.

Voraussetzungen

Abonnieren Sie die folgenden Produkte im AWS Marketplace.

- NetScaler VPX — Abonnieren Sie eine der folgenden Varianten:
    - NetScaler VPX BYOL — Abonnieren Sie, wenn Sie Flexed-Lizenzen erworben haben und diese im NetScaler Console-Dienst für die Lizenzierung von NetScaler-Instanzen verfügbar sind.
    - NetScaler VPX Premium — 1000 Mbit/s Abonnieren Sie, wenn Sie eine abonnementbasierte Lizenz vom AWS Marketplace wünschen.
    - NetScaler Agent Service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wählen Sie eine VPC aus — Wählen Sie eine VPC für die Einrichtung der Infrastruktur zur Anwendungsbereitstellung aus. Die VPC sollte einen CIDR von /22 oder mehr haben. Während des Infrastruktur-Bereitstellungsprozesses werden dedizierte Subnetze für die ADC-Infrastruktur erstellt, die für jede ausgewählte Availability Zone einen /24-Adressraum verbrauchen. Wählen Sie eine VPC aus der Liste basierend auf Ihrer Bereitstellung aus:
  - Dedizierte VPC, die von den Anwendungen getrennt ist, wenn Ihre Bereitstellung einer DMZ ähneln soll.
  - Dieselbe VPC, in der sich auch die Anwendungen befinden.
- NAT Gateway — Die Bereitstellungsinfrastruktur, wie z. B. der Console-Agent, die automatisch bereitgestellt wird, muss über das Internet auf den NetScaler Console-Dienst zugreifen können. Ein NAT-Gateway kann diesen Zugriff ermöglichen. Wenn Sie bereits ein NAT-Gateway haben, können Sie dieses auch für die Bereitstellungsinfrastruktur wiederverwenden, indem Sie es während der Bereitstellung auswählen. Wenn kein NAT-Gateway ausgewählt wird, erstellt der Bereitstellungsprozess eines.

Cloud-Zugriffsprofil

Ein Cloud-Zugriffsprofil wird verwendet, um dem NetScaler Console-Dienst Berechtigungen für das AWS-Konto des Kunden zu erteilen. Beim Erstellen eines Cloud-Zugriffsprofils muss der Administrator eine CloudFormationTemplate (CFT) in AWS ausführen. Die CFT erstellt IAM-Rollen und -Richtlinien im AWS-Konto des Kunden.

1. Navigieren Sie zu **Infrastructure > Provisioning > App based > Cloud Access Profiles**.
2. Befolgen Sie die Anweisungen auf dem Bildschirm, um ein Cloud-Zugriffsprofil für Ihr Abonnement zu erstellen.

HINWEIS:

Um dieses Profil zu erstellen, muss der NetScaler-Administrator auch der AWS-Konto-Administrator sein und über die erforderlichen Berechtigungen zum Erstellen von IAM-Entitäten verfügen.

App-Umgebung

Eine App-Umgebung repräsentiert die in einer VPC eingerichtete Bereitstellungsinfrastruktur für die Bereitstellung von Anwendungen. Wenn ein Administrator eine App-Umgebung im NetScaler Console-Dienst erstellt, werden alle Ressourcen für die Bereitstellung und Überwachung von Anwendungen, einschließlich Gateways, Sicherheitsgruppen, Subnetzen, NetScaler-Instanzen und

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konsolen-Agenten, als Teil einer App-Umgebung bereitgestellt. Weitere Informationen finden Sie im Abschnitt FAQ.

1. Navigieren Sie zu **InfraStructure > Provisioning > App based > Environments**.
2. Befolgen Sie die Anweisungen auf dem Bildschirm, um eine App-Umgebung zu erstellen.

HINWEIS:

Der Dienst nimmt keine Änderungen an den vom Kunden in seiner VPC erstellten Ressourcen vor. Er stellt lediglich die notwendige Infrastruktur zur Bereitstellung und Überwachung der Anwendungen bereit.

Anwendungsbereitstellung

Die Anwendungsbereitstellung ist die Kernkomponente der App-basierten Bereitstellungsfunktion und enthält die obligatorischen Informationen zur Anwendungsbereitstellung und -sicherheit. Im Rahmen der Anwendungsbereitstellungskonfiguration definieren Sie die folgenden Entitäten:

- Der Endpunkt, der darstellt, wie die Anwendung von den Clients aufgerufen wird, z. B. Protokoll, Port, Zertifikate und Chiffren. Zum Beispiel repräsentiert ein SSL-Profil eines Endpunkts den Satz von SSL-Konfigurationen, der die unterstützten Chiffren und Protokolle umfasst. Ein vordefiniertes A+-SSL-Profil ist standardmäßig verfügbar.
- Die Dienste, die die Komponente einer Anwendung darstellen, auf die basierend auf der spezifischen HTTP-Anfrage zugegriffen werden muss. Zum Beispiel könnte eine Komponente für eine E-Commerce-Anwendung ein Bestelldienst, ein Katalogdienst oder ein Zahlungsdienst sein, die auf verschiedenen Anwendungsservern installiert sind und Anfragen basierend auf der aufgerufenen URL weitergeleitet werden müssen. Das Dienstprofil eines Anwendungsdienstes stellt dar, wie die Bereitstellungsinfrastruktur auf den Anwendungsdienst zugreifen und ihn überwachen kann, z. B. Lastausgleich, SSL und Zustandsprüfungs-Einstellungen.
- Die Inhaltsrichtlinie, die definiert, wie der L7-Inhalt überprüft und geändert wird, wenn eine Anfrage für einen bestimmten Dienst eingeht. Sie wird verwendet, um eine vordefinierte Aktion für HTTP-Anfragen basierend auf Headern, URLs oder IP-Adressen auszuführen. Einige der Aktionen könnten Header-Anreicherung, Umleitung von Anfragen oder das Verwerfen von Anfragen sein.

1. Navigieren Sie zu **Infrastruktur > Bereitstellung > App-basiert > App-Bereitstellung**.
2. Befolgen Sie die Anweisungen auf dem Bildschirm, um eine neue Anwendung zu erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Häufig gestellte Fragen

Welche Entitäten werden vom NetScaler Console-Dienst für die Bereitstellung einer Anwendung in der Cloud erstellt?

Der NetScaler Console-Dienst erstellt die folgenden Entitäten im VPC des Kunden:

- NetScaler VPX-Cluster in jeder Verfügbarkeitszone.
  - Die VPX-Instanzen werden als EC2 Autoscale™-Gruppe bereitgestellt.
  - Ein Einzelknoten-Cluster wird während der Erstellung der App-Umgebung erstellt. Dieser Cluster kann auf maximal 8 Knoten skaliert werden.
- Console-Agent in jeder Verfügbarkeitszone.
- Subnetze: Jeweils ein Subnetz für Management-, Client- und Servernetzwerke.
- Sicherheitsgruppen: Jeweils eine Sicherheitsgruppe für Management-, Client- und Server-NICs.
  - Management-Sicherheitsgruppe: Diese Sicherheitsgruppe ist den Management-NICs der NetScaler-Instanzen und -Agenten zugeordnet. Sie besteht aus Regeln, die die Kommunikation zwischen NetScaler-Instanzen, Agenten und anderem Control-Plane-Traffic ermöglichen.
  - Client-Sicherheitsgruppe: Diese Sicherheitsgruppe ist den Client-NICs der NetScaler-Instanzen zugeordnet und wird verwendet, um den Datenverkehr zu den virtuellen NetScaler-Servern zuzulassen.
  - Server-Sicherheitsgruppe: Diese Sicherheitsgruppe ist den Server-NICs der NetScaler-Instanzen zugeordnet und enthält keine Standardregeln.
- Routing-Tabellen
  - Client-Routing-Tabelle: Diese Routing-Tabelle erleichtert den internetgebundenen Datenverkehr. Sie enthält eine Route, die den Datenverkehr zum Internet-Gateway leitet, das der VPC zugeordnet ist, was die Konnektivität zum Internet für Ressourcen innerhalb der VPC ermöglicht.
  - Management-Routing-Tabelle: Diese Routing-Tabelle erleichtert den Datenverkehr, der von NetScaler und Agenten für die Netzwerkadressübersetzung (NAT) durch das NAT-Gateway stammt.
- NAT-Gateway in jeder Availability Zone: Ein NAT-Gateway ermöglicht NetScaler- und Console-Agenten den Zugriff auf das Internet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Ein NAT-Gateway wird nicht erstellt, wenn Sie ein vorhandenes NAT-Gateway in Ihrer VPC wiederverwenden möchten.

- Secrets Manager: Ein Secrets Manager wird verwendet, um:
  - Das Agenten-Token und die URL zu speichern, die für die Registrierung des Agenten beim NetScaler Console-Dienst verwendet werden.
  - Das ADC-Passwort zur Authentifizierung zu speichern.
- Lambda-Funktionen
  - ClusterLambdaFunction: Diese Lambda-Funktion ist für die Erstellung und Verwaltung des NetScaler-Clusters verantwortlich.
  - StatsLambdaFunction: Diese Lambda-Funktion wird erstellt, um Metriken von NetScaler zu sammeln, die für die automatische Skalierung verwendet werden.

Welche Metriken werden zur automatischen Skalierung von NetScaler verwendet?

Die folgenden Metriken werden zur automatischen Skalierung von NetScaler verwendet:

- Die Mindestanzahl von Instanzen in der Autoscale-Gruppe beträgt 1 und die maximale Anzahl ist 8.
- Skalierung um 1 Kapazitätseinheit. Das heißt, cpu_use > 70 % oder Durchsatz > 70 % für 5 aufeinanderfolgende Zeiträume von 60 Sekunden.
- Skalierung um 1 Kapazitätseinheit. Das heißt, cpu_use =< 30 % und Durchsatz =< 30 % für 5 aufeinanderfolgende Zeiträume von 60 Sekunden.

Wie kann ein Administrator die vom NetScaler Console-Dienst in der Cloud erstellten Ressourcen identifizieren?

Alle AWS-Ressourcen werden standardmäßig mit dem Tag „UsedFor: AppDeliveryByNetScaler“ erstellt. Darüber hinaus werden die Ressourcen mit den Tags versehen, die während des Workflows zur Erstellung der App-Umgebung angegeben wurden.

Wie kann ein NetScaler-Administrator NetScaler in einer App-Umgebung aktualisieren?

Führen Sie die folgenden Schritte aus, um NetScaler zu aktualisieren:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Deaktivieren Sie in der AWS-Konsole die dynamische Skalierung für die für die App-Umgebung erstellte Autoscale-Gruppe.Namenskonvention: `Adc-<App Environment Name>-<Availability Zone>-<random alphanumeric string>`

- Aktualisieren Sie im NetScaler Console-Dienst die AMI-Details auf die ADC-Version, auf die der NetScaler aktualisiert werden soll, indem Sie die Option **Bearbeiten** für die App-Umgebung verwenden.

- Führen Sie im NetScaler Console-Dienst ein Upgrade der ADCs mithilfe der Funktion **Upgrade-Auftrag** durch.

- Aktivieren Sie in der AWS-Konsole die dynamische Skalierung für die Autoscale-Gruppe erneut.

App-basiertes Provisioning in Azure

Der NetScaler Console-Dienst führt ein „App-basiertes“ Provisioning ein, das darauf ausgelegt ist, NetScaler-Bereitstellungen in Cloud-Rechenzentren zu optimieren und zu vereinfachen und Anwendungen von dort bereitzustellen.

Der NetScaler Console-Dienst akzeptiert die Cloud-Anmeldeinformationen des Kunden und richtet die für die Anwendungsbereitstellung erforderliche Infrastruktur ein, indem er das Starten von NetScaler-Instanzen, NetScaler Console Agents und den notwendigen Cloud-Entitäten in Azure orchestriert. NetScaler-Administratoren können sowohl Flexed- als auch Cloud Marketplace-Lizenzen für ihre NetScaler-Instanzen nutzen, was Flexibilität bei den Lizenzierungsoptionen gewährleistet.

Administratoren können dann Anwendungen, die in ihrer Cloud vorhanden sind, bereitstellen, indem sie die Bereitstellungseinstellungen auf einfache, anwendungszentrierte Weise über den NetScaler Console-Dienst definieren. Der Dienst kümmert sich dann um die Konfiguration sowohl der ADCs als auch der Azure-Infrastruktur, um ihre Anwendungen bereitzustellen. Sobald die Anwendungen bereitgestellt sind, erhalten NetScaler-Administratoren Zugriff auf die umfangreichen Analyse- und Überwachungsfunktionen des NetScaler Console-Dienstes, um ihre Anwendungen effektiv zu verwalten und zu überwachen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Voraussetzungen

Konfigurieren Sie die programmatische Bereitstellung für die folgenden Produkte im Azure Marketplace:

- NetScaler VPX – Konfigurieren Sie die programmatische Bereitstellung für eine der folgenden Varianten:
  - NetScaler VPX BYOL – Abonnieren Sie, wenn Sie Flexed-Lizenzen erworben haben und diese im NetScaler Console-Dienst für die Lizenzierung von NetScaler-Instanzen verfügbar sind.
  - NetScaler VPX Premium - 1 Gbps – Abonnieren Sie, wenn Sie eine abonnementbasierte Lizenz vom Azure Marketplace wünschen.
  - NetScaler Agent-Dienst
- Wählen Sie ein VNet aus – Wählen Sie ein VNet für die Einrichtung der Infrastruktur zur Anwendungsbereitstellung aus. Das VNet sollte einen CIDR von /22 oder mehr haben. Während des Infrastruktur-Bereitstellungsprozesses werden dedizierte Subnetze für die ADC-Infrastruktur erstellt, die einen /24-Adressraum verbrauchen. Wählen Sie ein VNet aus der Liste basierend auf Ihrer Bereitstellung aus:
  - Dediziertes VNet, das von den Anwendungen getrennt ist, wenn Ihre Bereitstellung einer DMZ ähneln soll.
  - Dasselbe VNet, in dem sich auch die Anwendungen befinden.

Cloud-Zugriffsprofil

Ein Cloud-Zugriffsprofil wird verwendet, um dem NetScaler Console-Dienst Berechtigungen für das Azure-Konto des Kunden zu erteilen. Beim Erstellen eines Cloud-Zugriffsprofils muss der Administrator ein PowerShell-Skript in Azure CLI herunterladen und ausführen. Das Skript erstellt Dienstprinzipale im Azure-Konto des Kunden mit Besitzerberechtigungen auf Abonnementebene.

1. Navigieren Sie zu **Infrastructure > Provisioning > App based > Cloud Access Profiles**.
2. Befolgen Sie die Anweisungen auf dem Bildschirm, um ein Cloud-Zugriffsprofil für Ihr Abonnement zu erstellen.

HINWEIS:

Um dieses Profil zu erstellen, muss der NetScaler-Administrator auch der Besitzer des Azure-Abonnements sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

App-Umgebung

Die App-Umgebung repräsentiert die in einem VNet eingerichtete Bereitstellungsinfrastruktur für die Bereitstellung der Anwendungen. Wenn ein Administrator eine App-Umgebung im NetScaler Console-Dienst erstellt, werden alle Ressourcen für die Bereitstellung und Überwachung von Anwendungen, einschließlich Gateways, Sicherheitsgruppen, Subnetzen, NetScaler-Instanzen und NetScaler Console-Agenten, als Teil einer App-Umgebung bereitgestellt. Weitere Informationen finden Sie im Abschnitt FAQ.

1. Navigieren Sie zu **InfraStructure > Provisioning > App based > Environments**.
2. Befolgen Sie die Anweisungen auf dem Bildschirm, um eine App-Umgebung zu erstellen.

Anwendungsbereitstellung

Die Anwendungsbereitstellung ist die Kernkomponente der App-basierten Bereitstellungsfunktion und enthält die obligatorischen Informationen zur Anwendungsbereitstellung und -sicherheit. Im Rahmen der Konfiguration der Anwendungsbereitstellung definieren Sie die folgenden Entitäten:

- Der Endpunkt, der darstellt, wie die Anwendung von den Clients aufgerufen wird, z. B. Protokoll, Port, Zertifikate und Chiffren. Zum Beispiel repräsentiert ein SSL-Profil eines Endpunkts die Menge der SSL-Konfigurationen, die die unterstützten Chiffren und Protokolle umfassen. Ein vordefiniertes A+ SSL-Profil ist standardmäßig verfügbar.
- Die Dienste, die eine Anwendungskomponente darstellen, auf die basierend auf der spezifischen HTTP-Anfrage zugegriffen werden muss. Zum Beispiel könnte eine Komponente für eine E-Commerce-Anwendung ein Bestelldienst, ein Katalogdienst oder ein Zahlungsdienst sein, die auf verschiedenen Anwendungsservern installiert sind, und Anfragen müssen basierend auf der aufgerufenen URL weitergeleitet werden. Das Dienstprofil eines Anwendungsdienstes repräsentiert, wie die Bereitstellungsinfrastruktur auf den Anwendungsdienst zugreifen und ihn überwachen kann, z. B. Lastausgleich, SSL und Zustandsprüfungen.
- Die Inhaltsrichtlinie, die definiert, wie der L7-Inhalt überprüft und geändert wird, wenn eine Anfrage oder eine Antwort für einen bestimmten Dienst eintrifft. Sie wird verwendet, um eine vordefinierte Aktion auf HTTP-Anfragen basierend auf Headern, URLs oder IP-Adressen auszuführen. Einige der Aktionen könnten die Header-Anreicherung, die Umleitung von Anfragen oder das Verwerfen von Anfragen sein.

1. Navigieren Sie zu **InfraStructure > Provisioning > App based > App Delivery**.
2. Befolgen Sie die Anweisungen auf dem Bildschirm, um eine neue Anwendung zu erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FAQs

Welche Entitäten werden vom NetScaler Console Service für die Bereitstellung einer Anwendung in der Cloud erstellt?

Der NetScaler Console Service erstellt die folgenden Entitäten im VNet des Kunden:

- NetScaler VPX-Cluster.
  - Die VPX-Instanzen werden als Virtual Machine Scale Set (VMSS) bereitgestellt.
  - Ein Einzelknoten-Cluster wird während der Erstellung der App-Umgebung erstellt. Dieser Cluster kann auf maximal 10 Knoten skaliert werden.
- Ein NetScaler Console Agent.
- Subnetze: Je ein Subnetz für Verwaltung, Client und Server.
- Sicherheitsgruppen: Je eine Sicherheitsgruppe für Verwaltungs-, Client- und Server-NICs von NetScaler.
  - Verwaltungs-Sicherheitsgruppe: Diese Sicherheitsgruppe ist den Verwaltungs-NICs der NetScaler-Instanzen und NetScaler Console Agents zugeordnet. Sie besteht aus Regeln, die die Kommunikation zwischen NetScaler-Instanzen, NetScaler Console Agents und jeglichem anderen Control-Plane-Traffic ermöglichen.
  - Client-Sicherheitsgruppe: Diese Sicherheitsgruppe ist den Client-NICs der NetScaler-Instanzen zugeordnet und wird verwendet, um den Datenverkehr zu den virtuellen NetScaler-Servern zuzulassen.
  - Server-Sicherheitsgruppe: Diese Sicherheitsgruppe ist den Server-NICs der NetScaler-Instanzen zugeordnet und enthält keine Standardregeln.
- NAT-Gateway: Ein NAT-Gateway ermöglicht dem NetScaler Console Agent den Zugriff auf den NetScaler Console Service und den NetScaler-Instanzen den Zugriff auf das Internet.
- Azure Key Vault: Speichern Sie alle NetScaler- und Agent-Geheimnisse im Tresor.

Welche Metriken werden zum automatischen Skalieren von NetScaler verwendet?

Die folgenden Metriken werden zum automatischen Skalieren von NetScaler verwendet:

- Die Mindestanzahl der Instanzen im VMSS beträgt 1 und die Höchstanzahl 10.
- Skalierung um 1 Kapazitätseinheit nach oben. Das heißt, cpu_use > 70 % oder Durchsatz > 70 % für 5 aufeinanderfolgende Perioden von 60 Sekunden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Skalierung um 1 Kapazitätseinheit nach unten. Das heißt, cpu_use =< 30 % und Durchsatz =< 30 % für 5 aufeinanderfolgende Perioden von 60 Sekunden.

Wie kann ein Administrator die vom NetScaler Console-Dienst in der Cloud erstellten Ressourcen identifizieren?

Alle Azure-Ressourcen werden standardmäßig mit dem Tag „UsedFor: AppDeliveryByNetScaler“ erstellt. Darüber hinaus werden die Ressourcen mit den Tags versehen, die während des Workflows zur Erstellung der App-Umgebung angegeben wurden.

Wie kann ein NetScaler-Administrator NetScaler in einer App-Umgebung aktualisieren?

Führen Sie die folgenden Schritte aus, um NetScaler zu aktualisieren:

- Deaktivieren Sie in der Azure-Konsole die Skalierung für das VMSS, indem Sie die Werte der Skalierungsrichtlinie auf die aktuelle Anzahl der Instanzen im VMSS für die App-Umgebung festlegen.

  Namenskonvention: `vmss-adc-<App Environment Name>`

- Bearbeiten Sie im NetScaler Console-Dienst die App-Umgebung und wählen Sie die Version aus, auf die Sie aktualisieren möchten.

- Aktualisieren Sie im NetScaler Console-Dienst die ADCs auf die im vorherigen Schritt ausgewählte Version, indem Sie die Funktion **Upgrade-Job** verwenden.

- Aktivieren Sie über die Azure-Konsole die dynamische Skalierung für die VMSS wieder. Das Instanzlimit muss auf die ursprünglichen Werte festgelegt werden. Das heißt, Minimum=1, Maximum=10, Standard=1.

Bereitstellung von NetScaler VPX-Instanzen

Mit NetScaler Console können Sie die Bereitstellung, Einrichtung und Verwaltung von NetScaler VPX-Instanzen über öffentliche Cloud- und Virtualisierungsplattformen hinweg automatisieren. Die Bereitstellung von NetScaler VPX-Instanzen mithilfe von NetScaler Console kombiniert die Elastizität und Flexibilität der Cloud mit den Optimierungs-, Sicherheits- und Steuerungsfunktionen von NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn NetScaler Console Ihre NetScaler-Instanzen überwacht, erhalten Sie Einblick in den Zustand, die Leistung und die Sicherheit Ihrer Anwendungen, und Sie können Ihre Anwendungsbereitstellungsinfrastruktur in hybriden und Multi-Cloud-Umgebungen verwalten.

Sie können NetScaler VPX-Instanzen auf den folgenden Plattformen bereitstellen:

- AWS
- Microsoft Azure
- Google Cloud
- VMware vCenter

Bereitstellung von NetScaler VPX-Instanzen auf AWS

Wenn Sie Ihre Anwendungen in die Cloud verlagern, nimmt die Anzahl der Komponenten Ihrer Anwendung zu, sie werden stärker verteilt und müssen dynamisch verwaltet werden.

Mit NetScaler VPX-Instanzen auf AWS können Sie Ihren L4-L7-Netzwerk-Stack nahtlos auf AWS erweitern. Mit NetScaler VPX wird AWS zu einer natürlichen Erweiterung Ihrer lokalen IT-Infrastruktur. Sie können NetScaler VPX auf AWS verwenden, um die Elastizität und Flexibilität der Cloud mit denselben Optimierungs-, Sicherheits- und Steuerungsfunktionen zu kombinieren, die die anspruchsvollsten Websites und Anwendungen der Welt unterstützen.

Mit NetScaler Console, die Ihre NetScaler-Instanzen überwacht, erhalten Sie Einblick in den Zustand, die Leistung und die Sicherheit Ihrer Anwendungen. Sie können die Einrichtung, Bereitstellung und Verwaltung Ihrer Anwendungsbereitstellungsinfrastruktur in hybriden Multi-Cloud-Umgebungen automatisieren.

AWS-Terminologie

Der folgende Abschnitt bietet eine kurze Beschreibung der in diesem Dokument verwendeten AWS-Begriffe:

BEGRIFF	DEFINITION
Amazon Machine Image (AMI)	Ein Maschinen-Image, das die zum Starten einer Instanz erforderlichen Informationen bereitstellt; eine Instanz ist ein virtueller Server in der Cloud.
Elastic Compute Cloud (EC2)	Ein Webdienst, der sichere, in der Größe anpassbare Rechenkapazität in der Cloud bereitstellt. Er wurde entwickelt, um

© 1997–2026 Citrix Systems, Inc. All rights reserved.

BEGRIFF	DEFINITION
	Entwicklern das Cloud-Computing im Web-Maßstab zu erleichtern.
Elastische Netzwerkschnittstelle (ENI)	Eine virtuelle Netzwerkschnittstelle, die Sie an eine Instanz in einer VPC anhängen können.
Instanztyp	Amazon EC2 bietet eine große Auswahl an Instance-Typen, die für verschiedene Anwendungsfälle optimiert sind. Instance-Typen umfassen unterschiedliche Kombinationen aus CPU, Arbeitsspeicher, Speicher und Netzwerkkapazität und bieten Ihnen die Flexibilität, die passende Mischung von Ressourcen für Ihre Anwendungen auszuwählen.
Identitäts- und Zugriffsverwaltung (IAM)-Rolle	Eine AWS-Identität mit Berechtigungsrichtlinien, die festlegen, was die Identität in AWS tun und nicht tun kann. Sie können eine IAM-Rolle verwenden, um Anwendungen, die auf einer EC2-Instance ausgeführt werden, den sicheren Zugriff auf Ihre AWS-Ressourcen zu ermöglichen.
Sicherheitsgruppen	Ein benannter Satz zulässiger eingehender Netzwerkverbindungen für eine Instance.
Subnetze	Ein Segment des IP-Adressbereichs einer VPC, an das EC2-Instances angehängt werden können. Sie können Subnetze erstellen, um Instances entsprechend den Sicherheits- und Betriebsanforderungen zu gruppieren.

Voraussetzungen

Dieses Dokument geht von Folgendem aus:

- Sie besitzen ein AWS-Konto.
- Sie haben die erforderliche VPC erstellt und die Verfügbarkeitszonen ausgewählt.
- Sie haben den Agenten in AWS hinzugefügt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen zum Erstellen eines Kontos und zu anderen Aufgaben finden Sie unter AWS-Dokumentation.

Weitere Informationen zur Installation eines Agents auf AWS finden Sie unter Installieren eines NetScaler-Agents auf AWS.

Architekturdiagramm

Die folgende Abbildung bietet einen Überblick darüber, wie NetScaler Console eine Verbindung mit AWS herstellt, um NetScaler VPX-Instanzen in AWS bereitzustellen.

Konfigurationsaufgaben

Führen Sie die folgenden Aufgaben in AWS aus, bevor Sie NetScaler VPX-Instanzen in NetScaler Console bereitstellen:

- Subnetze erstellen
- Sicherheitsgruppen erstellen
- Eine IAM-Rolle erstellen und eine Richtlinie definieren

Führen Sie die folgenden Aufgaben in NetScaler Console aus, um die Instanzen in AWS bereitzustellen:

- Site erstellen
- NetScaler VPX-Instanz in AWS bereitstellen

SO ERSTELLEN SIE SUBNETZE

Erstellen Sie drei Subnetze in Ihrer VPC. Die drei Subnetze, die für die Bereitstellung von NetScaler VPX-Instanzen in Ihrer VPC erforderlich sind, sind Management, Client und Server. Geben Sie für jedes der Subnetze einen IPv4-CIDR-Block aus dem in Ihrer VPC definierten Bereich an. Geben Sie die Verfügbarkeitszone an, in der sich das Subnetz befinden soll. Erstellen Sie alle drei Subnetze in derselben Verfügbarkeitszone. Die folgende Abbildung zeigt die drei in Ihrer Region erstellten Subnetze und deren Konnektivität zum Clientsystem.

Weitere Informationen zu VPC und Subnetzen finden Sie unter VPCs und Subnetze.

SO ERSTELLEN SIE SICHERHEITSGRUPPEN

Erstellen Sie eine Sicherheitsgruppe, um den eingehenden und ausgehenden Datenverkehr in der NetScaler VPX-Instanz zu steuern. Eine Sicherheitsgruppe fungiert als virtuelle Firewall für Ihre Instanz. Erstellen Sie Sicherheitsgruppen auf Instanzebene und nicht auf Subnetzebene. Es ist

© 1997–2026 Citrix Systems, Inc. All rights reserved.

möglich, jeder Instanz in einem Subnetz in Ihrer VPC einen anderen Satz von Sicherheitsgruppen zuzuweisen. Fügen Sie Regeln für jede Sicherheitsgruppe hinzu, um den eingehenden Datenverkehr zu steuern, der über das Client-Subnetz zu den Instanzen geleitet wird. Sie können auch einen separaten Satz von Regeln hinzufügen, die den ausgehenden Datenverkehr steuern, der über das Server-Subnetz zu den Anwendungsservern geleitet wird. Obwohl Sie die Standardsicherheitsgruppe für Ihre Instanzen verwenden können, möchten Sie möglicherweise Ihre eigenen Gruppen erstellen. Erstellen Sie drei Sicherheitsgruppen – eine für jedes Subnetz. Erstellen Sie Regeln für den eingehenden und ausgehenden Datenverkehr, den Sie steuern möchten. Sie können beliebig viele Regeln hinzufügen.

Weitere Informationen zu Sicherheitsgruppen finden Sie unter Sicherheitsgruppen für Ihre VPC.

SO ERSTELLEN SIE EINE IAM-ROLLE UND DEFINIEREN EINE RICHTLINIE

Erstellen Sie eine IAM-Rolle, damit Sie eine Vertrauensbeziehung zwischen Ihren Benutzern und dem von Citrix vertrauten AWS-Konto herstellen und eine Richtlinie mit Citrix-Berechtigungen erstellen können.

1. Klicken Sie in AWS auf **Services**. Wählen Sie im linken Navigationsbereich **IAM > Roles** aus und klicken Sie auf **Create role**.
2. Sie verbinden Ihr AWS-Konto mit dem AWS-Konto in NetScaler Console. Wählen Sie daher **Another AWS account** aus, um NetScaler Console zu erlauben, Aktionen in Ihrem AWS-Konto auszuführen.

   Geben Sie die 12-stellige AWS-Konto-ID der NetScaler Console ein. Die Citrix-ID lautet 835822366011. Sie finden die Citrix-ID auch in der NetScaler Console, wenn Sie das Cloud-Zugriffsprofil erstellen.

3. Aktivieren Sie **Require external ID**, um eine Verbindung zu einem Drittanbieterkonto herzustellen. Sie können die Sicherheit Ihrer Rolle erhöhen, indem Sie eine optionale externe Kennung anfordern. Geben Sie eine ID ein, die eine beliebige Zeichenkombination sein kann.
4. Klicken Sie auf **Permissions**.
5. Klicken Sie auf der Seite **Attach permissions policies** auf **Create policy**.
6. Sie können eine Richtlinie im visuellen Editor oder mithilfe von JSON erstellen und bearbeiten.

   Die Liste der Berechtigungen von Citrix wird im folgenden Feld bereitgestellt:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
{

"Version": "2012-10-17",

"Statement":

[

    {

         "Effect": "Allow",

        "Action": [

            "ec2:DescribeInstances",

            "ec2:DescribeImageAttribute",

            "ec2:DescribeInstanceAttribute",

            "ec2:DescribeRegions",

            "ec2:DescribeDhcpOptions",

            "ec2:DescribeSecurityGroups",

            "ec2:DescribeHosts",

            "ec2:DescribeImages",

            "ec2:DescribeVpcs",

            "ec2:DescribeSubnets",

            "ec2:DescribeNetworkInterfaces",

            "ec2:DescribeAvailabilityZones",

            "ec2:DescribeNetworkInterfaceAttribute",

            "ec2:DescribeInstanceStatus",

            "ec2:DescribeAddresses",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "ec2:DescribeKeyPairs",
            "ec2:DescribeTags",
            "ec2:DescribeVolumeStatus",
            "ec2:DescribeVolumes",
            "ec2:DescribeVolumeAttribute",
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:CreateKeyPair",
            "ec2:DeleteKeyPair",
            "ec2:ResetInstanceAttribute",
            "ec2:RunScheduledInstances",
            "ec2:ReportInstanceStatus",
            "ec2:StartInstances",
            "ec2:RunInstances",
            "ec2:StopInstances",
            "ec2:UnmonitorInstances",
            "ec2:MonitorInstances",
            "ec2:RebootInstances",
            "ec2:TerminateInstances",
            "ec2:ModifyInstanceAttribute",
            "ec2:AssignPrivateIpAddresses",
            "ec2:UnassignPrivateIpAddresses",
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "ec2:CreateNetworkInterface",

            "ec2:AttachNetworkInterface",

            "ec2:DetachNetworkInterface",

            "ec2:DeleteNetworkInterface",

            "ec2:ResetNetworkInterfaceAttribute",

            "ec2:ModifyNetworkInterfaceAttribute",

            "ec2:AssociateAddress",

            "ec2:AllocateAddress",

            "ec2:ReleaseAddress",

            "ec2:DisassociateAddress",

            "ec2:GetConsoleOutput"

        ],

            "Resource": "*"

    }

]

}
```

7. Kopieren Sie die Liste der Berechtigungen auf der Registerkarte JSON und fügen Sie sie ein, und klicken Sie auf **Review policy**.
8. Geben Sie auf der Seite **Review policy** einen Namen für die Richtlinie ein, geben Sie eine Beschreibung ein und klicken Sie auf **Create policy**.

SO ERSTELLEN SIE EINE SITE IN NETSCALER CONSOLE

Erstellen Sie eine Site in NetScaler Console und fügen Sie die Details des VPC hinzu, das Ihrer AWS-Rolle zugeordnet ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Sites**.
2. Klicken Sie auf **Add**.
3. Wählen Sie den Diensttyp als AWS aus und aktivieren Sie **Use existing VPC as a site**.
4. Wählen Sie das Cloud-Zugriffsprofil aus.
5. Wenn das Cloud-Zugriffsprofil im Feld nicht vorhanden ist, klicken Sie auf **Add**, um ein Profil zu erstellen.

   a. Geben Sie auf der Seite **Create Cloud Access Profile** den Namen des Profils ein, mit dem Sie auf AWS zugreifen möchten.

   b. Geben Sie den ARN ein, der der Rolle zugeordnet ist, die Sie in AWS erstellt haben.

   c. Geben Sie die externe ID ein, die Sie beim Erstellen einer IAM-Rolle (Identity and Access Management) in AWS angegeben haben. Siehe Schritt 4 unter „So erstellen Sie eine IAM-Rolle und definieren eine Richtlinienaufgabe“. Stellen Sie sicher, dass der IAM-Rollenname, den Sie in AWS angegeben haben, mit „Citrix-ADM-“ beginnt und korrekt im Rollen-ARN angezeigt wird.

   Die Details des VPC, wie Region, VPC-ID, Name und CIDR-Block, die Ihrer IAM-Rolle in AWS zugeordnet sind, werden in NetScaler Console importiert.
6. Geben Sie einen Namen für die Site ein.
7. Klicken Sie auf **Erstellen**.

SO STELLEN SIE NETSCALER VPX AUF AWS BEREIT

Verwenden Sie die zuvor erstellte Site, um die NetScaler VPX-Instanzen auf AWS bereitzustellen. Geben Sie die Agent-Details an, um die Instanzen bereitzustellen, die an diesen Agent gebunden sind.

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Instances > NetScaler**.
2. Klicken Sie auf der Registerkarte **VPX** auf **Bereitstellen**.

   Diese Option zeigt die Seite **NetScaler VPX in der Cloud bereitstellen** an.
3. Wählen Sie **Amazon Web Services (AWS)** aus und klicken Sie auf **Weiter**.
4. Auf der Registerkarte **Grundlegende Parameter**,

   a. Wählen Sie den **Instanztyp** aus der Liste aus.

   - **Standalone:** Diese Option stellt eine eigenständige NetScaler VPX-Instanz auf AWS bereit.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **HA:** Diese Option stellt die hochverfügbaren NetScaler VPX-Instanzen auf AWS bereit.

  Um die NetScaler VPX-Instanzen in derselben Zone bereitzustellen, wählen Sie die Option **Einzelne Zone** unter **Zonentyp**.

  Um die NetScaler VPX-Instanzen über mehrere Zonen hinweg bereitzustellen, wählen Sie die Option **Mehrere Zonen** unter **Zonentyp**. Stellen Sie auf der Registerkarte **Bereitstellungsparameter** sicher, dass Sie die Netzwerkdetails für jede auf AWS erstellte Zone angeben.

b. Geben Sie den Namen einer NetScaler VPX-Instanz an.

c. Wählen Sie unter **Site** die zuvor erstellte Site aus.

d. Wählen Sie unter **Agent** den Agenten aus, der zur Verwaltung der NetScaler VPX-Instanz erstellt wurde.

e. Wählen Sie unter **Cloud Access Profile** das Cloud-Zugriffsprofil aus, das während der Site-Erstellung erstellt wurde.

f. Wählen Sie unter **Device Profile** das Profil zur Authentifizierung aus.

   NetScaler Console verwendet das Geräteprofil, wenn es sich bei der NetScaler VPX-Instanz anmelden muss.

g. Klicken Sie auf **Weiter**.

5. Wählen Sie auf der Registerkarte **Lizenz** eine der folgenden Modi aus, um eine Lizenz auf eine NetScaler-Instanz anzuwenden:

   - **Verwenden von NetScaler Console**: Die Instanz, die Sie bereitstellen möchten, ruft die Lizenzen von der NetScaler Console ab.
   - **Verwenden der AWS Cloud**: Die Option **Aus Cloud zuweisen** verwendet die NetScaler®-Produktlizenzen, die auf dem AWS Marketplace verfügbar sind. Die Instanz, die Sie bereitstellen möchten, verwendet die Lizenzen vom Marketplace.

     Wenn Sie Lizenzen vom AWS Marketplace verwenden möchten, geben Sie das Produkt oder die Lizenz auf der Registerkarte **Bereitstellungsparameter** an.

   Weitere Informationen finden Sie unter Lizenzierungsanforderungen.

6. Wenn Sie auf der Registerkarte **Lizenz** die Option **Aus NetScaler Console zuweisen** auswählen, geben Sie Folgendes an:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Lizenztyp – Wählen Sie entweder Bandbreiten- oder virtuelle CPU-Lizenzen aus:

  Bandbreitenlizenzen: Sie können eine der folgenden Optionen aus der Liste **Bandbreitenlizenztypen** auswählen:

  - **Gepoolte Kapazität:** Geben Sie die Kapazität an, die einer Instanz zugewiesen werden soll.

    Aus dem gemeinsamen Pool ruft die NetScaler-Instanz eine Instanzlizenz und nur die angegebene Bandbreite ab.
  - **VPX-Lizenzen:** Wenn eine NetScaler VPX-Instanz bereitgestellt wird, ruft die Instanz die Lizenz von der NetScaler Console ab.

  Virtuelle CPU-Lizenzen: Die bereitgestellte NetScaler VPX-Instanz ruft Lizenzen ab, abhängig von der Anzahl der in der Instanz laufenden CPUs.

  HINWEIS

  Wenn die bereitgestellten Instanzen entfernt oder zerstört werden, kehren die angewendeten Lizenzen in den Lizenzpool der NetScaler Console zurück. Diese Lizenzen können zur Bereitstellung neuer Instanzen wiederverwendet werden.

a. Wählen Sie unter **Lizenz-Edition** die Lizenz-Edition aus. Die NetScaler Console verwendet die angegebene Edition, um Instanzen bereitzustellen.

7. Klicken Sie auf **Weiter**.
8. Auf der Registerkarte **Bereitstellungsparameter**,

   a. Wählen Sie die in AWS erstellte **Citrix IAM-Rolle** aus. Eine IAM-Rolle ist eine AWS-Identität mit Berechtigungsrichtlinien, die festlegen, was die Identität in AWS tun und nicht tun kann.

   b. Wählen Sie im Feld **Produkt** die NetScaler-Produktversion aus, die Sie bereitstellen möchten.

   c. Wählen Sie den EC2-Instanztyp aus der Liste **Instanztyp** aus.

      Diese Liste zeigt die unterstützten AMI-Instanztypen für die ausgewählte NetScaler-Instanz an.

   d. Wählen Sie die **Version** von NetScaler aus, die Sie bereitstellen möchten. Wählen Sie sowohl die **Haupt-** als auch die **Nebenversion** von NetScaler aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. Wählen Sie unter **Sicherheitsgruppen** die Management-, Client- und Server-Sicherheitsgruppen aus, die Sie in Ihrem virtuellen Netzwerk erstellt haben.

f. Wählen Sie unter **IPs in Server-Subnetz pro Knoten** die Anzahl der IP-Adressen im Server-Subnetz pro Knoten für die Sicherheitsgruppe aus.

g. Wählen Sie unter **Subnetze** die Management-, Client- und Server-Subnetze für jede Zone aus, die in AWS erstellt wurden. Sie können die Region auch aus der Liste **Verfügbarkeitszone** auswählen.

h. Klicken Sie auf **Fertig stellen**.

Die NetScaler VPX-Instanz ist jetzt in AWS bereitgestellt.

HINWEIS

Derzeit unterstützt NetScaler Console die Aufhebung der Bereitstellung von NetScaler-Instanzen aus AWS nicht.

SO ZEIGEN SIE DIE IN AWS BEREITGESTELLTE NETSCALER VPX AN

1. Navigieren Sie auf der AWS-Startseite zu **Dienste** und klicken Sie auf **EC2**.
2. Klicken Sie auf der Seite **Ressourcen** auf **Ausgeführte Instanzen**.
3. Sie können die in AWS bereitgestellte NetScaler VPX anzeigen.

Der Name der NetScaler VPX-Instanz ist derselbe, den Sie bei der Bereitstellung einer Instanz in der NetScaler Console angegeben haben.

SO ZEIGEN SIE DIE IN NETSCALER CONSOLE BEREITGESTELLTE NETSCALER VPX AN

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Instanzen > NetScaler**.
2. Wählen Sie die Registerkarte **NetScaler VPX** aus.
3. Die in AWS bereitgestellte NetScaler VPX Instanz wird hier aufgeführt.

Bereitstellung von NetScaler VPX-Instanzen in Microsoft Azure

Anwendungen oder Dienste, die in Azure gehostet werden, erfordern ein sicheres Traffic-Management und eine effiziente Optimierung der Netzwerkressourcen sowie die Vorteile der Cloud. NetScaler VPX-Instanzen, die in Microsoft Azure bereitgestellt werden, bieten sicheres Traffic-Management, optimierten Ressourcenverbrauch und reduzierte Betriebskosten für Webanwendungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mit NetScaler Console können Sie die Bereitstellung, Einrichtung und Verwaltung der NetScaler VPX-Instanzen in Azure automatisieren. Die Bereitstellung von NetScaler VPX-Instanzen mit NetScaler Console kombiniert die Elastizität und Flexibilität der Cloud mit den Steuerungsfunktionen von NetScaler.

NetScaler Console Bereitstellungsarchitektur

Die folgende Abbildung bietet einen Überblick darüber, wie NetScaler Console eine Verbindung mit Azure herstellt, um NetScaler VPX-Instanzen in Microsoft Azure bereitzustellen.

Sie benötigen drei Subnetze, um die NetScaler VPX-Instanz in Microsoft Azure bereitzustellen und zu verwalten. Für jedes Subnetz muss eine Sicherheitsgruppe erstellt werden. Die in NetScaler Gateway angegebenen Regeln steuern die Kommunikation zwischen den Subnetzen.

Der Agent hilft Ihnen bei der Bereitstellung und Verwaltung der NetScaler VPX-Instanz.

Voraussetzungen

Dieser Abschnitt beschreibt die Voraussetzungen, die Sie in Microsoft Azure und NetScaler Console erfüllen müssen, bevor Sie NetScaler VPX-Instanzen bereitstellen.

Dieses Dokument geht von Folgendem aus:

- Sie besitzen ein Microsoft Azure-Konto, das das Azure Resource Manager-Bereitstellungsmodell unterstützt.
- Sie haben eine Ressourcengruppe in Microsoft Azure.

Weitere Informationen zum Erstellen eines Kontos und zu anderen Aufgaben finden Sie unter Microsoft Azure-Dokumentation.

MICROSOFT AZURE-KOMPONENTEN EINRICHTEN

Führen Sie die folgenden Aufgaben in Azure aus, bevor Sie NetScaler VPX-Instanzen in NetScaler Console bereitstellen.

1. Ein virtuelles Netzwerk erstellen.
2. Sicherheitsgruppen erstellen.
3. Subnetze erstellen.
4. NetScaler VPX-Lizenz in Microsoft Azure abonnieren.
5. Eine Anwendung erstellen und registrieren.
6. Einen Agenten einrichten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ein virtuelles Netzwerk erstellen

1. Melden Sie sich bei Ihrem Microsoft Azure-Portal an.
2. Wählen Sie **Ressource erstellen**.
3. Wählen Sie **Netzwerk** und klicken Sie auf **Virtuelles Netzwerk**.
4. Geben Sie die erforderlichen Parameter an.
    - Unter **Ressourcengruppe** müssen Sie die Ressourcengruppe angeben, in der Sie das NetScaler VPX-Produkt bereitstellen möchten.
    - Unter **Standort** müssen Sie die Standorte angeben, die Verfügbarkeitszonen unterstützen, wie zum Beispiel:
        - Central US
        - East US2
        - France Central
        - Nordeuropa
        - Südostasien
        - Westeuropa
        - West US2

    HINWEIS

    Die Anwendungsserver, die in dieser Ressourcengruppe vorhanden sind.
5. Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter Azure Virtual Network in der Microsoft-Dokumentation.
Sicherheitsgruppen erstellen
Erstellen Sie drei Sicherheitsgruppen in Ihrem virtuellen Netzwerk (VNet) – jeweils eine für die Verwaltungs-, Client- und Serververbindungen. Erstellen Sie eine Sicherheitsgruppe, um den eingehenden und ausgehenden Datenverkehr in der NetScaler VPX-Instanz zu steuern. Sie können beliebig viele Regeln hinzufügen.

- **Verwaltung:** Eine Sicherheitsgruppe in Ihrem Konto, die für die Verwaltung von NetScaler VPX vorgesehen ist. NetScaler muss Azure-Dienste kontaktieren und benötigt Internetzugang. Eingehende Regeln sind auf den folgenden TCP- und UDP-Ports zulässig.
    - TCP: 80, 22, 443, 3008–3011, 4001

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- UDP: 67, 123, 161, 500, 3003, 4500, 7000

HINWEIS

Stellen Sie sicher, dass die Sicherheitsgruppe dem Agenten den Zugriff auf die VPX ermöglicht.

- **Client:** Eine Sicherheitsgruppe in Ihrem Konto, die für die clientseitige Kommunikation von NetScaler VPX-Instanzen vorgesehen ist. Typischerweise sind eingehende Regeln auf den TCP-Ports 80, 22 und 443 zugelassen.
- **Server:** Eine Sicherheitsgruppe in Ihrem Konto, die für die serverseitige Kommunikation von NetScaler VPX vorgesehen ist.

Weitere Informationen zum Erstellen einer Sicherheitsgruppe in Microsoft Azure finden Sie unter Erstellen, Ändern oder Löschen einer Netzwerksicherheitsgruppe.

Subnetze erstellen

Erstellen Sie drei Subnetze in Ihrem virtuellen Netzwerk (VNet) – jeweils eines für die Verwaltungs-, Client- und Serververbindungen. Geben Sie für jedes Subnetz einen Adressbereich an, der in Ihrem VNet definiert ist. Geben Sie die Verfügbarkeitszone an, in der sich das Subnetz befinden soll.

- **Verwaltung:** Ein Subnetz in Ihrem virtuellen Netzwerk (VNet), das für die Verwaltung vorgesehen ist. NetScaler muss Azure-Dienste kontaktieren und benötigt Internetzugang.
- **Client:** Ein Subnetz in Ihrem virtuellen Netzwerk (VNet), das für die Clientseite vorgesehen ist. Typischerweise empfängt NetScaler Client-Traffic für die Anwendung über ein öffentliches Subnetz aus dem Internet.
- **Server:** Ein Subnetz, in dem die Anwendungsserver bereitgestellt werden. Alle Ihre Anwendungsserver befinden sich in diesem Subnetz und empfangen Anwendungs-Traffic vom NetScaler über dieses Subnetz.

HINWEIS

Weisen Sie dem Subnetz beim Erstellen eine geeignete Sicherheitsgruppe zu.

Weitere Informationen zum Erstellen eines Subnetzes in Microsoft Azure finden Sie unter Hinzufügen, Ändern oder Löschen eines Subnetzes für ein virtuelles Netzwerk.

NetScaler VPX-Lizenz in Microsoft Azure abonnieren

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Melden Sie sich bei Ihrem Microsoft Azure-Portal an.
2. Wählen Sie **Ressource erstellen**.
3. Suchen Sie in der Leiste **Marketplace durchsuchen** nach `NetScaler` und wählen Sie die erforderliche Produktversion aus.
4. Wählen Sie in der Liste **Softwareplan auswählen** einen der folgenden Lizenztypen aus:

   - Eigene Lizenz mitbringen
   - Erweitert
   - Premium

   HINWEIS

   - Wenn Sie die Option **Eigene Lizenz mitbringen** wählen, ruft die Instanz, die Sie bereitstellen möchten, die Lizenzen von der NetScaler Console ab, während NetScaler-Instanzen bereitgestellt werden.
   - In der NetScaler Console sind **Erweitert** und **Premium** die entsprechenden Lizenztypen für **Enterprise** bzw. **Platinum**.

5. Stellen Sie sicher, dass die programmatische Bereitstellung für das ausgewählte NetScaler-Produkt aktiviert ist.

   a. Klicken Sie neben **Programmatisch bereitstellen?** auf **Erste Schritte**.

   NetScaler VPX programmatisch bereitstellen(/en-us/netscaler-console-service/media/select-software-plan-azure.png)

   b. Wählen Sie unter **Abonnements auswählen** die Option **Aktivieren**, um die ausgewählte NetScaler VPX Edition programmatisch bereitzustellen.

   Programmatische Bereitstellung aktivieren(/en-us/netscaler-console-service/media/subscription.png)

   WICHTIG

   Die Aktivierung der programmatischen Bereitstellung ist erforderlich, um NetScaler VPX-Instanzen in Azure bereitzustellen.

   c. Klicken Sie auf **Speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Schließen Sie **Programmatische Bereitstellung konfigurieren**.

6. Klicken Sie auf **Erstellen**.

Eine Anwendung erstellen und registrieren
NetScaler Console verwendet diese Anwendung, um NetScaler VPX-Instanzen in Azure bereitzustellen.

So erstellen und registrieren Sie eine Anwendung in Azure:

1. Wählen Sie im Azure-Portal **Azure Active Directory** aus. Diese Option zeigt das Verzeichnis Ihrer Organisation an.
2. Wählen Sie **App-Registrierungen** aus:

   a. Geben Sie unter **Name** den Namen der Anwendung an.

   b. Wählen Sie den **Anwendungstyp** aus der Liste aus.

   c. Geben Sie in der **Anmelde-URL** die Anwendungs-URL an, um auf die Anwendung zuzugreifen.

3. Klicken Sie auf **Erstellen**.

Weitere Informationen zu App-Registrierungen finden Sie in der Microsoft-Dokumentation.

Azure weist der Anwendung eine Anwendungs-ID zu. Das Folgende ist ein Beispiel für eine in Microsoft Azure registrierte Anwendung:

Kopieren Sie die folgenden IDs und geben Sie diese IDs an, wenn Sie ein Cloud Access Profile in NetScaler Console konfigurieren:

- **Anwendungs-ID:** Schritte zum Abrufen der Anwendungs- oder Client-ID.
- **Verzeichnis-ID:** Schritte zum Abrufen der Verzeichnis-, Mandanten- oder Objekt-ID.
- **Schlüssel:** Schritte zum Abrufen des Schlüsselwerts oder der Client-Geheimnis-ID.

- **Abonnement-ID:** Kopieren Sie die Abonnement-ID von Ihrem Speicherkonto.

Weitere Informationen finden Sie unter Microsoft-Dokumentation.
Zuweisen der Rollenberechtigung zu einer Anwendung
NetScaler Console verwendet das Prinzip „Anwendung als Dienst“, um NetScaler-Instanzen in Microsoft Azure bereitzustellen. Diese Berechtigung gilt nur für die ausgewählte Ressourcengruppe.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Um Ihrer registrierten Anwendung eine Rollenberechtigung zuzuweisen, müssen Sie der Besitzer des Microsoft Azure-Abonnements sein.

1. Wählen Sie im Azure-Portal **Ressourcengruppen** aus.
2. Wählen Sie die Ressourcengruppe aus, der Sie die Rollenberechtigung zuweisen möchten.
3. Wählen Sie **Zugriffssteuerung (IAM)** aus.
4. Klicken Sie unter **Rollenzuweisungen** auf **Hinzufügen**.
5. Wählen Sie **Besitzer** aus der Liste **Rolle** aus.
6. Wählen Sie die Anwendung aus, die für die Bereitstellung von NetScaler-Instanzen registriert ist. Siehe Eine Anwendung erstellen und registrieren.
7. Klicken Sie auf **Speichern**.

Einrichten eines NetScaler-Agenten

Installieren Sie einen Agenten im Verwaltungs-Subnetz. Dieser Agent fungiert als Vermittler zwischen der NetScaler Console und den verwalteten Instanzen in Microsoft Azure. Weitere Informationen zur Installation eines Agenten in Microsoft Azure finden Sie unter Installieren eines NetScaler-Agenten in der Microsoft Azure Cloud.

EINRICHTEN VON NETSCALER CONSOLE-KOMPONENTEN

Führen Sie die folgenden Aufgaben in Azure aus, bevor Sie NetScaler VPX-Instanzen in NetScaler Console bereitstellen:

1. Erstellen Sie eine Site.
2. Verbinden Sie die Site mit einem Citrix Service Agent.

Erstellen einer Site in NetScaler Console

Erstellen Sie eine Site in NetScaler Console und fügen Sie die VNet-Details hinzu, die Ihrer Microsoft Azure-Ressourcengruppe zugeordnet sind.

1. Navigieren Sie in NetScaler Console zu **Infrastruktur > Instanzen > Sites**.
2. Klicken Sie auf **Hinzufügen**.
3. Im Bereich **Cloud auswählen**,
    a. Wählen Sie **Datencenter** als **Sitetyp**.
    b. Wählen Sie **Azure** aus der **Typ**-Liste.
    c. Aktivieren Sie das Kontrollkästchen **VNet von Azure abrufen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Diese Option hilft Ihnen, die vorhandenen VNet-Informationen aus Ihrem Microsoft Azure-Konto abzurufen.

d. Klicken Sie auf **Weiter**.

4. Im Bereich **Region auswählen**,

a. Wählen Sie unter **Cloud-Zugriffsprofil** das für Ihr Microsoft Azure-Konto erstellte Profil aus. Wenn keine Profile vorhanden sind, erstellen Sie ein Profil.

b. Um ein Cloud-Zugriffsprofil zu erstellen, klicken Sie auf **Hinzufügen**.

c. Geben Sie unter **Name** einen Namen an, um Ihr Azure-Konto in NetScaler Console zu identifizieren.

d. Geben Sie unter **Mandanten-Active Directory-ID / Mandanten-ID** die Active Directory-ID des Mandanten oder des Kontos in Microsoft Azure an.

e. Geben Sie die **Abonnement-ID** an.

f. Geben Sie die **Anwendungs-ID/Client-ID** an.

g. Geben Sie das **Anwendungsschlüssel-Passwort / Geheimnis** an.

h. Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter Erstellen und Registrieren einer Anwendung und Zuordnen des Cloud-Zugriffsprofils zur Azure-Anwendung.

Cloud-Zugriffsprofil erstellen(/en-us/netscaler-console-service/media/create-cloud-access-profile.png)

i. Wählen Sie unter **VNet** das virtuelle Netzwerk aus, das die NetScaler VPX-Instanzen enthält, die Sie verwalten möchten.

j. Geben Sie einen **Site-Namen** an.

k. Klicken Sie auf **Fertig stellen**.

Zuordnung des Cloud-Zugriffsprofils zur Azure-Anwendung

NETSCALER CONSOLE-BEGRIFF	MICROSOFT AZURE-BEGRIFF
Mandanten-Active Directory-ID / Mandanten-ID	Verzeichnis-ID
Abonnement-ID	Abonnement-ID
Anwendungs-ID/Client-ID	Anwendungs-ID

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETSCALER CONSOLE-BEGRIFF	MICROSOFT AZURE-BEGRIFF
Anwendungsschlüssel-Passwort / Geheimnis	Schlüssel oder Zertifikate oder Client-Geheimnisse

Site an einen Agenten anfügen

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Instances > Agents**.
2. Wählen Sie den Agenten aus, dem Sie eine Site anfügen möchten.
3. Klicken Sie auf **Site anfügen**.
4. Wählen Sie die Site aus der Liste aus, die Sie anfügen möchten.
5. Klicken Sie auf **Speichern**.

Konfigurationsaufgaben

Verwenden Sie die Site, die Sie Ihrer Microsoft Azure-Ressourcengruppe zugeordnet haben, um die NetScaler VPX-Instanzen bereitzustellen. Geben Sie die Agentendetails an, um die Instanzen bereitzustellen, die an diesen Agenten gebunden sind.

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Instances > NetScaler**.
2. Klicken Sie auf der Registerkarte **VPX** auf **Bereitstellen**.

   Diese Option zeigt die Seite **NetScaler VPX in der Cloud bereitstellen** an.
3. Wählen Sie **Microsoft Azure** aus und klicken Sie auf **Weiter**. Geben Sie die erforderlichen Parameter an, um eine Instanz bereitzustellen.

GRUNDLEGENDE PARAMETER KONFIGURIEREN

1. Geben Sie auf der Registerkarte **Grundlegende Parameter** Folgendes an:
   - **Instanztyp**: Wählen Sie eine der folgenden Optionen aus der Liste aus.
     - **Standalone** – Diese Option stellt eine eigenständige NetScaler VPX-Instanz in Microsoft Azure bereit.
     - **HA:** Diese Option stellt die Hochverfügbarkeits-NetScaler VPX-Instanzen in Microsoft Azure bereit.

       Um die NetScaler VPX-Instanzen in derselben Zone bereitzustellen, wählen Sie die Option **Single Zone** unter **Zone Type**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Um die NetScaler VPX-Instanzen über mehrere Zonen hinweg bereitzustellen, wählen Sie die Option **Multi Zone** unter **Zone type**. Stellen Sie auf der Registerkarte **Cloud Parameters** sicher, dass Sie die Netzwerkdetails für jede Zone angeben, die in Microsoft Azure erstellt werden.

- **Name** – Geben Sie den Namen einer NetScaler VPX-Instanz an.
- **Site** – Wählen Sie die zuvor erstellte Site aus.
- **Agent** – Wählen Sie den Agenten aus, der zur Verwaltung der NetScaler VPX-Instanz erstellt wurde.
- **Cloud Access Profile** – Wählen Sie das Cloud-Zugriffsprofil aus, das während der Site-Erstellung erstellt wurde.
- **NetScaler Profile** – Wählen Sie das Profil zur Authentifizierung aus.

  NetScaler Console verwendet das Geräteprofil, wenn es sich bei der NetScaler VPX-Instanz anmelden muss.

  HINWEIS

  Stellen Sie sicher, dass das ausgewählte Geräteprofil den Microsoft Azure-Kennwortregeln entspricht.

2. Klicken Sie auf **Weiter**.

LIZENZEN KONFIGURIEREN

Wählen Sie einen der folgenden Modi aus, um eine Lizenz auf eine NetScaler-Instanz anzuwenden:

- **Verwenden von NetScaler Console**: Die Instanz, die Sie bereitstellen möchten, ruft die Lizenzen von der NetScaler Console ab.
- **Verwenden von Microsoft Azure**: Die Option **Aus Cloud zuweisen** verwendet die im Azure Marketplace verfügbaren NetScaler®-Produktlizenzen. Die Instanz, die Sie bereitstellen möchten, verwendet die Lizenzen vom Marketplace.

  Wenn Sie Lizenzen vom Azure Marketplace verwenden möchten, geben Sie das Produkt oder die Lizenz auf der Registerkarte **Bereitstellungsparameter** an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen finden Sie unter Lizenzierungsanforderungen.

LIZENZEN VON NETSCALER CONSOLE VERWENDEN

Um diese Option zu verwenden, stellen Sie sicher, dass Sie das NetScaler-Produkt mit dem Softwareplan **Eigene Lizenz mitbringen** in Azure abonniert haben. Siehe NetScaler VPX-Lizenz in Microsoft Azure abonnieren.

1. Wählen Sie auf der Registerkarte **Lizenz** die Option **Von NetScaler Console zuweisen** aus.
2. Wählen Sie unter **Lizenztyp** eine der folgenden Optionen aus der Liste aus:

   - **Bandbreitenlizenzen:** Sie können eine der folgenden Optionen aus der Liste **Bandbreitenlizenztypen** auswählen:

     - **Gepoolte Kapazität:** Geben Sie die Kapazität an, die einer Instanz zugewiesen werden soll.

       Aus dem gemeinsamen Pool ruft die NetScaler-Instanz eine Instanzlizenz und nur die angegebene Bandbreite ab.

     - **VPX-Lizenzen:** Wenn eine NetScaler VPX-Instanz bereitgestellt wird, ruft die Instanz die Lizenz von der NetScaler Console ab.

   - **Virtuelle CPU-Lizenzen:** Die bereitgestellte NetScaler VPX-Instanz ruft Lizenzen ab, abhängig von der Anzahl der in der Instanz ausgeführten CPUs.

   HINWEIS

   Wenn die bereitgestellten Instanzen entfernt oder zerstört werden, kehren die angewendeten Lizenzen in den NetScaler Console-Lizenzpool zurück. Diese Lizenzen können zur Bereitstellung neuer Instanzen wiederverwendet werden.

3. Wählen Sie unter **Lizenzedition** die Lizenzedition aus. Die NetScaler Console verwendet die angegebene Edition, um Instanzen bereitzustellen.
4. Klicken Sie auf **Weiter**.

BEREITSTELLUNGSPARAMETER KONFIGURIEREN

1. Geben Sie auf der Registerkarte **Bereitstellungsparameter** Folgendes an:

   a. Wählen Sie die **Ressourcengruppe** aus, in der Sie die NetScaler VPX-Instanz bereitstellen möchten.

   b. Wählen Sie die unterstützte **VM-Größe** aus der Liste aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Diese Liste zeigt die unterstützten VM-Größen für das ausgewählte NetScaler-Produkt an.

c. Wählen Sie das Cloud Access Profile für NetScaler aus.

d. Wählen Sie die **Version** von NetScaler aus, die Sie bereitstellen möchten. Wählen Sie sowohl die **Haupt-** als auch die **Nebenversion** von NetScaler aus.

e. Wählen Sie unter **Sicherheitsgruppen** die Sicherheitsgruppen für Management, Client und Server aus, die Sie in Ihrem virtuellen Netzwerk erstellt haben.

f. Geben Sie unter **Subnetze** die erforderliche Anzahl von Verfügbarkeitszonen in Azure an.

g. Wählen Sie unter **Subnetze** die Subnetze für Management, Client und Server aus, die Sie in Ihrem virtuellen Netzwerk erstellt haben.

h. Klicken Sie auf **Fertig stellen**.

Die NetScaler VPX-Instanz ist jetzt in Microsoft Azure bereitgestellt.

Bereitgestellte NetScaler VPX-Instanzen anzeigen

Anzeigen in NetScaler Console:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Instances > NetScaler**.
2. Wählen Sie die Registerkarte **NetScaler VPX** aus.

   Die in Microsoft Azure bereitgestellte NetScaler VPX-Instanz wird hier aufgeführt.

Anzeigen in Microsoft Azure:

1. Melden Sie sich bei Ihrem Azure-Portal an.
2. Navigieren Sie zu der Ressourcengruppe, die zur Bereitstellung der NetScaler VPX-Instanz erstellt wurde.

   Diese Seite zeigt die bereitgestellte NetScaler VPX-Instanz an.

HINWEIS

Der Name der NetScaler VPX-Instanz ist derselbe, den Sie bei der Bereitstellung einer Instanz in der NetScaler Console angegeben haben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bereitstellen von NetScaler VPX-Instanzen in Google Cloud

Anwendungen oder Dienste, die in Google Cloud gehostet werden, erfordern eine sichere Datenverkehrsverwaltung und eine effiziente Optimierung der Netzwerkressourcen zusammen mit den Vorteilen der Cloud. NetScaler VPX-Instanzen, die in Google Cloud bereitgestellt werden, bieten eine sichere Datenverkehrsverwaltung, optimierten Ressourcenverbrauch und reduzierte Betriebskosten für Webanwendungen.

NetScaler Console ermöglicht Ihnen die Automatisierung der Bereitstellung, Einrichtung und Verwaltung der NetScaler VPX-Instanzen in Google Cloud. Die Bereitstellung von NetScaler VPX-Instanzen mit NetScaler Console kombiniert die Elastizität und Flexibilität der Cloud mit den Steuerungsfunktionen von NetScaler.

NetScaler Console-Bereitstellungsarchitektur

Die folgende Abbildung bietet einen Überblick darüber, wie NetScaler Console mit Google Cloud verbunden ist, um NetScaler VPX-Instanzen in Google Cloud bereitzustellen.

Sie benötigen drei Virtual Private Cloud (VPC)-Netzwerke, um die NetScaler VPX-Instanz in Google Cloud bereitzustellen und zu verwalten. Ein VPC-Netzwerk enthält ein Subnetz und eine Firewall. Die Firewall verfügt über Regeln, die den eingehenden und ausgehenden Datenverkehr zu einem Subnetz steuern.

Der Agent hilft Ihnen, die NetScaler VPX-Instanz bereitzustellen und zu verwalten.

Voraussetzungen

Dieser Abschnitt beschreibt die Voraussetzungen, die Sie in Google Cloud und NetScaler Console erfüllen müssen, bevor Sie NetScaler VPX-Instanzen bereitstellen.

Dieses Dokument geht davon aus, dass Sie über ein Google Cloud-Konto verfügen. Weitere Informationen zum Erstellen eines Kontos finden Sie unter Google Cloud-Dokumentation.

GOOGLE CLOUD-KOMPONENTEN EINRICHTEN

Bevor Sie NetScaler VPX-Instanzen in NetScaler Console bereitstellen, führen Sie die folgenden Aufgaben in Google Cloud aus:

1. APIs aktivieren
2. Dienstkonto erstellen
3. Ein VPC-Netzwerk erstellen
4. Eine Firewall erstellen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Die NetScaler VPX-Lizenz in Google Cloud abonnieren

APIs aktivieren

NetScaler Console erfordert programmatischen Zugriff, um die erforderlichen Ressourcen in Google Cloud bereitzustellen und zu provisionieren. Aktivieren Sie daher die folgenden APIs in Ihrem Google Cloud-Projekt:

- Compute Engine API
- Cloud DNS API

Weitere Informationen zum Aktivieren von APIs in Google Cloud finden Sie unter APIs aktivieren.

Ein Dienstkonto erstellen

Die NetScaler Console verwendet ein Dienstkonto, um auf Ihre Google Cloud-Ressourcen zuzugreifen. Gehen Sie wie folgt vor, um ein Dienstkonto zu erstellen:

1. Melden Sie sich bei Ihrem Google Cloud-Konto an.
2. Gehen Sie zu **IAM & Admin > Dienstkonten**.
3. Klicken Sie auf **+DIENSTKONTO ERSTELLEN**.

   Erstellen Sie zwei Dienstkonten, ein Dienstkonto wird für NetScaler Console verwendet. Und ein weiteres wird für NetScaler-Instanzen verwendet. Führen Sie die folgenden Schritte aus, um ein Dienstkonto zu erstellen.

   a. Geben Sie den Namen, die ID und die Beschreibung an und klicken Sie auf Erstellen.
   b. Weisen Sie die folgenden vordefinierten Rollen zu:

      - Für NetScaler Console erforderliche IAM-Rollen

        ```
        roles/iam.serviceAccountUser

        roles/compute.instanceAdmin.v1

        roles/compute.networkAdmin

        roles/dns.admin
        ```

      - Für die von NetScaler Console erstellten NetScaler-Instanzen erforderliche IAM-Rollen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
roles/compute.instanceAdmin.v1

roles/compute.networkAdmin
```

Diese Rollen ermöglichen Ihrem Dienstkonto den Zugriff auf Google Cloud-Ressourcen.

c. Klicken Sie auf **Fertig**.

Ein VPC-Netzwerk erstellen

Erstellen Sie drei Subnetze in Ihrem VPC-Netzwerk – jeweils eines für die Verwaltungs-, Client- und Serververbindungen. Wählen Sie die benutzerdefinierte Option, um ein Subnetz zu erstellen. Geben Sie einen Adressbereich für jedes der Subnetze an. Geben Sie die Region an, in der sich das Subnetz befinden soll.

- **Verwaltung**: Ein Subnetz in Ihrem Verwaltungs-VPC-Netzwerk, das für die Verwaltung vorgesehen ist. NetScaler muss Google Cloud-Dienste kontaktieren und benötigt Internetzugang.
- **Client**: Ein Subnetz in Ihrem Client-VPC-Netzwerk, das für die Clientseite vorgesehen ist. Typischerweise empfängt NetScaler Client-Traffic für die Anwendung über ein öffentliches Subnetz aus dem Internet.
- **Server**: Ein Subnetz, in dem die Anwendungsserver bereitgestellt werden. Alle Ihre Anwendungsserver befinden sich in diesem Subnetz und empfangen Anwendungs-Traffic vom NetScaler über dieses Subnetz. Weitere Informationen zum Erstellen eines Subnetzes in Google Cloud finden Sie unter VPC-Netzwerkübersicht.

Eine Firewall erstellen

Die Firewall verfügt über Regeln, die den eingehenden und ausgehenden Datenverkehr in der NetScaler VPX-Instanz steuern. Sie können beliebig viele Regeln hinzufügen. Um NetScaler-Instanzen automatisch zu skalieren, müssen Sie drei Firewalls erstellen:

- **Verwaltung**: Eine Firewall ist für die Verwaltung von NetScaler VPX vorgesehen. NetScaler muss Google Cloud-Dienste kontaktieren und benötigt Internetzugang. Eingehende Regeln sind für die folgenden TCP- und UDP-Ports zulässig.
  - TCP: 80, 22, 443, 3008–3011, 4001, 27000, 7279
  - UDP: 67, 123, 161, 500, 3003, 4500, 7000

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Stellen Sie sicher, dass die Firewall dem Agenten den Zugriff auf die VPX ermöglicht.

- **Client**: Eine Firewall ist für die clientseitige Kommunikation von NetScaler VPX-Instanzen vorgesehen. Typischerweise sind eingehende Regeln auf den TCP-Ports 80, 22 und 443 zugelassen.
- **Server**: Eine Firewall ist für die serverseitige Kommunikation von NetScaler VPX vorgesehen. Weitere Informationen zum Erstellen einer Firewall in Google Cloud finden Sie unter Übersicht über VPC-Firewallregeln.

NetScaler VPX-Lizenz in Google Cloud abonnieren

1. Melden Sie sich bei Ihrem Google Cloud-Portal an.
2. Suchen Sie im **Marketplace** nach NetScaler und wählen Sie die erforderliche Produktversion aus.
3. Wählen Sie einen der folgenden Lizenztypen aus:
    - Kundenlizenziert
    - Enterprise
    - Platinum

HINWEIS

Wenn Sie die Option **Kundenlizenziert** auswählen, ruft die Autoscale-Gruppe die Lizenzen von der NetScaler Console ab, während NetScaler-Instanzen bereitgestellt werden.

NETSCALER CONSOLE-KOMPONENTEN EINRICHTEN

Bevor Sie NetScaler VPX-Instanzen in NetScaler Console bereitstellen, führen Sie die folgenden Aufgaben in NetScaler Console aus:

1. Einen Standort erstellen.
2. NetScaler-Agent in Google Cloud bereitstellen.
3. Den Standort an einen NetScaler-Agenten anfügen.

Einen Standort erstellen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Erstellen Sie einen Standort in der NetScaler Console und fügen Sie die VNet-Details hinzu, die mit Ihrer Google Cloud verknüpft sind.

1. Navigieren Sie in der NetScaler Console zu **Infrastructure > Sites**.
2. Klicken Sie auf **Hinzufügen**.
3. Im Bereich **Cloud auswählen**,
    a. Wählen Sie **Data Center** als Standorttyp aus.
    b. Wählen Sie **Google Cloud** aus der Liste „Typ“ aus.
    c. Aktivieren Sie das Kontrollkästchen **Regionen aus der Google Cloud abrufen**.

        Diese Option hilft Ihnen, die vorhandenen Regionsinformationen aus Ihrem Google Cloud-Konto abzurufen.
    d. Klicken Sie auf **Weiter**.
4. Im Bereich **Region auswählen**,
    a. Wählen Sie unter **Cloud Access Profile** das für Ihr Google Cloud-Konto erstellte Profil aus. Wenn keine Profile vorhanden sind, erstellen Sie ein Profil.
    b. Um ein Cloud-Zugriffsprofil zu erstellen, klicken Sie auf **Hinzufügen**.
    c. Geben Sie unter **Name** einen Namen ein, um Ihr Google Cloud-Konto in NetScaler Console zu identifizieren.
    d. Geben Sie unter **Schlüssel des Dienstkontos** das in Google Cloud erstellte Dienstkonto-JSON an.

    e. Klicken Sie auf **Erstellen**.

        Weitere Informationen finden Sie unter Dienstkonto erstellen.
    f. Wählen Sie unter **Regionen** die Region aus, die das VPC-Netzwerk mit den NetScaler VPX-Instanzen enthält, die Sie verwalten möchten.
    g. Geben Sie einen **Site-Namen** an.
    h. Klicken Sie auf **Fertig stellen**.

NetScaler-Agent in Google Cloud bereitstellen

Der Agent fungiert als Vermittler zwischen der NetScaler Console und den erkannten Instanzen im Rechenzentrum oder in der Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie zu **Infrastruktur > Instanzen > Agents**.
2. Klicken Sie auf **Bereitstellen**.
3. Wählen Sie **Google Cloud** aus und klicken Sie auf **Weiter**.
4. Geben Sie auf der Registerkarte **Bereitstellungsparameter** Folgendes an:
    - **Name** – Geben Sie den Agentennamen an.
    - **Site** – Wählen Sie die Site aus, die Sie zum Bereitstellen eines Agenten und von NetScaler VPX-Instanzen erstellt haben.
    - **Cloud Access Profile** – Wählen Sie das Cloud-Zugriffsprofil aus der Liste aus.
    - **Zone** – Wählen Sie die Zonen aus, in denen Sie die Autoscale™-Gruppen erstellen möchten. Abhängig vom ausgewählten Cloud-Zugriffsprofil werden die Zonen dieses Profils ausgefüllt.
    - **Netzwerk** – Wählen Sie das VPC-Netzwerk aus, in dem Sie Autoscale-Gruppen erstellen möchten.
    - **Subnetz** – Wählen Sie das Verwaltungs-Subnetz aus, um einen Agenten bereitzustellen.
    - **Tags** – Geben Sie das Schlüssel-Wert-Paar für die Autoscale-Gruppen-Tags ein. Ein Tag besteht aus einem Groß-/Kleinschreibung-sensitiven Schlüssel-Wert-Paar. Diese Tags ermöglichen es Ihnen, die Autoscale-Gruppen einfach zu organisieren und zu identifizieren. Die Tags werden sowohl auf Google Cloud als auch auf NetScaler Console angewendet.
5. Klicken Sie auf **Fertig stellen**.

Alternativ können Sie den Agenten über den Google Cloud Marketplace installieren. Weitere Informationen finden Sie unter Installieren eines NetScaler-Agenten in der Google Cloud.
Site an einen NetScaler-Agenten anfügen

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Instances > Agents**.
2. Wählen Sie den Agenten aus, dem Sie eine Site anfügen möchten.
3. Klicken Sie auf **Site anfügen**.
4. Wählen Sie die Site aus der Liste aus, die Sie anfügen möchten.
5. Klicken Sie auf **Speichern**.

Konfigurationsaufgaben

Führen Sie die folgenden Schritte aus, um eine eigenständige NetScaler VPX-Instanz in Google Cloud bereitzustellen:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Instances > NetScaler**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Klicken Sie auf **Bereitstellen**.
3. Wählen Sie **Google Cloud** aus und klicken Sie auf **Weiter**. Geben Sie die erforderlichen Parameter an, um eine Instanz bereitzustellen.
4. Geben Sie die Basiskonfiguration, Lizenzen und Bereitstellungsparameter an.

BASISKONFIGURATION KONFIGURIEREN

1. Geben Sie auf der Registerkarte **Basiskonfiguration** Folgendes an:

   - **Name** — Geben Sie den Namen einer NetScaler VPX-Instanz an.
   - **Site** — Wählen Sie die zuvor erstellte Site aus.
   - **Agent** — Wählen Sie den Agenten aus, der zur Verwaltung der NetScaler VPX-Instanz erstellt wurde.
   - **Cloud Access Profile** — Wählen Sie das Cloud-Zugriffsprofil aus, das während der Site-Erstellung erstellt wurde.
   - **NetScaler Profile** — Wählen Sie das Profil zur Bereitstellung der Authentifizierung aus.

     NetScaler Console verwendet das Geräteprofil, wenn es sich bei der NetScaler VPX-Instanz anmelden muss.

2. Klicken Sie auf **Weiter**.

LIZENZEN KONFIGURIEREN

Wählen Sie einen der folgenden Modi aus, um eine Lizenz auf eine NetScaler-Instanz anzuwenden:

- **Verwenden von NetScaler Console**: Die Instanz, die Sie bereitstellen möchten, ruft die Lizenzen von der NetScaler Console ab.
- **Verwenden von Google Cloud**: Die Option **Aus Cloud zuweisen** verwendet die NetScaler®-Produktlizenzen, die im Google Cloud Marketplace verfügbar sind. Die Instanz, die Sie bereitstellen möchten, verwendet die Lizenzen vom Marketplace.

  Wenn Sie Lizenzen aus dem Google Cloud Marketplace verwenden möchten, geben Sie das Produkt oder die Lizenz auf der Registerkarte **Bereitstellungsparameter** an.

Weitere Informationen finden Sie unter Lizenzierungsanforderungen.
Lizenzen von NetScaler Console verwenden

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Um diese Option zu verwenden, stellen Sie sicher, dass Sie das NetScaler-Produkt mit dem Softwareplan **Eigene Lizenz mitbringen** in Google Cloud abonniert haben. Siehe Abonnieren der NetScaler VPX-Lizenz in Google Cloud.

1. Wählen Sie auf der Registerkarte **Lizenz** die Option **Aus NetScaler Console zuweisen**.
2. Wählen Sie unter **Lizenztyp** eine der folgenden Optionen aus der Liste aus:

   - **Bandbreitenlizenzen:** Sie können eine der folgenden Optionen aus der Liste **Bandbreitenlizenztypen** auswählen:

     - **Gepoolte Kapazität:** Geben Sie die Kapazität an, die einer Instanz zugewiesen werden soll.

       Aus dem gemeinsamen Pool ruft die NetScaler-Instanz eine Instanzlizenz und nur die angegebene Bandbreite ab.

     - **VPX-Lizenzen:** Wenn eine NetScaler VPX-Instanz bereitgestellt wird, ruft die Instanz die Lizenz von der NetScaler Console ab.

   - **Lizenzen für virtuelle CPUs:** Die bereitgestellte NetScaler VPX-Instanz ruft Lizenzen ab, abhängig von der Anzahl der in der Instanz laufenden CPUs.

   HINWEIS

   Wenn die bereitgestellten Instanzen entfernt oder zerstört werden, kehren die angewendeten Lizenzen in den NetScaler Console-Lizenzpool zurück. Diese Lizenzen können zur Bereitstellung neuer Instanzen wiederverwendet werden.

3. Wählen Sie unter **Lizenz-Edition** die Lizenz-Edition aus. Die NetScaler Console verwendet die angegebene Edition, um Instanzen bereitzustellen.
4. Klicken Sie auf **Weiter**.

BEREITSTELLUNGSPARAMETER KONFIGURIEREN

1. Geben Sie auf der Registerkarte **Bereitstellungsparameter** Folgendes an:

   - **NetScaler-Dienstkonto**: Wählen Sie das Dienstkonto aus, das Sie in Google Cloud erstellt haben. Die NetScaler Console verwendet ein Dienstkonto, um auf Ihre Google Cloud-Ressourcen zuzugreifen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Produkt/Lizenz**: Wählen Sie die NetScaler-Produktversion aus, die Sie bereitstellen möchten. Weitere Informationen finden Sie unter Abonnieren der NetScaler VPX-Lizenz in Google Cloud.
- **Maschinentypen**: Wählen Sie den erforderlichen Maschinentyp aus der Liste aus.

  Diese Liste zeigt die unterstützten Maschinentypen für das ausgewählte NetScaler-Image an.
- **Image**: Wählen Sie das erforderliche NetScaler-Versions-Image aus. Klicken Sie auf **Neu hinzufügen**, um ein NetScaler-Image hinzuzufügen.
- **Konfigurationsvorlage** – Wählen Sie die Konfigurationsvorlage aus, die Sie für die Bereitstellung auf den NetScaler-Instanzen verwenden möchten.
- **IPs im Server-Subnetz pro Instanz** – Geben Sie an, wie viele SNIP-Adressen jede Instanz im Server-Subnetz haben kann.

Auf dieser Registerkarte können Sie auch die erforderlichen NICs angeben und konfigurieren. Jede NIC enthält eine dedizierte Firewall und ein Subnetz.

Weitere Informationen finden Sie unter VPC-Netzwerk erstellen und Firewall erstellen.

2. Klicken Sie auf **Fertig stellen**.

Bereitgestellte NetScaler VPX-Instanzen anzeigen

Anzeige in NetScaler Console:

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Instances > NetScaler**.
2. Wählen Sie die Registerkarte **NetScaler VPX** aus.

   Die in Google Cloud bereitgestellte NetScaler VPX-Instanz wird hier aufgelistet.

Anzeige in Google Cloud:

1. Melden Sie sich bei Ihrem Google Cloud-Portal an.
2. Navigieren Sie zur Registerkarte **Resources**, die die bereitgestellte NetScaler VPX-Instanz anzeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Der Name der NetScaler VPX-Instanz ist derselbe, den Sie bei der Bereitstellung einer Instanz in der NetScaler Console angegeben haben.

NetScaler VPX-Instanzen auf VMware ESX bereitstellen

Sie können NetScaler Console verwenden, um die Bereitstellung und Verwaltung einer NetScaler VPX-Instanz in VMware ESX zu automatisieren. Wenn Sie NetScaler Console verwenden, um eine NetScaler VPX-Instanz auf VMware ESX bereitzustellen, ist die Instanz sofort in der NetScaler Console-GUI zur Verwaltung verfügbar.

Die NetScaler Console verwendet NetScaler-Vorlagen der bereits bereitgestellten Instanzen, um eine neue Instanz in VMware ESX bereitzustellen. Sie speichert das Datencenter des VMware vCenter, in dem die erforderlichen VMware ESX-Serverdetails vorhanden sind, an einem Standort. Außerdem verwendet sie ein Cloud-Zugriffsprofil, um auf das VMware vCenter zuzugreifen und die VPX auf dem VMware ESX bereitzustellen.

Voraussetzungen

Bevor Sie eine NetScaler VPX-Instanz in VMware ESX bereitstellen, stellen Sie sicher, dass Sie Folgendes abgeschlossen haben:

1. Installieren Sie eine unterstützte VMware ESXi-Version (6.0, 6.5 und 6.7).
2. Installieren Sie VMware Client auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.
3. Laden Sie die NetScaler VPX-Setup-Dateien herunter.
4. Konvertieren Sie NetScaler VPX-Dateien in Vorlagen in ESX.
5. Erstellen Sie Berechtigungen für NetScaler Console, um auf VMware vCenter zuzugreifen.
6. Erstellen Sie einen Standort in NetScaler Console.

NetScaler VPX-Dateien in Vorlagen konvertieren

Die NetScaler Console verwendet die in ESX konvertierte NetScaler-Vorlage aus einer NetScaler VPX-Datei. Führen Sie die folgenden Schritte aus, um VPX-Dateien in Vorlagen zu konvertieren.

1. Stellen Sie eine NetScaler VPX-Instanz auf VMware mithilfe der NetScaler-Setup-Dateien bereit.

   Verwenden Sie zum ersten Mal NetScaler-Setup-Dateien, um die VPX-Instanz bereitzustellen. Weitere Informationen finden Sie unter NetScaler VPX-Instanz auf VMware installieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Klicken Sie mit der rechten Maustaste auf die bereitgestellte VM und wählen Sie **Vorlage**.
3. Klicken Sie auf **In Vorlage konvertieren**.

Berechtigungen für NetScaler Console zum Zugriff auf VMware vCenter erstellen

Um NetScaler Console für die Bereitstellung und Verwaltung in VMware vCenter zu aktivieren, führen Sie die folgenden Schritte aus:

1. Erstellen Sie eine benutzerdefinierte Rolle mit Berechtigungen
    a. Melden Sie sich bei VMware vCenter an und navigieren Sie zum Abschnitt **Rollen**.
    b. Erstellen Sie eine benutzerdefinierte Rolle, die auf NetScaler Console zugeschnitten ist.
    c. Weisen Sie die folgenden Berechtigungen zu:

```
Datastore.AllocateSpace

Resource.AssignVMToPool

VirtualMachine.Config.AdvancedConfig

VirtualMachine.Inventory.CreateFromExisting

VirtualMachine.Inventory.Delete

VirtualMachine.Interact.PowerOff

VirtualMachine.Interact.PowerOn

VirtualMachine.Provisioning.DeployTemplate
```

2. Einen Benutzer erstellen
    a. Sobald die Rolle definiert ist, navigieren Sie zum Abschnitt **Benutzer und Gruppen**.
    b. Erstellen Sie einen Benutzer für NetScaler Console, um auf das VMware vCenter zuzugreifen.
    c. Geben Sie ein Kennwort für den neu erstellten Benutzer an.
3. Die Rolle dem Benutzer zuordnen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Navigieren Sie zum Abschnitt **Globale Berechtigungen** und ordnen Sie die benutzerdefinierte Rolle dem Benutzer zu.

b. Diese Zuordnung bietet NetScaler Console Berechtigungen, um die erforderlichen Aktionen in VMware vCenter auszuführen.

HINWEIS:

Die aufgeführten Berechtigungen sind die Mindestanforderungen für NetScaler Console, um auf VMware vCenter zuzugreifen. Das Erstellen eines Benutzers mit eingeschränkten Berechtigungen ist optional. Wenn ein Benutzer Berechtigungen besitzt, die eine Obermenge der angegebenen Berechtigungen umfassen, kann dieser Benutzer stattdessen diese Anmeldeinformationen angeben.

Weitere Informationen zum Konfigurieren von Benutzerrollen mit Berechtigungen in VMware vCenter finden Sie unter Benutzerzugriff konfigurieren.

Eine Site in NetScaler Console erstellen

Erstellen Sie eine Site in NetScaler Console und fügen Sie die VMware ESX-Details hinzu.

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Instances > Sites**.
2. Klicken Sie auf **Hinzufügen**.
3. Im Bereich **Cloud auswählen**:
   a. Wählen Sie **Data Center** als **Sitetyp** aus.
   b. Wählen Sie **VMware vCenter** aus der Liste **Typ** aus.
   c. Klicken Sie auf **Weiter**.
4. Im Bereich **Region auswählen**:
   a. Wählen Sie im Bereich **Cloud-Zugriffsprofil** das für Ihr VMware ESX erstellte Profil aus. Wenn keine Profile vorhanden sind, erstellen Sie ein Profil.
   b. Um ein Cloud-Zugriffsprofil zu erstellen, klicken Sie auf **Hinzufügen** und geben Sie Folgendes an:
      - **Name** – Geben Sie einen Namen an, um Ihr Cloud-Zugriffsprofil in NetScaler Console zu identifizieren.
      - **IP-Adresse** – Geben Sie die IP-Adresse des VMware vCenter an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Benutzername** – Geben Sie den Benutzernamen für den Zugriff auf das VMware vCenter an.
- **Passwort** – Geben Sie das Passwort für den Zugriff auf das VMware vCenter an und bestätigen Sie das Passwort.
- **Agent** – Wählen Sie den Agenten aus, der bei NetScaler Console registriert ist.

c. Wählen Sie unter **Netzwerk (Datacenter)** das Datencenter aus, in dem sich Ihre NetScaler VPX-Vorlagen befinden.

d. Geben Sie den **Site-Namen** an.

e. Geben Sie die **Region**, den **Breitengrad** und den **Längengrad** an, um den geografischen Standort Ihres Datencenters zu identifizieren.

f. Klicken Sie auf **Fertig stellen**.

NetScaler VPX-Instanz auf VMware ESX bereitstellen

Verwenden Sie die Site, die Sie Ihrem VMware ESX zugeordnet haben, um die NetScaler VPX-Instanzen bereitzustellen.

HINWEIS:

Derzeit unterstützt die NetScaler Console nur die Bereitstellung von eigenständigen NetScaler-Instanzen.

1. Navigieren Sie in NetScaler Console zu **Infrastructure > Instances > NetScaler**.
2. Klicken Sie auf der Registerkarte **VPX** auf **Provision**.

   Diese Option zeigt die Seite **Provision NetScaler VPX on Cloud** an.
3. Wählen Sie auf der Registerkarte **Choose Cloud** die Option **VMware vCenter** aus und klicken Sie auf **Next**.

4. Geben Sie auf der Registerkarte **Basic Parameters** Folgendes an:

   - **Name** – Geben Sie den Namen einer Instanz an.
   - **Site** – Wählen Sie den zuvor erstellten Standort aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Cloud Access Profile** – Wählen Sie das Cloud-Zugriffsprofil aus, das während der Standorterstellung erstellt wurde.
- **NetScaler profile** – Wählen Sie das NetScaler-Profil zur Authentifizierung aus.

5. Klicken Sie auf **Next**.
6. Auf der Registerkarte **License** wird die Option **Allocate from Cloud** automatisch ausgewählt und verwendet die in VMware vCenter verfügbaren NetScaler-Produktlizenzen. Die VPX-Instanz, die Sie bereitstellen möchten, verwendet Lizenzen aus dem VMware vCenter.

   a. **License Type** – Wählen Sie den Lizenztyp als Bandbreiten- oder virtuelle CPU-Lizenzen aus.

      i. Für den Bandbreitenlizenztyp können Sie eine der folgenden Optionen aus der Liste **Bandwidth License Type** auswählen:

         - **Gepoolte Kapazität** – Geben Sie die Kapazität an, die einer Instanz in der **Bandbreitenkapazität, die jeder NetScaler-Instanz zugewiesen werden soll**, zugewiesen werden soll.

           Aus dem gemeinsamen Pool entnimmt die NetScaler-Instanz eine Instanzlizenz und nur so viel Bandbreite, wie angegeben ist.
         - **VPX-Lizenzen** – Wenn eine NetScaler VPX-Instanz bereitgestellt wird, entnimmt die Instanz die Lizenz von der NetScaler Console.

      ii. **Virtuelle CPU-Lizenzen**: Die bereitgestellte NetScaler VPX-Instanz entnimmt Lizenzen abhängig von der Anzahl der in der Instanz laufenden CPUs.

   HINWEIS:

   Wenn die bereitgestellten VPX-Instanzen entfernt oder zerstört werden, kehren die angewendeten Lizenzen in den Lizenzpool der NetScaler Console zurück. Diese Lizenzen können zur Bereitstellung neuer VPX-Instanzen wiederverwendet werden.

   b. **Lizenzedition** – Wählen Sie die Lizenzedition aus der Liste aus.

      NetScaler Console verwendet die angegebene Edition, um die VPX-Instanzen bereitzustellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Klicken Sie auf **Weiter**.
8. Geben Sie auf der Registerkarte **Bereitstellungsparameter** die folgenden Details an:
    - **Cluster** – Wählen Sie den Cluster aus, in dem Sie eine Instanz bereitstellen möchten.
    - **Hosts** – Wählen Sie den gewünschten Host aus der Liste aus.
    - **Vorlagen** – Wählen Sie die Vorlage aus der Liste aus, die Sie auf eine Instanz anwenden möchten.
    - **Datenspeicher** – Wählen Sie den Datenspeicher aus der Liste aus.
    - **Konfigurationsvorlage** – Wählen Sie die Konfigurationsvorlage aus der Liste aus.
    - **IP-Adresse** – Geben Sie eine IP-Adresse für eine Instanz an.
    - **Netzmaske** – Geben Sie eine Netzmaske für eine Instanz an.
    - **Gateway** – Geben Sie ein Gateway für eine Instanz an.

9. Klicken Sie auf **Fertig stellen**, um eine VPX-Instanz bereitzustellen.

NetScaler Globaler Lastausgleich für Hybrid- und Multi-Cloud-Bereitstellungen

Die NetScaler Hybrid- und Multi-Cloud-Lösung für globales Lastenausgleich (GLB) ermöglicht es Ihnen, Anwendungsverkehr über mehrere Rechenzentren in Hybrid-Clouds, Multi-Clouds und lokalen Bereitstellungen zu verteilen. Die NetScaler Hybrid- und Multi-Cloud-GLB-Lösung hilft Ihnen, Ihre Lastenausgleichskonfiguration in Hybrid- oder Multi-Cloud-Umgebungen zu verwalten, ohne die bestehende Konfiguration zu ändern. Wenn Sie eine lokale Konfiguration haben, können Sie außerdem einige Ihrer Dienste in der Cloud testen, indem Sie die NetScaler Hybrid- und Multi-Cloud-GLB-Lösung verwenden, bevor Sie vollständig in die Cloud migrieren. Sie können beispielsweise nur einen kleinen Prozentsatz Ihres Datenverkehrs in die Cloud leiten und den Großteil des Datenverkehrs lokal verarbeiten. Die NetScaler Hybrid- und Multi-Cloud-GLB-Lösung ermöglicht es Ihnen auch, NetScaler-Instanzen über geografische Standorte hinweg von einer einzigen, einheitlichen Konsole aus zu verwalten und zu überwachen.

Eine Hybrid- und Multi-Cloud-Architektur kann auch die gesamte Unternehmensleistung verbessern, indem sie „Vendor Lock-in“ vermeidet und unterschiedliche Infrastrukturen nutzt, um die Anforderungen Ihrer Partner und Kunden zu erfüllen. Mit mehreren Cloud-Architekturen können Sie Ihre Infrastrukturkosten besser verwalten, da Sie jetzt nur noch für das bezahlen müssen, was Sie nutzen. Skalieren Sie auch Ihre Anwendungen besser, da Sie die Infrastruktur jetzt bei Bedarf

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nutzen. Es bietet auch die Möglichkeit, schnell von einer Cloud zur anderen zu wechseln, um die besten Angebote jedes Anbieters zu nutzen.

Architektur der NetScaler Hybrid- und Multi-Cloud-GLB-Lösung

Das folgende Diagramm veranschaulicht die Architektur der NetScaler Hybrid- und Multi-Cloud-GLB-Funktion.

Die NetScaler GLB-Knoten übernehmen die DNS-Namensauflösung. Jeder dieser GLB-Knoten kann DNS-Anfragen von jedem Client-Standort empfangen. Der GLB-Knoten, der die DNS-Anfrage empfängt, gibt die IP-Adresse des virtuellen Load-Balancer-Servers zurück, die durch die konfigurierte Lastenausgleichsmethode ausgewählt wurde. Metriken (Standort-, Netzwerk- und Persistenzmetriken) werden zwischen den GLB-Knoten über das Metrics Exchange Protocol (MEP) ausgetauscht, einem proprietären Citrix-Protokoll. Weitere Informationen zum MEP-Protokoll finden Sie unter Konfigurieren des Metrics Exchange Protocol.

Der im GLB-Knoten konfigurierte Monitor überwacht den Integritätsstatus des virtuellen Lastenausgleichsservers im selben Rechenzentrum. In einer Parent-Child-Topologie werden Metriken zwischen den GLB- und NetScaler-Knoten über MEP ausgetauscht. Das Konfigurieren von Monitor-Probes zwischen einem GLB- und einem NetScaler LB-Knoten ist in einer Parent-Child-Topologie jedoch optional.

Der Agent ermöglicht die Kommunikation zwischen der NetScaler Console und den verwalteten Instanzen in Ihrem Rechenzentrum. Weitere Informationen zu Agents und deren Installation finden Sie unter Erste Schritte.

HINWEIS

Dieses Dokument geht von den folgenden Annahmen aus:

- Wenn Sie eine bestehende Lastenausgleichskonfiguration haben, ist diese betriebsbereit.
- Auf jedem der NetScaler GLB-Knoten ist eine SNIP-Adresse oder eine GLB-Standort-IP-Adresse konfiguriert. Diese IP-Adresse wird als Quell-IP-Adresse des Rechenzentrums verwendet, wenn Metriken mit anderen Rechenzentren ausgetauscht werden.
- Auf jeder der NetScaler GLB-Instanzen ist ein ADNS- oder ADNS-TCP-Dienst konfiguriert, um den DNS-Verkehr zu empfangen.
- Die erforderlichen Firewall- und Sicherheitsgruppen sind bei den Cloud-Dienstanbietern konfiguriert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

KONFIGURATION DER SICHERHEITSGRUPPEN

Sie müssen die erforderliche Firewall-/Sicherheitsgruppenkonfiguration bei den Cloud-Dienstanbietern einrichten. Weitere Informationen zu AWS-Sicherheitsfunktionen finden Sie in der AWS-Dokumentation. Weitere Informationen zu Microsoft Azure-Netzwerksicherheitsgruppen finden Sie in der Microsoft Azure-Dokumentation.

Zusätzlich müssen Sie auf dem GLB-Knoten Port 53 für den ADNS-Dienst/die DNS-Server-IP-Adresse und Port 3009 für die GSLB-Site-IP-Adresse für den MEP-Verkehrsaustausch öffnen. Auf dem Lastenausgleichsknoten müssen Sie die entsprechenden Ports öffnen, um den Anwendungsdatenverkehr zu empfangen. Sie müssen beispielsweise Port 80 für den Empfang von HTTP-Verkehr und Port 443 für den Empfang von HTTPS-Verkehr öffnen. Öffnen Sie Port 443 für die NITRO-Kommunikation zwischen dem Agenten und der NetScaler Console.
Für die dynamische Round-Trip-Time-GLB-Methode müssen Sie Port 53 öffnen, um UDP- und TCP-Probes zuzulassen, abhängig vom konfigurierten LDNS-Probe-Typ. Die UDP- oder TCP-Probes werden über eine der SNIPs initiiert, und daher muss diese Einstellung für Sicherheitsgruppen vorgenommen werden, die an das serverseitige Subnetz gebunden sind.

Funktionen der NetScaler Hybrid- und Multi-Cloud-GLB-Lösung

Einige der Funktionen der NetScaler Hybrid- und Multi-Cloud-GLB-Lösung werden in diesem Abschnitt beschrieben:

Kompatibilität mit anderen Lastenausgleichslösungen

Die NetScaler Hybrid- und Multi-Cloud-GLB-Lösung unterstützt verschiedene Lastenausgleichslösungen, wie den NetScaler Load Balancer, Nginx und andere Lastenausgleichslösungen von Drittanbietern.

HINWEIS

Lastenausgleichslösungen, die nicht von NetScaler stammen, werden nur unterstützt, wenn proximitätsbasierte und nicht-metrikbasierte GLB-Methoden verwendet werden und wenn keine Parent-Child-Topologie konfiguriert ist.

GLB-Methoden

Die NetScaler Hybrid- und Multi-Cloud-GLB-Lösung unterstützt die folgenden GLB-Methoden.

- Metrikbasierte GLB-Methoden. Metrikbasierte GLB-Methoden sammeln Metriken von den anderen NetScaler-Knoten über das Metrikaustauschprotokoll.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Geringste Verbindungen: Die Client-Anfrage wird an den Lastenausgleich weitergeleitet, der die wenigsten aktiven Verbindungen hat.
    - Geringste Bandbreite: Die Client-Anfrage wird an den Lastenausgleich weitergeleitet, der derzeit die geringste Menge an Datenverkehr verarbeitet.
    - Geringste Pakete: Die Clientanfrage wird an den Load Balancer weitergeleitet, der in den letzten 14 Sekunden die wenigsten Pakete empfangen hat.

- Nicht-metrikbasierte GLB-Methoden

    - Round Robin: Die Clientanfrage wird an die IP-Adresse des Load Balancers weitergeleitet, der sich ganz oben in der Liste der Load Balancer befindet. Dieser Load Balancer rückt dann an das Ende der Liste.
    - Quell-IP-Hash: Diese Methode verwendet den Hash-Wert der Client-IP-Adresse, um einen Load Balancer auszuwählen.

- Proximity-basierte GLB-Methoden

    - Statische Proximity: Die Clientanfrage wird an den Load Balancer weitergeleitet, der der Client-IP-Adresse am nächsten ist.
    - Round-Trip Time (RTT): Diese Methode verwendet den RTT-Wert (die Zeitverzögerung bei der Verbindung zwischen dem lokalen DNS-Server des Clients und dem Rechenzentrum), um die IP-Adresse des am besten performenden Load Balancers auszuwählen.

Weitere Informationen zu den Lastausgleichsmethoden finden Sie unter Lastausgleichsalgorithmen.

GLB-Topologien

Die NetScaler Hybrid- und Multi-Cloud-GLB-Lösung unterstützt die Aktiv-Passiv-Topologie und die Parent-Child-Topologie.

- Aktiv-Passiv-Topologie – Bietet Disaster Recovery und gewährleistet die kontinuierliche Verfügbarkeit von Anwendungen, indem sie vor Ausfallpunkten schützt. Fällt das primäre Rechenzentrum aus, wird das passive Rechenzentrum betriebsbereit. Weitere Informationen zur GSLB-Aktiv-Passiv-Topologie finden Sie unter Konfigurieren von GSLB für Disaster Recovery.
- Parent-Child-Topologie – Kann verwendet werden, wenn Sie die metrikbasierten GLB-Methoden zur Konfiguration von GLB- und LB-Knoten verwenden und wenn die LB-Knoten auf einer anderen NetScaler-Instanz bereitgestellt werden. In einer Parent-Child-Topologie muss

© 1997–2026 Citrix Systems, Inc. All rights reserved.

der LB-Knoten (Child-Site) eine NetScaler-Appliance sein, da der Austausch von Metriken zwischen der Parent- und Child-Site über das Metrics Exchange Protocol (MEP) erfolgt.

Weitere Informationen zur Parent-Child-Topologie finden Sie unter Bereitstellung der Parent-Child-Topologie mit dem MEP-Protokoll.

IPv6-Unterstützung

Die NetScaler Hybrid- und Multi-Cloud-GLB-Lösung unterstützt auch IPv6.

Überwachung

Die NetScaler Hybrid- und Multi-Cloud-GLB-Lösung unterstützt integrierte Monitore mit der Option, die sichere Verbindung zu aktivieren. Wenn jedoch LB- und GLB-Konfigurationen auf derselben NetScaler-Instanz vorhanden sind oder wenn eine Parent-Child-Topologie verwendet wird, ist die Konfiguration von Monitoren optional.

Persistenz

Die NetScaler Hybrid- und Multi-Cloud-GLB-Lösung unterstützt Folgendes:

- Quell-IP-basierte Persistenzsitzungen, sodass mehrere Anfragen desselben Clients an denselben Dienst weitergeleitet werden, wenn sie innerhalb des konfigurierten Zeitfensters eintreffen. Wenn der Timeout-Wert abläuft, bevor der Client eine weitere Anfrage sendet, wird die Sitzung verworfen, und der konfigurierte Lastausgleichsalgorithmus wird verwendet, um einen neuen Server für die nächste Anfrage des Clients auszuwählen.
- Spillover-Persistenz, sodass der virtuelle Backup-Server die empfangenen Anfragen weiterhin verarbeitet, auch nachdem die Last auf dem primären Server unter den Schwellenwert fällt. Weitere Informationen finden Sie unter Spillover konfigurieren.
- Site-Persistenz, sodass der GLB-Knoten ein Rechenzentrum zur Verarbeitung einer Clientanfrage auswählt und die IP-Adresse des ausgewählten Rechenzentrums für alle nachfolgenden DNS-Anfragen weiterleitet. Wenn die konfigurierte Persistenz für eine Site gilt, die AUSGEFALLEN ist, verwendet der GLB-Knoten eine GLB-Methode, um eine neue Site auszuwählen, und die neue Site wird für nachfolgende Anfragen des Clients persistent.

Konfiguration mithilfe der NetScaler Console StyleBooks

Sie können das standardmäßige Multi-Cloud-GLB-StyleBook auf NetScaler Console verwenden, um die NetScaler-Instanzen mit einer Hybrid- und Multi-Cloud-GLB-Konfiguration zu konfigurieren.

Sie können das standardmäßige Multi-Cloud-GLB-StyleBook für LB-Knoten-StyleBook verwenden, um die NetScaler-Lastausgleichsknoten zu konfigurieren, die die untergeordneten Sites in einer Parent-Child-Topologie sind, die den Anwendungsverkehr verarbeiten. Verwenden Sie dieses

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBook nur, wenn Sie LB-Knoten im Falle einer Parent-Child-Topologie konfigurieren möchten. Jeder LB-Knoten muss jedoch separat mit diesem StyleBook konfiguriert werden.

Workflow der NetScaler Hybrid- und Multi-Cloud-GLB-Lösungskonfiguration

Sie können das mitgelieferte Multi-Cloud-GLB-StyleBook auf NetScaler Console verwenden, um die NetScaler-Instanzen mit einer Hybrid- und Multi-Cloud-GLB-Konfiguration zu konfigurieren.

Das folgende Diagramm zeigt den Workflow zur Konfiguration der NetScaler Hybrid- und Multi-Cloud-GLB-Lösung. Die Schritte im Workflow-Diagramm werden nach dem Diagramm ausführlicher erläutert.

Führen Sie die folgenden Aufgaben als Cloud-Administrator aus:

1. Registrieren Sie sich für ein Citrix Cloud™-Konto.

   Um NetScaler Console zu verwenden, erstellen Sie ein Citrix Cloud-Firmenkonto oder treten Sie einem bestehenden bei, das von jemandem in Ihrem Unternehmen erstellt wurde.
2. Nachdem Sie sich bei Citrix Cloud angemeldet haben, klicken Sie auf der Kachel **NetScaler Console** auf **Verwalten**, um die NetScaler Console zum ersten Mal einzurichten.
3. Laden Sie mehrere Agents herunter und installieren Sie sie.

   Sie müssen den Agent in Ihrer Netzwerkumgebung installieren und konfigurieren, um die Kommunikation zwischen der NetScaler Console und den verwalteten Instanzen in Ihrem Rechenzentrum oder Ihrer Cloud zu ermöglichen. Installieren Sie einen Agent in jeder Region, damit Sie LB- und GLB-Konfigurationen auf den verwalteten Instanzen konfigurieren können. Die LB- und GLB-Konfigurationen können einen einzigen Agent gemeinsam nutzen. Weitere Informationen zu den oben genannten drei Aufgaben finden Sie unter Erste Schritte.
4. Stellen Sie Load Balancer in Microsoft Azure/AWS Cloud/On-Premises-Rechenzentren bereit.

   Je nach Art der Load Balancer, die Sie in der Cloud und On-Premises bereitstellen, stellen Sie diese entsprechend bereit. Sie können beispielsweise NetScaler VPX-Instanzen in einem Microsoft Azure Resource Manager (ARM)-Portal, in einer Amazon Web Services (AWS) Virtual Private Cloud und in On-Premises-Rechenzentren bereitstellen. Konfigurieren Sie NetScaler-Instanzen so, dass sie als LB- oder GLB-Knoten im Standalone-Modus fungieren, indem Sie die virtuellen Maschinen erstellen und andere Ressourcen konfigurieren. Weitere Informationen zur Bereitstellung von NetScaler VPX-Instanzen finden Sie in den folgenden Dokumenten:

   - Starten des NetScaler VPX für AWS AMI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Konfigurieren von NetScaler VPX im Standalone-Modus in Azure Resource Manager.

5. Führen Sie Sicherheitskonfigurationen durch.

   Konfigurieren Sie Netzwerksicherheitsgruppen und Netzwerk-ACLs in ARM oder AWS, um den eingehenden und ausgehenden Datenverkehr für Ihre Instanzen und Subnetze zu steuern.

6. Fügen Sie NetScaler-Instanzen in NetScaler Console hinzu.

   NetScaler-Instanzen sind Netzwerk-Appliances oder virtuelle Appliances, die Sie von der NetScaler Console aus erkennen, verwalten und überwachen möchten. Um diese Instanzen zu verwalten und zu überwachen, müssen Sie die Instanzen zum Dienst hinzufügen und sowohl LB- (wenn Sie NetScaler für LB verwenden) als auch GLB-Instanzen registrieren. Weitere Informationen zum Hinzufügen von NetScaler-Instanzen in der NetScaler Console finden Sie unter Erste Schritte.

7. Implementieren Sie die GLB- und LB-Konfigurationen mithilfe der Standard-NetScaler Console StyleBooks.

   - Verwenden Sie das **Multi-Cloud GLB StyleBook**, um die GLB-Konfiguration auf den ausgewählten GLB NetScaler-Instanzen auszuführen.
   - Implementieren Sie die Lastverteilungskonfiguration. (Sie können diesen Schritt überspringen, wenn Sie bereits LB-Konfigurationen auf den verwalteten Instanzen haben.)

   Sie können Lastverteiler auf NetScaler-Instanzen auf zwei Arten konfigurieren:

   - Konfigurieren Sie die Instanzen manuell für die Lastverteilung der Anwendungen. Weitere Informationen zur manuellen Konfiguration der Instanzen finden Sie unter Einrichten der grundlegenden Lastverteilung.
   - Verwenden Sie StyleBooks. Sie können eines der NetScaler Console StyleBooks (HTTP/SSL LoadBalancing StyleBook oder HTTP/SSL LoadBalancing (mit Monitoren) StyleBook) verwenden, um die Lastverteilerkonfiguration auf der ausgewählten NetScaler-Instanz zu erstellen. Sie können auch Ihre eigenen StyleBooks erstellen. Weitere Informationen zu StyleBooks finden Sie unter StyleBooks.

8. Verwenden Sie **Multi-cloud GLB StyleBook for LB Node**, um die GLB-Parent-Child-Topologie in einem der folgenden Fälle zu konfigurieren:

   - Wenn Sie die metrikbasierten GLB-Algorithmen (Least Packets, Least Connections, Least Bandwidth) verwenden, um GLB- und LB-Knoten zu konfigurieren, und wenn die LB-Knoten auf einer anderen NetScaler-Instanz bereitgestellt werden.
   - Wenn Site-Persistenz erforderlich ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verwenden von StyleBooks zur Konfiguration von GLB

Sie können das Multi-Cloud-GLB-StyleBook verwenden, um GLB-Konfigurationen auf NetScaler-Instanzen zu konfigurieren, die in Ihren Rechenzentren bereitgestellt werden. Stellen Sie sicher, dass Sie die Site-IP-Adresse auf der NetScaler GLB-Instanz in jedem Rechenzentrum konfiguriert haben.

Sie können dieses StyleBook auch verwenden, um eine übergeordnete Site zu erstellen, die untergeordnete Sites akzeptiert, die Sie später in den GLB-Knoten hinzufügen könnten. So konfigurieren Sie die Multi-Cloud-GLB-Konfiguration auf NetScaler-Instanzen.

1. Navigieren Sie zu **Applications** > **Configuration**, und klicken Sie auf **Create New**.
2. Die Seite **Choose StyleBook** zeigt alle StyleBooks an, die Ihnen in der NetScaler Console zur Verfügung stehen. Scrollen Sie nach unten und wählen Sie **Multi-cloud GLB StyleBook**.

   Das Multi-Cloud-GLB-StyleBook wird verwendet, um GLB für eine Anwendung zu konfigurieren, die in mehreren Clouds und lokalen Sites bereitgestellt wird. Das StyleBook wird als Benutzeroberfläche angezeigt, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

   HINWEIS

   Die Begriffe Rechenzentrum und Sites werden in diesem Dokument synonym verwendet.

3. Legen Sie die folgenden Parameter fest:

   - **Application Name**. Geben Sie den Namen der Anwendung ein, die auf den GLB-Sites bereitgestellt wird.
   - **GLB Algorithm**. Wählen Sie den globalen Lastausgleichsalgorithmus (Methode) für die Auswahl der Site, die einen Client bedient. Die in der Dropdown-Liste verfügbaren Optionen sind LEASTCONNECTION, LEASTBANDWIDTH, LEASTPACKETS, ROUNDROBIN, STATICPROXIMITY, SOURCEIPHASH und RTT.
   - **Geo Database File**. Wenn Sie STATICPROXIMITY als GLB-Algorithmus ausgewählt haben, geben Sie den vollständigen Pfad und Namen der Datenbankdatei ein, die die statischen Proximity-Daten enthält. Stellen Sie sicher, dass die Datenbankdatei auf allen GLB NetScaler-Instanzen am angegebenen Speicherort vorhanden ist. Alternativ können Sie die Standarddatei beibehalten.
   - **Protocol**. Wählen Sie das Anwendungsprotokoll der bereitgestellten Anwendung aus der Dropdown-Liste aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Persistence Settings**. Die auf einem virtuellen Server konfigurierte Persistenz verwaltet die Zustände von Verbindungen auf den durch diesen virtuellen Server repräsentierten Servern (z. B. Verbindungen, die im E-Commerce verwendet werden). Die Persistenz überschreibt die Lastausgleichsmethoden, sobald der virtuelle Server ausgewählt ist. Wenn die Persistenzkonfiguration auf einen Dienst angewendet wird, der DOWN ist, verwendet die Instanz die Lastausgleichsmethoden, um einen neuen Dienst auszuwählen, und der neue Dienst wird für nachfolgende Anfragen vom Client persistent.
- **Persistence Type**. Wählen Sie den Persistenztyp aus, der für diese Anwendung verwendet werden soll. Wenn Sie beispielsweise die Persistenz als SOURCEIP auswählen, werden nach der anfänglichen Auswahl der Site, die die Anwendung hostet, alle nachfolgenden Anfragen vom selben Client an diese Site gesendet, um auf die Dienste der Anwendung zuzugreifen.
- **Persistenz-Timeout**. Wenn Sie SOURCEIP als Persistenztyp ausgewählt haben, geben Sie die Anzahl der Minuten ein, bevor die Persistenzsitzung nach der letzten Clientanfrage abläuft. Der Bereich liegt zwischen 2 und 1440 Minuten. Die Minuten werden in Sekunden aufgelöst.

4. **Spillover-Einstellungen**. Konfigurieren Sie die Spillover-Funktion, um die Spillover-Verbindungen an einen sekundären oder Backup-virtuellen Server weiterzuleiten, wenn beispielsweise das Verbindungslimit oder das Bandbreitenlimit des primären virtuellen Servers den Schwellenwert erreicht hat.

   - **Spillover-Methode**. Wählen Sie aus der Dropdown-Liste die Spillover-Methode aus. Die Spillover-Methode CONNECTION überwacht beispielsweise die Anzahl der aktiven Verbindungen auf dem primären Server. Wenn der Spillover-Schwellenwert für diese Methode erreicht ist, werden neue Verbindungen an den ersten verfügbaren virtuellen Server in der Backup-Kette umgeleitet. Die Spillover-Methode HEALTH ermöglicht Ihnen einen Spillover, wenn der Schwellenwert unter einen konfigurierten Wert fällt. Zum Beispiel weniger als 70 %.

     HINWEIS

     Mit Ausnahme der Spillover-Methode HEALTH sind andere Methoden nur anwendbar, wenn NetScaler als Load Balancer-Instanz verwendet wird.

   - **Spillover-Schwellenwert.** Geben Sie einen Schwellenwert für die von Ihnen ausgewählte Spillover-Methode ein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Spillover-Persistenz.** Aktivieren Sie die Spillover-Persistenz, wenn der Backup-virtuelle Server die empfangenen Anfragen weiterhin verarbeiten soll, auch nachdem die Last auf dem primären Server unter den Schwellenwert gefallen ist.
- **Spillover-Persistenz-Timeout**. Konfigurieren Sie den Zeitraum, für den die Spillover-Persistenz wirksam ist. Der Mindestwert beträgt 2 Minuten und der Höchstwert 1440 Minuten. Die Minuten werden in Sekunden aufgelöst.

5. **Persistenz-/Spillover-Persistenz-ID**. Wenn Sie SOURCEIP als Persistenztyp ausgewählt haben oder wenn die Spillover-Persistenz aktiviert ist, geben Sie eine eindeutige Nummer ein, um dieselbe Domäne auf allen GLB-Appliances zu identifizieren. Der Bereich liegt zwischen 1 und 65535.

   - **Health Check von GLB-Dienstendpunkten (Optional)**
   - **Health Check-Typ**. Wählen Sie aus der Dropdown-Liste den Sondentyp aus, der zur Überprüfung des Zustands der Load Balancer-VIP-Adresse verwendet wird, die die Anwendung an einem Standort darstellt.
   - **Sicherer Modus**. (Optional) Wählen Sie **Ja**, um diesen Parameter zu aktivieren, wenn SSL-basierte Health Checks erforderlich sind.
   - **HTTP-Anfrage**. (Optional) Wenn Sie HTTP als Health Check-Typ ausgewählt haben, geben Sie die vollständige HTTP-Anfrage ein, die zum Abfragen der VIP-Adresse verwendet wird.
   - **Liste der HTTP-Status-Antwortcodes**. (Optional) Wenn Sie HTTP als Health Check-Typ ausgewählt haben, geben Sie die Liste der HTTP-Statuscodes ein, die in Antworten auf HTTP-Anfragen erwartet werden, wenn die VIP fehlerfrei ist.

6. **GLB-Domänennamen**. Dieser Abschnitt ermöglicht Ihnen die Konfiguration der Liste der DNS-Domänennamen, die dieser Anwendung zugeordnet sind. Klicken Sie auf das Plus-Symbol (**+**), um einen DNS-Domänennamen für die Anwendung zu erstellen.
7. **GLB-Standorte**. In diesem Abschnitt können Sie die Liste der Standorte konfigurieren, auf denen diese Anwendung bereitgestellt wird.

   Der GLB-Standort ist die oberste Entität für die GLB-Kommunikation. Die bei der Konfiguration des Standorts angegebenen Informationen werden verwendet, um lokale Standorte mit Remote-Standorten zu verknüpfen und Überwachungsdaten mithilfe des Citrix Metrics Exchange Protocol (MEP) auszutauschen. Die IP-Adresse gehört der GLB NetScaler-Instanz und verwendet TCP-Port 3009. Der Abschnitt „GLB-Standorte“ im StyleBook ermöglicht es Ihnen, beliebig viele GLB-Standorte anzugeben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Klicken Sie auf das Plus-Symbol (**+**), um Standorte hinzuzufügen.

- **Standortname**. Geben Sie den Namen des Standorts ein.
- **Standort-IP-Adresse**. Geben Sie die IP-Adresse ein, die der Standort als Quell-IP-Adresse verwendet, wenn Metriken mit anderen Standorten ausgetauscht werden. Es wird davon ausgegangen, dass diese IP-Adresse bereits auf der GLB-Instanz an jedem Standort konfiguriert ist.
- **Öffentliche IP-Adresse des Standorts**. (Optional) Geben Sie die öffentliche IP-Adresse des Standorts ein, die zum Austausch von Metriken verwendet wird, falls die IP-Adresse dieses Standorts NAT-ed ist.

8. **Untergeordnete Standorte**. Klicken Sie auf das Plus-Symbol (+), um die erforderlichen untergeordneten Standorte zu konfigurieren.

   - **Name des untergeordneten Standorts**. Geben Sie den Namen des Standorts ein.
   - **IP-Adresse des untergeordneten Standorts**. Geben Sie die IP-Adresse des untergeordneten Standorts ein. Verwenden Sie hier die private IP-Adresse oder SNIP des NetScaler-Knotens, der als untergeordneter Standort konfiguriert wird.
   - **Öffentliche IP-Adresse des Standorts**. (Optional) Geben Sie die öffentliche IP-Adresse des Standorts ein, die zum Austausch von Metriken verwendet wird, falls die IP-Adresse dieses Standorts NAT-ed ist.

9. **Dienst-Standort-Persistenz**. Wählen Sie aus der Dropdown-Liste den Persistenztyp aus, der für die GLB-Dienste am Standort verwendet werden soll.

   - Wählen Sie ConnectionProxy, damit der Standort eine Verbindung zu dem GLB-Standort herstellen kann, der das Standort-Cookie eingefügt hat, die Client-Anfrage an den ursprünglichen Standort weiterleitet, eine Antwort vom ursprünglichen GLB-Standort empfängt, die Antwort an den Client zurückleitet und die Verbindung schließt.
   - Wählen Sie `HTTPRedirect`, damit der Standort die Anfrage an den Standort umleiten kann, der das Cookie ursprünglich eingefügt hat. Weitere Informationen zur Persistenz finden Sie unter Konfigurieren persistenter Verbindungen.

10. **Aktive GLB-Dienste**: In diesem Abschnitt können Sie die Liste der aktiven Dienste an den Standorten konfigurieren, an denen die Anwendung bereitgestellt wird.

    Dienst-IP. Geben Sie die IP-Adresse des GLB-Dienstes an diesem Standort ein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Öffentliche IP-Adresse des Dienstes**. Wenn die virtuelle IP-Adresse privat ist und eine öffentliche IP-Adresse per NAT darauf zugewiesen wurde, geben Sie die öffentliche IP-Adresse an.
- **Dienstport**. Geben Sie den Port des GLB-Dienstes an diesem Standort ein.
- **Dienstgewicht**. Geben Sie das Gewicht ein, das dem GLB-Dienst zugewiesen ist.

  HINWEIS

  Sie können den Diensten relative Gewichte zuweisen, abhängig vom Prozentsatz des Datenverkehrs, der an die Cloud gesendet werden muss, und dem Prozentsatz des Datenverkehrs, der vor Ort verarbeitet werden muss. Wenn Sie beispielsweise dem Cloud-basierten GLB-Dienst ein Gewicht von 3 und dem lokalen GLB-Dienst ein Gewicht von 7 zugewiesen haben, werden 30 % des Datenverkehrs an die Cloud geleitet und 70 % vor Ort verarbeitet.

- **Standortname**. Geben Sie den Namen des Standorts ein, an dem sich der GLB-Dienst befindet.
- **Standortpräfix**. Geben Sie ein Präfix für den Standort ein, an dem der GLB-Dienst konfiguriert ist. Dies ist anwendbar, wenn die Standortpersistenz aktiviert ist und die Methode `httpredirect` ist. Der Wert des Standortpräfixes muss für alle GLB-Dienste einer Anwendung eindeutig sein.
- **Maximale Client-Verbindungen**. Geben Sie die maximalen Client-Verbindungen ein, die im GLB-Dienst konfiguriert sind, wenn Sie DYNAMICCONNECTION als Spillover-Methode in den Einstellungen für **Spillover-Persistenz** ausgewählt haben. Wenn Sie keinen Wert angeben, weist das System standardmäßig eine Zahl für die maximal konfigurierbaren Client-Verbindungen zu.

11. **Passive GLB-Dienste**: Dieser Abschnitt ermöglicht es Ihnen, die Liste der passiven Dienste an den Standorten zu konfigurieren, an denen die Anwendung mit einer Aktiv-Passiv-Topologie bereitgestellt wird. Geben Sie Informationen für alle Backup-GLB-Dienste ähnlich den Informationen an, die Sie für aktive GLB-Dienste bereitgestellt haben.
12. Klicken Sie auf **Zielinstanzen**, und wählen Sie die NetScaler-Instanzen aus, die als GLB-Instanzen an jedem Standort konfiguriert sind, auf dem die GLB-Konfiguration bereitgestellt werden soll.
13. Klicken Sie auf **Erstellen**, um die GLB-Konfiguration auf den ausgewählten NetScaler-Instanzen zu erstellen. Sie können auch auf **Testlauf** klicken, um die Objekte zu überprüfen,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

die in den Zielinstanzen erstellt würden. Die von Ihnen erstellte StyleBook-Konfiguration (Konfigurationspaket) wird in der Liste der Konfigurationen auf der Seite Konfigurationen angezeigt. Sie können diese Konfiguration (Konfigurationspaket) mithilfe der NetScaler Console GUI überprüfen, aktualisieren oder entfernen.

Verwenden von StyleBooks zum Konfigurieren von GLB auf NetScaler LB-Knoten

Sie können das **Multi-cloud GLB StyleBook for LB Node** verwenden, wenn Sie die metrikbasierten GLB-Algorithmen (Least Packets, Least Connections, Least Bandwidth) zur Konfiguration von GLB und LB-Knoten verwenden und die LB-Knoten auf einer anderen NetScaler-Instanz bereitgestellt werden.

Sie können dieses StyleBook auch verwenden, um zusätzliche untergeordnete Sites für eine vorhandene übergeordnete Site zu konfigurieren. Dieses StyleBook konfiguriert jeweils eine untergeordnete Site. Erstellen Sie daher so viele Konfigurationen (Konfigurationspakete) aus diesem StyleBook, wie es untergeordnete Sites gibt. Das StyleBook wendet die GLB-Konfiguration auf die untergeordneten Sites an. Sie können maximal 1024 untergeordnete Sites konfigurieren.

HINWEIS

Verwenden Sie Multi-cloud GLB StyleBook, um die übergeordneten Sites zu konfigurieren.

Dieses StyleBook geht von folgenden Annahmen aus:

- Eine SNIP-Adresse oder eine GLB-Site-IP-Adresse ist konfiguriert.
- Die erforderlichen Firewall- und Sicherheitsgruppen sind bei den Cloud-Dienstanbietern konfiguriert.

Konfigurieren einer untergeordneten Site in einer Parent-Child-Topologie mithilfe des Multi-cloud GLB StyleBook für LB-Knoten

1. Navigieren Sie zu **Applications** > **Configuration**, und klicken Sie auf **Create New**.
2. Auf der Seite **Choose StyleBook** werden alle StyleBooks angezeigt, die Sie in NetScaler Console verwenden können. Scrollen Sie nach unten und wählen Sie **Multi-cloud GLB StyleBook for LB Node.**

   Das StyleBook wird als Benutzeroberfläche angezeigt, auf der Sie die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Die Begriffe Rechenzentrum und Sites werden in diesem Dokument synonym verwendet.

3. Legen Sie die folgenden Parameter fest:

   - **Anwendungsname**. Geben Sie den Namen der GLB-Anwendung ein, die auf den GLB-Sites bereitgestellt wird, für die Sie untergeordnete Sites erstellen möchten.
   - **Protokoll**. Wählen Sie das Anwendungsprotokoll der bereitgestellten Anwendung aus der Dropdown-Liste aus.
   - **LB-Zustandsprüfung (optional)**
     - **Typ der Zustandsprüfung**. Wählen Sie aus der Dropdown-Liste den Sondentyp aus, der zur Überprüfung des Zustands der Load Balancer VIP-Adresse verwendet wird, die die Anwendung auf einer Site darstellt.
     - **Sicherer Modus**. (Optional) Wählen Sie **Ja**, um diesen Parameter zu aktivieren, wenn SSL-basierte Zustandsprüfungen erforderlich sind.
     - **HTTP-Anfrage**. (Optional) Wenn Sie HTTP als Typ der Zustandsprüfung ausgewählt haben, geben Sie die vollständige HTTP-Anfrage ein, die zum Abfragen der VIP-Adresse verwendet wird.
     - **Liste der HTTP-Status-Antwortcodes**. (Optional) Wenn Sie HTTP als Typ der Zustandsprüfung ausgewählt haben, geben Sie die Liste der HTTP-Statuscodes ein, die in Antworten auf HTTP-Anfragen erwartet werden, wenn die VIP fehlerfrei ist.

4. Konfigurieren der übergeordneten Site.

   Geben Sie die Details der übergeordneten Site (GLB-Knoten) an, unter der Sie die untergeordnete Site (LB-Knoten) erstellen möchten.

   - **Site-Name**. Geben Sie den Namen der übergeordneten Site ein.
   - **Site-IP-Adresse**. Geben Sie die IP-Adresse ein, die die übergeordnete Site als ihre Quell-IP-Adresse verwendet, wenn sie Metriken mit anderen Sites austauscht. Es wird davon ausgegangen, dass diese IP-Adresse bereits auf dem GLB-Knoten in jeder Site konfiguriert ist.
   - **Öffentliche Site-IP-Adresse**. (Optional) Geben Sie die öffentliche IP-Adresse der übergeordneten Site ein, die zum Austausch von Metriken verwendet wird, falls die IP-Adresse dieser Site NAT-ed ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Konfigurieren der untergeordneten Site.

   Geben Sie die Details der untergeordneten Site an.

   - **Site-Name**. Geben Sie den Namen der Site ein.
   - **Site-IP-Adresse**. Geben Sie die IP-Adresse des untergeordneten Standorts ein. Verwenden Sie hier die private IP-Adresse oder SNIP des NetScaler-Knotens, der als untergeordneter Standort konfiguriert wird.
   - **Öffentliche Site-IP-Adresse**. (Optional) Geben Sie die öffentliche IP-Adresse des untergeordneten Standorts ein, die zum Austausch von Metriken verwendet wird, falls die IP-Adresse dieses Standorts NAT-ed ist.

6. Aktive GLB-Dienste konfigurieren (optional)

   Konfigurieren Sie aktive GLB-Dienste nur, wenn die IP-Adresse des virtuellen LB-Servers keine öffentliche IP-Adresse ist. Dieser Abschnitt ermöglicht es Ihnen, die Liste der lokalen GLB-Dienste an den Standorten zu konfigurieren, an denen die Anwendung bereitgestellt wird.

   - **Dienst-IP**. Geben Sie die IP-Adresse des virtuellen Lastausgleichsservers an diesem Standort ein.
   - **Öffentliche Dienst-IP-Adresse**. Wenn die virtuelle IP-Adresse privat ist und eine öffentliche IP-Adresse darauf NAT-ed ist, geben Sie die öffentliche IP-Adresse an.
   - **Dienst-Port**. Geben Sie den Port des GLB-Dienstes an diesem Standort ein.
   - **Site-Name**. Geben Sie den Namen des Standorts ein, an dem sich der GLB-Dienst befindet.

7. Klicken Sie auf **Zielinstanzen** und wählen Sie die NetScaler-Instanzen aus, die als GLB-Instanzen auf jedem Standort konfiguriert sind, auf dem die GLB-Konfiguration bereitgestellt werden soll.
8. Klicken Sie auf **Erstellen**, um die LB-Konfiguration auf der ausgewählten NetScaler-Instanz (LB-Knoten) zu erstellen. Sie können auch auf **Testlauf** klicken, um die Objekte zu überprüfen, die in den Zielinstanzen erstellt würden. Die von Ihnen erstellte StyleBook-Konfiguration wird in der Liste der Konfigurationen auf der Seite Konfigurationen angezeigt. Sie können diese Konfiguration über die NetScaler Console GUI überprüfen, aktualisieren oder entfernen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Orchestrierung

Die Orchestrierungsfunktionen von NetScaler Console ermöglichen Ihnen die Verwaltung von Container-Orchestrierungsplattformen, die in NetScaler integriert sind. Sie können den für den Service-Graphen verwendeten Kubernetes-Cluster überwachen und verwalten.

Die folgenden Themen helfen Ihnen bei der Verwaltung der Orchestrierung:

- Kubernetes

Verwalten des Kubernetes-Clusters für Service Graph

Kubernetes (K8s) ist eine Open-Source-Container-Orchestrierungsplattform, die die Bereitstellung, Skalierung und Verwaltung von Cloud-nativen Anwendungen automatisiert.

HINWEIS

- NetScaler Console unterstützt die Sichtbarkeit von Clustern für Service Graph mit Kubernetes Version 1.14–1.23.

Sie können die folgenden Aspekte der Kubernetes-Integration in NetScaler Console angeben:

- **Cluster** – Sie können Kubernetes-Cluster registrieren oder die Registrierung aufheben, für die NetScaler Console alle Microservices überwacht und den Service Graph füllt. Wenn Sie einen Cluster in NetScaler Console registrieren, geben Sie die Informationen zum Kubernetes-API-Server an. Wählen Sie dann einen Agenten aus, der den Kubernetes-Cluster erreichen kann.

Bevor Sie beginnen

Um Ihre Microservices auf Kubernetes-Clustern zu überwachen und zu visualisieren und mit Service Graph zu beginnen, stellen Sie sicher, dass Sie Folgendes haben:

- Kubernetes-Cluster vorhanden.
- Der Agent ist installiert und konfiguriert, um die Kommunikation zwischen NetScaler Console und dem Kubernetes-Cluster oder verwalteten Instanzen zu ermöglichen. Sie können die verwalteten Instanzen verwenden, die in Ihrem Rechenzentrum oder in der Cloud vorhanden sind.
- Kubernetes-Cluster in NetScaler Console registriert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler-Agent für die Registrierung beim Kubernetes-Cluster konfigurieren

Um die Kommunikation zwischen dem Kubernetes-Cluster und NetScaler Console zu ermöglichen, müssen Sie einen Agenten installieren und konfigurieren. Sie können einen Agenten auf den folgenden Plattformen bereitstellen:

- Hypervisor (ESX, XenServer®, KVM, Hyper-V)
- Öffentliche Cloud-Dienste (wie Microsoft Azure, AWS)

Befolgen Sie das Verfahren, um einen Agenten zu konfigurieren.

HINWEIS

Sie können auch einen vorhandenen Agenten verwenden, falls bereits einer bereitgestellt ist.

Konfigurieren Sie die NetScaler Console mit einem geheimen Token, um einen Kubernetes-Cluster zu verwalten

Damit die NetScaler Console Ereignisse von Kubernetes empfangen kann, müssen Sie ein Dienstkonto in Kubernetes für die NetScaler Console erstellen. Konfigurieren Sie das Dienstkonto anschließend mit den erforderlichen RBAC-Berechtigungen im Cluster.

1. Erstellen Sie ein Dienstkonto für die NetScaler Console. Der Name des Dienstkontos kann beispielsweise `citrixadm-sa` lauten. Informationen zum Erstellen eines Dienstkontos finden Sie unter Mehrere Dienstkonten verwenden.
2. Verwenden Sie die Rolle `cluster-admin`, um das NetScaler Console-Konto zu binden. Diese Bindung gewährt einem Dienstkonto eine `ClusterRole` über den Cluster hinweg. Das Folgende ist ein Beispielbefehl zum Binden einer `cluster-admin` Rolle an das Dienstkonto.

   ```
   kubectl create clusterrolebinding citrixadm-sa-admin --
   clusterrole=cluster-admin --serviceaccount=default:citrixadm-sa
   ```

   Nachdem das NetScaler Console-Konto an die Rolle `cluster-admin` gebunden wurde, hat das Dienstkonto clusterweiten Zugriff. Weitere Informationen finden Sie unter `kubectl` erstellen `clusterrolebinding`.
3. Rufen Sie das Token vom erstellten Dienstkonto ab.

   Führen Sie beispielsweise den folgenden Befehl aus, um das Token für das Dienstkonto `citrixadm-sa` anzuzeigen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
kubectl describe sa citrixadm-sa
```

4. Führen Sie den folgenden Befehl aus, um die geheime Zeichenfolge des Tokens abzurufen:

```
kubectl describe secret <token-name>
```

Fügen Sie den Kubernetes-Cluster in der NetScaler Console hinzu

Nachdem Sie einen Agenten konfiguriert und statische Routen eingerichtet haben, müssen Sie den Kubernetes-Cluster in der NetScaler Console registrieren.

So registrieren Sie den Kubernetes-Cluster:

1. Melden Sie sich mit Administratoranmeldeinformationen bei der NetScaler Console an.
2. Navigieren Sie zu **Orchestration** > **Kubernetes** > **Cluster**. Die Seite „Cluster“ wird angezeigt.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie auf der Seite **Cluster hinzufügen** die folgenden Parameter an:
    a. **Name** – Geben Sie einen Namen Ihrer Wahl an.
    b. **API-Server-URL** – Sie können die Details der API-Server-URL vom Kubernetes-Masterknoten abrufen.
        i. Führen Sie auf dem Kubernetes-Masterknoten den Befehl `kubectl cluster-info` aus.
        ii. Geben Sie die URL ein, die für **„Kubernetes master is running at.“** angezeigt wird.
    c. **Authentifizierungstoken** – Geben Sie die Authentifizierungstokenzeichenfolge an, die Sie beim Konfigurieren von NetScaler Console zur Verwaltung eines Kubernetes-Clusters erhalten haben. Das Authentifizierungstoken ist erforderlich, um den Zugriff für die Kommunikation zwischen dem Kubernetes-Cluster und NetScaler Console zu validieren. So generieren Sie ein Authentifizierungstoken:
        i. Führen Sie auf dem Kubernetes-Masterknoten die folgenden Befehle aus:

```
kubectl describe secret <token-name>
```

        ii. Kopieren Sie das generierte Token und fügen Sie es als Authentifizierungstoken ein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen finden Sie in der Kubernetes-Dokumentation.

d. Wählen Sie den Agenten aus der Liste aus.

e. Klicken Sie auf **Erstellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler® Lizenzen

Die Lizenzierungsfunktionen der NetScaler Console ermöglichen Ihnen die Verwaltung und Überwachung Ihrer NetScaler-Lizenzen. Sie können Lizenzen aktivieren und verwalten, Best Practices anwenden, Flexed-Lizenzierung konfigurieren, Lizenz-Dashboards und -Berichte anzeigen und Legacy-Lizenzen verwalten.

Die folgenden Themen helfen Ihnen bei der Verwaltung von NetScaler-Lizenzen:

- Lizenzaktivierungsdienst
- Best Practices
- Lizenzverwaltung
- Prüfung der Mindest- und Höchstkapazität
- Verhalten des NetScaler-Agenten
- Flexed-Lizenzierung
- Lizenz konfigurieren
- Lizenz-Dashboard
- Lizenzberichterstattung
- Umstellung auf Flexed-Lizenzierung
- Szenarien für den Ablauf von Flexed- oder Pooled-Lizenzen und das Verhalten bei Konnektivitätsproblemen
- NetScaler Console-Server nur als Flexed- oder Pooled-Lizenzserver konfigurieren
- Legacy-Lizenzen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lizenzaktivierungsdienst

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Suite der Citrix-Produkte. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, und unterstützt NetScaler Flexed-Lizenzen (Citrix Platform License/Universal Hybrid Multi-Cloud), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed Term Bandwidth-Lizenzen. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Wird ab Anfang September 2025 unterstützt.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 in den Console on-prem-Versionen 14.1-51.x und höher sowie 13.1-60.x und höher eingestellt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch auf Console on-prem Version 14.1-51.x oder höher aktualisieren und vor 15th April 2026 auf LAS umstellen, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie NetScaler Virtual CPU Licensing (Pooled vCPU), NetScaler VPX Check-In und Check-Out (CICO) sowie unbefristete Lizenzen werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden nach dem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind Kunden möglicherweise nicht verfügbar, wo dies gesetzlich oder durch Vorschriften verboten ist.
Bei Fragen oder Bedenken wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix Maintenance bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder

© 1997–2026 Citrix Systems, Inc. All rights reserved.

aussetzen, zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften verboten sind.
Bevor Sie mit der Umstellung auf LAS beginnen, empfehlen wir Ihnen, LAS für NetScaler zu lesen. Dies stellt sicher, dass Sie die allgemeinen Voraussetzungen, die unterstützten oder nicht unterstützten Lizenztypen, den genauen Workflow für Ihre spezifischen Lizenz- und Bereitstellungstypen sowie andere wichtige Informationen verstehen.

Der License Activation Service (LAS) ist eine cloudbasierte Lizenzierungslösung, die die traditionelle dateibasierte Lizenzierung ersetzt. LAS führt neue Module zur Aktivierung von Citrix- und NetScaler-Produkten ein und bietet einen optimierten, modernen Ansatz für die Lizenzverwaltung.

HINWEISE:

- LAS ist ein Lizenzmechanismus, keine Lizenzart.
- Dateibasierte Lizenzierung bezieht sich auf die ältere Methode der Lizenzierung unter Verwendung manueller Berechtigungen. In diesem Dokument werden „Dateibasierte Lizenzierung“ und „manuell verwaltete Berechtigungen“ synonym verwendet, da sie dasselbe Konzept beschreiben.

Die folgenden sind die Hauptvorteile von LAS:

- Automatisierte Bereitstellung von Berechtigungen über einen Berechtigungs-Blob.
- Ein externer Agent für die Lizenzkommunikation ist optional.
- LAS eliminiert die Notwendigkeit von Z-Cap-Softwarelizenzdateien auf den NetScaler MPX™- und SDX-Instanzen.

HINWEIS:

Wenn Sie neu bei NetScaler Console sind, beginnen Sie mit Erste Schritte.

Das folgende Diagramm zeigt LAS mit dem Console-Dienst.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Voraussetzungen

Um LAS zu verwenden, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllt haben:

- Sie müssen über ein gültiges Citrix Cloud-Konto verfügen. Weitere Informationen zu bestehenden Cloud-Konten oder zum Onboarding neuer Cloud-Konten finden Sie unter Kontoverwaltung.
- Die mit dem für den LAS-Aktivierungsworkflow verwendeten Citrix Cloud-Konto verknüpfte Organisations-ID (Org ID) muss über gültige erworbene Berechtigungen verfügen. Um die aktuellen Berechtigungen anzuzeigen, siehe Berechtigungen.
- Die NetScaler-Instanz führt eine LAS-kompatible Version aus.
- Die NetScaler-Instanz wird als verwaltete Instanz in NetScaler Console hinzugefügt.

Automatische Aktivierung und Kompatibilität

LAS wird automatisch auf dem NetScaler Console-Dienst aktiviert. Nach der Aktivierung werden alle NetScaler Flexed- und Pooled-Lizenzberechtigungen in der NetScaler Console-GUI angezeigt.

Sie können Ihre Berechtigungen anzeigen, indem Sie zur Registerkarte **NetScaler Licensing > License management > License Activation Service (LAS)** navigieren.

HINWEISE:

- Die neue Option „Lizenzen synchronisieren“ ermöglicht es Ihnen, diese Synchronisierung bei Bedarf manuell auszulösen, wodurch sichergestellt wird, dass die Berechtigungen sofort aktuell sind.
- Die Standardfrequenz für die Berechtigungssynchronisierung beträgt alle 8 Stunden, wenn LAS-Berechtigungen nicht mit dem NetScaler Console-Dienst synchronisiert wurden, und danach alle 24 Stunden. Für die bedarfsgesteuerte Synchronisierung klicken Sie auf `Sync Now`.

NetScaler-Versionskompatibilität für LAS

Um LAS zu verwenden, müssen Ihre NetScaler-Instanzen eine der folgenden Mindestversionen ausführen:

- NetScaler: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console-Dienst: Unterstützt ab Anfang September 2025.
- NetScaler Console On-Prem: 14.1-51.x

HINWEISE:

- Um LAS zu verwenden, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllt haben:
  - Die NetScaler-Instanz führt eine LAS-kompatible Version aus.
  - Die NetScaler-Instanz ist als verwaltete Instanz in NetScaler Console hinzugefügt.
- Aktualisieren Sie für SDX-Appliances den Management Service (SVM) auf einen von LAS unterstützten Build und stellen Sie auf LAS-basierte Lizenzierung um. Die VPX-Build-Version hat keinen Einfluss auf die LAS-Kompatibilität.

Bei der dateibasierten Lizenzierung sind Ihre angewendeten Berechtigungen und Konfigurationen unter **NetScaler Licensing > License management > Manual License File management** sichtbar.

HINWEIS:

LAS unterstützt Flexed Licensing (UHMC/CPL), Pooled Bandwidth Licensing und Fixed-term Bandwidth Licensing. Alle anderen Formen älterer NetScaler-Lizenzen, wie Pooled vCPU und CICO, werden von LAS nicht unterstützt.

Umstellung auf LAS

Wenn Sie zu **NetScaler Licensing > License management > License Activation Service (LAS)** navigieren, wird die NetScaler-GUI dynamisch basierend auf der Kompatibilität Ihrer NetScaler-Instanzen aktualisiert.

Eine Meldung wird in der GUI angezeigt, wenn Sie keine NetScaler-Instanzen haben, die auf LAS-kompatiblen Versionen laufen. Die Meldung fordert Sie auf, eine NetScaler-Instanz zu aktualisieren oder hinzuzufügen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Wenn einige Ihrer NetScaler-Instanzen auf eine kompatible Version aktualisiert wurden, können Sie LAS für diese spezifischen Instanzen verwenden.

Wenn eine oder mehrere NetScaler-Instanzen mit LAS kompatibel sind, werden sie in eine von zwei Gruppen kategorisiert:

- NetScaler-Instanzen mit LAS lizenzieren
- Migrieren Sie die lizenzierten NetScaler-Instanzen zu LAS

Die GUI passt sich dynamisch an, je nachdem, ob Sie ein erstmaliger LAS-Benutzer (mit null migrierten Instanzen) oder ein bestehender Benutzer sind (der bereits einige Instanzen zu LAS verschoben hat und nun weitere hinzufügt).

HINWEIS:

Löschen Sie die lokalen dateibasierten Lizenzen auf der SVM, sobald die Lizenzierung oder Migration zu LAS abgeschlossen ist. Die dateibasierten Lizenzen befinden sich im SVM-Ordner `/mpsconfig/license` und müssen aus diesem Ordner über die Shell-Eingabeaufforderung gelöscht werden. Dieser Hinweis gilt für die Workflows **License with LAS** und **Migrate to LAS** sowohl für erstmalige als auch für bestehende Benutzer.

Erstmaliger LAS-Benutzer

Das folgende Bild wird für den erstmaligen Benutzer angezeigt:

NetScaler-Instanzen mit LAS lizenzieren

Der Abschnitt **NetScaler-Instanzen mit LAS lizenzieren** listet NetScaler-Instanzen auf, die derzeit nicht lizenziert sind oder die keine dateibasierte Lizenz für flexible Bandbreite oder gepoolte Bandbreite verwenden.

Um eine Instanz zu lizenzieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie **NetScaler-Instanzen mit LAS lizenzieren** aus, und klicken Sie auf **Weiter**.
2. Wählen Sie eine Instanz aus, und klicken Sie auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Geben Sie die Details ein und klicken Sie auf **Senden**. Wiederholen Sie diesen Vorgang für jede Instanz.

HINWEIS:

Die ausgewählten Instanzen werden neu gestartet, damit die Lizenz wirksam wird, außer bei SDX-Instanzen.

Vorhandene lizenzierte Instanzen zu LAS migrieren

Der Abschnitt **Vorhandene lizenzierte Instanzen zu LAS migrieren** listet alle NetScaler-Instanzen mit Flexed- oder Pooled-Dateibasierten Lizenzen auf. Sie sind wie folgt kategorisiert:

- **Zur Migration bereite Instanzen:** Listet die Instanzen auf, die auf LAS-kompatiblen Versionen oder Builds laufen und zur Migration zu LAS bereit sind.

Führen Sie zur Migration die folgenden Schritte aus:

```
1.  Select **Migrate your existing licensed NetScaler instances to LAS**
and click **Next**.

2.  Select the instances and click **Migrate**.
```

- **Instanzen, die vor der Migration ein Upgrade erfordern:** Listet die Instanzen auf, die vor der Migration auf eine kompatible Version oder Builds aktualisiert werden müssen.

  Voraussetzung:

  Um die LAS-basierte Lizenzierung zu verwenden, muss die Edition Ihrer NetScaler-Instanz mit der Edition Ihrer Pooled- oder Flexed-Dateibasierten Lizenz übereinstimmen. Stellen Sie sicher, dass Sie die Edition der Instanz an die neue Lizenz anpassen, bevor Sie mit der Migration beginnen.

  a. Wählen Sie **Vorhandene lizenzierte NetScaler-Instanzen zu LAS migrieren** und klicken Sie auf **Upgrade**.

  b. Wählen Sie auf der Seite **NetScaler aktualisieren** die Instanz aus und aktualisieren Sie die Instanzen auf mit LAS kompatible Versionen oder Builds.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Für NetScaler-Instanzen im Workflow „Zu LAS migrieren“, die von der älteren dateibasierten Lizenzierung auf die LAS-basierte Pooled-Bandbreiten- oder Flexed-Lizenzierung umgestellt werden, ist kein Neustart erforderlich.

Bestehender LAS-Benutzer

Das folgende Bild wird für den bestehenden Benutzer angezeigt:

Hinweis: Um die mit LAS lizenzierten CPX-Instanzen anzuzeigen, siehe die Flexed Dashboard GUI. CPX-Instanzen werden nicht unter **NetScaler-Instanz mit LAS** aufgeführt.

NetScaler-Instanzen mit LAS lizenzieren

Der Abschnitt **NetScaler-Instanzen mit LAS lizenzieren** listet NetScaler-Instanzen auf, die derzeit nicht lizenziert sind oder eine andere Lizenz als eine Flexed-Bandbreiten- oder Pooled-Bandbreiten-Dateibasis-Lizenz verwenden.

Um eine Instanz zu lizenzieren, führen Sie die folgenden Schritte aus:

1. Unter **Mit License Activation Service (LAS) lizenzieren**, klicken Sie auf **Mit LAS lizenzieren**.
2. Wählen Sie eine Instanz aus, und klicken Sie auf **Weiter**.
3. Geben Sie die Details ein und klicken Sie auf **Senden**.

   Wiederholen Sie die Schritte für jede NetScaler-Instanz, die Sie mit LAS lizenzieren möchten.

HINWEIS:

Die ausgewählten Instanzen werden neu gestartet, damit die Lizenz wirksam wird.

Die lizenzierten NetScaler-Instanzen zu LAS migrieren

Der Abschnitt **Die lizenzierten NetScaler-Instanzen zu LAS migrieren** listet alle NetScaler-Instanzen mit einer Flexed- oder Pooled-Dateibasis-Lizenz auf. Sie sind wie folgt kategorisiert:

- **Instanzen in LAS**: Listet die Instanzen auf, die bereits LAS-basierte Lizenzierung verwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Instanzen, die zur Migration bereit sind**: Listet kompatible Instanzen auf, die zur Migration bereit sind.

  Führen Sie zur Migration die folgenden Schritte aus:

  a. Wählen Sie **Die lizenzierten NetScaler-Instanzen zu LAS migrieren** und klicken Sie auf **Migrieren**.

  b. Wählen Sie eine oder mehrere NetScaler-Instanzen aus und migrieren Sie die ausgewählten Instanzen zu LAS.

- **Instanzen erfordern ein Upgrade vor der Migration:** Listet Instanzen auf, die auf eine kompatible Version aktualisiert werden müssen. Führen Sie zum Upgrade die folgenden Schritte aus:

  Voraussetzung:

  Um die LAS-basierte Lizenzierung zu verwenden, muss die Edition Ihrer NetScaler-Instanz mit der Edition Ihrer Pooled- oder Flexed-Lizenz übereinstimmen. Stellen Sie sicher, dass Sie die Edition der Instanz an die neue Lizenz anpassen, bevor Sie mit der Migration beginnen.

  a. Wählen Sie **Die lizenzierten NetScaler-Instanzen zu LAS migrieren** und klicken Sie auf **Upgrade**.

  b. Wählen Sie eine oder mehrere NetScaler-Instanzen aus und aktualisieren Sie die Instanzen auf eine kompatible Version oder Build.

HINWEIS:

Für NetScaler-Instanzen im Workflow „Zu LAS migrieren“, die von der älteren dateibasierten Lizenzierung auf die LAS-basierte Pooled-Bandbreiten- oder Flexed-Lizenzierung umgestellt werden, ist kein Neustart erforderlich.

Informationen, die während des LAS-Lizenzierungs-Workflows an LAS gesendet werden

Dieser Abschnitt enthält alle Informationen, die als Teil der Anforderung für einen Aktivierungs-Blob an LAS gesendet werden, und zwar bei jeder ersten Anforderung und jeder Aktualisierungsanforderung für einen LAS-Aktivierungs-Blob. Die folgende Tabelle fasst die Parameter zusammen, die während des Lizenzierungs-Workflows an LAS gesendet werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	BESCHREIBUNG	BEDARF DAFÜR IM LAS-WORKFLOW
Lizenzdienst-GUID	Eindeutige ID des Console-Dienst-Mandanten	LAS-Bindungsparameter
Lizenzdienst-ID	Eindeutige ID des Console-Dienst-Mandanten	LAS-Bindungsparameter
Pubkey	Öffentlicher Schlüssel der Console-Dienst-Bereitstellung	Stellt sicher, dass LAS diese Konsole autorisiert hat
Client-ID	Citrix Cloud ID, die zum Onboarding des Console-Dienstes verwendet wird	LAS-Bindungsparameter
Lizenzdienst-Build	Build-Version oder Beispielwert	LAS-Aktivierungsanforderung
Hostname	Hostname des Konsolendienstes (POP-Name)	LAS-Aktivierungsanforderung
LPE-ID	Eindeutige ID des aktivierten NetScaler.	LAS-Bindungsparameter
Lizenzpool-Entitäts-Hostname	Hostname des aktivierten NetScaler	LAS-Bindungsparameter
burnin_date	Software-Burn-in-Datum des NetScaler	LAS-Bindungsparameter
Produkte	Die Funktionen, die LAS zur Generierung der Aktivierungslizenz validiert	LAS-Berechtigungsvalidierungsparameter

Bewährte Methoden zur Überwachung Ihrer LAS-migrierten NetScaler Console Service-Umgebung

Dieses Dokument konzentriert sich auf die bewährten Methoden, die Sie zur Überwachung Ihrer NetScaler-Umgebungen, die LAS verwenden, befolgen können. Dieses Dokument gilt für Bereitstellungen, die LAS mit dem Console-Dienst verwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Voraussetzungen

- Lesen Sie die Seite LAS für NetScaler, einschließlich der FAQ für LAS mit dem Console-Dienst.
- Lesen Sie den Lizenzaktivierungsdienst und schließen Sie Ihre LAS-Migration ab.
- Stellen Sie sicher, dass Sie die relevanten Benachrichtigungen einrichten und die NetScaler GUI und CLI regelmäßig überwachen.

HINWEIS:

Wir beabsichtigen, Benachrichtigungen kontinuierlich zu verbessern und diese Dokumentation entsprechend zu aktualisieren.

Überwachung des Ablaufs von LAS-Aktivierungs-Blobs

Für den NetScaler Console-Dienst wird das LAS-Aktivierungs-Blob direkt von LAS an die NetScaler-Instanzen bereitgestellt, die den NetScaler Console-Dienst als Lizenzserver verwenden. Das Blob ist 30 Tage lang oder bis zum Ablauf des Lizenzanspruchs gültig, je nachdem, was zuerst eintritt, und wird alle acht Stunden aktualisiert.

Wenn die Konnektivität zwischen NetScaler und dem NetScaler Console-Dienst unterbrochen wird, kann der NetScaler Console-Dienst das LAS-Aktivierungs-Blob der NetScaler-Instanz nicht aktualisieren. Der NetScaler Console-Dienst versucht dies alle acht Stunden erneut, und nach drei fehlgeschlagenen Versuchen (8 Stunden x 3 = 24 Stunden) wechselt NetScaler in den Status **Grace**. Die NetScaler Console-Dienst-GUI zeigt solche NetScaler-Instanzen dann im Grace-Status an.

Dieser Abschnitt beschreibt die Benachrichtigungen, die ausgelöst werden, wenn ein LAS-Aktivierungs-Blob kurz vor dem Ablauf steht (weniger als 30 Tage), was darauf hinweist, dass die Bereitstellung Aufmerksamkeit erfordert. Um dies zu beheben, überprüfen und beheben Sie alle Konnektivitätsprobleme oder wenden Sie sich an den Citrix Support.

NetScaler-Instanzen über die GUI anzeigen

Um NetScaler-Instanzen anzuzeigen, die sich im Grace-Status befinden, navigieren Sie zu **Console Service GUI > NetScaler Licensing > Flexed Licensing > Dashboard**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler-Instanzstatus über die CLI anzeigen

Um NetScaler-Instanzen im Status **Grace** und die verbleibende Kulanzzeitdauer anzuzeigen, führen Sie den Befehl `sh licenseserver` aus.

Beispiel:

```
> sh licenseserver

     License Server: 10.102.123.31 Status: Disconnected

        Grace: Yes         Grace Time Left: 652

Done
```

Benachrichtigungen

Banner im NetScaler Console-Dienst:

Die GUI des NetScaler Console-Dienstes zeigt ein Banner an, das NetScaler-Instanzen auflistet, deren LAS-Aktivierungs-Blob in x Tagen abläuft, wobei x weniger als 30 Tage beträgt.

Banner im NetScaler Console-Dienst(/en-us/netscaler-console-service/media/blob-service-gui-banner.png)

Banner in der NetScaler-GUI:

Die GUI des NetScaler Console-Dienstes zeigt ein Banner an, wenn sich die NetScaler-Instanz im Kulanzstatus befindet.

Banner in der NetScaler-GUI(/en-us/netscaler-console-service/media/blob-gui-banner.png)

Von NetScaler generierte SNMP-Traps für den Kulanzstatus:

Wenn sich NetScaler-Instanzen im Kulanzstatus befinden, generiert NetScaler die folgenden SNMP-Traps:

- `pooledLicenseGraceStarted`: Wird ausgelöst, wenn die Instanz in die Kulanzzeit eingetreten ist.
- `pooledLicenseGraceNormal`: Wird ausgelöst, wenn die Kulanzzeit von 30 Tagen endet, was bedeutet, dass die Bereitstellung beeinträchtigt ist und die Instanz nicht lizenziert wird.
- `pooledLicenseGracePeriodOver`: Wird ausgelöst, wenn die Kulanzzeit abgelaufen ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Beispiel:

```
May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGraceStarted
(nsPartitionName = default)

May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGraceNormal
(nsPartitionName = default)

May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGracePeriodOver
(nsPartitionName = default)
```

Überwachung des Ablaufs von Lizenzberechtigungen

Das **Ablaufdatum der Lizenzberechtigung** bezieht sich auf die Lizenzberechtigung des Kunden oder das Vertragsablaufdatum.

Um Informationen zum Ablauf der Lizenzberechtigung über die GUI anzuzeigen, navigieren Sie zu **Console Service GUI > NetScaler Licensing > License Management > LAS**.

Die **Tage bis zum Ablauf** zeigen das Ablaufdatum der Berechtigung für die entsprechende Lizenz an.

Benachrichtigungen

NetScaler Console Service GUI-Banner:

Die NetScaler Console Service GUI zeigt ein Banner an, das darauf hinweist, dass die Lizenzberechtigung in x Tagen abläuft.

E-Mail-basierte Benachrichtigungen:

So konfigurieren Sie Benachrichtigungen für den Ablauf der Lizenzberechtigung:

1. Navigieren Sie zu **Console Service GUI > NetScaler Licensing > License Management > Notification Settings**.
2. Geben Sie den gewünschten Wert unter **Wie viele Tage vor Ablauf der Lizenz möchten Sie benachrichtigt werden?** ein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lizenzverwaltung

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Suite von Citrix-Produkten. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, und unterstützt NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed Term Bandwidth-Lizenzen. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Release 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 in Console on-prem Releases ab 14.1-51.x und ab 13.1-60.x eingestellt. Wenn Sie auf Console on-prem Release 14.1-51.x oder Release 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch vor 15th April 2026 auf Console on-prem Release 14.1-51.x oder höher aktualisieren und zu LAS wechseln, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, Perpetual werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden bei einem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies gesetzlich oder durch Vorschriften verboten ist.
Wenn Sie Fragen oder Bedenken haben, wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix-Wartung bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder

© 1997–2026 Citrix Systems, Inc. All rights reserved.

aussetzen, zusätzlich zu allen anderen Rechtsmitteln, die Citrix gesetzlich oder nach Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften verboten sind.

LAS-basierte Lizenz

Mit dem License Activation Service (LAS) werden die Berechtigungen automatisch in der NetScaler Console-Benutzeroberfläche angezeigt, sodass keine manuellen Maßnahmen erforderlich sind.

Lizenzserver-Ports

Das LAS verwendet Port 443 für die gesamte Lizenzkommunikation.

HINWEIS:

Um LAS zu verwenden, fügen Sie Ihre NetScaler-Instanz als verwaltete Instanz hinzu.

Informationen zum Lizenzablauf

Lizenzablauf anzeigen

1. Navigieren Sie zu **NetScaler Licensing > License Management**.
2. Der Abschnitt **Informationen zum Ablauf der Lizenzberechtigung** enthält Details zu Lizenzen, die demnächst ablaufen.
    - **Feature**: Art der Lizenz, die abläuft.
    - **Anzahl**: Anzahl der Instanzen oder Bandbreite (in Mbit/s), die betroffen sind.
    - **Tage bis zum Ablauf**: Anzahl der Tage bis zum Lizenzablauf (Vertragsenddatum).

HINWEIS:

Neu erworbene gepoolte oder flexible Berechtigungen werden automatisch im Abschnitt **Informationen zum Ablauf der Lizenzberechtigung** angezeigt.

Verhalten beim Lizenzablauf

Wenn eine über die NetScaler Console verwaltete Lizenz abläuft, stellt die zugehörige NetScaler-Instanz die Verarbeitung des Datenverkehrs ein, und ihre Konfiguration kann verloren gehen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benachrichtigungs-E-Mail und ein Pop-up-Banner am Lizenzablaufdatum

In der NetScaler Console GUI wird eine Pop-up-Meldung zum Lizenzablaufdatum angezeigt. Standardmäßig erhalten Sie in der GUI (jedes Mal nach der Anmeldung) eine Pop-up-Meldung, die 30 Tage (Standard) vor dem Lizenzablaufdatum beginnt.Sie können die Anzahl der Tage unter **Benachrichtigungseinstellungen > Einstellung für Lizenzablauf** konfigurieren.

Als Administrator erhalten Sie auch eine Benachrichtigungs-E-Mail für das Lizenzablaufdatum, wenn die E-Mail-Benachrichtigung in den **Benachrichtigungseinstellungen** konfiguriert ist. Eine Benachrichtigungs-E-Mail wird in einer Häufigkeit von 60, 30, 20 und 10 Tagen vor dem Lizenzablaufdatum gesendet.

Benachrichtigungseinstellungen

Führen Sie die folgenden Schritte aus, um Benachrichtigungen für ablaufende Flexed- oder Pooled-Lizenzen einzurichten, die von LAS verwaltet werden:

1. Navigieren Sie zu **NetScaler-Lizenzen > Lizenzverwaltung > Benachrichtigungseinstellungen**.
2. Wählen Sie im Abschnitt **Benachrichtigungseinstellungen** die Option **Mich über Lizenznutzung benachrichtigen** aus. Legen Sie den Warnschwellenwert als Prozentsatz der flexiblen oder gepoolten Lizenzkapazität fest, die zugewiesen werden soll, um eine Benachrichtigung zu senden.
3. Wählen Sie den Benachrichtigungstyp aus, den Sie senden möchten, wenn Lizenzen den Schwellenwert erreichen oder kurz vor dem Ablauf stehen, indem Sie das entsprechende Kontrollkästchen aktivieren. Die Benachrichtigungstypen sind wie folgt.

    - **E-Mail**: E-Mail-Profil oder Verteilerliste zum Senden von Benachrichtigungen. Weitere Informationen finden Sie unter Verteilerliste erstellen.
    - **Slack**: Slack-Profildetails zum Senden von Benachrichtigungen.
    - **PagerDuty**: PagerDuty-Profil zum Senden von Benachrichtigungen.
    - **ServiceNow**: Das Citrix ServiceNow-Profil ist standardmäßig angegeben und die einzige verfügbare Option. Weitere Informationen zum Erstellen dieser Profile finden Sie unter Benachrichtigungen konfigurieren
    - Wählen Sie einen Benachrichtigungstyp aus und klicken Sie auf **Hinzufügen**, um Details hinzuzufügen. Sie können auch jedes Benachrichtigungssystem testen, bevor Sie Ihre Einstellungen speichern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Geben Sie die **Tage bis zum Ablauf** an, d. h. die Anzahl der Tage, bevor Sie über den Lizenzablauf benachrichtigt werden möchten.
5. Klicken Sie auf **Speichern**.

E-Mail-Verteilerliste erstellen

Führen Sie die folgenden Schritte aus, um eine E-Mail-Verteilerliste zu erstellen:

1. Wählen Sie **E-Mail** aus und klicken Sie auf **Hinzufügen**.
2. Geben Sie unter **E-Mail-Verteilerliste erstellen** die folgenden Details an:
   - **Name** – Geben Sie den Namen der Verteilerliste an.
   - **An** – Geben Sie die E-Mail-Adressen an, an die die NetScaler Console die Nachricht sendet.
   - **Cc** – Geben Sie die E-Mail-Adressen an, an die die NetScaler Console die Nachricht kopiert.
   - **Bcc** – Geben Sie die E-Mail-Adressen an, an die die NetScaler Console die Nachricht als Blindkopie sendet (die E-Mail-Adresse wird nicht angezeigt).
3. Klicken Sie auf **Erstellen**.

Slack-Profil erstellen

Führen Sie die folgenden Schritte aus, um ein Slack-Profil zu erstellen:

1. Klicken Sie unter **Slack** auf **Hinzufügen**.
2. Geben Sie unter **Slack-Profil erstellen** die folgenden Details an:
   - **Benachrichtigungen** – Wenn aktiviert, werden Warnungen und Ereignisbenachrichtigungen direkt an einen bestimmten Slack-Kanal gesendet.
   - **Benachrichtigungen mit Anhängen** – Wenn aktiviert, werden detaillierte Informationen zu ausgelösten Warnungen und Ereignissen als E-Mail-Anhang oder als JSON-Payload innerhalb eines Webhooks gesendet.
   - **Profilname** – Geben Sie den Profilnamen an. Dieser Name wird in der Slack-Profilliste angezeigt.
   - **Kanalname** – Geben Sie den Slack-Kanalnamen an, an den die NetScaler Console die Benachrichtigung sendet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Webhook-URL** – Geben Sie die Webhook-URL des Kanals an. Eingehende Webhooks sind eine einfache Möglichkeit, Nachrichten von externen Quellen in Slack zu posten. Die URL ist intern mit dem Kanalnamen verknüpft. Alle Ereignisbenachrichtigungen, die an diese URL gesendet werden, werden auf dem dafür vorgesehenen Slack-Kanal gepostet. Ein Beispiel für einen Webhook ist wie folgt: `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`.

Ein PagerDuty-Profil erstellen

PagerDuty ermöglicht es Ihnen, Benachrichtigungen per E-Mail, Push-Benachrichtigungen und Telefonanrufe an eine registrierte Nummer zu konfigurieren. Bevor Sie ein PagerDuty-Profil in der NetScaler Console hinzufügen, stellen Sie sicher, dass Sie die erforderlichen Konfigurationen in PagerDuty abgeschlossen haben. Um mit PagerDuty zu beginnen, lesen Sie die PagerDuty-Dokumentation.

Führen Sie die folgenden Schritte aus, um ein PagerDuty-Profil zu erstellen:

1. Klicken Sie in **PagerDuty** auf **Hinzufügen**.
2. Geben Sie unter **PagerDuty-Profil erstellen** die folgenden Details an:
   - **Profilname** – Geben Sie einen Profilnamen an. Dieser Name wird von verschiedenen Modulen, wie z. B. Ereignisregeln und SSL-Benachrichtigungen, verwendet, um PagerDuty-Warnungen zu senden.
   - **Integrationsschlüssel** – Geben Sie den Integrationsschlüssel an. Diesen Schlüssel erhalten Sie über Ihr PagerDuty-Portal. Wenn Sie einen Dienst in PagerDuty für die Integration erstellen, verwenden Sie die Option **Generische Ereignis-API-Integration**.
3. Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter Dienste und Integrationen in der PagerDuty-Dokumentation.

Das ServiceNow-Profil anzeigen

Um ServiceNow-Benachrichtigungen für NetScaler-Ereignisse zu aktivieren, müssen Sie die NetScaler Console mithilfe des ITSM-Connectors in ServiceNow integrieren. Weitere Informationen finden Sie unter NetScaler Console in die ServiceNow-Instanz integrieren.

Führen Sie die folgenden Schritte aus, um das ServiceNow-Profil anzuzeigen und zu überprüfen:

1. In **ServiceNow** ist das Profil **Citrix_Workspace_SN** standardmäßig ausgewählt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Klicken Sie auf **Testen**, um ein ServiceNow-Ticket automatisch zu generieren und die Konfiguration zu überprüfen.

Hinweis

Informationen zu den verschiedenen Arten von NetScaler-Lizenzen finden Sie unter Lizenzierungsübersicht.

RBAC-Unterstützung für LAS

Sie können die rollenbasierte Zugriffssteuerung (RBAC) verwenden, um den LAS-Anwendungszugriff mit den folgenden Steuerungsebenen zu verwalten:

- **Funktionsebene**: Beschränken Sie die Sichtbarkeit der Lizenzierungsfunktion für bestimmte Administratoren.
- **Instanzebene**: Beschränken Sie autorisierte Administratoren darauf, Lizenzen nur auf ausgewählte NetScaler-Instanzen anzuwenden.

Konfigurationsdetails finden Sie unter Rollenbasierte Zugriffssteuerung.

Manuell verwaltete Berechtigungen (dateibasierte Lizenzen)

Die folgenden Abschnitte gelten für manuell verwaltete Berechtigungen (dateibasierte Lizenzierung).

HINWEIS:

Wenn Sie eine Universal Hybrid Multi-Cloud (UHMC) oder eine Citrix Platform License (CPL) erwerben, werden die gelieferten NetScaler-Lizenzen als Flexed-Lizenzen bezeichnet. Weitere Informationen finden Sie unter UHMC/CPL-Angebote.

Lizenzdateien

Die NetScaler Flexed-Lizenz enthält die folgenden Dateien, die Sie vom MyCitrix-Portal herunterladen müssen. Weitere Informationen zum Übergang von Ihrem aktuellen NetScaler-Lizenztyp zu Flexed Licensing finden Sie unter Übergang zu Flexed Licensing.

Die auf Ihrem NetScaler vorhandenen Lizenzdateien sind in diesem Abschnitt aufgeführt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DATEINAME ENTHÄLT	BESCHREIBUNG	DOWNLOAD-INFORMATIONEN	WO DIE LIZENZ HOCHGELADEN/ ANGEWENDET WIRD
NetScaler Flexed VPX SW-Instanz	Berechtigt Sie zu VPX-/CPX-/BLX-Softwareinstanzen	Laden Sie diese Datei mit Ihrer NetScaler Console Host-ID herunter	Auf NetScaler Console
NetScaler Flexed MPX SW-Instanz	Berechtigt Sie zu MPX-Softwareinstanzen	Laden Sie diese Datei mit Ihrer NetScaler Console Host-ID herunter	Auf NetScaler Console
NetScaler Flexed SDX SW-Instanz	Berechtigt Sie zu SDX-Softwareinstanzen	Laden Sie diese Datei mit Ihrer NetScaler Console Host-ID herunter	Auf NetScaler Console
NetScaler Flexed Platinum BW	Berechtigt Sie zu Flexed Platinum Durchsatzkapazität	Laden Sie diese Datei mit Ihrer NetScaler Console Host-ID herunter	Auf NetScaler Console
NetScaler Flexed VPX FIPS SW-Instanz	Berechtigt Sie zu VPX FIPS Softwareinstanzen	Laden Sie diese Datei mit Ihrer NetScaler Console Host-ID herunter	Auf NetScaler Console
Zero Capacity MPX-Z Plattformlizenz	Berechtigt Sie, Ihre NetScaler MPX HW/ NetScaler MPX FIPS HW an der Flexed-Lizenzierung teilnehmen zu lassen	Laden Sie diese Datei herunter	Auf NetScaler MPX
Zero Capacity SDX-Z Plattformlizenz	Berechtigt Sie, Ihre NetScaler SDX HW/ NetScaler SDX FIPS HW an der Flexed-Lizenzierung teilnehmen zu lassen	Diese Datei herunterladen	Auf NetScaler SDX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wichtige Hinweise

- Sie können Lizenzen auf mehrere NetScaler Console Service-Mandanten oder mehrere lokale NetScaler Console-Instanzen hochladen.
- Wenn Sie von einer Pool-Lizenz zu einer Flexed-Lizenz wechseln und Ihre MPX- und SDX-Instanzen bereits unbefristete Z-Cap-Lizenzen besitzen, ist die Anwendung der mit der Flexed-Lizenz erhaltenen Z-Cap-Lizenzen nicht erforderlich. Wenn die aktuellen Z-Cap-Lizenzen, die auf NetScaler MPX oder NetScaler SDX angewendet werden, jedoch für eine bestimmte Dauer gültig sind, müssen Sie die mit der Flexed-Lizenz erhaltenen Z-Cap-Lizenzen anwenden.
- MPX-Z- oder SDX-Z-Plattformlizenzen, die als Teil von Flexed-Lizenzen geliefert werden, sind unbefristet. Nachdem die MPX-Z- oder SDX-Z-Plattformlizenzdatei auf den spezifischen Instanzen angewendet wurde, kann sie bis zum End of Life (EOL) der Instanz verwendet werden.
- Sie müssen die Flexed-Lizenzen auf NetScaler Console für den NetScaler-Formfaktor anwenden, den Sie in Ihrer Bereitstellung verwenden. Zum Beispiel:

  Wenden Sie die folgenden Lizenzen an, wenn Sie den NetScaler SDX-Formfaktor verwenden:

  |Lizenzdatei|Anwenden auf| |-|-| |NetScaler Flexed SDX SW-Instanz|NetScaler Console| |NetScaler Flexed VPX SW-Instanz|NetScaler Console| |NetScaler Flexed Platinum BW|NetScaler Console| |ADC Zero Capacity SDX-Z Platform|NetScaler SDX|

  Wenden Sie die folgenden Lizenzen an, wenn Sie den NetScaler MPX Formfaktor verwenden:

  |Lizenzdatei|Anwenden auf| |-|-| |NetScaler Flexed MPX SW Instance|NetScaler Console| |NetScaler Flexed Platinum BW|NetScaler Console| |ADC Zero Capacity MPX-Z Platform|NetScaler MPX|

  Wenden Sie die folgenden Lizenzen an, wenn Sie den NetScaler VPX-, NetScaler BLX- oder NetScaler CPX-Formfaktor verwenden:

  |Lizenzdatei|Anwenden auf| |-|-| |NetScaler Flexed VPX SW-Instanz|NetScaler Console| |NetScaler Flexed Platinum BW|NetScaler Console|

  Wenden Sie die folgenden Lizenzen an, wenn Sie den NetScaler VPX FIPS Formfaktor verwenden

  |Lizenzdatei|Anwenden auf| |-|-| |NetScaler Flexed VPX FIPS SW-Instanz|NetScaler Console| |NetScaler Flexed Platinum BW|NetScaler Console|

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Eine Lizenzdatei anwenden

Sie können Lizenzen hinzufügen, löschen und herunterladen. Sie müssen Lizenzen anwenden, bevor sie verwendet werden können.

1. Navigieren Sie zu **NetScaler Licensing > License Management**.
2. Klicken Sie im Abschnitt **License Files** auf **Add License File** und wählen Sie eine der folgenden Optionen aus:
   - **Lizenzdateien von einem lokalen Computer hochladen**: Wenn eine Lizenzdatei bereits auf Ihrem lokalen Computer vorhanden ist, können Sie sie in die NetScaler Console hochladen.
   - **Lizenzzugriffscode verwenden**: Geben Sie den Lizenzzugriffscode für die Lizenz an, die Sie von Citrix erworben haben. Klicken Sie auf **Get Licenses** und dann auf **Finish**.
3. Klicken Sie auf „Fertig stellen“. Die Lizenzdateien werden der NetScaler Console hinzugefügt. Der Abschnitt **License Expiry Information** listet die in der NetScaler Console vorhandenen Lizenzen, die Anzahl und die verbleibenden Tage bis zum Ablauf auf.

   HINWEIS:

   Das Lizenzenddatum ist das Datum, bis zu dem Ihr Vertrag gültig ist, und Sie müssen ihn vor dem Enddatum verlängern.

   Der folgende Screenshot zeigt die Anzahl der Flexed NetScaler VPX-, NetScaler MPX-, NetScaler SDX- und NetScaler VPX FIPS-Softwareinstanzlizenzen, die vorhandene Flexed Premium-Bandbreitenkapazität und die Tage bis zum Ablauf (Vertragsenddatum).

   Der folgende Screenshot zeigt die verfügbare Pooled Standard-, Advanced- und Premium-Bandbreite und die Tage bis zum Ablauf (Vertragsenddatum).

4. Wählen Sie eine Lizenzdatei aus und klicken Sie auf **Apply licenses**.

Lizenzdatei löschen

Um eine Lizenzdatei zu löschen, wählen Sie eine oder mehrere Dateien aus und klicken Sie auf **Delete**. Wenn Sie eine Lizenz löschen, müssen Sie die Lizenz zuerst hinzufügen und erst dann können Sie sie anwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lizenzdatei herunterladen

Um eine Lizenzdatei herunterzuladen, wählen Sie eine Datei aus und klicken Sie auf **Herunterladen**. Sie können die Lizenzdatei als Sicherung offline speichern.

Porteinstellungen des Lizenzservers

Ports werden von NetScaler-Instanzen verwendet, um mit dem Lizenzserver zu kommunizieren. Klicken Sie auf das Symbol **Bearbeiten** und geben Sie Werte für die folgenden Parameter an:

- **Lizenzserver-Port**: Der Proxy-Server-Port, der von NetScaler-Instanzen verwendet wird, um auf das Citrix-Lizenzierungsportal für die Lizenzzuweisung zuzugreifen. Standardwert: 27000.
- **Vendor-Daemon-Port**: Der Lizenzserver-Port, der von NetScaler-Instanzen verwendet wird, um mit dem Lizenzserver zu kommunizieren. Standardwert: 7279.

Informationen zum Lizenzablauf

Sie können den Schwellenwert für den Lizenzablauf für flexible oder gepoolte Kapazitätslizenzen konfigurieren. Wenn der Schwellenwert festgelegt ist, sendet NetScaler Console E-Mail-Benachrichtigungen, wenn eine Lizenz abläuft. Ein SNMP-Trap und eine Benachrichtigung werden auch gesendet, wenn die Lizenz in NetScaler Console abgelaufen ist.

Ein Ereignis wird generiert, wenn eine Lizenzablaufbenachrichtigung gesendet wird, und dieses Ereignis kann in NetScaler Console unter **Infrastruktur > Ereignisse** angezeigt werden.

Lizenzablauf anzeigen

1. Navigieren Sie zu **NetScaler Licensing > License Management**.
2. Auf der Seite **Lizenz-Einstellungen** finden Sie im Abschnitt **Informationen zum Lizenzablauf** die Details der Lizenzen, die ablaufen werden:
    - **Funktion**: Art der Lizenz, die abläuft.
    - **Anzahl**: Anzahl der betroffenen virtuellen Server oder Instanzen.
    - **Tage bis zum Ablauf**: Anzahl der Tage bis zum Lizenzablauf (Vertragsenddatum).

HINWEIS:

Wenn Sie dem Pool neue Lizenzen hinzufügen, verwenden die NetScaler-Instanzen die neuen Lizenzen nach Ablauf ihrer bestehenden Lizenzen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benachrichtigungs-E-Mail und Pop-up-Banner zum Lizenzenddatum

In der NetScaler Console-GUI wird eine Pop-up-Meldung zum Lizenzenddatum angezeigt. Als Administrator erhalten Sie außerdem eine Benachrichtigungs-E-Mail für das Lizenzenddatum. Standardmäßig erhalten Sie 60 Tage vor dem Lizenzenddatum eine Pop-up-Meldung in der GUI (jedes Mal nach dem Login) und eine Benachrichtigungs-E-Mail in einer Frequenz von 60, 30, 20 und 10 Tagen vor dem Lizenzenddatum.

Verhalten bei Lizenzablauf

NetScaler-Instanzen mit abgelaufenen Lizenzen, die über NetScaler Console verwaltet werden, verarbeiten keinen Datenverkehr mehr und können zu Konfigurationsverlusten führen.

Benachrichtigungseinstellungen

Geben Sie die Einstellungen an, auf deren Grundlage Benachrichtigungen über die Lizenzzuweisung und die verbleibenden Tage bis zum Ablauf gesendet werden.

1. Klicken Sie im Abschnitt **Benachrichtigungseinstellungen** auf das Symbol **Bearbeiten** und wählen Sie **Mich über Lizenznutzung benachrichtigen**. Legen Sie den Warnschwellenwert als Prozentsatz der flexiblen oder gepoolten Lizenzkapazität fest, der zugewiesen werden soll, um eine Benachrichtigung zu senden.
2. Wählen Sie den Benachrichtigungstyp aus, den Sie senden möchten, wenn Lizenzen den Schwellenwert erreichen oder kurz vor dem Ablauf stehen, indem Sie das entsprechende Kontrollkästchen aktivieren. Die Benachrichtigungstypen sind wie folgt.

   - **E-Mail**: E-Mail-Profil oder Verteilerliste zum Senden von Benachrichtigungen. Weitere Informationen finden Sie unter Erstellen einer E-Mail-Verteilerliste.
   - **Slack**: Slack-Profildetails zum Senden von Benachrichtigungen.
   - **PagerDuty**: PagerDuty-Profil zum Senden von Benachrichtigungen.
   - **ServiceNow**: Das Citrix ServiceNow-Profil ist standardmäßig angegeben und die einzige verfügbare Option. Weitere Informationen zum Erstellen dieser Profile finden Sie unter Benachrichtigungen konfigurieren

   Wählen Sie einen Benachrichtigungstyp aus und klicken Sie auf **Hinzufügen**, um Details hinzuzufügen. Sie können auch jedes Benachrichtigungssystem testen, bevor Sie Ihre Einstellungen speichern.
3. Geben Sie die **Tage bis zum Ablauf** an, d. h. die Anzahl der Tage, bevor Sie über den Lizenzablauf benachrichtigt werden möchten.
4. Klicken Sie auf **Speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

E-Mail-Verteilerliste erstellen

Führen Sie die folgenden Schritte aus, um eine E-Mail-Verteilerliste zu erstellen:

1. Wählen Sie **E-Mail** aus und klicken Sie auf **Hinzufügen**.
2. Geben Sie unter **E-Mail-Verteilerliste erstellen** die folgenden Details an:
    - **Name** – Geben Sie den Namen der Verteilerliste an.
    - **E-Mail-Server** – Wählen Sie den E-Mail-Server aus, der die E-Mail-Benachrichtigung sendet. Um einen E-Mail-Server hinzuzufügen, klicken Sie auf Hinzufügen. Geben Sie den Servernamen/die IP-Adresse und den Port an. Wählen Sie Authentifizierung aus, um die Authentifizierung für den Zugriff auf den E-Mail-Server zu erzwingen. Wählen Sie Sicher aus, wenn der E-Mail-Server die SSL-Authentifizierung unterstützt. Klicken Sie auf Erstellen.
    - **Von** – Geben Sie die E-Mail-Adresse an, von der die NetScaler Console die Nachricht sendet.
    - **An** – Geben Sie die E-Mail-Adressen an, an die die NetScaler Console die Nachricht sendet.
    - **Cc** – Geben Sie die E-Mail-Adressen an, an die die NetScaler Console die Nachricht als Kopie sendet.
    - **Bcc** – Geben Sie die E-Mail-Adressen an, an die die NetScaler Console die Nachricht als Blindkopie sendet (die E-Mail-Adresse wird nicht angezeigt).
3. Klicken Sie auf **Erstellen**.

Slack-Profil erstellen

Führen Sie die folgenden Schritte aus, um ein Slack-Profil zu erstellen:

1. Klicken Sie unter **Slack** auf **Hinzufügen**.
2. Geben Sie unter **Slack-Profil erstellen** die folgenden Details an:
    - **Profilname** – Geben Sie den Profilnamen an. Dieser Name wird in der Slack-Profilliste angezeigt.
    - **Kanalname** – Geben Sie den Slack-Kanalnamen an, an den die NetScaler Console die Benachrichtigung sendet.
    - **Webhook-URL** – Geben Sie die Webhook-URL des Kanals an. Eingehende Webhooks sind eine einfache Möglichkeit, Nachrichten von externen Quellen in Slack zu posten. Die URL ist intern mit dem Kanalnamen verknüpft. Alle Ereignisbenachrichtigungen, die an

© 1997–2026 Citrix Systems, Inc. All rights reserved.

diese URL gesendet werden, werden auf dem angegebenen Slack-Kanal veröffentlicht. Ein Beispiel für einen Webhook ist wie folgt: `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`.

Ein PagerDuty-Profil erstellen

PagerDuty ermöglicht es Ihnen, Benachrichtigungen per E-Mail, Push-Benachrichtigungen und Telefonanrufe an eine registrierte Nummer zu konfigurieren. Bevor Sie ein PagerDuty-Profil in NetScaler Console hinzufügen, stellen Sie sicher, dass Sie die erforderlichen Konfigurationen in PagerDuty abgeschlossen haben. Informationen zu den ersten Schritten mit PagerDuty finden Sie in der PagerDuty-Dokumentation.

Führen Sie die folgenden Schritte aus, um ein PagerDuty-Profil zu erstellen:

1. Klicken Sie unter **PagerDuty** auf **Hinzufügen**.
2. Geben Sie unter **PagerDuty-Profil erstellen** die folgenden Details an:
   - **Profilname** – Geben Sie einen Profilnamen an. Dieser Name wird von verschiedenen Modulen, wie z. B. Ereignisregeln und SSL-Benachrichtigungen, verwendet, um PagerDuty-Warnungen zu senden.
   - **Integrationsschlüssel** – Geben Sie den Integrationsschlüssel an. Diesen Schlüssel erhalten Sie über Ihr PagerDuty-Portal. Wenn Sie einen Dienst in PagerDuty für die Integration erstellen, verwenden Sie die Option **Generic Events API Integration**.
3. Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter Services and Integrations in der PagerDuty-Dokumentation.

ServiceNow-Profil anzeigen

Um ServiceNow-Benachrichtigungen für NetScaler-Ereignisse zu aktivieren, müssen Sie NetScaler Console mithilfe des ITSM-Konnektors in ServiceNow integrieren. Weitere Informationen finden Sie unter NetScaler Console in die ServiceNow-Instanz integrieren.

Führen Sie die folgenden Schritte aus, um das ServiceNow-Profil anzuzeigen und zu überprüfen:

1. In **ServiceNow** ist das Profil **Citrix_Workspace_SN** standardmäßig ausgewählt.
2. Klicken Sie auf **Test**, um ein ServiceNow-Ticket automatisch zu generieren und die Konfiguration zu überprüfen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Informationen zu den verschiedenen Arten von NetScaler-Lizenzen finden Sie unter Lizenzierungsübersicht.

Mindest- und Höchstkapazität für die Ausleihe

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener On-Premises-Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Citrix Produktpalette. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, wobei NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed Term Bandwidth-Lizenzen unterstützt werden. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler®-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 für Console on-prem-Versionen ab 14.1-51.x und ab 13.1-60.x eingestellt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis April 15 2026 weiterhin verwenden. Sie müssen jedoch auf Console on-prem Version 14.1-51.x oder höher aktualisieren und vor April 15 2026 auf LAS umstellen, da Console on-prem 13.1 LAS nicht unterstützt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, Perpetual werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden nach dem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies gesetzlich oder durch Vorschriften untersagt ist.
Wenn Sie Fragen oder Bedenken haben, wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix-Wartung bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder aussetzen, zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit zustehen. Diese Anforderungen gelten nicht, wo dies gesetzlich oder durch Vorschriften untersagt ist.
Die NetScaler Flexed-Lizenzierung verwendet NetScaler Console, die als Lizenzserver konfiguriert ist, um Flexed-Lizenzen zu verwalten: Bandbreiten-Pool-Lizenzen und Instanz-Pool-Lizenzen.

Beim Ausleihen von Lizenzen aus dem Bandbreiten- und Instanz-Pool bestimmen der NetScaler-Formfaktor und die Hardware-Modellnummer auf einer Hardware ohne Kapazität:

- Die minimale Bandbreite und die Anzahl der Instanzen, die eine NetScaler-Instanz ausleihen muss, bevor sie funktionsfähig ist.
- Die maximale Bandbreite und die Anzahl der Instanzen, die ein NetScaler auschecken kann.
- Die minimale Bandbreiteneinheit für jeden Bandbreiten-Checkout. Die minimale Bandbreiteneinheit ist die kleinste Bandbreiteneinheit, die ein NetScaler aus einem Pool auschecken muss. Jeder Checkout muss ein ganzzahliges Vielfaches der minimalen Bandbreiteneinheit sein. Wenn beispielsweise die minimale Bandbreiteneinheit eines NetScalers 1 Gbit/s beträgt, können 1000 Mbit/s ausgecheckt werden, aber nicht 200 Mbit/s oder 150,5 Gbit/s. Die minimale Bandbreiteneinheit unterscheidet sich von der minimalen Bandbreitenanforderung. Eine NetScaler-Instanz kann nur betrieben werden, nachdem sie mit mindestens der minimalen Bandbreite lizenziert wurde. Sobald die minimale Bandbreite erreicht ist, kann die Instanz weitere Bandbreite in Vielfachen der minimalen Bandbreiteneinheit auschecken.

Die Tabellen 1 bis 5 fassen die maximale Bandbreite/Instanzen, die minimale Bandbreite/Instanzen und die minimale Bandbreiteneinheit für alle unterstützten NetScaler-Instanzen zusammen. Tabelle 6 fasst die Lizenzanforderungen für verschiedene Formfaktoren für alle unterstützten NetScaler-Instanzen zusammen. Die folgenden Tabellen beziehen sich auf die Systemanforderungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Die minimale Bandbreiten-Checkout-Einheit für NetScaler CPX/BLX/VPX beträgt 10 Mbit/s.
Die minimale Bandbreiten-Checkout-Einheit für NetScaler MPX/SDX beträgt 1 Gbit/s.

Tabelle 1. Unterstützte Flexed-Kapazität für MPX

PRODUKTLINIE	MINIMALE BANDBREITE (GBIT/S)	MAXIMALE BANDBREITE (GBIT/S)	MINIMALE BANDBREITENEINHEIT
MPX 5900Z	1	10	1 Gbit/s
MPX 8900Z	5	30	1 Gbps
MPX 8900Z FIPS	5	20	1 Gbps
MPX 9100Z	10	95	1 Gbps
MPX 9100Z FIPS	10	95	1 Gbps
MPX 14000Z	20	100	1 Gbit/s
MPX 14000Z-40G	20	100	1 Gbit/s
MPX 14000Z-40S	40	100	1 Gbit/s
MPX 14000Z FIPS	30	80	1 Gbit/s
MPX 15000Z	20	120	1 Gbit/s
MPX 15000Z-50G	20	120	1 Gbit/s
MPX 15000Z FIPS	30	120	1 Gbit/s
MPX 16000Z	30	250	1 Gbit/s
MPX 22000Z	40	120	1 Gbit/s
MPX 24000Z	100	150	1 Gbit/s
MPX 25000Z	100	160	1 Gbit/s

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRODUKTLINIE	MINIMALE BANDBREITE (GBIT/S)	MAXIMALE BANDBREITE (GBIT/S)	MINIMALE BANDBREITENEINHEIT
MPX 25000Z-40G	100	200	1 Gbit/s
MPX 26000Z	100	200	1 Gbit/s
MPX 26000Z-50S	100	200	1 Gbit/s
MPX 26000Z-100G	100	200	1 Gbit/s

Tabelle 2A. Unterstützte Flexed-Kapazität für NetScaler SDX-Versionen vor Build 13.0-47.x

PRODUKTLINIE	MINIMALE BANDBREITE (GBIT/S)	MAXIMALE BANDBREITE (GBIT/S)	MINIMALE INSTANZEN	MAXIMALE INSTANZEN	MINIMALE BANDBREITENEINHEIT
SDX 8900Z	10	30	2	7	1 Gbit/s
SDX 14000Z	20	100	5	25	1 Gbps
SDX 14000Z-40G	40	100	20	25	1 Gbps
SDX 15000Z	20	120	5	55	1 Gbit/s
SDX 15000Z-50G	20	120	5	55	1 Gbit/s
SDX 22000Z	40	120	80	80	1 Gbit/s
SDX 24000Z	100	150	80	80	1 Gbps
SDX 25000Z	100	200	20	115	1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRODUKTLINIE	MINIMALE BANDBREITE (GBIT/S)	MAXIMALE BANDBREITE (GBIT/S)	MINIMALE INSTANZEN	MAXIMALE INSTANZEN	MINIMALE BANDBREITENEINHEIT
SDX 25000Z-40G	100	200	20	115	1 Gbps
SDX 26000Z	100	200	20	115	1 Gbps
SDX 26000Z-50S	100	200	20	115	1 Gbps
SDX 26000Z-100G	100	200	20	115	1 Gbps

Tabelle 2B. Unterstützte Flexed-Kapazität für NetScaler SDX Version 13 (Build 13.0-47.x und höher), Version 13.1 (Build vor 51.x) und Version 14.1 (Build vor 12.x)

PRODUKTLINIE	MINIMALE BANDBREITE (GBPS)	MAXIMALE BANDBREITE (GBPS)	MINIMALE INSTANZEN	MAXIMALE INSTANZEN	MINIMALE BANDBREITENEINHEIT
SDX 8900Z	5	30	1	7	1 Gbps
SDX 9100Z	10	95	2	7	1 Gbps
SDX 14000Z	10	100	2	25	1 Gbps
SDX 14000Z-40G	20	100	10	25	1 Gbps
SDX 15000Z	10	120	2	55	1 Gbps
SDX 15000Z-50G	10	120	2	55	1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRODUKTLINIE	MINIMALE BANDBREITE (GBPS)	MAXIMALE BANDBREITE (GBPS)	MINIMALE INSTANZEN	MAXIMALE INSTANZEN	MINIMALE BANDBREITENEINHEIT
SDX 16000Z	15	250	10	55	1 Gbps
SDX 22000Z	20	120	40	80	1 Gbps
SDX 24000Z	50	150	40	80	1 Gbit/s
SDX 25000Z	50	200	10	115	1 Gbit/s
SDX 25000Z-40G	50	200	10	115	1 Gbit/s
SDX 26000Z	50	200	10	115	1 Gbit/s
SDX 26000Z-50S	50	200	10	115	1 Gbit/s
SDX 26000Z-100G	50	200	10	115	1 Gbit/s

Tabelle 2C. Unterstützte Flexed-Kapazität für NetScaler SDX Version 13.1 (Build 51.x und höher) und Version 14.1 (Build 12.x und höher)

PRODUKTLINIE	MINIMALE BANDBREITE (GBIT/S)	MAXIMALE BANDBREITE (GBIT/S)	MINIMALE INSTANZEN	MAXIMALE INSTANZEN	MINIMALE BANDBREITENEINHEIT
SDX 8900Z	5	30	1	7	1 Gbit/s
SDX 9100Z	10	95	1	7	1 Gbit/s

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PRODUKTLINIE	MINIMALE BANDBREITE (GBIT/S)	MAXIMALE BANDBREITE (GBIT/S)	MINIMALE INSTANZEN	MAXIMALE INSTANZEN	MINIMALE BANDBREITENEINHEIT
SDX 14000Z	10	100	1	25	1 Gbit/s
SDX 14000Z-40G	20	100	1	25	1 Gbps
SDX 15000Z	10	120	1	55	1 Gbps
SDX 15000Z-50G	10	120	1	55	1 Gbps
SDX 16000Z	15	250	1	55	1 Gbps
SDX 22000Z	20	120	1	80	1 Gbps
SDX 24000Z	50	150	1	80	1 Gbps
SDX 25000Z	50	200	1	115	1 Gbps
SDX 25000Z-40G	50	200	1	115	1 Gbit/s
SDX 26000Z	50	200	1	115	1 Gbit/s
SDX 26000Z-50S	50	200	1	115	1 Gbit/s
SDX 26000Z-100G	50	200	1	115	1 Gbps

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEISE:

- Die Mindestbestellmenge kann von der Mindestsystemanforderung abweichen.
- Auf NetScaler SDX mit Build 14.1-12.x und höher wird mit einer Flexed-Lizenz die Beschränkung, eine Mindestanzahl von Instanzlizenzen auszuchecken, aufgehoben. Das heißt, Sie können mindestens eine Instanzlizenz auschecken.

Tabelle 3. Unterstützte minimale/maximale Bandbreite und minimale/maximale Instanzen für NetScaler CPX-Instanzen

PRODUKTLINIE	MAXIMALE BANDBREITE (GBPS)	MINIMALE BANDBREITE (MBPS)	MINIMALE INSTANZEN	MAXIMALE INSTANZEN	MINIMALE BANDBREITENEINHEIT
CPX	10	10	1	1	10 Mbit/s

Tabelle 4. Unterstützte minimale/maximale Bandbreite und minimale/maximale Instanzen für NetScaler VPX-Instanzen auf Hypervisoren und Cloud-Diensten

HYPERVISOR/CLOUD-DIENST	MAXIMALE BANDBREITE (GBIT/S)	MINIMALE BANDBREITE (MBIT/S)	MINIMALE INSTANZEN	MAXIMALE INSTANZEN	MINIMALE BANDBREITENEINHEIT
Citrix Hypervisor	40 Gbps	10 Mbps	1	1	10 Mbps
VMware ESXI	100 Gbps	10 Mbps	1	1	10 Mbps
Linux KVM	100 Gbps	10 Mbps	1	1	10 Mbps
Microsoft Hyper-V	3 Gbps	10 Mbps	1	1	10 Mbps
AWS	30 Gbps	10 Mbps	1	1	10 Mbps
Azure	10 Gbit/s	10 Mbit/s	1	1	10 Mbit/s

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HYPERVISOR/CLOUD-DIENST	MAXIMALE BANDBREITE (GBIT/S)	MINIMALE BANDBREITE (MBIT/S)	MINIMALE INSTANZEN	MAXIMALE INSTANZEN	MINIMALE BANDBREITENEINHEIT
Google Cloud	10 Gbit/s	10 Mbit/s	1	1	10 Mbit/s

Hinweis

Die Mindestbestellmenge unterscheidet sich von den Mindestsystemanforderungen.

Tabelle 5. Unterstützte minimale/maximale Bandbreite und minimale/maximale Instanzen für NetScaler BLX-Instanzen

PRODUKTLINIE	MAXIMALE BANDBREITE (GBPS)	MINIMALE BANDBREITE (MBPS)	MINIMALE INSTANZEN	MAXIMALE INSTANZEN	MINIMALE BANDBREITENEINHEIT
BLX	100	10	1	1	10 Mbps

Tabelle 6. Lizenzanforderung für Nullkapazität für verschiedene Formfaktoren

PRODUKTLINIE	HARDWARE MIT NULLKAPAZITÄT
MPX	Lizenz erforderlich
SDX	Lizenz erforderlich
VPX	-
CPX	-
BLX	-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verhalten des NetScaler-Agenten

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Suite der Citrix-Produkte. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, und unterstützt NetScaler Flexed-Lizenzen (Citrix Platform License/Universal Hybrid Multi-Cloud), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed term Bandwidth licenses. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 in den Console on-prem-Versionen 14.1-51.x und 13.1-60.x und höher eingestellt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch vor 15th April 2026 auf Console on-prem Version 14.1-51.x oder höher aktualisieren und zu LAS wechseln, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen, wie z. B. NetScaler Virtual CPU Licensing (Pooled vCPU), NetScaler VPX Check-In und Check-Out (CICO), unbefristete Lizenzen, werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden bei einem Upgrade auf die oben genannten Softwareversionen unlizenziert. LAS-basierte Lizenzen sind Kunden möglicherweise nicht zugänglich, wo dies gesetzlich oder durch Vorschriften verboten ist.
Bei Fragen oder Bedenken wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix-Wartung bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder aussetzen, zusätzlich

© 1997–2026 Citrix Systems, Inc. All rights reserved.

zu allen anderen Rechtsmitteln, die Citrix nach Gesetz oder Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften verboten sind.
Der NetScaler-Agent fungiert als Vermittler zwischen NetScaler Console und den erkannten Instanzen in verschiedenen Rechenzentren und öffentlichen Clouds. Der NetScaler Console-Dienst erfordert mindestens einen Agenten pro Mandanten, damit die Flexed- oder Pooled-Lizenzierung funktioniert. Es können mehrere NetScaler-Agenten pro Standort oder an mehreren Standorten bereitgestellt werden, aber nur ein Agent kann die Rolle des License Server Agent (LSA) für die gesamte Mandantenbereitstellung innehaben.

LAS-basierte Lizenzierung

Bei der Verwendung von LAS-basierter Lizenzierung übernimmt ein integrierter Agent innerhalb von NetScaler die Lizenzkommunikation. Ein externer Agent ist eine optionale Komponente, die Sie in Ihrer Architektur bereitstellen können, um als Proxy für die Lizenzkommunikation zu dienen.

Informationen zum Konfigurieren des integrierten NetScaler-Agenten für LAS finden Sie unter Konfigurieren des integrierten Agenten zum Verwalten von Instanzen.

Informationen zum Aktivieren des Agent-Failovers finden Sie unter NetScaler Console-Dienst/Erste Schritte/Integrierten Agenten initiieren.

HINWEIS:

Wenn Sie einen integrierten Agenten verwenden, können Sie nur über die NetScaler Console-GUI auf die LAS-basierte Lizenzierung umstellen.

Manuell verwaltete Berechtigung (dateibasierte Lizenzierung)

Ein LSA ist ein Agent, der als Lizenzserver in einer NetScaler Console-Dienst-basierten Pool-Lizenzierungsbereitstellung fungiert. Wenn der LSA ausfällt, wartet der Dienst 24 Stunden, um einen neuen LSA zu wählen.

Bis dahin gehen die NetScaler-Instanzen, die eine gepoolte oder flexible Lizenz verwenden, in die Kulanzperiode. Als Administrator können Sie auch manuell einen LSA wählen.

Das folgende Beispiel zeigt zwei bereitgestellte Agenten, von denen einer die LSA-Rolle hat:

Die folgenden Abschnitte gelten für manuell verwaltete Berechtigungen (dateibasierte Lizenzierung).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manuelles Auswählen eines NetScaler Console-Agenten als LSA

Administratoren können manuell einen NetScaler Console-Agenten als LSA für die NetScaler Pool-Lizenzierung oder die NetScaler Flexible Lizenzierung auswählen. Wenn der LSA ausfällt, wartet der NetScaler Console-Dienst 24 Stunden, bevor er den nächsten LSA automatisch wählt. Der Administrator kann den neuen LSA in der Zwischenzeit manuell über diese Funktion wählen. Der Administrator muss jedoch sicherstellen, dass der Status des neu gewählten LSA UP ist und sein Diagnosestatus OK ist.

Wenn der Administrator manuell einen neuen LSA auswählt, kann es bis zu 5 Minuten dauern, bis die Lizenzierungsfunktionalität korrekt funktioniert. Während dieser Zeit befinden sich die NetScaler-Instanzen in der Kulanzperiode, und jeder neue Lizenz-Checkout schlägt fehl.

So wählen Sie einen LSA aus:

1. Navigieren Sie zu **Infrastructure > Instances Dashboard > Agents** und wählen Sie einen Agenten aus.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Als LSA festlegen**.
3. Klicken Sie zur Bestätigung auf **Ja**. Der ausgewählte Agent übernimmt die LSA-Rolle.

Verhalten mehrerer NetScaler-Agents

In einer Bereitstellung mit einer Kombination aus mehreren Agents und mehreren Sites folgen die NetScaler-Agents der Client/Server-Architektur.

Der erste oder älteste Agent, der in einem UP-Zustand registriert ist, erhält die LSA-Rolle. Alle anderen später hinzugefügten Agents fungieren als Proxy und kommunizieren mit dem Agent, der die Haupt-LSA-Rolle hostet, zur Lizenzzuweisung. Jeder Agent, der die Proxy-Rolle hostet, kommuniziert über den NetScaler Console-Dienst mit dem Agenten, der die aktuelle LSA-Rolle innehat.

HINWEIS:

Es gibt keine direkte Kommunikation zwischen dem Agenten, der die LSA-Rolle innehat, und den anderen (Nicht-LSA-)Agents. Alle Verbindungen laufen ausschließlich über den NetScaler Console-Dienst.

Failover-Verhalten des NetScaler-Agents

Das Agent-Failover funktioniert in einer Multi-Agent-Bereitstellung auf folgende Weise.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Angenommen, es gibt zwei Agents, AG1 und AG2, im selben Rechenzentrum.

- AG1 ist so konfiguriert, dass es ADC11, ADC12, ADC13 als Remote-Lizenzhost oder LSA verwendet.
- AG2 ist so konfiguriert, dass es ADC21, ADC22, ADC23 als Remote-Lizenzhost oder LSA verwendet.
- AG2 fungiert als Lizenzserver.
    - Wenn AG1 ausfällt, verbinden sich ADC11, ADC12 und ADC13 automatisch über AG2 zur Lizenzabstimmung.
        - ADC11, ADC12 und ADC13 bemerken möglicherweise immer noch eine kleine Kulanzzeit, wenn einige Heartbeats verpasst werden, während diese Wiederverbindung stattfindet.
    - Wenn AG2 ausfällt, bleiben alle ADCs im Kulanzzeitraum, bis:
        - Entweder AG2 wieder hochfährt/wiederhergestellt wird, oder AG1 als neuer LSA ausgewählt wird, entweder automatisch nach 24 Stunden durch den NetScaler Console-Dienst oder manuell durch den Administrator.
        - Oder AG2 wird aus dem NetScaler Console-Dienst gelöscht. Nach der Deregistrierung weist der NetScaler Console-Dienst AG1 die LSA-Rolle als Agent zu.
        - Nach Abschluss der Wahl beginnt AG1 mit der Zuweisung und Abstimmung von Ressourcen für die konfigurierten Instanzen.

Bei Fragen zum LSA siehe FAQs zum Lizenzserver-Agent.

Lizenzserver über den integrierten NetScaler-Agenten konfigurieren

Wenn Sie einen Lizenzserver-Agenten (LSA) an einem Standort konfiguriert haben und denselben LSA von anderen Standorten aus verwenden möchten, können Sie einen integrierten NetScaler-Agenten verwenden. Bei Verwendung des integrierten Agenten müssen Sie den Lizenzserver mit dem folgenden Befehl auf der NetScaler-Instanz konfigurieren.

```
add licenseserver 127.0.0.1 -port 27000
```

In dieser Konfiguration kann NetScaler den Lizenzserver-Agenten (LSA) über den Console-Dienst erreichen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Dem integrierten NetScaler-Agenten kann die LSA-Rolle nicht zugewiesen werden.

Flexed-Lizenz

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 End of Life (EOL) sein. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Citrix-Produktsuite. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, und unterstützt NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed Term Bandwidth-Lizenzen. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 für Console on-prem-Versionen ab 14.1-51.x und ab 13.1-60.x eingestellt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis April 15 2026 weiterhin verwenden. Sie müssen jedoch vor April 15 2026 auf Console on-prem Version 14.1-51.x oder höher aktualisieren und zu LAS wechseln, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, Perpetual werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden bei einem Upgrade auf die oben genannten Softwareversionen nicht mehr lizenziert sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LAS-basierte Lizenzen sind Kunden möglicherweise nicht verfügbar, wo dies gesetzlich oder durch Vorschriften verboten ist.
Wenn Sie Fragen oder Bedenken haben, wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix-Wartung bei Nichteinhaltung dieser Anforderungen ohne Haftung zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit zustehen, einschränken oder aussetzen. Diese Anforderungen gelten nicht, wo dies gesetzlich oder durch Vorschriften verboten ist.
Die NetScaler Flexed-Lizenzierung ist das neue Lizenzierungsframework, das darauf abzielt, den Lizenzverwaltungsprozess zu vereinfachen. Ihre Flexed-Lizenz umfasst Software-Instanzlizenzen (VPX/CPX/BLX, SDX, MPX und VPX FIPS) und Bandbreitenkapazitätslizenzen. Sie müssen die Flexed-Lizenz auf dem NetScaler Console-Dienst oder NetScaler ADM on-prem anwenden. Sie müssen auch die MPX Z-Cap- und SDX Z-Cap-Lizenz auf NetScaler MPX bzw. NetScaler SDX-Hardware anwenden. Sie können diese dann auf alle in der Cloud oder lokal bereitgestellten NetScaler-Formfaktoren verteilen.

LAS-basierte Lizenzierung – Bei Verwendung der LAS-basierten Lizenzierung werden Ihre Flexed-Berechtigungen automatisch in den NetScaler Console-Dienst übernommen und in der Benutzeroberfläche angezeigt.

Manuell verwaltete Berechtigungen (dateibasierte Lizenzierung):

Bei Verwendung manuell verwalteter Berechtigungen (dateibasierte Lizenzierung) führen Sie die folgenden Schritte aus:

1. Wenden Sie die Flexed-Lizenz auf Ihren NetScaler Console-Dienst oder Ihre NetScaler Console On-Prem an.
2. Wenden Sie die spezifischen MPX Z-Cap- und SDX Z-Cap-Lizenzen auf Ihre NetScaler MPX™- bzw. SDX-Hardware an.
3. Sobald die Lizenzen angewendet wurden, können Sie sie über alle NetScaler-Formfaktoren hinweg zuweisen, unabhängig davon, ob sie in der Cloud oder On-Premises bereitgestellt werden.

Eine Flexed-Lizenz bietet auch Analysen für unbegrenzte virtuelle Server.

Wenn Sie zuvor Pooled-Lizenzen hatten und eine Flexed-Lizenz erworben haben, können Sie Ihre Lizenzdetails im Flexed-Lizenz-Dashboard anzeigen. Die kombinierte Bandbreite und die Instanzen werden im Flexed-Lizenz-Dashboard angezeigt.

Eine Bandbreitenlizenz umfasst typischerweise nur die Premium Edition, es sei denn, Sie hatten zuvor eine Pooled Standard- oder Advanced-Lizenz; in diesem Fall werden die Standard-, Advanced- und Premium-Editionen im Flexed-Lizenz-Dashboard angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Flexed- und Pooled-Bandbreiten- und Instanzlizenzen(/en-us/netscaler-console-service/media/flexed-pooled-bw-instance-license.png)

Weitere Details finden Sie unter Flexed-Lizenz-Dashboard.

Sie können die Flexed-Lizenzierung verwenden, um die Bandbreitenauslastung zu maximieren, indem Sie die notwendige Bandbreitenzuweisung für eine Instanz sicherstellen und nicht mehr als deren Bedarf. Erhöhen oder verringern Sie die einer Instanz zugewiesene Bandbreite zur Laufzeit, ohne den Datenverkehr zu beeinträchtigen.

Nullkapazitäts-Hardware

Wenn sie über die NetScaler Flexed-Lizenzierung verwaltet werden, werden MPX- und SDX-Instanzen als „Nullkapazitäts-Hardware“ bezeichnet, da diese Instanzen erst funktionieren können, wenn sie Ressourcen aus dem Bandbreitenpool entnehmen. Daher werden diese Plattformen auch als MPX-Z- und SDX-Z-Appliances bezeichnet.

Nullkapazitäts-Hardware erfordert eine Z-Cap-Lizenz, um Bandbreite aus dem gemeinsamen Pool zu entnehmen.

HINWEIS:

- Die Installation der Nullkapazitätslizenz funktioniert genauso wie bei anderen lokalen NetScaler-Lizenzen. Weitere Informationen zum Erwerb und zur Installation einer Nullkapazitätslizenz finden Sie unter Lizenzierungshandbuch für NetScaler.
- Wenn Sie LAS-basierte Lizenzierung verwenden, müssen Sie keine Z-Cap-Lizenzen anwenden.

Z-Cap-Lizenzen verwalten und installieren

Sie müssen eine Z-Cap-Lizenz manuell installieren, indem Sie die Hardware-Seriennummer oder den Lizenzzugriffscode verwenden. Nachdem eine Z-Cap-Lizenz installiert wurde, ist sie an die Hardware gebunden und kann nicht bedarfsgesteuert über NetScaler-Hardwareinstanzen hinweg gemeinsam genutzt werden. Sie können die Z-Cap-Lizenz jedoch manuell auf eine andere NetScaler-Hardwareinstanz verschieben.

NetScaler MPX-Instanzen, die die NetScaler-Softwareversion 11.1 Build 54.14 oder höher ausführen, und NetScaler SDX-Instanzen, die 11.1 Build 58.13 oder höher ausführen, unterstützen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

die NetScaler Flexed-Lizenzierung. Weitere Informationen finden Sie in den Tabellen 1 und 2 unter Mindest- und Höchstkapazität für Flexed- und Pooled-Lizenzierung.

Eigenständige NetScaler VPX-Instanzen

NetScaler VPX-Instanzen, die NetScaler-Softwareversion 11.1 Build 54.14 und höher auf den folgenden Hypervisoren ausführen, unterstützen Flexed-Lizenzen:

- VMware ESX 6.0
- Citrix Hypervisor™
- Linux KVM

NetScaler VPX-Instanzen, die NetScaler-Softwareversion 12.0 Build 51.24 und höher auf den folgenden Hypervisoren und Cloud-Plattformen ausführen, unterstützen Flexed-Lizenzierung:

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

NetScaler VPX-Instanzen, die NetScaler-Softwareversion 13.0 und 13.1 (alle Versionen) auf den folgenden Hypervisoren und Cloud-Plattformen ausführen, unterstützen Flexed-Lizenzierung:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

Eigenständige NetScaler CPX-Instanzen

NetScaler CPX-Instanzen, die auf einem Docker-Host bereitgestellt werden, unterstützen Flexed Licensing. Im Gegensatz zu Hardware ohne Kapazität benötigt NetScaler CPX keine Z-Cap-Lizenz. Eine einzelne NetScaler CPX-Instanz, die bis zu 1 Gbit/s Durchsatz verbraucht, entnimmt nur 1 Instanz und keine Bandbreite aus dem Lizenzpool. Betrachten Sie zum Beispiel, dass Sie 20 NetScaler CPX-Instanzen mit einem 20 Gbit/s Bandbreitenpool haben. Wenn eine der NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CPX-Instanzen 500 Mbit/s Durchsatz verbraucht, bleibt der Bandbreitenpool für die verbleibenden 19 NetScaler CPX-Instanzen bei 20 Gbit/s.

Wenn dieselbe NetScaler CPX-Instanz beginnt, 1500 Mbit/s Durchsatz zu verbrauchen, stehen den verbleibenden 19 NetScaler CPX-Instanzen 19,5 Gbit/s des Bandbreitenpools zur Verfügung.

Für Flexed Licensing können Sie zusätzliche Bandbreite nur in Vielfachen von 10 Mbit/s hinzufügen.

Eigenständige NetScaler BLX-Instanzen

NetScaler BLX-Instanzen unterstützen Flexed Licensing. Eine NetScaler BLX-Instanz benötigt keine Z-Cap-Lizenz. Um Datenverkehr zu verarbeiten, muss eine NetScaler BLX-Instanz Bandbreite und eine Instanzlizenz aus dem Pool entnehmen.

Bandbreitenpool

Der Bandbreitenpool ist die Gesamtbandbreite, die von NetScaler-Instanzen, sowohl physischen als auch virtuellen, gemeinsam genutzt werden kann. Der Bandbreitenpool umfasst einen Pool für die Premium-Software-Edition. Wenn Sie von Pooled auf Flexed Licensing umstellen, finden Sie möglicherweise eine Mischung aus Standard-, Advanced- und Premium-Software-Editionen. Eine gegebene NetScaler MPX/VPX/CPX/BLX-Instanz kann nicht gleichzeitig Bandbreite aus verschiedenen Pools entnommen haben. Der Bandbreitenpool, aus dem sie Bandbreite entnehmen kann, hängt von ihrer Software-Edition ab, für die sie lizenziert ist.

Instanzpool

Es gibt drei Arten von Software-Instanzpools:

- VPX/CPX/BLX Softwareinstanz
- MPX Softwareinstanz (derselbe Pool gilt für MPX FIPS)
- SDX Softwareinstanz (derselbe Pool gilt für SDX FIPS)
- VPX FIPS Softwareinstanz

Beim Auschecken aus dem Pool schaltet eine Lizenz die Ressourcen der Softwareinstanz frei, einschließlich CPUs/PEs, SSL-Kerne, Pakete pro Sekunde und Bandbreite.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lizenz konfigurieren

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Citrix Produktpalette. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, und unterstützt NetScaler Flexed-Lizenzen (Citrix Platform License/Universal Hybrid Multi-Cloud), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed Term Bandwidth-Lizenzen. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 in den Console on-prem-Versionen 14.1-51.x und höher sowie 13.1-60.x und höher eingestellt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch vor 15th April 2026 auf Console on-prem Version 14.1-51.x oder höher aktualisieren und zu LAS wechseln, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen, wie z. B. NetScaler Virtual CPU-Lizenzierung (Pooled vCPU), NetScaler VPX Check-In und Check-Out (CICO), unbefristete Lizenzen, werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden nach dem Upgrade auf die oben genannten Softwareversionen unlizenziert. LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies gesetzlich oder durch Vorschriften untersagt ist.
Wenn Sie Fragen oder Bedenken haben, wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix Maintenance bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder

© 1997–2026 Citrix Systems, Inc. All rights reserved.

aussetzen, zusätzlich zu allen anderen Rechtsmitteln, die Citrix nach Gesetz oder Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften untersagt sind.
Die NetScaler Flexed- oder Pooled-Lizenzierung ermöglicht es Ihnen, Bandbreiten- oder Instanzlizenzen über verschiedene NetScaler-Formfaktoren hinweg zu teilen. Wenn eine Instanz die Ressourcen nicht mehr benötigt, gibt sie die zugewiesene Kapazität an den gemeinsamen Pool zurück. Verwenden Sie die freigegebene Kapazität auf anderen NetScaler-Instanzen, die Ressourcen benötigen.

HINWEIS:

Wenn Sie Pooled-Lizenzen besitzen und nun Flexed-Lizenzen erworben und angewendet haben, wird die kombinierte Berechtigung im Flexed-Lizenz-Dashboard angezeigt.

Sie können Flexed- oder Pool-Lizenzen verwenden, um die Bandbreitennutzung zu maximieren, indem Sie sicherstellen, dass einer Instanz die notwendige Bandbreite zugewiesen wird und nicht mehr als benötigt. Erhöhen oder verringern Sie die einer Instanz zugewiesene Bandbreite zur Laufzeit, ohne den Datenverkehr zu beeinträchtigen. Mit den Pool-Kapazitätslizenzen können Sie die Instanzbereitstellung automatisieren.

LAS-basierte Lizenzierung

Bei der Verwendung von LAS ist ein externer Agent optional. Die Lizenzberechtigungen werden automatisch in den NetScaler Console-Dienst übernommen und in der NetScaler Console-GUI angezeigt.

Voraussetzung

- Stellen Sie sicher, dass Port 443 für Instanzen verfügbar ist, um Lizenzen von NetScaler Console auszuchecken. Weitere Informationen finden Sie unter Systemanforderungen.

Schritt 1 – Überprüfung der Berechtigungsanzeige

1. Navigieren Sie zu **Licensing Management > LAS**, um zu überprüfen, ob Ihre NetScaler-Berechtigungen angezeigt werden.

Schritt 2 – NetScaler-Instanz zum Konsolendienst hinzufügen

1. Fügen Sie Ihre NetScaler-Instanz zum Konsolendienst hinzu.

Weitere Informationen finden Sie unter NetScaler-Instanzen hinzufügen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-  **Using an External Agent**: If you are using an external agent for
proxying licensing communication, you must explicitly add the NetScaler
instances to the Console.



-  **Using a Built-in Agent**: If you are using a built-in agent, the
NetScaler instance is automatically added to the NetScaler Console service
when you configure the agent. For more informatiion about built-in agent,
see Configure Built-in Agent for NetScaler Console On-Prem.
```

Schritt 3 – Lizenz mit LAS aktivieren

1. Navigieren Sie zu **Licensing Management > LAS**.
2. Klicken Sie auf **License with LAS** oder **Migrate to LAS**.
3. Wählen Sie eine Instanz aus und klicken Sie auf **Continue**.

   Weitere Informationen finden Sie unter License Activation Service.

Schritt 4 – Flexed-Durchsatzkapazität für NetScaler-Instanzen bearbeiten

1. Navigieren Sie zu **NetScaler Licensing > Flexed Licensing > Dashboard > LAS managed entitlements**.
2. Wählen Sie im Abschnitt **Licensed NetScalers** eine Instanz aus und klicken Sie auf **Edit Throughput Capacity**.
3. Geben Sie den gewünschten Durchsatzwert in die **Allocate*** Spalte ein.
4. Klicken Sie auf **Submit**.

Spezielle Lizenzierung für nicht lizenzierte MPX-Appliances mit einem externen Agenten

Bei Verwendung eines externen Agenten mit einer nicht lizenzierten MPX werden HTTPS-Verbindungen zum Console Service nicht unterstützt. Daher ist Schritt 2 nicht durchführbar. Navigieren Sie stattdessen zum NetScaler, um die folgenden Schritte auszuführen.

1. Navigieren Sie zu **System > Licenses > ADC License > Manage Licenses > Add New License**.
2. Wählen Sie auf der Seite „Lizenzen“ das Optionsfeld **Use remote licensing** aus und wählen Sie den Modus **LAS** aus dem Remote-Lizenzierungsmodus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Geben Sie im Feld **Server Name/IP address** die IP-Adresse Ihres externen NetScaler Console-Agenten ein.
4. Geben Sie Ihre NetScaler-Agent-Anmeldeinformationen ein, um die Instanz zu registrieren, und klicken Sie dann auf **Continue**.

   HINWEISE:

   - Aktivieren Sie das Kontrollkästchen **Validate Certificate** nur, wenn Sie ein gültiges digitales Zertifikat (ausgestellt von einer Zertifizierungsstelle (CA)) auf den NetScaler-Agenten hochgeladen haben.
   - Einer der Agenten in NetScaler Console dient als Lizenzserver.

5. Geben Sie im Feld **Device Profile Name** das Instanzprofil an, das NetScaler Console für den Zugriff auf die Instanz verwendet. Dieses Profil enthält den Benutzernamen und das Kennwort für die Instanzen, die Sie hinzufügen möchten. Das Standardprofil ist ns_nsroot_profile. Wenn Sie jedoch die Standard-Administratoranmeldeinformationen geändert haben, stellen Sie sicher, dass Sie einen benutzerdefinierten Instanzprofilnamen erstellen und angeben.
6. Wählen Sie im Abschnitt **Lizenzen zuweisen** die Lizenzedition aus und geben Sie die erforderliche Bandbreite an. Wenn Sie zum ersten Mal Lizenzen in NetScaler zuweisen, können Sie die Zuweisung später direkt über die NetScaler Console-GUI ändern oder freigeben.
7. Klicken Sie auf **Lizenzen abrufen**.

   HINWEIS:

   Wenn Sie die Lizenzedition ändern, starten Sie die Instanz neu (Warmstart). Die Konfigurationsänderungen werden erst wirksam, wenn Sie die Instanz neu starten.

Manuell verwaltete Berechtigungen (dateibasierte Lizenzierung)

Um NetScaler Flexed- oder Pooled-Lizenzierung zu verwenden, müssen Sie einen NetScaler Console-Agent an eine NetScaler-Instanz anbinden. NetScaler-Instanzen checken Lizenzen über einen Agenten bei NetScaler Console ein und aus.

Sie können auch Pooled Capacity-Lizenzen für NetScaler FIPS-Instanzen verwenden. Sie können die folgenden Aufgaben in NetScaler Console ausführen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Laden Sie die Flexed- oder Pooled-Lizenzdateien (Bandbreitenpool oder Softwareinstanzpool) auf den Lizenzserver hoch.
2. Weisen Sie Lizenzen aus dem Lizenzpool bei Bedarf NetScaler-Instanzen zu.
    - Checken Sie die Lizenzen von NetScaler-Instanzen (MPX-Z /SDX-Z/VPX/CPX/BLX) basierend auf der minimalen und maximalen Kapazität der Instanz aus.

Sie können Flexed- oder Pooled-Lizenzen, einschließlich Bandbreiten-, Instanz- und Z-Cap-Lizenzen, von citrix.com herunterladen. Weitere Informationen finden Sie unter Lizenzierungshandbuch für NetScaler.

Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie die Flexed-Lizenzierung konfigurieren:

- Installieren und registrieren Sie einen Agenten in NetScaler Console. Informationen zum Installieren und Registrieren eines Agenten finden Sie unter Erste Schritte.
- Stellen Sie sicher, dass alle registrierten Agenten den Status „UP“ haben, damit die Flexed-Lizenzierung ordnungsgemäß funktioniert. Wenn Agenten den Status „DOWN“ haben, aber noch nicht außer Betrieb genommen oder beendet wurden, versetzen Sie sie in den Status „UP“. Wenn DOWN-Agenten außer Betrieb genommen oder beendet wurden oder nicht mehr verwendet werden, löschen Sie sie aus NetScaler Console.
- Die Ports `27000` und `7279` stehen zur Verfügung, um Lizenzen von NetScaler Console auf eine Instanz auszuchecken. Siehe Systemanforderungen.

Schritt 1 – Lizenzen in NetScaler Console anwenden

1. Navigieren Sie zu **NetScaler Licensing > License Management**.
2. Wählen Sie im Abschnitt **Lizenzdateien** die Option **Lizenzdatei hinzufügen** und eine der folgenden Optionen aus:
    - **Lizenzdateien von einem lokalen Computer hochladen**. Wenn eine Lizenzdatei bereits auf Ihrem lokalen Computer vorhanden ist, können Sie sie in NetScaler Console hochladen.
    - **Lizenzzugriffscode verwenden**. Geben Sie den Lizenzzugriffscode für die von Citrix erworbene Lizenz an. Wählen Sie dann **Lizenzen abrufen** aus. Wählen Sie anschließend **Fertig stellen** aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Sie können jederzeit weitere Lizenzen über die **Lizenzeinstellungen** zu NetScaler Console hinzufügen.

3. Klicken Sie auf **Fertig stellen**.

   Die Lizenzdateien werden zu NetScaler Console hinzugefügt. Der Abschnitt **Lizenzablaufinformationen** listet die in NetScaler Console vorhandenen Lizenzen und die verbleibenden Tage bis zum Ablauf auf.

4. Wählen Sie unter **Lizenzdateien** eine Lizenzdatei aus, die Sie anwenden möchten, und klicken Sie auf **Lizenzen anwenden**.

   Diese Aktion ermöglicht NetScaler-Instanzen, die ausgewählte Lizenz als Flexed- oder Pool-Lizenz zu verwenden.

Schritt 2 – NetScaler Console als Lizenzserver registrieren und Lizenzen zuweisen

Sie können die NetScaler Console mithilfe eines Agenten als Lizenzserver bei einer NetScaler-Instanz registrieren.

Registrieren Sie einen NetScaler Console-Agenten über die GUI

Registrieren Sie in der NetScaler Console-GUI den NetScaler Console-Agenten, der einer NetScaler-Instanz zugeordnet ist.

1. Melden Sie sich bei der NetScaler-GUI an.
2. Navigieren Sie zu **System > Lizenzen > Lizenzen verwalten**.
3. Klicken Sie auf **Neue Lizenz hinzufügen**.
4. Wählen Sie **Remote-Lizenzierung verwenden** und unter **Remote-Lizenzierungsmodus** wählen Sie **Pooled Licensing** aus der Liste aus.
5. Geben Sie im Feld **Servername/IP-Adresse** die zugehörige IP-Adresse des NetScaler Console-Agenten an, der bei NetScaler Console registriert ist.
6. Der Standard-Lizenzport ist 27000.
7. Geben Sie Ihre NetScaler-Agenten-Anmeldeinformationen ein, um eine Instanz bei NetScaler Console zu registrieren, und klicken Sie auf **Weiter**. In NetScaler Console ist einer der Agenten der Lizenzserver.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEISE:

- Aktivieren Sie das Kontrollkästchen **Zertifikat validieren** nur, wenn Sie ein gültiges digitales Zertifikat (ausgestellt von einer Zertifizierungsstelle (CA)) auf den NetScaler-Agenten hochgeladen haben. Navigieren Sie in NetScaler Console zu Infrastruktur > Instanzen > Agenten und wählen Sie aus der Liste „Aktion auswählen“ die Option „Zertifikat installieren“, um das Zertifikat hochzuladen.
- Die Geräteregistrierung kann fehlschlagen, wenn NetScaler nur über eine NAT-IP erreichbar ist. Sie können die Lizenz trotzdem auschecken, aber NetScaler Console zeigt diese NetScaler-Instanzen als nicht verwaltete Instanzen an.

8. Geben Sie unter **Geräteprofilname** das Instanzprofil an, das NetScaler Console für den Zugriff auf die Instanz verwenden kann. Dieses Instanzprofil enthält den Benutzernamen und das Kennwort der Instanzen, die Sie zu NetScaler Console hinzufügen möchten. Das Standardprofil ist **ns_nsroot_profile**. Wenn Sie die Standard-Administratoranmeldeinformationen Ihrer Instanzen geändert haben, können Sie einen benutzerdefinierten Instanzprofilnamen definieren.

9. Wählen Sie unter **Lizenzen zuweisen** die Lizenzedition aus und geben Sie die erforderliche Bandbreite an.

   Weisen Sie zum ersten Mal Lizenzen in NetScaler zu. Sie können die Lizenzzuweisung später über die NetScaler Console GUI ändern oder freigeben.

10. Klicken Sie auf **Lizenzen abrufen**.

WICHTIG

Starten Sie die Instanz warm neu, wenn Sie die Lizenzedition ändern. Die Konfigurationsänderungen werden erst wirksam, wenn Sie die Instanz neu starten.

Agenten über die CLI hinzufügen

Wenn eine NetScaler-Instanz keine GUI hat, verwenden Sie die folgenden CLI-Befehle, um einen Agenten hinzuzufügen, der einer Instanz zugeordnet ist:

1. Melden Sie sich bei der NetScaler Console an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Fügen Sie die IP-Adresse des zugehörigen Agenten hinzu, der bei der NetScaler Console registriert ist:

```
> add ns licenseserver <adm-agent-IP-address> -port <adm-agent-license-port-number>
```

3. Zeigen Sie die im Lizenzserver verfügbare Lizenzbandbreite an:

```
> sh ns licenseserverpool
```

4. Weisen Sie die Lizenzbandbreite aus der erforderlichen Lizenzedition zu:

```
> set ns capacity -unit gbps -bandwidth <specify-license-bandwidth> edition <specify-license-edition>
```

WICHTIG

Starten Sie die Instanz warm neu, wenn Sie die Lizenzedition ändern.

`reboot -w`

Die Konfigurationsänderungen werden erst wirksam, wenn Sie die Instanz neu starten.

Schritt 3 – Gehen Sie je nach Lizenztyp zum entsprechenden Lizenzverfahren

Flexed Durchsatzkapazität für NetScaler-Instanzen bearbeiten

1. Navigieren Sie zu **NetScaler Licensing > Flexed Licensing > Dashboard**.
2. Wählen Sie im Abschnitt **Licensed NetScalers** eine Instanz aus und klicken Sie auf **Edit Throughput Capacity**.
3. Geben Sie auf der Seite **Edit Throughput Capacity** eine Zahl in die Spalte **Allocate** ein.
4. Klicken Sie auf **Submit**.

Gepoolte Lizenzen NetScaler-Instanzen zuweisen

So weisen Sie gepoolte Kapazitätslizenzen über die NetScaler Console-GUI zu:

1. Melden Sie sich bei NetScaler Console an.
2. Navigieren Sie zu **Infrastructure > Pooled Licensing > Bandwidth Licenses > Pooled Capacity**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die FIPS-Instanzkapazität wird nur angezeigt, wenn Sie FIPS-Instanzlizenzen in NetScaler Console hochladen.

3. Klicken Sie auf den Lizenzpool, den Sie verwalten möchten.

   HINWEIS:

   Das Feld **Allocated Capacity** spiegelt die geänderte Bandbreite nicht sofort wider. Die Bandbreitenänderung wird nach dem Warmstart des NetScalers wirksam.

   Unter **Allocation Details** werden die Felder **Requested** und **Applied** aktualisiert, wenn Sie die Bandbreitenzuweisung der Instanz ändern.

4. Wählen Sie eine NetScaler-Instanz aus der Liste der verfügbaren Instanzen aus, indem Sie auf die Schaltfläche **>** klicken.

   Die Spalte „Lizenzstatus“ zeigt entsprechende Statusmeldungen zur Lizenzzuweisung an.

   HINWEIS:

   Die Registerkarte **Nicht verwaltete Instanzen** zeigt die Instanzen an, die erkannt, aber nicht in NetScaler Console verwaltet werden.

5. Klicken Sie auf **Zuweisung ändern** oder **Zuweisung freigeben**, um die Lizenzzuweisung zu ändern.
6. Ein Pop-up-Fenster mit den verfügbaren Lizenzen auf dem Lizenzserver wird angezeigt.
7. Sie können die Bandbreiten- oder Instanzzuweisung zur Instanz auswählen, indem Sie die Optionen der Liste „Zuweisen“ festlegen. Nachdem Sie Ihre Auswahl getroffen haben, klicken Sie auf **Zuweisen**.
8. Sie können die zugewiesene Lizenzedition auch über die Listenoptionen im **Fenster „Lizenzzuweisung ändern“** ändern.

   HINWEIS:

   Starten Sie eine Instanz neu (Warmstart), wenn Sie die Lizenzedition ändern.

Flexed- oder Pooled-Kapazität auf NetScaler-Instanzen konfigurieren

Sie können Pooled-Kapazitätslizenzen auf den folgenden NetScaler-Instanzen konfigurieren:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler MPX-Z-Instanzen
- NetScaler SDX-Z-Instanzen
- NetScaler VPX-Instanzen
- NetScaler Hochverfügbarkeitspaar

NetScaler MPX-Z

MPX-Z ist die für Flexed-Capacity aktivierte NetScaler MPX Appliance. MPX-Z unterstützt Bandbreitenpools nur für Lizenzen der Premium Edition.

MPX-Z benötigt eine Lizenz, bevor es sich mit dem Lizenzserver verbinden kann. Sie können die MPX-Z-Lizenz auf eine der folgenden Arten installieren:

- Hochladen der Lizenzdatei von einem lokalen Computer.
- Verwenden der Hardware-Seriennummer der Instanz.
- Der Lizenzzugriffscode aus dem Abschnitt **System** > **Lizenzen** der GUI der Instanz.

Wenn Sie die MPX-Z-Lizenz entfernen, wird MPX unlizenziert. Die Instanzlizenzen werden an den Lizenzserver freigegeben.

Sie können die Bandbreite einer MPX-Z-Instanz dynamisch ohne Neustart ändern. Ein Neustart ist nur erforderlich, wenn Sie die Lizenzedition ändern möchten.

HINWEIS:

Wenn Sie die Instanz neu starten, werden die für die konfigurierte Kapazität erforderlichen Flexed-Lizenzen automatisch ausgecheckt.

NetScaler SDX-Z

SDX-Z ist die für Flexed-Capacity aktivierte NetScaler SDX Appliance. SDX-Z unterstützt Bandbreiten- und Instanzpools für Lizenzen der Premium Edition.

SDX-Z benötigt eine Lizenz, bevor es sich mit dem Lizenzserver verbinden kann. Sie können die SDX-Z-Lizenz auf eine der folgenden Arten installieren:

- Hochladen der Lizenzdatei von einem lokalen Computer.
- Verwenden der Hardware-Seriennummer der Instanz.
- Der Lizenzzugriffscode aus dem Abschnitt **System** > **Lizenzen** der GUI der Instanz.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Sie die SDX-Z-Lizenz entfernen, wird SDX unlizenziert. Die Instanzlizenzen werden an den Lizenzserver freigegeben.

Sie können die Bandbreite einer SDX-Z-Instanz dynamisch ohne Neustart ändern. Ein Neustart ist nur erforderlich, wenn Sie die Lizenzedition ändern möchten.

HINWEIS:

Wenn Sie die Instanz neu starten, werden die für die konfigurierte Kapazität erforderlichen Flexed-Lizenzen automatisch ausgecheckt.

Lizenzanforderungen für NetScaler Hochverfügbarkeitspaar (gemeinsam für LAS und dateibasierte Lizenzierung)

HINWEIS:

Diese Anforderungen gelten sowohl für manuell verwaltete Berechtigungen (dateibasierte Lizenzierung) als auch für LAS.

Wenn Sie ein NetScaler Hochverfügbarkeitspaar (HA) konfigurieren, stellen Sie sicher, dass sowohl die primäre als auch die sekundäre Instanz die folgenden Anforderungen erfüllen:

Bevor Sie beginnen, stellen Sie sicher, dass der NetScaler Console-Server als Lizenzserver konfiguriert ist. Weitere Informationen finden Sie unter NetScaler Console als Lizenzserver konfigurieren

Wenn Sie einem NetScaler HA-Paar die Bandbreite zuweisen, checkt die NetScaler Console die zugewiesene Bandbreite für die primäre Instanz aus. Sie müssen den Vorgang für die sekundäre Instanz wiederholen.

Um Pool-Lizenzen einem NetScaler HA-Paar zuzuweisen, siehe

Die Seite **Flexed Capacity** zeigt die Instanzen und ihre zugewiesene Kapazität separat an.

NetScaler Flexed-Lizenzierungsstatus (Gemeinsam für LAS- und dateibasierte Lizenzierung)

Die Flexed-Lizenzierungsstatus geben die Lizenzanforderung für eine NetScaler-Instanz an. Die mit Flexed-Lizenzierung konfigurierten NetScaler-Instanzen zeigen einen der folgenden Status an:

- **Zugewiesen**: Die Instanz läuft mit der richtigen Lizenzkapazität.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Gnadenfrist**: Die Instanz läuft mit einer Gnadenlizenz. **Hinweis**: Dieser Status gilt nur für manuell verwaltete Berechtigungen (dateibasierte Lizenzierung).
- **Verbindung verloren**: Die Kommunikation von NetScaler Console zur Instanz funktioniert nicht. **Hinweis**: Wenn die Verbindung zwischen NetScaler und dem Console Service für 24 Stunden oder länger unterbrochen ist, wechselt der NetScaler-Status zu Gnadenfrist.

Lizenz-Dashboard

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Citrix Produktpalette. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, und unterstützt NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed Term Bandwidth-Lizenzen. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 für Console on-prem-Versionen ab 14.1-51.x und ab 13.1-60.x eingestellt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch auf Console on-prem Version 14.1-51.x oder höher aktualisieren und vor 15th April 2026 auf LAS umstellen, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, Perpetual werden von LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden nach dem Upgrade auf die oben genannten Softwareversionen unlizenziert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies gesetzlich oder durch Vorschriften untersagt ist.
Wenn Sie Fragen oder Bedenken haben, wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix Maintenance bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder aussetzen, zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften untersagt sind.
Lesen Sie den folgenden Hinweis, bevor Sie fortfahren.

HINWEISE:

- Wenn Sie zuvor Pooled-Lizenzen hatten und jetzt Flexed-Lizenzen erworben und angewendet haben, wird die kombinierte Berechtigung nun im Flexed-Lizenz-Dashboard angezeigt.
- Wenn Sie nur gepoolte Lizenzen haben, überprüfen Sie das Dashboard für gepoolte Lizenzen.
- Wenn Sie nur Flexed-Lizenzen oder sowohl Flexed- als auch gepoolte Lizenzen haben, überprüfen Sie das Dashboard für Flexed-Lizenzen.
- **Wichtiger Hinweis basierend auf der Lizenzierungsmethode:**
  - Um LAS-basierte Lizenzlizenzen anzuzeigen, navigieren Sie zu **NetScaler-Lizenzen > Flexed Licensing > Dashboard > Registerkarte „LAS managed entitlements“**
  - Um manuell verwaltete Berechtigungen (dateibasierte Lizenzierung) anzuzeigen, navigieren Sie zu **NetScaler-Lizenzen > Flexed Licensing > Dashboard > Registerkarte „Manually managed entitlements“**
  - Wenn Sie beide Lizenzmechanismen verwenden, beachten Sie beide Registerkarten.

Das Flexed-Lizenz-Dashboard bietet Ihnen eine umfassende Übersicht über die von Ihnen erworbene Bandbreitenkapazität und Instanzen.

Bandbreitenkapazität über Editionen hinweg und Instanzdetails für verschiedene Formfaktoren wie MPX, VPX und SDX werden auf dieser Seite angezeigt. MPX und MPX FIPS verwenden dieselbe Lizenzdatei. Ebenso verwenden SDX und SDX FIPS dieselbe Lizenzdatei. VPX FIPS hat jedoch eine andere Datei als VPX und wird separat angezeigt. Außerdem erfordern VPX (einschließlich VPX auf SDX), BLX und CPX VPX-Lizenzen und sind Teil der Berechtigung und Zuweisung für VPX. Eine Flexed-Lizenz unterstützt nur die Premium Edition. Wenn Sie jedoch Flexed-Lizenzen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

erworben und zuvor eine gepoolte Standard- oder Advanced-Bandbreitenkapazität hatten, werden die Details zur Bandbreitenkapazität (Standard oder Advanced) ebenfalls im Flexed-Lizenz-Dashboard aufgeführt.

VPX (einschließlich VPX auf SDX), BLX und CPX Formfaktoren erfordern die NetScaler Flexed VPX SW Instance Lizenzdatei. Das heißt, diese Formfaktoren sind Teil der Berechtigung und Zuweisung für Flexed VPX SW Instance Lizenzen.

Details zu Ihren lizenzierten NetScaler-Instanzen finden Sie im Abschnitt **Licensed NetScalers**. Sie können eine Instanz auswählen und die Bandbreite bearbeiten oder die Lizenz für diese Instanz freigeben.

Sie können die Ergebnisse nach den folgenden Parametern filtern:

- Nach Bandbreiten-/Durchsatzkapazität filtern
  - Premium
  - Advanced
  - Standard
- Formfaktor
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
- Lizenzstatus
  - Verbindung verloren
  - Gnadenfrist
  - Zugewiesen

Zugewiesene Durchsatzkapazität auf einer NetScaler-Instanz bearbeiten

1. Navigieren Sie zu **NetScaler Licensing > Flexed Licensing > Dashboard**.
2. Wählen Sie im Abschnitt **Licensed NetScalers** eine Instanz aus und klicken Sie auf **Edit Throughput Capacity**.
3. Geben Sie auf der Seite **Edit Throughput Capacity** eine Zahl in die Spalte **Allocate** ein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Klicken Sie auf **Submit**.

Lizenzen auf einer NetScaler-Instanz freigeben

Um Lizenzen auf eine andere Instanz zu übertragen, müssen Sie die Lizenz auf der aktuellen Instanz freigeben und die Lizenz dann auf die neue Instanz anwenden. Die Auswahl von **Lizenz freigeben** bewirkt Folgendes:

- Gibt alle Lizenzen, die auf dieser Instanz ausgecheckt sind, an den Lizenzserver frei.
- Löscht die Lizenzserverkonfiguration auf dieser Instanz.

Wenn Sie **Ja** auswählen, wird Ihre NetScaler-Instanz unlizenziert und kann keinen Datenverkehr verarbeiten.

Fehlerbehebung bei Lizenzierungsproblemen

Sie können die Option **Fehlerbehebung** verwenden, um einige lizenzbezogene Probleme anzuzeigen und zu analysieren.

Einige mögliche Lizenzierungsprobleme sind die Kommunikation von der Konsole zu den Instanzen, die Verfügbarkeit der Lizenzserver-Agenten (LSA) und so weiter. Die Option **Fehlerbehebung** bietet eine Liste von Problemkategorien wie Lizenzserver, LSA, Prozesse, Kommunikation und deren Status. Als Administrator können Sie, wenn Sie Lizenzierungsprobleme feststellen, diese Kategorien analysieren und beheben.

Das Folgende ist ein Beispielszenario, das Aufmerksamkeit erfordert:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lizenzberichterstattung

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Citrix Produktpalette. LAS wird nach April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, und unterstützt NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed term Bandwidth-Lizenzen. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Wird ab Anfang September 2025 unterstützt.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 in den Console on-prem-Versionen 14.1-51.x und 13.1-60.x und höher nicht mehr unterstützt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch auf Console on-prem Version 14.1-51.x oder höher aktualisieren und vor 15th April 2026 auf LAS umstellen, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO und Perpetual werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden nach dem Upgrade auf die oben genannten Softwareversionen unlizenziert. LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies gesetzlich oder durch Vorschriften verboten ist.
Wenn Sie Fragen oder Bedenken haben, wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix-Wartung bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder aussetzen, zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit

© 1997–2026 Citrix Systems, Inc. All rights reserved.

zustehen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften verboten sind.

In diesem Dashboard können Sie Details zu Folgendem anzeigen:

HINWEIS:

Wenn Sie zuvor Pooled-Lizenzen hatten und jetzt Flexed-Lizenzen erworben und angewendet haben, wird die kombinierte Berechtigung nun im Flexed-Lizenz-Dashboard angezeigt.

- Software-Instanz (VPX, MPX und SDX sowie VPX FIPs) Berechtigung und Zuweisung
- Berechtigung, Zuweisung und tatsächliche Nutzung der Bandbreiten-/Durchsatzkapazität
- Spitzen- und durchschnittliche Zuweisung über alle verwalteten oder ausgewählten Instanzen
- Spitzen- und durchschnittliche Nutzung über alle verwalteten oder ausgewählten Instanzen

FUNKTIONEN (FÜR NETSCALER-INSTANZEN)	BESCHREIBUNG
Berechtigung	Die gesamten Instanzberechtigungen für Software-Instanztypen (VPX, SDX, MPX).
Zuweisung	Die gesamte Instanzzuweisung für Software-Instanztypen (VPX, SDX, MPX).

FUNKTIONEN (FÜR BANDBREITEN-/DURCHSATZKAPAZITÄT)	BESCHREIBUNG
Berechtigung	Die gesamten Berechtigungen für Bandbreiten-/Durchsatzkapazität über alle verwalteten NetScaler-Instanzen. Die Gesamtberechtigungen werden aus den Lizenzen berechnet, die in der Lizenzverwaltung (**NetScaler Licensing > License Management**) angewendet werden.
Zuweisung	Die Bandbreiten-/Durchsatzkapazität, die **lizenzierten NetScalern** im Flexed License Dashboard zugewiesen ist (**NetScaler Licensing > Flexed Licensing > Dashboard**).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FUNKTIONEN (FÜR BANDBREITEN-/ DURCHSATZKAPAZITÄT)	BESCHREIBUNG
Nutzung	Der gesamte Durchsatz, der von den NetScaler-Instanzen verbraucht wird.

HINWEIS:

Eine Flexed-Lizenz unterstützt nur die Premium Edition. Wenn Sie jedoch Flexed-Lizenzen erworben und angewendet haben und zuvor über eine gepoolte Standard- oder erweiterte Bandbreitenkapazität verfügten, werden auch die Details zur Bandbreiten-/ Durchsatzkapazität (Standard oder erweitert) aufgeführt. Wenn Sie beispielsweise eine 1000 Gbit/s Flexed-Lizenz (die Premium ist) angewendet haben und auch eine aktive gepoolte Lizenz mit 100 Gbit/s erweiterter Bandbreite besitzen, zeigt das Reporting-Dashboard sowohl Premium 1000 Gbit/s als auch 100 erweiterte Bandbreite an.

Das folgende Beispiel hilft Ihnen zu verstehen, wie das Dashboard die Spitzenauslastung und die durchschnittliche Auslastung anzeigt:

Angenommen, es gibt 3 verwaltete NetScaler-Instanzen (NetScaler A, NetScaler B und NetScaler C) mit Flexed-Lizenz (Premium-Bandbreite) und die ausgewählte Dauer beträgt 1 Tag. Für Berechnungen berücksichtigt NetScaler Console Datenpunkte (in Mbit/s) für jede Stunde pro NetScaler-Instanz. Für 1 Tag gibt es 24 Datenpunkte für jede NetScaler-Instanz. Für 3 NetScaler-Instanzen gibt es also (24 * 3) Datenpunkte.

- **Spitzenauslastung** = Die Summe des höchsten Datenpunkts (Mbit/s) aus den 24 Stunden aller NetScaler-Instanzen. Wenn beispielsweise der höchste Datenpunkt aus dem 24-Stunden-Zeitraum für NetScaler A 30 Mbit/s, für NetScaler B 45 Mbit/s und für NetScaler C 120 Mbit/s beträgt, wird die Spitzenauslastung als 195 Mbit/s (30 + 45 + 120) angezeigt.
- **Durchschnittliche Auslastung** = Die Summe aller 24-Stunden-Datenpunkte, geteilt durch 24 für jede NetScaler-Instanz. Für 3 NetScaler-Instanzen wird also der Gesamtdurchschnitt aller 3 NetScaler-Instanzen durch 3 geteilt. Wenn beispielsweise der Durchschnitt von NetScaler A 25 Mbit/s, der von NetScaler B 20 Mbit/s und der von NetScaler C 45 Mbit/s beträgt, wird die durchschnittliche Auslastung als 30 Mbit/s (25 + 20 + 35 geteilt durch 3) angezeigt.

Ähnlich werden die Details zur Spitzen- und Durchschnittszuweisung nach derselben Logik angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können die Dauer aus der Liste auswählen, von einer Stunde bis zu einem Jahr, und die Details sowohl in Tabellenansicht als auch in grafischer Ansicht anzeigen.

Das folgende Beispiel zeigt die Tabellenansicht für die Instanzen, die eine Flexed-Lizenz (Premium-Bandbreite) verwenden:

Die folgenden Details werden im Dashboard angezeigt:

- **Spitzenauslastung** – Die höchste Nutzung (in Mbit/s) für die ausgewählte Dauer.
- **Durchschnittliche Nutzung** – Die durchschnittliche Nutzung (in Mbps) für den ausgewählten Zeitraum.
- **Spitzenzuweisung** – Die höchste Zuweisung für den ausgewählten Zeitraum.
- **Durchschnittliche Zuweisung** – Die durchschnittliche Zuweisung für den ausgewählten Zeitraum.
- **Filter** – Sie können eine oder mehrere Instanzen auswählen, um die Nutzungs- und Zuweisungsdetails für die spezifischen Instanzen anzuzeigen.
- **Exportieren** – Sie können Details im PDF-, JPEG- und PNG-Format exportieren.

Das folgende Beispiel zeigt die grafische Ansicht für die Instanzen, die eine Flexed-Lizenz (Premium-Bandbreite) verwenden:

Umstellung auf Flexed-Lizenzierung

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener On-Premises-Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Citrix Produktpalette. LAS wird nach April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, wobei NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed term Bandwidth-Lizenzen unterstützt werden. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die mindestens erforderlichen NetScaler®-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 in Console on-prem-Versionen ab 14.1-51.x und ab 13.1-60.x eingestellt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch auf Console on-prem Version 14.1-51.x oder höher aktualisieren und vor 15th April 2026 auf LAS umstellen, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, Perpetual werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden nach dem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies durch Gesetze oder Vorschriften verboten ist.
Bei Fragen oder Bedenken wenden Sie sich bitte an den Kundendienst. Citrix kann Ihre Citrix Maintenance bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder aussetzen, zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie durch Gesetze oder Vorschriften verboten sind.
Lesen Sie den folgenden Hinweis, bevor Sie fortfahren.

HINWEIS:

Sie müssen vor Ablauf Ihrer aktuellen Lizenz auf die Flexed-Lizenzierung umstellen. Berücksichtigen Sie bei der Planung der Umstellung die folgenden Schritte und planen Sie ein Wartungsfenster ein, falls die Schritte eine Lizenzneukonfiguration oder einen NetScaler-Neustart erfordern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LAS-basierte Lizenzen

HINWEIS:

Stellen Sie sicher, dass Ihre NetScaler-Instanzen (ADC und SDX) auf LAS-kompatiblen Versionen ausgeführt werden.

Informationen zur Migration für die folgende Lizenz finden Sie unter Vorhandene lizenzierte Instanzen migrieren.

- Flexed Licensing (dateibasierte Lizenzen) zu Flexed Licensing (LAS-basierte Lizenzen)
- Pooled Licensing (dateibasierte Lizenzen) zu Flexed Licensing (LAS-basierte Lizenzen)

Informationen zum Übergang für die folgende Lizenz finden Sie unter License Activation Service.

- Pooled vCPU Licensing (dateibasierte Lizenzen) zu Flexed Licensing (LAS-basierte Lizenzen)
- Fixed Subscription oder Perpetual Licensing (dateibasierte Lizenzen) zu Flexed Licensing (LAS-basierte Lizenzen)
- Fixed vCPU Licensing (dateibasierte Lizenzen) zu Flexed Licensing (LAS-basierte Lizenzen)
- CICO Licensing (dateibasierte Lizenzen) zu Flexed Licensing (LAS-basierte Lizenzen)
- Self-Managed Licensing (dateibasierte Lizenzen) zu Flexed Licensing (LAS-basierte Lizenzen)
- Self-Managed vCPU Licensing (dateibasierte Lizenzen) zu Flexed Licensing (LAS-basierte Lizenzen)

Manuell verwaltete Berechtigungen (dateibasierte Lizenzen)

Die folgenden Abschnitte beschreiben die Schritte zum Übergang von bestehenden Lizenztypen zu Flexed Licensing (dateibasierte Lizenzen).

Pooled-Bandbreitenlizenz zu Flexed-Lizenzierung

Einige Schritte sind bei MPX, SDX und VPX gleich. Diese Schritte werden zuerst aufgeführt, gefolgt von den spezifischen Schritten für MPX, SDX oder VPX.

Gemeinsame Schritte für VPX/MPX/SDX

1. Laden Sie Flexed-Lizenzen auf NetScaler Console hoch und wenden Sie sie an. Siehe Lizenzdateien.
2. Wenn Sie eine Z-Cap-Softwarelizenz haben, die für einen bestimmten Zeitraum gültig ist, wenden Sie diese Lizenz auf NetScaler-Hardware (MPX/SDX) an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Für VPX/MPX

Die folgenden zusätzlichen Schritte sind erforderlich:

1. Wenn Sie eine Pooled Premium (Platinum)-Bandbreitenlizenz haben, wechselt die Lizenz nach Ablauf der alten Lizenz automatisch zu Flexed.
2. Wenn Sie eine Pooled Standard- oder Pooled Advanced-Bandbreitenlizenz haben, checken Sie die Premium-Bandbreite manuell aus und starten Sie NetScaler warm neu.

Für SDX

HINWEIS:

Stellen Sie sicher, dass Sie vor Ablauf Ihrer aktuellen Lizenz zur Flexed-Lizenzierung wechseln.

Die folgenden zusätzlichen Schritte sind erforderlich:

1. Checken Sie die erforderliche Instanz- und Bandbreitenlizenz von der Flexed-Lizenzierung auf SDX aus. Ein SDX-Neustart ist nicht erforderlich.
2. Wenn alle VPX auf SDX eine Premium Edition haben, wechselt die Lizenz nach Ablauf der alten Lizenz automatisch zu Flexed.
3. Ändern Sie die Edition für alle VPX (auf SDX) mit Standard oder Advanced auf Premium. Diese VPX-Instanzen werden automatisch neu gestartet.
4. Reduzieren Sie die Standard- und Advanced-Bandbreitenkapazität auf SDX auf Null.

Von Pooled vCPU zu Flexed Licensing

Für VPX

1. Laden Sie Flexed Licenses auf NetScaler Console hoch und wenden Sie sie an. Siehe Lizenzdateien.
2. Entfernen Sie den vorhandenen Lizenzserver über die NetScaler GUI. NetScaler ist unlizenziert, bis alle Schritte abgeschlossen sind.
3. Fügen Sie den Lizenzserver mit der Option Flexed/Pooled hinzu.
4. Checken Sie die erforderlichen Instanz- und Bandbreitenlizenzen für NetScaler aus.
5. Führen Sie einen Warm-Reboot von NetScaler durch.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Von Fixed Subscription oder Perpetual License zu Flexed Licensing

Einige Schritte sind für MPX, SDX und VPX gleich. Diese Schritte werden zuerst aufgeführt, gefolgt von den spezifischen Schritten für MPX, SDX oder VPX.

Gemeinsame Schritte für VPX/MPX/SDX

1. Onboarding in NetScaler Console.
2. Stellen Sie den NetScaler-Agent bereit.
3. Laden Sie Flexed Licenses auf NetScaler Console hoch und wenden Sie sie an. Siehe Lizenzdateien.
4. Wenden Sie die Z-Cap-Softwarelizenz auf NetScaler-Hardware (MPX/SDX) an.

Für VPX/MPX

Die folgenden zusätzlichen Schritte sind erforderlich:

1. Checken Sie die erforderlichen Instanz- und Bandbreitenlizenzen für NetScaler aus.
2. Führen Sie einen Warmstart von NetScaler durch.
3. Löschen Sie die feste Abonnementlizenz, nachdem NetScaler neu gestartet wurde.

Für SDX

Die folgenden zusätzlichen Schritte sind erforderlich:

1. Checken Sie die erforderliche Instanz- und Bandbreitenlizenz aus der Flexed-Lizenzierung auf SDX aus.
2. Wenn alle VPX auf SDX die Premium Edition haben, ist kein SDX-Neustart erforderlich.
3. Wenn ein VPX die Advanced- oder Standard-Edition hat, muss dieser VPX auf die Premium-Edition umgestellt werden. Der VPX wird automatisch neu gestartet.
4. Wenden Sie die Z-Cap-Softwarelizenz auf NetScaler SDX an.
5. Checken Sie die erforderliche Instanz- und Bandbreitenlizenz aus der Flexed-Lizenzierung auf SDX aus.
6. Löschen Sie die feste Abonnementlizenz, nachdem NetScaler neu gestartet wurde.

Feste vCPU zu Flexed-Lizenzierung

Für VPX

1. In NetScaler Console integrieren.
2. Den NetScaler-Agent bereitstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Flexed-Lizenzen in NetScaler Console hochladen und anwenden. Siehe Lizenzdateien.
4. Den Lizenzserver auf NetScaler im Flexed/Pooled-Modus konfigurieren.
5. Die erforderlichen Instanz- und Bandbreitenlizenzen für NetScaler auschecken.
6. NetScaler warm neu starten.
7. Die Fixed-Lizenz nach dem Neustart von NetScaler löschen.

CICO zu Flexed-Lizenzierung

Für VPX

1. Flexed-Lizenzen in NetScaler Console hochladen und anwenden. Siehe Lizenzdateien.
2. Den vorhandenen Lizenzserver über die NetScaler-GUI entfernen. NetScaler ist unlizenziert, bis alle Schritte abgeschlossen sind.
3. Den Lizenzserver mit der Option Flexed/Pooled hinzufügen.
4. Die erforderlichen Instanz- und Bandbreitenlizenzen für NetScaler auschecken.
5. NetScaler warm neu starten.

Selbstverwaltete Bandbreitenlizenz zur Flex-Lizenzierung

Einige Schritte sind für MPX, SDX und VPX gemeinsam. Diese Schritte werden zuerst aufgeführt, gefolgt von den Schritten, die spezifisch für MPX, SDX oder VPX sind.

Gemeinsame Schritte für VPX/MPX/SDX

1. Laden Sie Flex-Lizenzen auf die NetScaler Console hoch und wenden Sie sie an. Siehe Lizenzdateien.
2. Wenn Sie eine Z-Cap-Softwarelizenz haben, die für einen bestimmten Zeitraum gültig ist, wenden Sie diese Lizenz auf NetScaler-Hardware (MPX/SDX) an.

Für VPX/MPX

1. Wenn Sie eine selbstverwaltete Premium-Lizenz haben, ändern Sie den Lizenzmodus über die NetScaler-GUI vom selbstverwalteten Pool zu Flexed/Pooled.
2. Ein NetScaler-Neustart ist nicht erforderlich.
3. Wenn Sie eine selbstverwaltete Standard- oder Advanced-Lizenz haben, entfernen Sie den vorhandenen Lizenzserver über die NetScaler-GUI.
4. Fügen Sie den Lizenzserver mit der Option Flexed/Pooled hinzu.
5. Weisen Sie die Flexed Premium Bandbreitenkapazität VPX/MPX zu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Starten Sie NetScaler warm neu.

Für SDX

1. Wenn alle VPX auf SDX eine selbstverwaltete Premium-Lizenz haben, ändern Sie den Lizenzmodus über die NetScaler-GUI vom selbstverwalteten Pool zu Flexed/Pooled.
2. Ein NetScaler-Neustart ist nicht erforderlich.
3. Wenn einige VPX auf SDX eine Self Managed Standard- oder Advanced-Lizenz haben, wenden Sie sich an den Citrix Support.

Self Managed vCPU zu Flexed-Lizenzierung

Für VPX

1. Laden Sie Flexed-Lizenzen auf die NetScaler Console hoch und wenden Sie sie an. Siehe Lizenzdateien.
2. Entfernen Sie den vorhandenen Lizenzserver über die NetScaler GUI. NetScaler ist unlizenziert, bis alle Schritte abgeschlossen sind.
3. Fügen Sie den Lizenzserver mit der Option Flexed/Pooled hinzu.
4. Checken Sie die erforderlichen Instanz- und Bandbreitenlizenzen für NetScaler aus.
5. Führen Sie einen Warm-Neustart von NetScaler durch.

Szenarien für den Ablauf von Flexed- oder Pooled-Lizenzen und das Verhalten bei Konnektivitätsproblemen

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener On-Premises-Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Suite der Citrix-Produkte. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, wobei NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed-Term-Bandbreitenlizenzen unterstützt werden. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die mindestens erforderlichen NetScaler®-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Release 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 für Console on-prem Releases ab 14.1-51.x und ab 13.1-60.x eingestellt. Wenn Sie auf Console on-prem Release 14.1-51.x oder Release 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch vor 15th April 2026 auf Console on-prem Release 14.1-51.x oder höher aktualisieren und auf LAS umstellen, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, unbefristet werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden nach dem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies gesetzlich oder durch Vorschriften verboten ist.
Wenn Sie Fragen oder Bedenken haben, wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix Maintenance bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder aussetzen, zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften verboten sind.

LAS-basierte Lizenzen

Vor Ablauf der Laufzeit

Wenn die Lizenz vor ihrem Ablauf erneuert wird:

- Die NetScaler-Instanz wechselt nahtlos zur neuen Lizenz, nachdem die alte abgelaufen ist, vorausgesetzt, das Gerät ist in Betrieb.
- Ein Neustart ist nicht erforderlich.
- Der NetScaler benötigt keine manuelle Kapazitätsneukonfiguration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nach Ablauf der Laufzeit

Wenn die Lizenz vor Ablauf ihrer Laufzeit nicht verlängert wird, stellt die NetScaler-Instanz den normalen Betrieb ein.

- Sie verliert ihre Konfiguration.
- Die gesamte Datenverkehrsverarbeitung wird vollständig heruntergefahren.

Szenarien für das Verhalten bei Konnektivitätsproblemen

Geht die Konnektivität zwischen einem NetScaler und dem NetScaler Console-Dienst verloren, tritt das Gerät in eine 30-tägige Nachfrist ein.

Während der Nachfrist funktionieren die Lizenzierungsfunktionen normal. Am einunddreißigsten Tag tritt jedoch Folgendes ein:

- NetScaler VPX™, CPX, BLX und MPX Instanzen werden zwangsweise neu gestartet und verlieren ihre Lizenz.
- Der Durchsatz für alle VPX-Instanzen auf einem NetScaler SDX™ wird auf 1 Mbit/s reduziert.

Manuell verwaltete Lizenz (dateibasierte Lizenz)

Dieses Dokument beschreibt verschiedene Szenarien des Lizenzablaufs und des Verhaltens bei Konnektivitätsproblemen in NetScaler MPX, NetScaler SDX und NetScaler VPX/NetScaler BLX/ NetScaler CPX.

Komponenten von Flexed-Lizenzen

- Softwareinstanz (VPX/BLX/CPX, SDX, MPX, VPX FIPS)
- Bandbreitenkapazität

Szenario: MPX-Formfaktor

Sie verwenden Flexed- oder Pooled-Lizenzierung, und die Lizenzen laufen bald ab. Die folgenden Szenarien erläutern das Verhalten, wenn eine neue Lizenz auf NetScaler Console vor und nach Ablauf der Laufzeit hochgeladen wird oder wenn keine Lizenzdatei vorhanden ist.

Vor Ablauf der Laufzeit

Wenn die neue Lizenz vor Ablauf der Laufzeit hochgeladen wird und die alte Lizenz noch gültig ist, stehen zwei verschiedene Kapazitätspools (alt und neu) zur Verfügung.

- Wenn NetScaler läuft, wechselt es nach Ablauf der alten Lizenz nahtlos zur neuen Flexed- oder Pooled-Lizenz.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Ein Neustart ist nicht erforderlich.
- NetScaler erfordert keine manuelle Neukonfiguration der Kapazität.

Nach Ablauf der Laufzeit

Die NetScaler-Instanz stellt ihren normalen Betrieb nach Ablauf der Lizenz ein, einschließlich Konfigurationsverlust und vollständiger Abschaltung der Datenverkehrsverarbeitung.

Vor oder nach Ablauf der Laufzeit, wenn die Lizenzedition von alt und neu unterschiedlich ist

Wenn die Lizenzedition von alt und neu unterschiedlich ist, müssen Sie unabhängig davon, ob die Laufzeit abgelaufen ist oder nicht, Folgendes tun:

- Die Bandbreite muss manuell neu konfiguriert werden. In der NetScaler-GUI:
  a. Navigieren Sie zu **System > Lizenzen > Lizenzen verwalten**.
  b. Klicken Sie auf **Release Allocation**, um die Zuweisung freizugeben.
  c. Klicken Sie auf **Change Allocation**, um die Bandbreite neu zuzuweisen und die Bandbreite auf Premium zu ändern.
- NetScaler neu starten.

Szenario: SDX-Formfaktor

Sie verwenden Flexed- oder Pooled-Lizenzen, und die Lizenzen laufen bald ab. Die folgenden Szenarien erläutern das Verhalten, wenn eine neue Lizenz auf NetScaler Console hochgeladen wird, bevor und nachdem die Laufzeit abläuft, oder wenn keine Lizenzdatei vorhanden ist.

Vor Ablauf der Laufzeit

Wenn die neue Lizenz vor Ablauf der Laufzeit hochgeladen wird und die alte Lizenz noch gültig ist, stehen zwei verschiedene Kapazitätspools (alt und neu) zur Verfügung.

- Wenn NetScaler läuft, wechselt es nach Ablauf der alten Lizenz nahtlos zur neuen Flexed- oder Pooled-Lizenz.
- Ein Neustart ist nicht erforderlich.
- NetScaler erfordert keine manuelle Neukonfiguration der Kapazität.

Nach Ablauf der Laufzeit

Die NetScaler-Instanz stellt ihren normalen Betrieb nach Ablauf der Lizenz ein, einschließlich Konfigurationsverlust und vollständiger Abschaltung der Datenverkehrsverarbeitung.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn die Lizenzedition von alt und neu unterschiedlich ist

Vor Ablauf der Laufzeit

- Stellen Sie sicher, dass sowohl alte als auch neue Lizenzdateien auf der Console vorhanden sind.
- Die Bandbreite muss manuell neu konfiguriert werden. In der NetScaler SDX GUI:
  a. Navigieren Sie zu **System > Lizenzen > Lizenzen verwalten**.
  b. Klicken Sie auf **Zuweisung freigeben**, um die Zuweisung freizugeben.
  c. Klicken Sie auf **Zuweisung ändern**, um die Bandbreite neu zuzuweisen und die Bandbreite auf Premium zu ändern.
- Ändern Sie alle VPX-Editionen auf Premium, um die VPX-Instanzen neu zu starten.
- Klicken Sie auf **Zuweisung ändern** und behalten Sie nur die Premium-Bandbreite bei. Löschen Sie alle anderen Bandbreitenzuweisungen.

Nach Ablauf der Laufzeit

Die NetScaler-Instanz stellt nach Ablauf der Lizenz ihren normalen Betrieb ein, einschließlich Konfigurationsverlust und vollständiger Abschaltung der Datenverkehrsverarbeitung.

- Löschen Sie die VPX-Instanzen auf SDX.
- Klicken Sie auf **Zuweisung ändern**, um die Bandbreite für SDX auf der Konsole neu zuzuweisen.
- Stellen Sie die VPX mit der Premium Edition auf SDX neu bereit.

Szenario: VPX/BLX/CPX-Formfaktor

Sie verwenden Flexed- oder Pooled-Lizenzen, und die Lizenzen laufen bald ab. Die folgenden Szenarien erläutern das Verhalten, wenn eine neue Lizenz auf der NetScaler Console vor und nach Ablauf der Laufzeit hochgeladen wird oder wenn keine Lizenzdatei vorhanden ist.

Vor Ablauf der Laufzeit

Wenn die neue Lizenz vor Ablauf der Laufzeit hochgeladen wird und die alte Lizenz noch gültig ist, stehen zwei verschiedene Kapazitätspools (alt und neu) zur Verfügung.

- Wenn NetScaler läuft, wechselt es nahtlos zur neuen Flexed- oder Pooled-Lizenz, nachdem die alte Lizenz abgelaufen ist.
- Ein Neustart ist nicht erforderlich.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler erfordert keine manuelle Neukonfiguration der Kapazität.

Nach Ablauf der Laufzeit

NetScaler-Instanzen mit abgelaufenen Lizenzen, die über NetScaler Console verwaltet werden, verarbeiten keinen Datenverkehr mehr und können zu Konfigurationsverlusten führen.

Vor oder nach Ablauf der Laufzeit, wenn die Lizenzedition der alten und neuen Lizenz unterschiedlich ist

Wenn die Lizenzedition der alten und neuen Lizenz unterschiedlich ist, müssen Sie unabhängig davon, ob die Laufzeit vor oder nach dem Ablauf liegt, Folgendes tun:

- Die Bandbreite muss manuell neu konfiguriert werden. In der NetScaler VPX/BLX/CPX GUI:
  a. Navigieren Sie zu **System > Lizenzen > Lizenzen verwalten**.
  b. Klicken Sie auf **Zuweisung freigeben**, um die Zuweisung freizugeben.
  c. Klicken Sie auf **Zuweisung ändern**, um die Bandbreite neu zuzuweisen und die Bandbreite auf Premium zu ändern.
- Starten Sie die VPX/BLX/CPX-Instanz neu.

Szenarien für das Verhalten bei Konnektivitätsproblemen

Wenn die Konnektivität zwischen NetScaler und Agent oder Agent und NetScaler Console-Dienst unterbrochen wird, ist das Verhalten wie folgt:

- NetScaler geht für 30 Tage in den Kulanzzeitraum.
- Während dieser Kulanzperiode funktioniert die Lizenzierungsfunktionalität bis zum dreißigsten Tag weiterhin.
- Am einunddreißigsten Tag,
  - werden NetScaler VPX/NetScaler CPX/NetScaler BLX und NetScaler MPX zwangsweise neu gestartet und verlieren ihre Lizenz.
  - Der Durchsatz aller VPX auf NetScaler SDX wird auf 1 Mbit/s reduziert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console-Server nur als Flexed- oder Pooled-Lizenzserver konfigurieren

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Citrix Produktpalette. LAS wird nach April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, wobei NetScaler Flexed-Lizenzen (Citrix Platform License/Universal Hybrid Multi-Cloud), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed term Bandwidth-Lizenzen unterstützt werden. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 für Console on-prem-Versionen ab 14.1-51.x und ab 13.1-60.x eingestellt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch vor 15th April 2026 auf Console on-prem Version 14.1-51.x oder höher aktualisieren und zu LAS wechseln, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie NetScaler Virtual CPU-Lizenzierung (Pooled vCPU), NetScaler VPX Check-In und Check-Out (CICO), unbefristete Lizenzen werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden nach dem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies gesetzlich oder durch Vorschriften verboten ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bei Fragen oder Bedenken wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix Maintenance bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder aussetzen, zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften verboten sind.
Als Administrator können Sie die NetScaler Console nur für die Pooled-Lizenzierungsfunktion konfigurieren. Mit dieser Konfiguration empfängt die NetScaler Console nur Lizenzdaten von NetScaler-Instanzen.

Manchmal kann es ein regulatorisches Mandat geben, das die Beschränkung von Daten von NetScaler-Instanzen erfordert, die die regulatorische Zone verlassen. In solchen Situationen können Sie eine lokale Instanz eines NetScaler Console-Servers in Ihrer regulatorischen Zone bereitstellen, um Verwaltungs-, Überwachungs- und Analysefunktionen zu nutzen. Wenn Sie denselben Ansatz verfolgen, um die Funktion für Pooled-Lizenzen zu verwenden, müssen Sie die Pooled-Lizenzen auf verschiedene NetScaler Console-Lizenzserver aufteilen. Dieser Ansatz bietet Ihnen nicht die Flexibilität, Pooled-Lizenzen auf Ihre global bereitgestellten NetScaler-Instanzen zu verteilen.

Konfigurieren Sie daher die NetScaler Console nur für die Pooled-Lizenzierungsfunktion. Die NetScaler Console empfängt nur Lizenzdaten von allen NetScaler-Instanzen. So können Sie das regulatorische Mandat einhalten und Pooled-Kapazitätslizenzen dynamisch auf global bereitgestellte NetScaler-Instanzen verteilen.

Dieses Dokument erklärt, wie die NetScaler Console nur für die Pooled-Lizenzierungsfunktion konfiguriert wird.

Voraussetzungen

Bevor Sie die NetScaler Console nur für die Pooled-Lizenzierungsfunktion konfigurieren, schließen Sie das erstmalige Onboarding und die Einrichtung der NetScaler Console ab. Stellen Sie sicher, dass Sie die Agent-Spezifikationen in den Systemanforderungen überprüfen.

WICHTIG

Wenn Sie die NetScaler Console zum ersten Mal onboarden oder einrichten, stellen Sie Folgendes sicher:

- Die Option „Benutzerdefinierte Bereitstellung“ ist ausgewählt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler-Instanzen, die hinzugefügt werden sollen, nachdem Sie Schritt 4 in diesem Konfigurationsverfahren abgeschlossen haben

Weitere Informationen zum Onboarding und zur Einrichtung der NetScaler Console finden Sie unter Erste Schritte.

Nachdem Sie die Onboarding-Schritte abgeschlossen haben, konfigurieren Sie die NetScaler Console nur für die Pooled-Lizenzierungsfunktion.

So konfigurieren Sie die NetScaler Console nur als Flexed- oder Pooled-Lizenzserver

Führen Sie die folgenden Schritte aus, um die NetScaler Console nur für die Lizenzierungsfunktion zu konfigurieren:

1. Navigieren Sie zu **Einstellungen > Globale Einstellungen > Systemkonfigurationen > Systembereitstellung**.
2. Wählen Sie unter **NetScaler Console-Bereitstellung** die Option **NetScaler Console nur als Flexed-/Pooled-Lizenzserver**.
3. Klicken Sie auf **OK**.

   Diese Aktion behält nur die Pooled-Lizenzierungsfunktion bei und deaktiviert die folgenden NetScaler Console-Funktionen:

   - NetScaler Console-Sicherung
   - Ereignisverwaltung
   - SSL-Zertifikatsverwaltung
   - Netzwerkberichterstattung
   - Netzwerkfunktionen
   - Konfigurationsprüfung

   HINWEIS

   Standardmäßig ist die NetScaler Console-Analysefunktion deaktiviert. Stellen Sie sicher, dass Sie diese Funktion deaktivieren, falls Sie sie aktiviert haben.

   Klicken Sie im Bestätigungsfeld auf **Ja**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die NetScaler Console-GUI zeigt nun nur noch die Pooled-Lizenzierungsfunktion an. Die restlichen Funktionen werden nicht angezeigt.

4. Nachdem Sie NetScaler Console nur für die Lizenzierungsfunktion konfiguriert haben, fügen Sie NetScaler-Instanzen auf der Seite **Infrastruktur > Instanzen** hinzu.

HINWEIS

- Sie können eine NetScaler-Instanz in der NetScaler Console und auch auf anderen NetScaler Console-Servern hinzufügen. Wenn Sie das Kennwort solcher NetScaler-Instanzen ändern, stellen Sie sicher, dass Sie das Kennwort auf allen NetScaler Console-Servern aktualisieren, auf denen die Instanz erkannt wird. Dieser Hinweis gilt, wenn die NetScaler Console nur für die Verwendung der Pooled-Lizenzierungsfunktion konfiguriert ist.
- Ein Benutzer kann in der NetScaler Console GUI immer noch einige Operationen der deaktivierten Funktionen ausführen. Zum Beispiel Ereignisabfrage und NetScaler-Backup. Als Superadministrator: Wenn Sie solche Operationen einschränken möchten, deaktivieren Sie den Benutzerzugriff für andere Administratoren mithilfe einer geeigneten Zugriffsrichtlinie. Weitere Informationen finden Sie unter Zugriffsrichtlinien in NetScaler Console konfigurieren.

Legacy-Lizenzen

Die Legacy-Lizenzierungsoptionen ermöglichen es Ihnen, die früheren NetScaler-Lizenzierungsmodelle zu verwalten, wie z. B. Pooled Capacity, Check-in- und Check-out-Lizenzierung und virtuelle CPU-Lizenzierung. Sie können auch unbefristete Lizenzen aktualisieren und Probleme mit Pooled Capacity-Lizenzen für NetScaler®-Bereitstellungen beheben.

Die folgenden Themen helfen Ihnen bei der Verwaltung von Legacy-Lizenzen:

- NetScaler Pooled Capacity
- Aktualisieren einer unbefristeten Lizenz in NetScaler MPX auf ADC Pooled Capacity
- Aktualisieren einer unbefristeten Lizenz in NetScaler SDX auf ADC Pooled Capacity
- NetScaler VPX Check-in- und Check-out-Lizenzierung
- NetScaler virtuelle CPU-Lizenzierung
- FAQs und weitere Ressourcen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Beheben von Problemen mit Pooled Capacity-Lizenzen

Gepoolte Kapazität

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 End of Life (EOL) sein. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Suite der Citrix-Produkte. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, und unterstützt NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed Term Bandwidth-Lizenzen. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler®-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 für Console on-prem-Versionen ab 14.1-51.x und ab 13.1-60.x eingestellt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch auf Console on-prem Version 14.1-51.x oder höher aktualisieren und vor 15th April 2026 auf LAS umstellen, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, Perpetual werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden bei einem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies gesetzlich oder durch Vorschriften verboten ist.
Bei Fragen oder Bedenken wenden Sie sich bitte an den Kundendienst. Citrix kann Ihre Citrix Maintenance bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder

© 1997–2026 Citrix Systems, Inc. All rights reserved.

aussetzen, zusätzlich zu allen anderen Rechtsmitteln, die Citrix gesetzlich oder nach Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften verboten sind.

Gepoolte Kapazität in NetScaler ist ein Lizenzierungsframework, das einen gemeinsamen Bandbreiten- und Instanzpool umfasst, der auf der NetScaler Console gehostet und von dieser bereitgestellt wird. Aus diesem gemeinsamen Pool entnimmt jede NetScaler-Instanz in Ihrem Rechenzentrum, unabhängig von Plattform oder Formfaktor, eine Instanzlizenz und nur so viel Bandbreite, wie sie benötigt. Die Lizenzdatei und die Bandbreite sind nicht an die Instanz gebunden. Wenn die Instanz diese Ressourcen nicht mehr benötigt, gibt sie diese an den gemeinsamen Pool zurück, wodurch die Ressourcen anderen Instanzen zur Verfügung stehen, die sie benötigen.

HINWEIS

In NetScaler Console ist einer der Agenten der Lizenzserver.

Dieses Lizenzierungs-Framework maximiert die Bandbreitenauslastung, indem sichergestellt wird, dass Instanzen nicht mehr Bandbreite zugewiesen bekommen, als sie benötigen. Die Möglichkeit der NetScaler-Instanzen, Lizenzen und Bandbreite aus einem gemeinsamen Pool ein- und auszuchecken, ermöglicht Ihnen auch die Automatisierung der Instanzbereitstellung.

Sie können die einer Instanz zugewiesene Bandbreite zur Laufzeit erhöhen oder verringern, ohne den Datenverkehr zu beeinträchtigen. Sie können die Lizenzen im Pool auch von einer Instanz auf eine andere übertragen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dauerlizenz in NetScaler MPX auf NetScaler Pooled Capacity aktualisieren

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Citrix Produktpalette. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, wobei NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed Term Bandwidth-Lizenzen unterstützt werden. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler®-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 für Console on-prem-Versionen ab 14.1-51.x und ab 13.1-60.x eingestellt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch vor 15th April 2026 auf Console on-prem Version 14.1-51.x oder höher aktualisieren und zu LAS wechseln, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, Perpetual werden mit LAS nicht unterstützt. NetScaler-Instanzen, die Dauerlizenzen ohne aktive Wartung verwenden, werden bei einem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies gesetzlich oder durch Vorschriften verboten ist.
Wenn Sie Fragen oder Bedenken haben, wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix-Wartung bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder aussetzen, zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit

© 1997–2026 Citrix Systems, Inc. All rights reserved.

zustehen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften verboten sind.
Eine NetScaler MPX Appliance mit Dauerlizenz kann auf eine NetScaler Pooled Capacity Lizenz aktualisiert werden. Das Upgrade auf eine NetScaler Pooled Capacity Lizenz ermöglicht es Ihnen, Lizenzen aus dem Lizenzpool bei Bedarf NetScaler Appliances zuzuweisen. NetScaler kann jeweils eine Lizenz verwenden, entweder eine Dauerlizenz oder eine Pooled-Lizenz. Ein Kunde kann von einer Pooled-Lizenz zu einer Dauerlizenz wechseln. Solange die Dauerlizenz gültig ist, können Sie den NetScaler neu konfigurieren und die Pooled-Lizenzierungskonfiguration entfernen. Wenn ein Kunde von einer Dauerlizenz zu einer Pooled-Lizenz oder von einer Pooled-Lizenz zu einer Dauerlizenz wechselt, werden alle NetScaler-Instanzen neu gestartet.

Sie können die NetScaler Pooled Capacity Lizenz auch für NetScaler-Instanzen konfigurieren, die im Hochverfügbarkeitsmodus konfiguriert sind. Informationen zum Konfigurieren der NetScaler Pooled Capacity Lizenz für NetScaler MPX-Instanzen im Hochverfügbarkeitsmodus finden Sie unter Aktualisieren der Dauerlizenz in einem NetScaler MPX Hochverfügbarkeitspaar auf NetScaler Pooled Capacity.

HINWEIS

Zum Upgrade der NetScaler MPX Appliance auf eine NetScaler Pooled Capacity Lizenz müssen Sie die MPX-Z Lizenz auf die Appliance hochladen.

So führen Sie ein Upgrade auf NetScaler Pooled Capacity durch:

1. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler Appliance ein, z. B. `<http://192.168.100.1>`.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der Seite **Willkommen** auf **Weiter**.
4. Laden Sie die Zero-Capacity-Lizenz (MPX-Z-Lizenz) hoch. Navigieren Sie auf der Registerkarte Konfiguration zu **System** \> **Lizenzen**.
5. Klicken Sie im Detailbereich auf **Lizenzen verwalten** und dann auf **Neue Lizenz hinzufügen**.
6. Wählen Sie auf der Seite **Lizenzen** die Option **Lizenzdateien hochladen** aus und klicken Sie auf **Durchsuchen**, um die Zero-Capacity-Lizenz von Ihrem lokalen Computer auszuwählen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Nachdem die Lizenz hochgeladen wurde, klicken Sie auf **Neustart**, um die Appliance neu zu starten.

   WARNUNG

   Nach dem Anwenden der MPX-Z-Lizenz werden die Funktionen, einschließlich der SSL-Auslagerung auf der Appliance, nicht mehr lizenziert. Die Appliance verarbeitet keine HTTPS-Anfragen mehr.

   Wenn die Option **Nur sicherer Zugriff** auf der Appliance vor dem Upgrade aktiviert ist, können Sie keine Verbindung zur Appliance über die NetScaler Console GUI mit HTTPS herstellen.
   ☐
8. Klicken Sie auf der Seite **Bestätigen** auf **Ja**.

   Ja(/en-us/netscaler-console-service/media/upgrade-mpx-4-confirm.jpg)
9. Melden Sie sich nach dem Neustart der Appliance bei der Appliance an.
10. Klicken Sie auf der Willkommensseite auf den Abschnitt **Lizenzen**.

    Konfiguration speichern und neu starten(/en-us/netscaler-console-service/media/upgrade-mpx-4-welcome.jpg)
11. Führen Sie im Abschnitt **Lizenzserver** die folgenden Schritte aus:

    Lizenzserver konfigurieren(/en-us/netscaler-console-service/media/upgrade-mpx-5.jpg)

    a. Geben Sie im Feld **Servername/IP-Adresse** die Details des Lizenzservers ein.
    b. Geben Sie im Feld **Lizenzport** den Lizenzserver-Port ein. Standardwert: 27000.
    c. Wenn Sie die Poollizenzen Ihrer Instanz über NetScaler Console verwalten möchten, aktivieren Sie das Kontrollkästchen **Bei Lizenzserver zur Verwaltbarkeit registrieren** und geben Sie die NetScaler Console-Anmeldeinformationen ein.
    d. Klicken Sie auf **Weiter**.
12. Führen Sie im Fenster „Lizenzen zuweisen“ die folgenden Schritte aus:

    a. Wählen Sie die Lizenzedition aus der Dropdown-Liste aus.

       Lizenzen zuweisen(/en-us/netscaler-console-service/media/upgrade-mpx-6.jpg)
    b. Weisen Sie der NetScaler-Appliance die Bandbreite aus dem Menü **Zuweisen** zu und klicken Sie auf **Lizenzen abrufen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lizenzen abrufen(/en-us/netscaler-console-service/media/upgrade-mpx-7.jpg)

c. Klicken Sie bei Aufforderung auf **Reboot**, um die Appliance neu zu starten.

13. Sobald die NetScaler MPX-Appliance neu gestartet ist, melden Sie sich bei der NetScaler MPX-Appliance an. Klicken Sie auf der Seite **Welcome** auf **Continue**.

    ☐

    Die Seite **Licenses** listet alle lizenzierten Funktionen auf.

    ☐

14. Navigieren Sie zu **System \> Pooled Licensing** und klicken Sie auf **Manage Licenses**.

    ☐

    Auf der Seite **Manage Licenses** können Sie die Details des Lizenzservers, der Lizenzedition und der zugewiesenen Bandbreite anzeigen.

    ☐

Upgrade der unbefristeten Lizenz in einem NetScaler MPX Hochverfügbarkeitspaar auf NetScaler Pooled Capacity

Für NetScaler MPX-Appliances, die im Hochverfügbarkeitsmodus konfiguriert sind, müssen Sie NetScaler Pooled Capacity auf beiden NetScaler-Instanzen (primär und sekundär) im HA-Paar konfigurieren. Sie müssen beiden NetScaler-Instanzen (primär und sekundär) im HA-Paar Lizenzen mit der gleichen Kapazität zuweisen. Wenn Sie beispielsweise 1 Gbit/s Kapazität von jeder Instanz im HA-Paar wünschen, müssen Sie 2 Gbit/s Kapazität aus dem gemeinsamen Pool zuweisen, damit Sie jeder NetScaler-Instanz (primär und sekundär) im HA-Paar 1 Gbit/s Kapazität zuweisen können.

WICHTIG

Um die NetScaler MPX-Appliance für die Verwendung einer NetScaler Pooled Capacity-Lizenz zu aktualisieren, müssen Sie die MPX-Z auf die Appliance hochladen.

Voraussetzungen

Stellen Sie sicher, dass Sie die MPX-Z-Lizenz auf beide Instanzen (primär und sekundär) im HA-Paar hochladen.

So laden Sie die MPX-Z-Lizenz auf die NetScaler MPX-Instanzen im HA-Paar hoch:

1. Geben Sie in einem Webbrowser die IP-Adresse des Geräts ein, z. B. `<http://192.168.100.1>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Geben Sie in den Feldern **Benutzername** und **Passwort** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der Seite **Willkommen** auf **Weiter**.
4. Laden Sie die Zero-Capacity-Lizenz (MPX-Z-Lizenz) hoch. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System \> Lizenzen**.
5. Klicken Sie im Detailbereich auf **Lizenzen verwalten** und dann auf **Neue Lizenz hinzufügen**.
6. Wählen Sie auf der Seite **Lizenzen** die Option **Lizenzdateien hochladen** und klicken Sie auf **Durchsuchen**, um die Zero-Capacity-Lizenz von Ihrem lokalen Computer auszuwählen.

   Sobald die Lizenz hochgeladen wurde, werden Sie aufgefordert, das Gerät neu zu starten.
7. Klicken Sie auf **Neustart**, um das Gerät neu zu starten.
8. Klicken Sie auf der Seite **Bestätigen** auf **Ja**.

So aktualisieren Sie eine vorhandene HA-Einrichtung auf NetScaler Pooled Capacity:

1. Melden Sie sich bei der sekundären NetScaler MPX-Instanz an. Geben Sie in einem Webbrowser die IP-Adresse des NetScaler-Geräts ein, z. B. `<http://192.168.100.1>`.
2. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der Seite **Willkommen** auf den Abschnitt **Lizenzen**.
4. Führen Sie im Abschnitt **Lizenzserver** Folgendes aus:
   a. Geben Sie im Feld **Servername/IP-Adresse** die Details des Lizenzservers ein.
   b. Geben Sie im Feld **Lizenzport** den Lizenzserver-Port ein. Standardwert: 27000.
   c. Wenn Sie die Poollizenzen Ihrer Instanz über NetScaler Console verwalten möchten, aktivieren Sie das Kontrollkästchen **Bei Lizenzserver zur Verwaltbarkeit registrieren** und geben Sie die NetScaler Console-Anmeldeinformationen ein.
   d. Klicken Sie auf **Weiter**.
5. Führen Sie im Fenster **Lizenzen zuweisen** Folgendes aus:
   a. Wählen Sie die Lizenzedition aus der Dropdown-Liste aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. Weisen Sie der NetScaler Appliance die Bandbreite aus dem Menü **Zuweisen** zu und klicken Sie auf **Lizenzen abrufen**.

c. Klicken Sie bei Aufforderung auf **Neustart**, um die Appliance neu zu starten.

   Nachdem die sekundäre NetScaler MPX Appliance neu gestartet wurde, wird sie zur primären NetScaler MPX Appliance im HA-Paar.

6. Melden Sie sich bei der vorhandenen primären NetScaler MPX Appliance an und starten Sie die Appliance neu. Führen Sie Folgendes aus:

   a. Geben Sie in einem Webbrowser die IP-Adresse der NetScaler Appliance ein, z. B. `<http://192.168.100.1>`.

   b. Geben Sie in den Feldern **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.

   c. Klicken Sie auf der Seite **Willkommen** auf **Weiter**.

   d. Klicken Sie auf der Registerkarte **Konfiguration** auf **System**.

   e. Klicken Sie auf der Seite **System** auf **Neustart**.

   f. Wählen Sie auf der Seite **Neustart** die Option **Warmstart** aus und klicken Sie auf **OK**.

   Nachdem die primäre NetScaler MPX Appliance neu gestartet wurde, wird sie zur sekundären NetScaler MPX Appliance im HA-Paar. Bei Bedarf können Sie die primären und sekundären Instanzen im HA-Paar mithilfe des folgenden Befehls auf einer beliebigen Instanz im HA-Paar in Ihre ursprüngliche HA-Paar-Konfiguration ändern:

```
> force ha failover
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Aktualisieren einer unbefristeten Lizenz in einem NetScaler SDX auf NetScaler Pooled Capacity

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Citrix-Produktsuite. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, wobei NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed Term Bandwidth-Lizenzen unterstützt werden. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler®-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Wird ab Anfang September 2025 unterstützt.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 für Console on-prem-Versionen ab 14.1-51.x und ab 13.1-60.x eingestellt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch vor 15th April 2026 auf Console on-prem Version 14.1-51.x oder höher aktualisieren und zu LAS wechseln, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO und unbefristete Lizenzen werden von LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden nach dem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies durch Gesetze oder Vorschriften untersagt ist.
Wenn Sie Fragen oder Bedenken haben, wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix-Wartung bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder

© 1997–2026 Citrix Systems, Inc. All rights reserved.

aussetzen, zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie durch Gesetze oder Vorschriften untersagt sind.
Ein NetScaler SDX mit unbefristeter Lizenz kann auf eine NetScaler Pooled Capacity-Lizenz aktualisiert werden. Das Upgrade auf eine NetScaler Pooled Capacity-Lizenz ermöglicht es Ihnen, Lizenzen aus dem Lizenzpool bei Bedarf NetScaler-Appliances zuzuweisen. NetScaler kann jeweils eine Lizenz verwenden, entweder eine unbefristete Lizenz oder eine Pooled-Lizenz. Ein Kunde kann von einer Pooled-Lizenz zu einer unbefristeten Lizenz wechseln. Solange die unbefristete Lizenz gültig ist, kann ein Kunde den NetScaler neu konfigurieren und die Pooled-Lizenzierungskonfiguration entfernen. Wenn ein Kunde von einer unbefristeten Lizenz zu einer Pooled-Lizenz oder von einer Pooled-Lizenz zu einer unbefristeten Lizenz wechselt, werden alle NetScaler-Instanzen neu gestartet.

Sie können die NetScaler Pooled Capacity-Lizenz auch für NetScaler-Instanzen konfigurieren, die im Hochverfügbarkeitsmodus konfiguriert sind.

HINWEIS

Um die SDX-Appliance auf die NetScaler Pooled Capacity Lizenz zu aktualisieren, müssen Sie die SDX-Z-Lizenz auf die Appliance hochladen.

Stellen Sie sicher, dass Sie die Berechtigung haben, NetScaler-Instanzen in NetScaler Console hinzuzufügen.
So aktualisieren Sie auf NetScaler Pooled Capacity:

1. Geben Sie in einem Webbrowser die IP-Adresse der SDX-Appliance ein, z. B. `<http://192.168.100.1>`.
2. Geben Sie in den Feldern **Benutzername** und **Passwort** die Administratoranmeldeinformationen ein.
3. Klicken Sie auf der Seite **Willkommen** auf **Weiter**.
4. Laden Sie die Zero-Capacity-Lizenz hoch. Navigieren Sie auf der Registerkarte Konfiguration zu **System** > **Lizenzen**.
5. Klicken Sie auf der Seite **Lizenzen verwalten** auf **Lizenzdatei hinzufügen**.
6. Wählen Sie auf der Seite **Lizenzen** die Option **Lizenzdateien von einem lokalen Computer hochladen** und klicken Sie auf **Durchsuchen**, um die Zero-Capacity-Lizenz von Ihrem lokalen Computer auszuwählen. Klicken Sie anschließend auf **Fertig stellen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sobald die Zero-Capacity-Lizenz erfolgreich angewendet wurde, wird ein Abschnitt **Gepoolte Lizenzen** auf der Seite **Lizenzen** angezeigt.

7. Führen Sie im Abschnitt **Gepoolte Lizenzen** die folgenden Schritte aus:

   a. Geben Sie im Feld **Name oder IP-Adresse des Lizenzservers** die Details des Lizenzservers ein.

      Wenn Sie den NetScaler Console-Server als Lizenzserver konfigurieren möchten, geben Sie die IP-Adresse des NetScaler Console-Servers an.

      Wenn Sie einen Agenten für die Kommunikation mit dem NetScaler Console-Server verwenden, geben Sie die IP-Adresse des Agenten an.

   b. Geben Sie im Feld **Portnummer** den Lizenzserver-Port ein. Standardwert: 27000.

   c. Klicken Sie auf **Lizenzen abrufen**.

8. Geben Sie im Fenster **Lizenzen zuweisen** die erforderlichen Instanzen und die Bandbreite an und klicken Sie auf **Zuweisen**.

   Auf der Seite **Lizenzen verwalten** können Sie die Details des Lizenzservers, der Lizenzedition sowie der zugewiesenen Instanzen und Bandbreite aus dem Pool anzeigen.

HINWEIS

Das Upgrade einer unbefristeten Lizenz auf Pooled Capacity erfordert keinen Neustart der SDX-Appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler VPX Check-in- und Check-out-Lizenzierung

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Suite der Citrix-Produkte. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, wobei NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed Term Bandwidth-Lizenzen unterstützt werden. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler®-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Release 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 in Console on-prem Releases 14.1-51.x und höher sowie 13.1-60.x und höher eingestellt. Wenn Sie auf Console on-prem Release 14.1-51.x oder Release 13.1-60.x oder später aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch vor 15th April 2026 auf Console on-prem Release 14.1-51.x oder später aktualisieren und auf LAS umstellen, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, unbefristet werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden nach dem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind Kunden möglicherweise nicht verfügbar, wo dies gesetzlich oder durch Vorschriften verboten ist.
Wenn Sie Fragen oder Bedenken haben, wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix Wartung bei Nichteinhaltung dieser Anforderungen ohne Haftung zusätzlich zu allen anderen Rechtsmitteln, die Citrix nach Gesetz oder Billigkeit zustehen, einschränken oder aussetzen. Diese Anforderungen gelten nicht, wo dies gesetzlich oder durch Vorschriften verboten ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können NetScaler VPX-Lizenzen bei Bedarf von NetScaler Console NetScaler VPX-Instanzen zuweisen. Die Lizenzen werden von NetScaler Console gespeichert und verwaltet, die über ein Lizenzierungs-Framework verfügt, das eine skalierbare und automatisierte Lizenzbereitstellung ermöglicht. Eine NetScaler VPX-Instanz kann, wenn sie bereitgestellt wird, die Lizenz von der NetScaler Console auschecken oder ihre Lizenz wieder in die NetScaler Console einchecken, wenn eine Instanz entfernt oder zerstört wird.

Lizenzen in NetScaler Console installieren

So installieren Sie Lizenzdateien auf der NetScaler Console:

1. Navigieren Sie zu **NetScaler Licensing > License Management**.
2. Klicken Sie im Abschnitt **License Files** auf **Add License File** und wählen Sie eine der folgenden Optionen aus:
   - **Lizenzdateien von einem lokalen Computer hochladen**: Wenn eine Lizenzdatei bereits auf Ihrem lokalen Computer vorhanden ist, können Sie sie in die Konsole hochladen.
   - **Lizenzzugriffscode verwenden**: Geben Sie den Lizenzzugriffscode für die Lizenz an, die Sie von Citrix erworben haben. Klicken Sie auf **Get Licenses** und dann auf **Finish**.
3. Klicken Sie auf „Finish“. Die Lizenzdateien werden zu NetScaler Console hinzugefügt.

HINWEIS

Stellen Sie sicher, dass Sie mit dem Internet verbunden sind, bevor Sie den Lizenzzugriffscode zur Installation der Lizenzen verwenden.

Zuweisen einer NetScaler VPX-Lizenz zu einer NetScaler VPX-Instanz mithilfe der NetScaler-GUI

1. Melden Sie sich bei der NetScaler VPX-Instanz an und navigieren Sie zu **System > Licenses > Manage Licenses**, klicken Sie auf **Add New License** und wählen Sie **Use remote licensing**.
2. Geben Sie die Details des Lizenzservers in das Feld **Server Name/IP Address** ein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hinweis

Wenn Sie die NetScaler VPX-Lizenzen Ihrer Instanz über die NetScaler Console verwalten möchten, aktivieren Sie das Kontrollkästchen **Register with NetScaler MA Service** und geben Sie die NetScaler Console-Anmeldeinformationen ein.

3. Klicken Sie auf **Continue**.
4. Wählen Sie im Fenster **Allocate licenses** den Lizenztyp aus. Das Fenster zeigt die gesamten und die verfügbaren virtuellen CPUs sowie die CPUs an, die zugewiesen werden können. Klicken Sie auf **Get Licenses**.
5. Klicken Sie auf der nächsten Seite auf **Reboot**, um die Lizenz anzuwenden.

HINWEIS

Sie können auch die aktuelle Lizenz freigeben und von einer anderen Edition auschecken. Wenn Sie beispielsweise bereits eine Lizenz der Standard Edition auf Ihrer Instanz ausführen, können Sie diese Lizenz freigeben und dann von der Advanced Edition auschecken.

6. Sie können die Lizenzzuweisung ändern oder freigeben, indem Sie zu **System > Lizenzen > Lizenzen verwalten** navigieren und **Zuweisung ändern** oder **Zuweisung freigeben** auswählen.
7. Wenn Sie auf **Zuweisung ändern** klicken, wird ein Pop-up-Fenster angezeigt, das die auf dem Lizenzserver verfügbaren Lizenzen zeigt. Wählen Sie die erforderliche Lizenz aus und klicken Sie auf **Lizenzen abrufen**.

Zuweisen einer NetScaler VPX-Lizenz zu einer NetScaler VPX-Instanz mithilfe der NetScaler CLI

1. Geben Sie in einem SSH-Client die IP-Adresse der NetScaler-Instanz ein und melden Sie sich mit Administratoranmeldeinformationen an.
2. Um einen Lizenzserver hinzuzufügen, geben Sie den folgenden Befehl ein:

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <port
number >]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Um die auf dem Lizenzserver verfügbaren Lizenzen anzuzeigen, geben Sie den folgenden Befehl ein:

```
sh licenseserverpool
```

4. Um einer NetScaler VPX-Instanz eine Lizenz zuzuweisen, geben Sie den folgenden Befehl ein:

```
set capacity –platform V\[S/E/P\]\[Bandwidth\]
```

Ablaufprüfungen für NetScaler VPX Check-in/Check-out-Lizenzen konfigurieren

Sie können jetzt den Lizenzablaufschwellenwert für NetScaler VPX-Lizenzen konfigurieren. Durch das Festlegen von Schwellenwerten sendet NetScaler Console Benachrichtigungen per E-Mail oder SMS, wenn eine Lizenz abläuft. Ein SNMP-Trap und eine Benachrichtigung werden auch gesendet, wenn die Lizenz auf NetScaler Console abgelaufen ist.

Ein Ereignis wird generiert, wenn eine Lizenzablaufbenachrichtigung gesendet wird, und dieses Ereignis kann auf NetScaler Console angezeigt werden.

Weitere Informationen finden Sie unter Lizenzverwaltung.

NetScaler Virtual-CPU-Lizenzierung

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Suite von Citrix-Produkten. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, wobei NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed-Term-Bandbreitenlizenzen unterstützt werden. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen eine LAS-kompatible Version verwenden.

Die mindestens erforderlichen NetScaler®-Versionen, die LAS-kompatibel sind, sind:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung ist jedoch ab April 15 2026 für Console on-prem-Versionen ab 14.1-51.x und ab 13.1-60.x veraltet. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis April 15 2026 weiterhin verwenden. Sie müssen jedoch vor April 15 2026 auf Console on-prem Version 14.1-51.x oder höher aktualisieren und zu LAS wechseln, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, Perpetual werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden bei einem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies gesetzlich oder durch Vorschriften verboten ist.
Bei Fragen oder Bedenken wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix-Wartung bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder aussetzen, zusätzlich zu allen anderen Rechtsmitteln, die Citrix nach Gesetz oder Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften verboten sind.
Rechenzentrumsadministratoren wie Sie wechseln zu neueren Technologien, die Netzwerkfunktionen vereinfachen und gleichzeitig niedrigere Kosten und größere Skalierbarkeit bieten. Neuere Rechenzentrumsarchitekturen müssen mindestens die folgenden Funktionen umfassen:

- Softwaredefiniertes Netzwerk (SDN)
- Netzwerkfunktionsvirtualisierung (NFV)
- Netzwerkvirtualisierung (NV)
- Microservices

Eine solche Bewegung erfordert auch, dass die Softwareanforderungen dynamisch, flexibel und agil sind, um den sich ständig ändernden Geschäftsanforderungen gerecht zu werden. Lizenzen sollen auch von einem zentralen Verwaltungstool mit vollständiger Transparenz über die Nutzung verwaltet werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Virtuelle CPU-Lizenzierung für NetScaler VPX

Früher wurden NetScaler VPX-Lizenzen basierend auf dem Bandbreitenverbrauch der Instanzen zugewiesen. Ein NetScaler VPX ist darauf beschränkt, eine bestimmte Bandbreite und andere Leistungsmetriken basierend auf der Lizenzedition zu verwenden, an die er gebunden ist. Um die verfügbare Bandbreite zu erhöhen, müssen Sie auf eine Lizenzedition aktualisieren, die mehr Bandbreite bietet. In bestimmten Szenarien ist der Bandbreitenbedarf möglicherweise geringer, aber der Bedarf an anderer L7-Leistung wie SSL-TPS, Komprimierungsdurchsatz usw. ist höher. Ein Upgrade der NetScaler VPX-Lizenz ist in solchen Fällen möglicherweise nicht geeignet. Sie müssen jedoch möglicherweise immer noch eine Lizenz mit großer Bandbreite erwerben, um die für CPU-intensive Verarbeitung erforderlichen Systemressourcen freizuschalten. NetScaler Console unterstützt jetzt die Zuweisung von Lizenzen an die NetScaler-Instanz basierend auf den Anforderungen an die virtuelle CPU.

Bei der virtuellen CPU-Nutzungsbasierten Lizenzierungsfunktion gibt die Lizenz die Anzahl der CPUs an, auf die ein bestimmter NetScaler VPX Anspruch hat. Der NetScaler VPX kann also nur Lizenzen für die Anzahl der darauf laufenden virtuellen CPUs vom Lizenzserver auschecken. NetScaler VPX checkt Lizenzen abhängig von der Anzahl der im System laufenden CPUs aus. NetScaler VPX berücksichtigt die inaktiven CPUs beim Auschecken der Lizenzen nicht. Ähnlich wie bei den Funktionen für die Pool-Lizenzkapazität und die CICO-Lizenzierung verwaltet der NetScaler Console-Lizenzserver einen separaten Satz von virtuellen CPU-Lizenzen. Auch hier werden die drei Editionen für virtuelle CPU-Lizenzen verwaltet: Standard, Advanced und Premium. Diese Editionen schalten dieselben Funktionen frei wie die Editionen für Bandbreitenlizenzen.

Es kann zu einer Änderung der Anzahl der virtuellen CPUs oder zu einer Änderung der Lizenzedition kommen. In einem solchen Fall müssen Sie die Instanz immer herunterfahren, bevor Sie eine Anforderung für einen neuen Satz von Lizenzen initiieren. Starten Sie den NetScaler VPX neu, nachdem Sie die Lizenzen ausgecheckt haben.

So konfigurieren Sie den Lizenzserver in NetScaler VPX über die GUI

1. Navigieren Sie in NetScaler VPX zu **System** > **Lizenzen** und klicken Sie auf **Lizenzen verwalten**.
2. Klicken Sie auf der Seite **Lizenz** auf **Neue Lizenz hinzufügen**.
3. Wählen Sie auf der Seite **Lizenzen** die Option **Remote-Lizenzierung verwenden**.
4. Wählen Sie **CPU-Lizenzierung** aus der Liste **Remote-Lizenzierungsmodus**.
5. Geben Sie die IP-Adresse des Lizenzservers und die Portnummer ein.
6. Klicken Sie auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

Registrieren Sie die NetScaler VPX-Instanz immer bei NetScaler Console. Falls noch nicht geschehen, aktivieren Sie „Bei NetScaler Console registrieren“ und geben Sie die Anmeldeinformationen für NetScaler Console ein.

7. Wählen Sie im Fenster **Lizenzen zuweisen** den Lizenztyp aus. Das Fenster zeigt die gesamten und die verfügbaren virtuellen CPUs sowie die CPUs an, die zugewiesen werden können. Klicken Sie auf **Lizenzen abrufen**.

   HINWEIS

   Für ein NetScaler HA-Paar weisen Sie jedem Knoten separat virtuelle CPU-Lizenzen zu.

8. Klicken Sie auf der nächsten Seite auf **Neustart**, um die Lizenzen anzuwenden.

   HINWEIS

   Sie können auch die aktuelle Lizenz freigeben und eine andere Edition auschecken. Zum Beispiel verwenden Sie bereits die Standard Edition-Lizenz auf Ihrer Instanz. Sie können diese Lizenz freigeben und dann die Advanced Edition auschecken.

Häufig gestellte Fragen und weitere Ressourcen

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 das End of Life (EOL) erreichen. Der Lizenzaktivierungsdienst (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Citrix Produktpalette. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, und unterstützt NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed Term Bandwidth-Lizenzen. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler®-Versionen, die LAS-kompatibel sind, sind:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung ist jedoch ab April 15 2026 in Console on-prem-Versionen ab 14.1-51.x und ab 13.1-60.x veraltet. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiter verwenden. Sie müssen jedoch auf Console on-prem Version 14.1-51.x oder höher aktualisieren und vor 15th April 2026 auf LAS umstellen, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, unbefristete Lizenzen werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden bei einem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies gesetzlich oder durch Vorschriften verboten ist.
Wenn Sie Fragen oder Bedenken haben, wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix Maintenance bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder aussetzen, zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie gesetzlich oder durch Vorschriften verboten sind.
Dieser Abschnitt listet die Referenzdokumentationen zur Konfiguration und zum Betrieb der Pooled-Lizenzierung auf. Sie können diese Dokumente zur Unterstützung bei Konfigurations- und Betriebsproblemen heranziehen.

Konfiguration

1. Wo finde ich Informationen zur Übersicht und den Funktionen der Pooled-Kapazität?

   Antwort: Siehe Gepoolte Kapazität konfigurieren.

2. Wie konvertiere oder migriere ich dauerhafte in gepoolte Lizenzen und umgekehrt?

   Antwort: Die Konvertierung einer unbefristeten Lizenz in eine Lizenz für gepoolte Kapazität ist ein Einwegprozess für den Lizenzanspruch. Sie können die Lizenz für gepoolte Kapazität nicht wieder in eine unbefristete Lizenz umwandeln.

3. Wie stelle ich den NetScaler Console-Server bereit?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Antwort: Befolgen Sie das Dokument Erste Schritte.

4. Wie füge ich einer bestehenden gepoolten Lizenz eine Lizenz hinzu und weise sie zu?

   Antwort: Befolgen Sie das Dokument Lizenzverwaltung.

5. Wie weise ich Kapazität und Bandbreite auf Instanzen zu/erhöhe sie?

   Antwort: Befolgen Sie das Dokument Lizenzverwaltung.

Lizenzserver-Agent

1. Wie weise ich einem bestimmten Agenten die LSA-Rolle zu?

   Antwort: Dem ersten bereitgestellten Agenten wird die LSA-Rolle zugewiesen. Wenn der LSA-Agent ausfällt, treten alle NetScaler-Instanzen, die für die gepoolte Lizenzierung mit NetScaler Console verbunden sind, für einen Tag in eine Kulanzperiode ein. Am nächsten Tag wählt NetScaler Console einen neuen Agenten als LSA aus. Dieses Verhalten ist standardmäßig aktiviert.

   Administratoren können einen NetScaler-Agenten innerhalb von 24 Stunden manuell als LSA auswählen, anstatt darauf zu warten, dass der NetScaler Console-Dienst nach 24 Stunden Ausfallzeit des LSA automatisch einen Agenten auswählt.

   HINWEIS:

   Während dieses Übergangs wird die NetScaler-Funktionalität nicht beeinträchtigt.

2. Wie können wir feststellen, welcher Agent die Lizenzserver-Rolle hostet?

   Antwort: Um zu erfahren, welcher Agent die LSA-Rolle hostet, können Sie den folgenden Befehl in der Shell ausführen:

   ```
   cat /mpsconfig/.lmp/agent
   ```

   Wenn der Ausgabewert für „role“ **lsa** ist, dann hostet dieser Agent die Lizenzserver-Rolle.

   ☐
   In der NetScaler Console-GUI sehen Sie LSA neben der IP-Adresse des zugewiesenen Agenten.

   ☐

3. Was passiert, wenn der Agent, der die LSA-Rolle hostet, ausfällt?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Antwort: Wenn der Agent, der die LSA-Rolle hostet, offline ist, wechseln alle bereitgestellten NetScaler-Geräte, die für die Lizenzierung mit gemeinsam genutzter Kapazität konfiguriert sind, in den Kulanzzeitraum. Der Kulanzzeitraum dauert 30 Tage und die den NetScaler-Geräten zugewiesenen Ressourcen bleiben in diesem Zeitraum bestehen. NetScaler-Instanzen in diesem Zustand können keine Lizenzzuweisung vornehmen oder ändern, bis der Agent, der die LSA-Rolle hostet, wieder online ist oder ein neuer Agent mit der LSA-Rolle zugewiesen wird.

4. Wenn der Agent, der die LSA-Rolle hostet, für einen längeren Zeitraum offline geht, wird es eine Neuwahl geben?

   Antwort: Wenn der Administrator innerhalb von 24 Stunden keinen neuen LSA auswählt, wählt der NetScaler Console-Dienst automatisch den nächsten verfügbaren Agenten als neuen LSA aus, nachdem der LSA-Agent 24 Stunden lang ausgefallen war. Der Kulanzzeitraum der NetScaler-Geräte endet, nachdem der neue LSA gewählt wurde.

Häufige Probleme

1. Instanzen, die im Kulanzmodus ausgeführt werden, aufgrund von Konnektivitätsfehlern, Upgrades, Split-Brain und anderen Ursachen.

   Antwort: Siehe das Verhalten des NetScaler Console-Lizenzservers, das unter Konfigurieren der NetScaler-Poolkapazität dokumentiert ist.

2. Lizenzen werden auf Instanzen nicht angewendet oder widergespiegelt.

   Antwort: Siehe Beheben von Problemen mit Pooled Capacity-Lizenzen.

3. Die Lizenzzuweisung steckt in „Synchronisierung läuft“ fest.

   Antwort: Siehe Beheben von Problemen mit Pooled Capacity-Lizenzen.

4. Fehler aufgrund einer falschen Host-ID in der Lizenzdatei.

   Antwort: Um einen NetScaler Console-Server zu identifizieren, können Sie dem Server einen Hostnamen zuweisen. Der Hostname wird auf der Universal-Lizenz für NetScaler Console angezeigt. Weitere Informationen finden Sie unter Zuweisen eines Hostnamens zu einem NetScaler Console-Server.

Migration

1. Ist eine Neuzuweisung von Bandbreite und Instanzen für VPX auf SDX erforderlich, wenn von einem Console-Mandanten zu einem anderen Console-Mandanten migriert wird, während gepoolte oder flexible Lizenzen verwendet werden?

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Antwort: Wenn die Lizenzierungsedition auf beiden Mandanten gleich ist und SDX die zuvor zugewiesene Kapazität erhalten kann, ist keine Neuzuweisung von Bandbreite und Instanzen für VPX auf SDX erforderlich.

Beheben von Problemen mit der Pooled-Kapazitätslizenz

WICHTIG:

Das dateibasierte Lizenzierungssystem (auch als manuell verwaltete Berechtigungen bezeichnet), das traditionell zur Aktivierung verschiedener lokaler Komponenten verwendet wird, wird am April 15, 2026 End of Life (EOL) erreichen. Der License Activation Service (LAS) ist die Technologie der nächsten Generation für Produktaktivierungen in der gesamten Citrix Produktpalette. LAS wird nach dem April 15, 2026 die einzige Möglichkeit sein, NetScaler-Instanzen zu aktivieren und zu lizenzieren, und unterstützt NetScaler Flexed-Lizenzen (CPL/UHMC), ältere NetScaler Pooled-Lizenzen und NetScaler Fixed-Term-Bandbreitenlizenzen. Um weiterhin unterstützt zu werden, müssen Ihre NetScaler- und NetScaler Console-Bereitstellungen auf einer LAS-kompatiblen Version sein.

Die mindestens erforderlichen NetScaler®-Versionen, die LAS-kompatibel sind, sind:

- NetScaler ADCs: 14.1-51.x, 13.1-60.x, 13.1-37.246 (FIPS), 14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x, 13.1-60.x
- NetScaler Console Service: Unterstützt ab Anfang September 2025.
- NetScaler Console on-prem: 14.1-51.x

  Hinweis: Die LAS-Unterstützung für Console on-prem ist ab Version 14.1-51.x verfügbar. Die dateibasierte Lizenzierung wird jedoch ab April 15 2026 in Console on-prem-Versionen ab 14.1-51.x und ab 13.1-60.x nicht mehr unterstützt. Wenn Sie auf Console on-prem Version 14.1-51.x oder Version 13.1-60.x oder höher aktualisieren, können Sie die dateibasierte Lizenzierung bis 15th April 2026 weiterhin verwenden. Sie müssen jedoch vor 15th April 2026 auf Console on-prem Version 14.1-51.x oder höher aktualisieren und zu LAS wechseln, da Console on-prem 13.1 LAS nicht unterstützt.

Alle anderen Formen älterer NetScaler-Lizenzen wie Pooled vCPU, CICO, unbefristet werden mit LAS nicht unterstützt. NetScaler-Instanzen, die unbefristete Lizenzen ohne aktive Wartung nutzen, werden nach dem Upgrade auf die oben genannten Softwareversionen unlizenziert.
LAS-basierte Lizenzen sind möglicherweise für Kunden nicht verfügbar, wo dies durch Gesetze oder Vorschriften untersagt ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bei Fragen oder Bedenken wenden Sie sich an den Kundendienst. Citrix kann Ihre Citrix-Wartung bei Nichteinhaltung dieser Anforderungen ohne Haftung einschränken oder aussetzen, zusätzlich zu allen anderen Rechtsbehelfen, die Citrix nach Gesetz oder Billigkeit zustehen. Diese Anforderungen gelten nicht, wo sie durch Gesetze oder Vorschriften untersagt sind.
Dieser Abschnitt beschreibt, wie gängige Probleme mit der Pooled-Kapazität analysiert und behoben werden können, und die Fehlerbehebungsszenarien gelten auch für manuell verwaltete Berechtigungen (dateibasierte Lizenzen).

Lizenzstatus überprüfen

Die NetScaler Console fungiert als Lizenzserver für Ihre NetScaler Pooled-Kapazitätslizenz. Sie können die NetScaler Console GUI verwenden, um den Status der Lizenz zu überprüfen. Navigieren Sie zu **Infrastructure > Pooled Licensing > Throughput Capacity > License Usage**.

Die folgende Tabelle listet die Arten des Lizenzstatus und deren Bedeutung auf.

STATUS	BEDEUTUNG
Zugewiesen	Der Lizenzstatus ist in Ordnung.
Zugewiesen: nicht auf NetScaler angewendet	NetScaler erfordert möglicherweise einen Neustart, wenn die Lizenz von NetScaler ausgecheckt oder eingecheckt wurde, NetScaler aber noch nicht neu gestartet wurde.
Nicht zugewiesen	Die Lizenz ist in der NetScaler-Instanz nicht zugewiesen.
Gnadenfrist	Die NetScaler-Instanz befindet sich für 30 Tage in der Lizenz-Gnadenfrist.
Synchronisierung läuft	NetScaler Console ruft Informationen von NetScaler in 2-Minuten-Intervallen ab. Die Synchronisierung von Lizenzen zwischen NetScaler Console und NetScaler kann bis zu 15 Minuten dauern. NetScaler Console wurde möglicherweise neu gestartet oder ein NetScaler Console HA-Failover wurde ausgelöst.
Teilweise zugewiesen	NetScaler kann die zugewiesene Kapazität nicht akzeptieren, da es möglicherweise mit

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STATUS	BEDEUTUNG
	seiner maximalen Zuweisung läuft. Beispielsweise läuft NetScaler mit einer Lizenzpoolkapazität von 10 Gbit/s. Wenn NetScaler neu startet, werden die 10 Gbit/s wieder beim NetScaler Console-Lizenzserver eingecheckt. Wenn NetScaler wieder online ist, versucht es, die zuvor zugewiesenen 10 Gbit/s automatisch auszuchecken. In der Zwischenzeit könnten andere NetScaler-Instanzen diese Bandbreite ausgecheckt haben. „Teilweise zugewiesen“ (Partially Allocated) wird angezeigt, wenn der Lizenzpool nicht über genügend Kapazität verfügt, um diesem NetScaler die vollständigen 10 Gbit/s oder sogar eine Teilkapazität zuzuweisen.
Nicht verwaltet	NetScaler wurde der NetScaler Console zur Verwaltbarkeit nicht hinzugefügt. Dies hat keine Auswirkungen auf die NetScaler-Lizenzierung, kann aber die Lizenzüberwachung über die NetScaler Console beeinträchtigen.
Nicht verwaltet	NetScaler wurde der NetScaler Console zur Verwaltbarkeit nicht hinzugefügt. Dies hat keine Auswirkungen auf die NetScaler-Lizenzierung, kann aber die Lizenzüberwachung über die NetScaler Console beeinträchtigen.
Verbindung verloren	NetScaler ist von der NetScaler Console aus zur Verwaltbarkeit nicht erreichbar. Beispielsweise gibt es Probleme mit der Netzwerkkonnektivität, NITRO funktioniert nicht oder die NetScaler-Passwörter stimmen nicht überein. Wenn NITRO nicht funktioniert oder die NetScaler-Passwörter nicht übereinstimmen, hat dies keine Auswirkungen auf die NetScaler-Lizenzierung. Es kann jedoch die Lizenzüberwachung über die NetScaler Console beeinträchtigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Serverstatus prüfen

Dieser Abschnitt beschreibt die häufigsten Probleme mit dem Serverstatus sowie mögliche Ursachen und Lösungen.

Problem: NetScaler zeigt den Lizenzserver als nicht erreichbar an und der Lizenzstatus wechselt in den Kulanzmodus (grace).

- Die Verbindung zum Lizenzserver (NetScaler Console oder Agent) ist seit mehr als 15 Minuten unterbrochen. Überprüfen Sie, ob der Lizenzserver aktiv und erreichbar ist.
- NetScaler befindet sich im Kulanzmodus (grace mode).

Problem: NetScaler zeigt den Lizenzserverstatus als erreichbar an, aber der Benutzerversuch, die Zuweisung zu ändern, hat keine Auswirkung. Das Klicken auf **Zuweisung ändern** (Change Allocation) gibt 0 0 zurück. Dieser Wert könnte den Anschein erwecken, dass die konfigurierte Kapazität verloren gegangen ist.

- Die Verbindung zum Lizenzserver ist kürzlich unterbrochen worden, aber der NetScaler hat den zweiten Heartbeat noch nicht verpasst. Daher befindet er sich (noch) nicht im Kulanzmodus (Grace). Überprüfen Sie, ob der Lizenzserver aktiv und erreichbar ist.

Problem: NetScaler zeigt Kapazitäts- und Instanzanzahlen an, aber der Lizenzserver ist **Erreichbar/Nicht erreichbar** (Reachable/Unreachable). Das Klicken auf **Zuweisung ändern** (Change Allocation) gibt einige Zahlen zurück, berücksichtigt aber nicht die konfigurierte Kapazität.

- Die Verbindung zum Lizenzserver wurde wiederhergestellt, aber der NetScaler hat den zweiten Heartbeat noch nicht verpasst oder die Reconnect-Probe gesendet.

Problem: NetScaler meldet „Verbindung zum Lizenzserver nicht möglich“ bei der Konfiguration von Pooled Licensing mit NetScaler Console

- Überprüfen Sie die Firewall-Regeln, um sicherzustellen, dass die Ports 27000 und 7279 geöffnet sind.
- Der Agent ist nicht registriert. Weitere Informationen finden Sie unter Erste Schritte.
- In NetScaler Console wurden keine Lizenzdateien hochgeladen. Weitere Informationen finden Sie unter NetScaler Pooled Capacity konfigurieren
- NetScaler Console hat die falsche Lizenzdatei.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Lizenznutzungsbericht prüfen

Unter **NetScaler Licensing > Pooled Licensing > Throughput Capacity > License Usage** in der NetScaler Console-GUI sehen Sie die monatliche Spitzenauslastung Ihrer Lizenz. Sie können diesen Bericht verwenden, um Ihre Lizenznutzung zu erhöhen oder den Kauf einer zusätzlichen Lizenz zu planen.

Im Folgenden finden Sie einige Details, wie der Bericht generiert und verwendet werden kann.

Abfrage: Lizenzdaten werden alle 15 Minuten von den NetScaler-Instanzen abgefragt.

Beibehaltung stündlicher Spitzenwerte: NetScaler Console speichert nur die maximale Lizenznutzung pro Stunde und pro Gerät.

Berichterstellung: Sie können einen GUI-Bericht für jede Instanz und für einen bestimmten Zeitraum generieren.

Exportieren: Sie können Berichte entweder im CSV-Format oder im XLS-Format exportieren.

Bereinigung: NetScaler Console bereinigt Daten am ersten Tag jedes Monats um 00:10 Uhr. Der Bereinigungszeitraum ist konfigurierbar (der Standardzeitraum beträgt zwei Monate).

Zähler und Statistiken für Pooled Capacity Licensing

Die folgenden Zähler, Protokolle und Befehle zeigen die NetScaler Pooled-Lizenzierungsmetriken an, die das Verhalten von NetScaler Console und NetScaler-Instanzen im Pooled-Lizenzierungsmodus angeben.

- **SNMP-Traps**: verfügbar ab NetScaler Version 13.xx.
- **NSCONMSG-Zähler für Ratenbegrenzung**: verfügbar ab NetScaler Version 12.1 57.xx.
- **NetScaler Console-Zähler** NetScaler Console-Befehlsaktionen sind im NetScaler Cloud-Dienst verfügbar.

SNMP-Traps

Sie können die folgenden SNMP-Traps v.13 Pooled-Lizenzalarme konfigurieren

- `POOLED-LICENSE-CHECKOUT-FAILURE`
- `POOLED-LICENSE-ONGRACE`
- `Configure POOLED-LICENSE-PARTIAL`

Weitere Informationen zu diesen Alarmen finden Sie unter NetScaler SNMP OID-Referenz.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NSCONMSG-Zähler

Überprüfen Sie die folgenden `NCCONMSG` Zähler und deren Bedeutung:

- `allnic_err_rl_cpu_pkt_drops`: aggregierte (alle NICs) Paketverluste, nachdem die CPU-Grenze erreicht wurde
- `allnic_err_rl_pps_pkt_drops`: aggregierte Paketverluste systemweit nach pps-Grenze
- `allnic_err_rl_rate_pkt_drops`: aggregierte Ratenverluste systemweit
- `allnic_err_rl_pkt_drops`: kumulative Ratenbegrenzungs-Drops aufgrund von Rate, pps und CPU
- `rl_tot_ssl_rl_enforced`: Anzahl der Male, bei denen SSL-RL angewendet wurde (bei neuen SSL-Verbindungen)
- `rl_tot_ssl_rl_data_limited`: Anzahl der Male, bei denen das SSL-Durchsatzlimit erreicht wurde
- `rl_tot_ssl_rl_sess_limited`: Anzahl der Male, bei denen das SSL-TPS-Limit erreicht wurde

NetScaler Console-Zähler

Wenn Sie die Ereignisaktion **Befehlsaktion ausführen** auswählen, können Sie einen Befehl oder ein Skript erstellen, das auf der NetScaler Console für Ereignisse ausgeführt werden kann, die einem bestimmten Filterkriterium entsprechen. Sie können auch die folgenden Parameter für das Skript **Befehlsaktion ausführen** festlegen:

PARAMETER	BESCHREIBUNG
Quelle	Dieser Parameter entspricht der Quell-IP-Adresse des empfangenen Ereignisses.
Kategorie	Dieser Parameter entspricht dem Typ der Traps, die unter der Kategorie des Filters definiert sind.
Entität	Dieser Parameter entspricht den Entitätsinstanzen oder Zählern, für die ein Ereignis generiert wurde. Er kann die Zählernamen für alle schwellenwertbezogenen Ereignisse, Entitätsnamen für alle entitätsbezogenen Ereignisse und

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	BESCHREIBUNG
	Zertifikatsnamen für alle zertifikatsbezogenen Ereignisse umfassen.
Schweregrad	Dieser Parameter entspricht dem Schweregrad des Ereignisses.
$Fehlerobjekt	Das Fehlerobjekt beeinflusst die Art und Weise, wie ein Ereignis verarbeitet wird, und stellt sicher, dass das Fehlerobjekt das exakte Problem widerspiegelt, wie es gemeldet wurde. Dieser Parameter kann verwendet werden, um Probleme schnell aufzuspüren und den Grund für den Fehler zu identifizieren, anstatt nur Rohereignisse zu melden.

HINWEIS

Während der Befehlsausführung werden diese Parameter durch tatsächliche Werte ersetzt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Einstellungen

Mit den NetScaler Console-Einstellungen können Sie das Verhalten des Dienstes konfigurieren und verwalten. Sie können die rollenbasierte Zugriffssteuerung, Datenspeicherung und -aufbewahrung, Systemalarme, Observability-Integrationen, Benachrichtigungen und andere globale Einstellungen für NetScaler®-Bereitstellungen verwalten.

Die folgenden Themen helfen Ihnen bei der Konfiguration der NetScaler Console-Einstellungen:

- On-Prem-Instanzen der Console, die über Cloud Connect mit dem Console-Dienst verbunden sind
- Telemetrie-Upload von On-Prem-Instanzen der Console
- Analysen auf virtuellen Servern konfigurieren
- Rollenbasierte Zugriffssteuerung konfigurieren
- Ein Netzprofil für die verwaltete NetScaler-Instanz zuweisen
- Datenspeicherverwaltung
- Datenaufbewahrungsrichtlinie
- Systemalarme konfigurieren und anzeigen
- Observability-Integration
- Analyseeinstellungen konfigurieren
- Benachrichtigungen konfigurieren
- Exportberichte exportieren oder planen
- Globale Einstellungen
- Aktionsrichtlinien konfigurieren
- Audit-Protokollmeldungen
- IPAM konfigurieren

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mit dem Console-Dienst über Cloud Connect verbundene Console On-Prem-Instanzen

Unter **Einstellungen > NetScaler Console On-Prem** können Sie Details der NetScaler Console On-Prem-Instanzen anzeigen, die über Cloud Connect mit dem NetScaler Console-Dienst-Mandanten verbunden sind.

- **Name** – Die IP-Adresse der NetScaler Console On-Prem
- **Kundenname** – Der Name des NetScaler Console-Dienst-Mandanten
- **Status** – Der Konnektivitätsstatus zwischen der NetScaler Console On-Prem-Instanz und dem NetScaler Console-Dienst
- **Version** – Die Build-Version der NetScaler Console On-Prem-Instanz

Console On-Prem-Upload

Diese Seite gilt nur für NetScaler® On-Prem-Benutzer, die den manuellen Modus gewählt haben, um ihre Telemetriedaten in den NetScaler Console-Dienst hochzuladen. Stellen Sie sicher, dass Sie die Telemetriedaten von Ihrer NetScaler Console On-Prem heruntergeladen haben (klicken Sie auf der **NetScaler Telemetry**-Homepage auf **Download Telemetry**, um die Bundle-Datei (.tgz) herunterzuladen, die die erforderlichen Telemetriedaten enthält).

Ab Build **14.1-43.x** müssen Sie für jede NetScaler Console On-Prem-Instanz ein Profil erstellen, um die Telemetriedatei in den NetScaler Console-Dienst hochzuladen. Möglicherweise haben Sie mehrere NetScaler Console On-Prem-Instanzen global bereitgestellt. Durch das Erstellen eines Profils für jede On-Prem-Instanz können Sie die Telemetriedatei für diese On-Prem-Instanzen hochladen und die Upload-Frist separat überwachen.

So erstellen Sie ein Profil:

1. Navigieren Sie zu **Settings > Console on-prem telemetry upload** und klicken Sie auf **Create Profile**.
2. Geben Sie auf der Seite **Create Profile** Folgendes an:
    a. Einen Profilnamen Ihrer Wahl.
    b. Die NetScaler Console On-Prem-IP-Adresse.
    c. Den Administratornamen der NetScaler Console On-Prem.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Klicken Sie auf **Next**.

   Der Profilname wurde erstellt. Sie können entweder die Telemetriedatei hochladen und auf Fertig klicken oder sie später hochladen.

e. Wiederholen Sie den Vorgang, um mehrere Profile für alle NetScaler Console On-Prem-Instanzen zu erstellen.

Nachdem Sie Profile erstellt haben, können Sie die erstellten Profile anzeigen:

HINWEIS:

Wenn Sie ein bestehender NetScaler Console On-Prem-Benutzer sind und die Telemetriedatei zuvor in den NetScaler Console-Dienst hochgeladen haben, müssen Sie ein neues Profil erstellen und dann die Telemetriedatei hochladen. Nach dem Erstellen des Profils stellen Sie möglicherweise eine Diskrepanz zwischen der NetScaler Console On-Prem-Frist und der NetScaler Console-Dienst-Frist fest. Stellen Sie sicher, dass Sie die Telemetriedatei am oder vor dem Fälligkeitsdatum, das in Ihrer NetScaler Console On-Prem angezeigt wird, in den NetScaler Console-Dienst hochladen. Diese Diskrepanz wird nach einem Upload mit dem neuen Profil behoben.

So laden Sie Ihre Datentelemetrie im NetScaler Console-Dienst hoch:

1. Klicken Sie auf der Seite **NetScaler Console On-Prem-Upload** auf **Telemetrie hochladen** aus dem erstellten Profil und wählen Sie die heruntergeladene (.tgz)-Datei aus, um den Upload-Vorgang abzuschließen.
2. Schließen Sie den ersten Upload innerhalb von 30 Tagen nach Auswahl des manuellen Modus ab. Wiederholen Sie den gleichen Vorgang und laden Sie die Telemetriedatei danach alle 90 Tage hoch.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEISE:

- Der Upload schlägt fehl, wenn die Datei nicht im gültigen (.tgz)-Format vorliegt oder die Datei die Integritätsprüfungen nicht besteht. Es wird empfohlen, die Datei erneut herunterzuladen und den Upload zu wiederholen. Wenn das Problem weiterhin besteht, wenden Sie sich an den Kundendienst.
- Der NetScaler Console-Dienst lehnt Telemetriedateien ab, die älter als 90 Tage sind. Um es erneut zu versuchen, laden Sie eine neue Telemetriedatei herunter und laden Sie sie hoch.
- Sie können die optionalen Telemetriedaten deaktivieren. Um dies zu deaktivieren, müssen Sie in NetScaler Console On-Prem zunächst **Security Advisory** auf der Seite **NetScaler Telemetry** deaktivieren, dann zu **Settings > Administration > Enable or disable the Console feature data sharing** navigieren und das Kontrollkästchen **I agree to share Console feature usage data** deaktivieren.

So bearbeiten oder löschen Sie ein Profil:

1. Navigieren Sie zu **Settings > Console on-prem telemetry upload** und wählen Sie das Profil aus, das Sie bearbeiten oder löschen möchten.
2. Zum Bearbeiten klicken Sie auf das Symbol **Edit**. Aktualisieren Sie die erforderlichen Felder und klicken Sie auf **Save**.
3. Zum Löschen klicken Sie auf das Symbol **Delete**.

Analysen auf virtuellen Servern konfigurieren

Ab Build 14.1-21.x werden alle erkannten virtuellen Server und die nachfolgenden virtuellen Server automatisch lizenziert. Sie können mit der Konfiguration der Analysen fortfahren.

Sie können Analysen auf zwei Arten konfigurieren. Navigieren Sie zu **Settings > Analytics Configuration**, um Folgendes anzuzeigen:

- **Virtual Server Analytics Summary** – Ermöglicht die Konfiguration von Analysen auf den erkannten virtuellen Servern.
- **Global Analytics Summary** – Ermöglicht die Konfiguration von Analysen auf sowohl erkannten als auch nachfolgenden virtuellen Servern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analysen auf den erkannten virtuellen Servern konfigurieren

HINWEIS:

Stellen Sie sicher, dass sich die virtuellen Server, für die Sie Analysen aktivieren möchten, im Status **UP** befinden.

1. Klicken Sie unter **Virtual Server Analytics Summary** auf **Configure Analytics**.

   Die Seite **All Virtual Servers** wird angezeigt. Sie können:

   - Analysen aktivieren
   - Analysen bearbeiten
   - Analysen deaktivieren

   HINWEIS:

   Die unterstützten virtuellen Server, für die Analysen aktiviert werden können, sind Load Balancing, Content Switching und NetScaler Gateway.

2. Wählen Sie die virtuellen Server aus und klicken Sie dann auf **Enable Security & Analytics**.

   HINWEIS

   Alternativ können Sie Analysen für eine Instanz aktivieren:

   a. Navigieren Sie zu **Infrastructure > Instances > NetScaler** und wählen Sie dann den Instanztyp aus. Zum Beispiel VPX.

   b. Wählen Sie die Instanz aus und wählen Sie aus der Liste **Select Action** die Option **Configure Analytics**.

   c. Wählen Sie auf der Seite **Configure Analytics on Virtual Servers** den virtuellen Server aus und klicken Sie auf **Enable Security & Analytics**.

3. Im Fenster **Enable Security & Analytics**:

   a. Wählen Sie die Insight-Typen aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Ab Build 14.1-44.x ist **Web Transaction Analytics** auf der Ebene des virtuellen Servers verfügbar. Um dies zu aktivieren, wählen Sie die Option **Detailed Web Transactions** unter **Web Insight** aus.

b. Unter **Advanced Settings (optional)**:

- Wählen Sie **Logstream** als Transport Mode aus.

HINWEIS:

Für NetScaler 12.0 oder früher ist **IPFIX** die Standardoption für den Transport Mode. Für NetScaler 12.0 oder höher können Sie entweder **Logstream** oder **IPFIX** als Transport Mode auswählen.

Weitere Informationen zu IPFIX und Logstream finden Sie unter Logstream-Übersicht.

- **HTTP X-Forwarded-For aktivieren** – Wählen Sie diese Option, um die IP-Adresse für die Verbindung zwischen Client und Anwendung über HTTP-Proxy oder Lastenausgleich zu identifizieren.
- **Benutzerdefinierter Header** – Definieren Sie einen benutzerdefinierten Header wie X-Real-IP, X-Client-IP oder einen anderen benutzerdefinierten Header, um die tatsächliche Client-IP-Adresse anstelle der Proxy-IP-Adresse abzurufen. Stellen Sie sicher, dass die verwaltete NetScaler-Instanz Version 14.1–38.24 oder höher ist.
- **NetScaler Gateway** – Wählen Sie diese Option, um Analysen für NetScaler Gateway anzuzeigen.

c. Der Ausdruck ist standardmäßig wahr.

d. Klicken Sie auf **OK**.

HINWEIS:

- Für Administratorpartitionen wird nur **Web Insight** unterstützt.
- Für virtuelle Server wie Cache-Umleitung, Authentifizierung und GSLB können Sie keine Analysen aktivieren. Eine Fehlermeldung wird angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Nachdem Sie auf **OK** geklickt haben, verarbeitet NetScaler Console die Aktivierung von Analysen auf den ausgewählten virtuellen Servern.

HINWEIS

NetScaler Console verwendet NetScaler SNIP für Logstream und NSIP für IPFIX. Wenn eine Firewall zwischen dem NetScaler-Agent und der NetScaler-Instanz aktiviert ist, stellen Sie sicher, dass Sie den folgenden Port öffnen, damit NetScaler Console den AppFlow-Datenverkehr erfassen kann:

TRANSPORTMODUS	QUELL-IP	TYP	PORT
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

Analysen bearbeiten

So bearbeiten Sie Analysen auf den virtuellen Servern:

1. Wählen Sie die virtuellen Server aus.

   HINWEIS:

   Alternativ können Sie Analysen auch für eine Instanz bearbeiten:

   a. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** und wählen Sie dann den Instanztyp aus. Zum Beispiel VPX.

   b. Wählen Sie die Instanz aus und klicken Sie auf **Sicherheit & Analysen bearbeiten**.

2. Klicken Sie auf **Sicherheit & Analysen bearbeiten**.
3. Bearbeiten Sie die Parameter, die Sie im Fenster **Analysekonfiguration bearbeiten** anwenden möchten.
4. Klicken Sie auf **OK**.

Analysen deaktivieren

So deaktivieren Sie Analysen auf den ausgewählten virtuellen Servern:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Wählen Sie die virtuellen Server aus.
2. Klicken Sie auf **Analysen deaktivieren**.

NetScaler Console deaktiviert die Analysen auf den ausgewählten virtuellen Servern.

Die folgende Tabelle beschreibt die Funktionen von NetScaler Console, die IPFIX und Logstream als Transportmodus unterstützen:

FUNKTION	IPFIX	LOGSTREAM
Web Insight	Unterstützt	Unterstützt
WAF-Sicherheitsverletzungen	Unterstützt	Unterstützt
Gateway Insight	Unterstützt	Unterstützt
HDX Insight	Unterstützt	Unterstützt
SSL Insight	Nicht unterstützt	Unterstützt
CR Insight	Unterstützt	Unterstützt
IP-Reputation	Unterstützt	Unterstützt
AppFirewall	Unterstützt	Unterstützt
Clientseitige Messung	Unterstützt	Unterstützt
Syslog/Auditlog	Unterstützt	Unterstützt

Globale Analysen konfigurieren

Sie können globale Analysen aktivieren, indem Sie entweder eine benutzerdefinierte Richtlinie oder eine globale Richtlinie erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEISE:

- Sie können nur bis zu 10 Richtlinien erstellen. Die Richtlinien können eine Kombination aus neun benutzerdefinierten Richtlinien und einer globalen Richtlinie oder 10 benutzerdefinierten Richtlinien sein.
- Wenn Sie sowohl benutzerdefinierte als auch globale Richtlinien haben, werden die in beiden Richtlinien ausgewählten Einblicke auf die virtuellen Server angewendet. Wenn Sie Einblicke entfernen möchten, müssen Sie diese manuell entfernen.

Benutzerdefinierte Richtlinie

Mithilfe einer benutzerdefinierten Richtlinie können Sie Instanzen oder virtuelle Server steuern, die nur bestimmte Einblicke erfordern. Möglicherweise haben Sie Hunderte von virtuellen Servern, die über verschiedene NetScaler-Instanzen konfiguriert sind, die in Ihrer NetScaler Console verwaltet werden. In einigen Szenarien möchten Sie möglicherweise selektive Einblicke (z. B. Bot-Sicherheitsverletzungen und WAF-Sicherheitsverletzungen) nur auf einige der virtuellen Server oder Instanzen anwenden. Für solche Szenarien können Sie eine benutzerdefinierte Richtlinie konfigurieren, bestimmte Analysefunktionen auswählen und diese auf die relevanten Instanzen und virtuellen Server anwenden.

So konfigurieren Sie eine benutzerdefinierte Richtlinie:

1. Klicken Sie unter **Global Analytics Summary** auf **Global Analytics Configuration**.

2. Wählen Sie unter **Policy details** die Option **Custom policy** aus und geben Sie einen Richtliniennamen Ihrer Wahl an.

   HINWEIS:

   Sie können den Richtliniennamen später nicht mehr bearbeiten.

3. Erstellen Sie unter **Define Conditions** Bedingungen, indem Sie den Satz von Instanz-IPs oder bestimmte Instanzen oder den Namen des virtuellen Servers oder beides auswählen.

4. Wählen Sie unter **Enable analytics** den Analysetyp aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Wenn Sie **Diese Analyseeinstellungen auf die nachfolgenden virtuellen Server anwenden** aktivieren, werden die Analysen auf die nachfolgenden virtuellen Server basierend auf den definierten Analysefunktionen angewendet.

5. Klicken Sie auf **Speichern**.

Hinweise:

- Wenn Sie die Richtlinie ändern, indem Sie einen vorhandenen Insight entfernen und einen anderen Insight hinzufügen, wird die aktualisierte Richtlinie mit dem neuen Insight angewendet. Wenn Sie einen Insight entfernen möchten, müssen Sie die bereits konfigurierten Insights manuell löschen.

  Angenommen, Sie haben eine benutzerdefinierte Richtlinie mit HDX Insight und Web Insight erstellt. Wenn Sie die Richtlinie aktualisieren, um HDX Insight zu entfernen und Bot Security Violations hinzuzufügen, werden die virtuellen Server/Instanzen mit HDX Insight, Web Insight und Bot Security Violations aktualisiert. Wenn Sie HDX Insight entfernen möchten, müssen Sie dies manuell über die Option Analysen bearbeiten tun.
- Dieselbe Logik gilt auch, wenn Sie eine vorhandene Richtlinie löschen und eine andere Richtlinie erstellen, indem Sie dieselben Instanzen oder virtuellen Server hinzufügen.

Globale Richtlinie

Mithilfe der globalen Richtlinie können Sie Analysen sowohl auf erkannten als auch auf nachfolgenden virtuellen Servern aktivieren. So erstellen Sie eine globale Richtlinie:

1. Klicken Sie unter **Globale Analyseübersicht** auf **Globale Analysekonsfiguration**.
2. Wählen Sie unter **Richtliniendetails** die Option **Globale Richtlinie** aus.
3. Wählen Sie unter **Analysen aktivieren** den Typ der Analysefunktion aus.

HINWEIS:

Wenn Sie **Diese Analyseeinstellungen auf die nachfolgenden virtuellen Server anwenden** aktivieren, werden die Analysen auf die nachfolgenden virtuellen Server basierend auf der definierten Kategorie angewendet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Klicken Sie auf **Speichern**.

Nach der Konfiguration ist die Analyse sowohl auf erkannten als auch auf nachfolgenden virtuellen Servern aktiviert.

Hinweise

- Angenommen, Sie haben die globale Richtlinie zum ersten Mal konfiguriert, indem Sie **Web Insight**, **HDX™ Insight** und **Gateway Insight** ausgewählt haben. Wenn Sie die Analyseeinstellungen später erneut ändern und **Gateway Insight** deaktivieren, wirken sich die Änderungen nicht auf die virtuellen Server aus, für die die Analyse bereits aktiviert ist. Sie müssen Gateway Insight manuell von den virtuellen Servern entfernen.
- Angenommen, Sie haben 10 virtuelle Server und zwei davon sind bereits mit der Option **Analyse konfigurieren** für die Analyse aktiviert. In diesem Szenario wird die Analyse, wenn Sie die globale Richtlinie konfigurieren, nur auf die verbleibenden acht virtuellen Server angewendet.
- Angenommen, Sie haben 10 virtuelle Server und Sie haben die Analyse für zwei virtuelle Server manuell deaktiviert. In diesem Szenario wird die Analyse, wenn Sie die globale Richtlinie konfigurieren, nur auf die verbleibenden acht virtuellen Server angewendet und überspringt die virtuellen Server, für die die Analyse manuell deaktiviert wurde.

Analyse migrieren

Ab Build **14.1-40.x** wird die Analyse, wenn Sie sie auf virtuellen Servern aktivieren, über eine profilbasierte Konfiguration angewendet. Zuvor wurde die Analyse über eine AppFlow-Richtlinie konfiguriert. Die profilbasierte Konfiguration bietet folgende Vorteile:

- Verbesserte Leistung und Flexibilität
- Einfachere Konfiguration und Verwaltung

HINWEIS:

Verbesserungen im Zusammenhang mit Analysekonsfigurationen werden nur über eine profilbasierte Konfiguration unterstützt. Wir empfehlen Ihnen, alle Ihre vorhandenen virtuellen Server, die für die Analyse aktiviert sind, auf eine profilbasierte Konfiguration zu migrieren.

1. Navigieren Sie zu **Einstellungen > Analysekonsfiguration** und wählen Sie dann **Analyse migrieren**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Auf der Seite **Analyse migrieren** können Sie Instanzen anzeigen, die einen oder mehrere virtuelle Server über die AppFlow®-Richtlinie konfiguriert haben.

   Ein Bestätigungsfenster wird angezeigt. Klicken Sie auf **Ja**, um die Migration abzuschließen.

Rollenbasierte Zugriffssteuerung konfigurieren

NetScaler Console bietet eine detaillierte, rollenbasierte Zugriffssteuerung (RBAC), mit der Sie Zugriffsberechtigungen basierend auf den Rollen einzelner Benutzer in Ihrem Unternehmen erteilen können.

In NetScaler Console werden alle Benutzer in Citrix Cloud hinzugefügt. Als erster Benutzer Ihrer Organisation müssen Sie zunächst ein Konto in Citrix Cloud erstellen und sich dann mit den Citrix Cloud-Anmeldeinformationen bei der NetScaler Console-GUI anmelden. Ihnen wird die Super-Admin-Rolle zugewiesen, und standardmäßig haben Sie alle Zugriffsberechtigungen in NetScaler Console. Später können Sie weitere Benutzer in Ihrer Organisation in Citrix Cloud erstellen.

Benutzer, die später erstellt werden und sich als reguläre Benutzer bei NetScaler Console anmelden, werden als delegierte Administratoren bezeichnet. Diese Benutzer haben standardmäßig alle Berechtigungen außer den Benutzerverwaltungsberechtigungen. Sie können jedoch spezifische Benutzerverwaltungsberechtigungen erteilen, indem Sie entsprechende Richtlinien erstellen und diese diesen delegierten Benutzern zuweisen. Die Benutzerverwaltungsberechtigungen finden Sie unter **Einstellungen** > **Benutzer & Rollen**.

Weitere Informationen zum Zuweisen spezifischer Berechtigungen finden Sie unter So weisen Sie delegierten Administratorbenutzern zusätzliche Berechtigungen zu.

Weitere Informationen zum Erstellen von Richtlinien, Rollen und Gruppen sowie zum Binden von Benutzern an Gruppen finden Sie in den folgenden Abschnitten.

Beispiel:

Das folgende Beispiel veranschaulicht, wie RBAC in NetScaler Console erreicht werden kann.

Chris, der NetScaler-Gruppenleiter, ist der Super-Administrator von NetScaler Console in seiner Organisation. Er erstellt drei Administratorrollen: Sicherheitsadministrator, Anwendungsadministrator und Netzwerkadministrator.

- David, der Sicherheitsadministrator, muss vollen Zugriff auf die SSL-Zertifikatsverwaltung und -überwachung haben, aber nur Lesezugriff auf Systemverwaltungsoperationen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Steve, ein Anwendungsadministrator, benötigt Zugriff auf nur bestimmte Anwendungen und nur bestimmte Konfigurationsvorlagen.
- Greg, ein Netzwerkadministrator, benötigt Zugriff auf die System- und Netzwerkverwaltung.
- Chris muss auch RBAC für alle Benutzer bereitstellen, unabhängig davon, ob sie lokal oder extern sind.

Die folgende Abbildung zeigt die Berechtigungen, die die Administratoren und andere Benutzer haben, sowie deren Rollen in der Organisation.

Um seinen Benutzern eine rollenbasierte Zugriffskontrolle zu ermöglichen, muss Chris die Benutzer zuerst in Citrix Cloud hinzufügen. Erst danach kann er die Benutzer in NetScaler Console sehen. Chris muss für jeden Benutzer, abhängig von dessen Rolle, Zugriffsrichtlinien erstellen. Zugriffsrichtlinien sind eng an Rollen gebunden. Daher muss Chris auch Rollen erstellen, und dann Gruppen erstellen, da Rollen nur Gruppen und nicht einzelnen Benutzern zugewiesen werden können.

Zugriff ist die Fähigkeit, eine bestimmte Aufgabe auszuführen, z. B. eine Datei anzuzeigen, zu erstellen, zu ändern oder zu löschen. Rollen werden entsprechend der Autorität und Verantwortung der Benutzer innerhalb des Unternehmens definiert. Beispielsweise darf ein Benutzer alle Netzwerkoperationen ausführen, während ein anderer Benutzer den Datenverkehr in Anwendungen beobachten und bei der Erstellung von Konfigurationsvorlagen helfen kann.

Richtlinien bestimmen die Benutzerrollen. Nach dem Erstellen von Richtlinien können Sie Rollen erstellen, jede Rolle an eine oder mehrere Richtlinien binden und Benutzern Rollen zuweisen. Sie können Rollen auch Benutzergruppen zuweisen. Eine Gruppe ist eine Sammlung von Benutzern, die gemeinsame Berechtigungen haben. Beispielsweise können Benutzer, die ein bestimmtes Rechenzentrum verwalten, einer Gruppe zugewiesen werden. Eine Rolle ist eine Identität, die Benutzern gewährt wird, indem sie basierend auf bestimmten Bedingungen zu bestimmten Gruppen hinzugefügt werden. In NetScaler Console sind das Erstellen von Rollen und Richtlinien spezifisch für die RBAC-Funktion in NetScaler. Rollen und Richtlinien können leicht erstellt, geändert oder eingestellt werden, wenn sich die Anforderungen des Unternehmens ändern, ohne dass die Berechtigungen für jeden Benutzer einzeln aktualisiert werden müssen.

Rollen können funktionsbasiert oder ressourcenbasiert sein. Betrachten Sie zum Beispiel einen SSL-/Sicherheitsadministrator und einen Anwendungsadministrator. Ein SSL-/Sicherheitsadministrator muss vollen Zugriff auf die SSL-Zertifikatsverwaltung und Überwachungsfunktionen haben, aber nur Lesezugriff für Systemadministrationsvorgänge. Anwendungsadministratoren können nur auf die Ressourcen in ihrem Bereich zugreifen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Führen Sie daher in Ihrer Rolle als Chris, dem Super-Admin, die folgenden Beispielaufgaben in NetScaler Console aus, um Zugriffsrichtlinien, Rollen und Benutzergruppen für David, den Sicherheitsadministrator in Ihrer Organisation, zu konfigurieren.

Benutzer in NetScaler Console konfigurieren

Als Super-Admin können Sie weitere Benutzer erstellen, indem Sie Konten für diese in Citrix Cloud und nicht in NetScaler Console konfigurieren. Wenn die neuen Benutzer zu NetScaler Console hinzugefügt werden, können Sie deren Berechtigungen nur definieren, indem Sie dem Benutzer die entsprechenden Gruppen zuweisen.

So fügen Sie neue Benutzer in Citrix Cloud™ hinzu:

1. Klicken Sie in der NetScaler Console-GUI oben links auf das Hamburger-Symbol und wählen Sie **Identity and Access Management**.

2. Wählen Sie auf der Seite „Identity and Access Management“ die Registerkarte **Administratoren** aus.

   Diese Registerkarte listet die in Citrix Cloud erstellten Benutzer auf.

3. Wählen Sie den Identitätsanbieter aus der Liste aus.

   - **Citrix Identity**: Geben Sie die E-Mail-Adresse des Benutzers ein, den Sie in NetScaler Console hinzufügen möchten, und klicken Sie auf **Einladen**.

     HINWEIS:

     Der Benutzer erhält eine E-Mail-Einladung von Citrix Cloud. Der Benutzer muss auf den in der E-Mail enthaltenen Link klicken, um den Registrierungsprozess durch Angabe seines vollständigen Namens und Passworts abzuschließen und sich später mit seinen Anmeldeinformationen bei NetScaler Console anzumelden.

   - **Azure Active Directory (AD)**: Diese Option wird nur angezeigt, wenn Ihr Azure AD mit Citrix Cloud verbunden ist. Siehe Azure Active Directory mit Citrix Cloud verbinden. Wenn Sie diese Option zum Einladen von Benutzern oder Gruppen auswählen, können Sie für den ausgewählten Benutzer oder die ausgewählte Gruppe nur **Benutzerdefinierten Zugriff** angeben. Die Benutzer können sich mit ihren Azure AD-Anmeldeinformationen bei NetScaler Console anmelden. Und Sie müssen keine Citrix Identity für die Benutzer

© 1997–2026 Citrix Systems, Inc. All rights reserved.

erstellen, die Teil des ausgewählten Azure AD sind. Wenn ein Benutzer der eingeladenen Gruppe hinzugefügt wird, müssen Sie keine Einladung für den neu hinzugefügten Benutzer senden. Dieser Benutzer kann mit den Azure AD-Anmeldeinformationen auf NetScaler Console zugreifen.

4. Wählen Sie **Benutzerdefinierten Zugriff** für den angegebenen Benutzer oder die Gruppe.
5. Wählen Sie **Application Delivery Management**.

   Diese Option listet die in NetScaler Console erstellten Benutzergruppen auf. Wählen Sie die Gruppe aus, der Sie den Benutzer hinzufügen möchten.

   |Citrix Identity|Azure AD| |-|-| |

   |

   | |Klicken Sie auf **Einladung senden**.|Klicken Sie auf **Admin-Gruppe hinzufügen**.|

Als Administrator sehen Sie den neuen Benutzer in der NetScaler Console Benutzerliste erst, nachdem sich der Benutzer bei NetScaler Console angemeldet hat.

So konfigurieren Sie Benutzer in NetScaler Console:

1. Navigieren Sie in der NetScaler Console-GUI zu **Einstellungen** > **Benutzer & Rollen** > **Benutzer**.
2. Der Benutzer wird auf der Seite **Benutzer** angezeigt.
3. Sie können die dem Benutzer gewährten Berechtigungen bearbeiten, indem Sie den Benutzer auswählen und auf **Bearbeiten** klicken. Sie können auch Gruppenberechtigungen auf der Seite **Gruppen** unter dem Knoten **Einstellungen** bearbeiten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Die Benutzer werden in NetScaler Console nur aus der Citrix Cloud hinzugefügt. Daher können Sie, selbst wenn Sie Administratorberechtigungen haben, keine Benutzer in der NetScaler Console-GUI hinzufügen oder löschen. Sie können nur die Gruppenberechtigungen bearbeiten. Benutzer können aus der Citrix Cloud hinzugefügt oder gelöscht werden.
- Die Benutzerdetails werden in der Dienst-GUI erst angezeigt, nachdem sich der Benutzer mindestens einmal bei NetScaler Console angemeldet hat.

Zugriffsrichtlinien in NetScaler Console konfigurieren

Zugriffsrichtlinien definieren Berechtigungen. Eine Richtlinie kann auf eine Benutzergruppe oder auf mehrere Gruppen angewendet werden, indem Rollen erstellt werden. Richtlinien bestimmen die Benutzerrollen. Nach dem Erstellen von Richtlinien müssen Sie Rollen erstellen, jede Rolle an eine oder mehrere Richtlinien binden und Rollen Benutzergruppen zuweisen. NetScaler Console bietet fünf vordefinierte Zugriffsrichtlinien:

- **admin_policy**. Gewährt Zugriff auf alle NetScaler Console-Knoten. Der Benutzer hat sowohl Anzeige- als auch Bearbeitungsberechtigungen, kann alle NetScaler Console-Inhalte anzeigen und alle Bearbeitungsvorgänge ausführen. Das heißt, der Benutzer kann Ressourcen hinzufügen, ändern und löschen.
- **adminExceptSystem_policy**. Gewährt Benutzern Zugriff auf alle Knoten in der NetScaler Console-GUI, mit Ausnahme des Zugriffs auf den Knoten Einstellungen.
- **readonly_policy**. Gewährt schreibgeschützte Berechtigungen. Der Benutzer kann alle Inhalte in NetScaler Console anzeigen, ist aber nicht berechtigt, Vorgänge auszuführen.
- **appadmin_policy**. Gewährt administrative Berechtigungen für den Zugriff auf die Anwendungsfunktionen in NetScaler Console. Ein Benutzer, der an diese Richtlinie gebunden ist, kann:
  - Benutzerdefinierte Anwendungen hinzufügen, ändern und löschen
  - Dienste, Dienstgruppen und die verschiedenen virtuellen Server aktivieren oder deaktivieren, z. B. Content Switching und Cache-Umleitung
- **appreadonly_policy**. Gewährt schreibgeschützte Berechtigungen für Anwendungsfunktionen. Ein Benutzer, der an diese Richtlinie gebunden ist, kann die Anwendungen anzeigen, aber keine Hinzufüge-, Änderungs-, Lösch-, Aktivierungs- oder Deaktivierungsvorgänge ausführen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Obwohl Sie diese vordefinierten Richtlinien nicht bearbeiten können, können Sie Ihre eigenen (benutzerdefinierten) Richtlinien erstellen.

Früher, als Sie Richtlinien Rollen zugewiesen und die Rollen an Benutzergruppen gebunden haben, konnten Sie Berechtigungen für die Benutzergruppen auf Knotenebene in der NetScaler Console GUI bereitstellen. Sie konnten beispielsweise nur Zugriffsrechte für den gesamten Knoten **Load Balancing** bereitstellen. Ihre Benutzer hatten die Berechtigung, auf alle entitätsspezifischen Unterknoten unter **Load Balancing** zuzugreifen (z. B. virtuelle Server, Dienste und andere), oder sie hatten keine Berechtigung, auf einen Knoten unter **Load Balancing** zuzugreifen.

In NetScaler Console 507.x Build und späteren Versionen wurde die Zugriffsrichtlinienverwaltung erweitert, um auch Berechtigungen für Unterknoten bereitzustellen. Zugriffsrichtlinieneinstellungen können für alle Unterknoten wie virtuelle Server, Dienste, Dienstgruppen und Server konfiguriert werden.

Derzeit können Sie eine derart granulare Zugriffsberechtigung nur für Unterknoten unter einem **Load Balancing**-Knoten und auch für Unterknoten unter dem **GSLB**-Knoten bereitstellen.

Als Administrator möchten Sie dem Benutzer beispielsweise nur die Berechtigung zum Anzeigen virtueller Server erteilen, nicht aber für die Backend-Dienste, Dienstgruppen und Anwendungsserver im Knoten **Load Balancing**. Benutzer, denen eine solche Richtlinie zugewiesen ist, können nur auf die virtuellen Server zugreifen.

So erstellen Sie benutzerdefinierte Zugriffsrichtlinien:

1. Navigieren Sie in der NetScaler Console GUI zu **Einstellungen** > **Benutzer & Rollen** > **Zugriffsrichtlinien**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Seite **Zugriffsrichtlinien erstellen** im Feld **Richtlinienname** den Namen der Richtlinie und im Feld **Richtlinienbeschreibung** die Beschreibung ein.

   Der Abschnitt **Berechtigungen** listet alle NetScaler Console-Funktionen mit Optionen zum Angeben von schreibgeschütztem, Aktivieren/Deaktivieren- oder Bearbeitungszugriff auf.

   a. Klicken Sie auf das (+) Symbol, um jede Funktionsgruppe zu erweiternieren.
   b. Aktivieren Sie das Kontrollkästchen für die Berechtigung neben dem Funktionsnamen, um Benutzern die Berechtigung zu erteilen.

      - **Anzeigen:** Diese Option ermöglicht es dem Benutzer, die Funktion in NetScaler Console anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Aktivieren-Deaktivieren:** Diese Option ist nur für die Funktionen unter **Netzwerkfunktionen** verfügbar, die eine Aktivierungs- oder Deaktivierungsaktion in NetScaler Console zulassen. Der Benutzer kann die Funktion aktivieren oder deaktivieren. Der Benutzer kann auch die Aktion **Jetzt abfragen** ausführen.

  Wenn Sie einem Benutzer die Berechtigung **Aktivieren-Deaktivieren** erteilen, wird auch die Berechtigung **Anzeigen** erteilt. Sie können diese Option nicht abwählen.

- **Edit:** Diese Option gewährt dem Benutzer vollen Zugriff. Der Benutzer kann die Funktion und ihre Eigenschaften ändern.

  Wenn Sie die Berechtigung **Edit** erteilen, werden sowohl die Berechtigungen **View** als auch **Enable-Disable** erteilt. Sie können die automatisch ausgewählten Optionen nicht abwählen.

Wenn Sie das Kontrollkästchen für die Funktion aktivieren, werden alle Berechtigungen für die Funktion ausgewählt.

HINWEIS:

erweitern **Load Balancing** und **GSLB**, um weitere Konfigurationsoptionen anzuzeigen.

In der folgenden Abbildung haben die Konfigurationsoptionen der Funktion Load Balancing unterschiedliche Berechtigungen:

Richtlinie konfigurieren(/en-us/netscaler-console-service/media/service-rbac-configure-policies-2.png)

Die Berechtigung **View** wird einem Benutzer für die Funktion **Virtual Servers** erteilt. Der Benutzer kann die virtuellen Load-Balancing-Server in NetScaler Console anzeigen. Um virtuelle Server anzuzeigen, navigieren Sie zu **Infrastructure > Network Functions > Load Balancing** und wählen Sie die Registerkarte **Virtual Servers**.

Die Berechtigung **Enable-Disable** wird einem Benutzer für die Funktion **Services** erteilt. Diese Berechtigung erteilt auch die Berechtigung **View**. Der Benutzer kann die an einen virtuellen Load-Balancing-Server gebundenen Dienste aktivieren oder deaktivieren. Außerdem kann der Benutzer die Aktion **Poll Now** für Dienste ausführen. Um Dienste zu aktivieren oder zu deaktivieren, navigieren Sie zu **Infrastructure > Network Functions > Load Balancing** und wählen Sie die Registerkarte **Services**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Wenn ein Benutzer die Berechtigung **Enable-Disable** besitzt, ist die Aktivierungs- oder Deaktivierungsaktion für einen Dienst auf der folgenden Seite eingeschränkt:

a. Navigieren Sie zu **Infrastructure > Network Functions**.

b. Wählen Sie einen virtuellen Server aus und klicken Sie auf **Configure**.

c. Wählen Sie die **Load Balancing Virtual Server Service Binding**-Seite. Diese Seite zeigt eine Fehlermeldung an, wenn Sie **Enable** oder **Disable** auswählen.

Die Berechtigung **Edit** wird einem Benutzer für die Funktion **Service Groups** erteilt. Diese Berechtigung gewährt vollen Zugriff, wobei die Berechtigungen **View** und **Enable-Disable** erteilt werden. Der Benutzer kann die Dienstgruppen ändern, die an einen virtuellen Load-Balancing-Server gebunden sind. Um Dienstgruppen zu bearbeiten, navigieren Sie zu **Infrastructure > Network Functions > Load Balancing** und wählen Sie die Registerkarte **Service Groups**.

4. Klicken Sie auf **Erstellen**.

HINWEIS:

Das Auswählen von **Bearbeiten** kann intern abhängige Berechtigungen zuweisen, die im Abschnitt „Berechtigungen“ nicht als aktiviert angezeigt werden. Wenn Sie beispielsweise Bearbeitungsberechtigungen für die Fehlerverwaltung aktivieren, stellt NetScaler Console intern die Berechtigung zum Konfigurieren eines E-Mail-Profils oder zum Erstellen von SMTP-Server-Setups bereit, damit der Benutzer den Bericht als E-Mail senden kann.

StyleBook-Berechtigungen für Benutzer erteilen

Sie können eine Zugriffsrichtlinie erstellen, um StyleBook-Berechtigungen wie Importieren, Löschen, Herunterladen und mehr zu erteilen.

HINWEIS:

Die Anzeigeberechtigung wird automatisch aktiviert, wenn Sie andere StyleBook-Berechtigungen erteilen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Rollen in NetScaler Console konfigurieren

In NetScaler Console ist jede Rolle an eine oder mehrere Zugriffsrichtlinien gebunden. Sie können Eins-zu-Eins-, Eins-zu-Viele- und Viele-zu-Viele-Beziehungen zwischen Richtlinien und Rollen definieren. Sie können eine Rolle an mehrere Richtlinien binden und mehrere Rollen an eine Richtlinie binden.

Beispielsweise kann eine Rolle an zwei Richtlinien gebunden sein, wobei eine Richtlinie Zugriffsrechte für eine Funktion und die andere Richtlinie Zugriffsrechte für eine andere Funktion definiert. Eine Richtlinie könnte die Berechtigung zum Hinzufügen von NetScaler-Instanzen in NetScaler Console erteilen, und die andere Richtlinie könnte die Berechtigung zum Erstellen und Bereitstellen eines StyleBooks sowie zum Konfigurieren von NetScaler-Instanzen erteilen.

Wenn mehrere Richtlinien die Bearbeitungs- und schreibgeschützten Berechtigungen für eine einzelne Funktion definieren, haben die Bearbeitungsberechtigungen Vorrang vor den schreibgeschützten Berechtigungen.

NetScaler Console bietet fünf vordefinierte Rollen:

- **admin_role**. Hat Zugriff auf alle NetScaler Console-Funktionen. (Diese Rolle ist an `adminpolicy` gebunden.)
- **adminExceptSystem_role**. Hat Zugriff auf die NetScaler Console-GUI, mit Ausnahme der Berechtigungen für Einstellungen. (Diese Rolle ist an adminExceptSystem_policy gebunden.)
- **readonly_role**. Hat schreibgeschützten Zugriff. (Diese Rolle ist an `readonlypolicy` gebunden.)
- **appAdmin_role**. Hat administrativen Zugriff nur auf die Anwendungsfunktionen in NetScaler Console. (Diese Rolle ist an appAdminPolicy gebunden).
- **appReadonly_role**. Hat schreibgeschützten Zugriff auf die Anwendungsfunktionen. (Diese Rolle ist an appReadOnlyPolicy gebunden.)

Obwohl Sie die vordefinierten Rollen nicht bearbeiten können, können Sie Ihre eigenen (benutzerdefinierten) Rollen erstellen.

So erstellen Sie Rollen und weisen ihnen Richtlinien zu:

1. Navigieren Sie in der NetScaler Console-GUI zu **Settings** > **Users & Roles** > **Roles**.
2. Klicken Sie auf **Add**.
3. Geben Sie auf der Seite **Create Roles** im Feld **Role Name** den Namen der Rolle ein und geben Sie die Beschreibung im Feld **Role Description** an (optional).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Fügen Sie im Abschnitt **Policies** eine oder mehrere Richtlinien zur Liste **Configured** hinzu.

   HINWEIS:

   Die Richtlinien sind mit einer Mandanten-ID (z. B. `maasdocfour`) versehen, die für alle Mandanten eindeutig ist.

   HINWEIS:

   Sie können eine Zugriffsrichtlinie erstellen, indem Sie auf **New** klicken, oder Sie können zu **Settings** > **Users & Roles** > **Access Policies** navigieren und Richtlinien erstellen.

5. Klicken Sie auf **Create**.

Gruppen in NetScaler Console konfigurieren

In NetScaler Console kann eine Gruppe sowohl Feature- als auch Ressourcenzugriff haben. Zum Beispiel könnte eine Benutzergruppe nur Zugriff auf ausgewählte NetScaler-Instanzen haben; eine andere Gruppe nur auf einige ausgewählte Anwendungen und so weiter.

Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, der Gruppe Zugriff auf Anwendungsebene gewähren und Benutzer der Gruppe zuweisen. Alle Benutzer in dieser Gruppe erhalten in NetScaler Console dieselben Zugriffsrechte.

Sie können den Benutzerzugriff in NetScaler Console auf individueller Ebene von Netzwerkfunktionseinheiten verwalten. Sie können dem Benutzer oder der Gruppe auf Entitätsebene dynamisch spezifische Berechtigungen zuweisen.

NetScaler Console behandelt virtuelle Server, Dienste, Dienstgruppen und Server als Netzwerkfunktionseinheiten.

- **Virtueller Server (Anwendungen)** – Lastenausgleich (`lb`), GSLB, Kontextwechsel (`CS`), Cache-Umleitung (`CR`), Authentifizierung (`Auth`) und NetScaler Gateway (`vpn`)
- **Dienste** – Lastenausgleichs- und GSLB-Dienste
- **Dienstgruppe** – Lastenausgleichs- und GSLB-Dienstgruppen
- **Server** – Lastenausgleichs-Server

So erstellen Sie eine Gruppe:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie in NetScaler Console zu **Settings** > **Users & Roles** > **Groups**.
2. Klicken Sie auf **Add**.

   Die Seite **Create System Group** wird angezeigt.
3. Geben Sie im Feld **Group Name** den Namen der Gruppe ein.
4. Geben Sie im Feld **Group Description** eine Beschreibung Ihrer Gruppe ein. Eine gute Beschreibung hilft Ihnen, die Rolle und Funktion der Gruppe zu verstehen.
5. Verschieben Sie im Abschnitt **Roles** eine oder mehrere Rollen in die Liste **Configured**.

   HINWEIS:

   Die Rollen sind mit einer Mandanten-ID (zum Beispiel `maasdocfour`) vorangestellt, die für alle Mandanten eindeutig ist.
6. In der Liste **Verfügbar** können Sie auf **Neu** oder **Bearbeiten** klicken und Rollen erstellen oder ändern.

   Alternativ können Sie zu **Einstellungen > Benutzer & Rollen > Benutzer** navigieren und Benutzer erstellen oder ändern.

7. Klicken Sie auf **Weiter**.
8. Auf der Registerkarte **Autorisierungseinstellungen** können Sie Ressourcen aus den folgenden Kategorien auswählen:

   - **Autoscale™-Gruppen**
   - **Instanzen**
   - **Anwendungen**
   - **Konfigurationsvorlagen**
   - **IPAM-Anbieter und -Netzwerke**
   - **StyleBooks**
   - **Konfigurationspakete**
   - **Domänennamen**

   Wählen Sie bestimmte Ressourcen aus den Kategorien aus, auf die Benutzer zugreifen können.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Autoscale-Gruppen:

So wählen Sie die spezifischen Autoscale-Gruppen aus, die ein Benutzer anzeigen oder verwalten kann:

a. Deaktivieren Sie das Kontrollkästchen **Alle AutoScale-Gruppen** und klicken Sie auf **AutoScale-Gruppen hinzufügen**.
b. Wählen Sie die erforderlichen Autoscale-Gruppen aus der Liste aus und klicken Sie auf **OK**.

Instanzen:

So wählen Sie die spezifischen Instanzen aus, die ein Benutzer anzeigen oder verwalten kann:

a. Deaktivieren Sie das Kontrollkästchen **Alle Instanzen** und klicken Sie auf **Instanzen auswählen**.
b. Wählen Sie die erforderlichen Instanzen aus der Liste aus und klicken Sie auf **OK**.

Tags:

So autorisieren Sie Benutzer, bestimmte Instanzen basierend auf zugehörigen Tags anzuzeigen oder zu verwalten:

a. Deaktivieren Sie das Kontrollkästchen **Alle Instanzen** und klicken Sie auf **Tags auswählen**.
b. Wählen Sie die erforderlichen Tags aus der Liste aus und klicken Sie auf **OK**.

Wenn Sie später weitere Instanzen mit den ausgewählten Tags verknüpfen, erhalten die autorisierten Benutzer automatisch Zugriff auf die neuen Instanzen.

Weitere Informationen zu Tags und zum Verknüpfen von Tags mit Instanzen finden Sie unter So erstellen Sie Tags und weisen sie Instanzen zu.

Anwendungen:

Die Liste **Anwendungen auswählen** ermöglicht es Ihnen, einem Benutzer Zugriff auf die erforderlichen Anwendungen zu gewähren.

Sie können Anwendungen Zugriff gewähren, ohne deren Instanzen auszuwählen. Denn Anwendungen sind unabhängig von ihren Instanzen, um Benutzerzugriff zu gewähren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wenn Sie einem Benutzer Zugriff auf eine Anwendung gewähren, ist der Benutzer nur zum Zugriff auf diese Anwendung berechtigt, unabhängig von der Instanzauswahl.

Diese Liste bietet Ihnen die folgenden Optionen:

- **Alle Anwendungen:** Diese Option ist standardmäßig ausgewählt. Sie fügt alle Anwendungen hinzu, die in der NetScaler Console vorhanden sind.
- **Alle Anwendungen ausgewählter Instanzen:** Diese Option wird nur angezeigt, wenn Sie Instanzen aus der Kategorie **Alle Instanzen** auswählen. Sie fügt alle Anwendungen hinzu, die auf der ausgewählten Instanz vorhanden sind.
- **Spezifische Anwendungen:** Diese Option ermöglicht es Ihnen, die erforderlichen Anwendungen hinzuzufügen, auf die Benutzer zugreifen sollen. Klicken Sie auf **Anwendungen hinzufügen** und wählen Sie die erforderlichen Anwendungen aus der Liste aus.
- **Einzelnen Entitätstyp auswählen:** Diese Option ermöglicht es Ihnen, den spezifischen Typ der Netzwerkfunktionsentität und die entsprechenden Entitäten auszuwählen.

  Sie können entweder einzelne Entitäten hinzufügen oder alle Entitäten unter dem erforderlichen Entitätstyp auswählen, um einem Benutzer Zugriff zu gewähren.

  Die Option **Auch auf gebundene Entitäten anwenden** autorisiert die Entitäten, die an den ausgewählten Entitätstyp gebunden sind. Wenn Sie beispielsweise eine Anwendung auswählen und **Auch auf gebundene Entitäten anwenden** auswählen, autorisiert NetScaler Console alle Entitäten, die an die ausgewählte Anwendung gebunden sind.

  HINWEIS:

  Stellen Sie sicher, dass Sie nur einen Entitätstyp ausgewählt haben, wenn Sie gebundene Entitäten autorisieren möchten.

Sie können reguläre Ausdrücke verwenden, um die Netzwerkfunktionsentitäten zu suchen und hinzuzufügen, die die Regex-Kriterien für die Gruppen erfüllen. Der angegebene Regex-Ausdruck wird in NetScaler Console beibehalten. Um einen regulären Ausdruck hinzuzufügen, führen Sie die folgenden Schritte aus:

a. Klicken Sie auf **Regulären Ausdruck hinzufügen**.
b. Geben Sie den regulären Ausdruck in das Textfeld ein.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die folgende Abbildung erklärt, wie man einen regulären Ausdruck verwendet, um eine Anwendung hinzuzufügen, wenn Sie die Option **Spezifische Anwendungen** auswählen:

Die folgende Abbildung erklärt, wie man einen regulären Ausdruck verwendet, um Netzwerkfunktionsentitäten hinzuzufügen, wenn Sie die Option **Individuellen Entitätstyp auswählen** wählen:

Wenn Sie weitere reguläre Ausdrücke hinzufügen möchten, klicken Sie auf das **+**-Symbol.

HINWEIS:

Der reguläre Ausdruck stimmt nur mit dem Servernamen für den Entitätstyp **Server** überein und nicht mit der Server-IP-Adresse.

Wenn Sie die Option **Auch auf gebundene Entitäten anwenden** für eine erkannte Entität auswählen, kann ein Benutzer automatisch auf die Entitäten zugreifen, die an die erkannte Entität gebunden sind.

Der reguläre Ausdruck wird im System gespeichert, um den Autorisierungsbereich zu aktualisieren. Wenn die neuen Entitäten dem regulären Ausdruck ihres Entitätstyps entsprechen, aktualisiert NetScaler Console den Autorisierungsbereich auf die neuen Entitäten.

Konfigurationsvorlagen:

Wenn Sie die spezifische Konfigurationsvorlage auswählen möchten, die ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

a. Deaktivieren Sie **Alle Konfigurationsvorlagen** und klicken Sie auf **Konfigurationsvorlage hinzufügen**.
b. Wählen Sie die gewünschte Vorlage aus der Liste aus und klicken Sie auf **OK**.

IPAM-Anbieter und -Netzwerke:

Wenn Sie die spezifischen IPAM-Anbieter und -Netzwerke hinzufügen möchten, die ein Benutzer anzeigen oder verwalten kann, führen Sie Folgendes aus:

- **Anbieter hinzufügen** – Deaktivieren Sie **Alle Anbieter** und klicken Sie auf **Anbieter hinzufügen**. Sie können die erforderlichen Anbieter auswählen und auf **OK** klicken.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Netzwerke hinzufügen** – Deaktivieren Sie **Alle Netzwerke** und klicken Sie auf **Netzwerke hinzufügen**. Sie können die erforderlichen Netzwerke auswählen und auf **OK** klicken.

StyleBooks:

Wenn Sie das spezifische StyleBook auswählen möchten, das ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

a. Deaktivieren Sie das Kontrollkästchen **Alle StyleBooks** und klicken Sie auf **StyleBook zur Gruppe hinzufügen**. Sie können entweder einzelne StyleBooks auswählen oder eine Filterabfrage angeben, um StyleBooks zu autorisieren.

   Wenn Sie die einzelnen StyleBooks auswählen möchten, wählen Sie die StyleBooks im Bereich **Einzelne StyleBooks** aus und klicken Sie auf **Auswahl speichern**.

   Wenn Sie eine Abfrage zum Suchen von StyleBooks verwenden möchten, wählen Sie den Bereich **Benutzerdefinierte Filter** aus. Eine Abfrage ist eine Zeichenfolge von Schlüssel-Wert-Paaren, wobei die Schlüssel `name`, `namespace` und `version` sind.

   Sie können auch reguläre Ausdrücke als Werte verwenden, um StyleBooks zu suchen und hinzuzufügen, die die Regex-Kriterien für die Gruppen erfüllen. Eine benutzerdefinierte Filterabfrage zum Suchen von StyleBooks unterstützt sowohl die Operation `And` als auch `Or`.

   Beispiel:

   ```
   name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
   version=1.0
   ```

   Diese Abfrage listet die StyleBooks auf, die die folgenden Bedingungen erfüllen:

   - Der StyleBook-Name ist entweder `lb-mon` oder `lb`.
   - StyleBook-Namespace ist `com.citrix.adc.stylebooks`.
   - StyleBook-Version ist `1.0`.

   Verwenden Sie eine `Or` Operation zwischen Wertausdrücken, die für den Schlüssel-Ausdruck definiert ist.

   Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die `name=lb-mon|lb` Abfrage ist gültig. Sie gibt die StyleBooks zurück, die entweder den Namen `lb-mon` oder `lb` haben.
- Die `name=lb-mon | version=1.0` Abfrage ist ungültig.

Drücken Sie `Enter`, um die Suchergebnisse anzuzeigen, und klicken Sie auf **Abfrage speichern**.

Benutzerdefinierte Filter(/en-us/netscaler-console-service/media/custom-filter-query.gif)

Die gespeicherte Abfrage wird in der **Benutzerdefinierten Filterabfrage** angezeigt. Basierend auf der gespeicherten Abfrage gewährt die NetScaler Console den Benutzern Zugriff auf diese StyleBooks.

b. Wählen Sie die erforderlichen StyleBooks aus der Liste aus und klicken Sie auf **OK**.

Sie können die erforderlichen StyleBooks auswählen, wenn Sie Gruppen erstellen und Benutzer zu dieser Gruppe hinzufügen. Wenn Ihr Benutzer das zulässige StyleBook auswählt, werden auch alle abhängigen StyleBooks ausgewählt.

Konfigurationspakete:

Wählen Sie in den Konfigurationspaketen eine der folgenden Optionen aus:

- **Alle Konfigurationen**: Diese Option ist standardmäßig ausgewählt. Sie ermöglicht Benutzern, alle Konfigurationen in ADM zu verwalten.
- **Alle Konfigurationen der ausgewählten StyleBooks**: Diese Option fügt alle Konfigurationspakete des ausgewählten StyleBooks hinzu.
- **Spezifische Konfigurationen**: Diese Option ermöglicht es Ihnen, spezifische Konfigurationen eines beliebigen StyleBooks hinzuzufügen.
- **Alle vom Benutzergruppe erstellten Konfigurationen**: Diese Option ermöglicht Benutzern den Zugriff auf Konfigurationen, die nur von Benutzern derselben Gruppe erstellt wurden.

Sie können die anwendbaren Konfigurationspakete auswählen, wenn Sie Gruppen erstellen und Benutzer dieser Gruppe zuweisen.

Domänennamen:

Wenn Sie den spezifischen Domänennamen auswählen möchten, den ein Benutzer anzeigen oder verwalten kann, führen Sie die folgenden Schritte aus:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Deaktivieren Sie das Kontrollkästchen **Alle Domänennamen** und klicken Sie auf **Domänennamen hinzufügen**.

b. Wählen Sie die erforderlichen Domänennamen aus der Liste aus und klicken Sie auf **OK**.

c. Klicken Sie auf **Gruppe erstellen**.

d. Wählen Sie im Abschnitt **Benutzer zuweisen** den Benutzer in der Liste **Verfügbar** aus und fügen Sie den Benutzer der Liste **Konfiguriert** hinzu.

HINWEIS:

Sie können auch neue Benutzer hinzufügen, indem Sie auf **Neu** klicken.

a. Klicken Sie auf **Fertig stellen**.

Wie sich der Benutzerzugriff basierend auf dem Autorisierungsbereich ändert

Wenn ein Administrator einen Benutzer zu einer Gruppe hinzufügt, die unterschiedliche Zugriffsrichtlinieneinstellungen hat, wird der Benutzer mehreren Autorisierungsbereichen und Zugriffsrichtlinien zugeordnet.

In diesem Fall gewährt die NetScaler Console dem Benutzer Zugriff auf Anwendungen, abhängig vom spezifischen Autorisierungsbereich.

Betrachten Sie einen Benutzer, der einer Gruppe zugewiesen ist, die zwei Richtlinien (Policy-1 und Policy-2) hat.

- **Policy-1** – Nur-Lese-Berechtigung für Anwendungen.
- **Policy-2** – Lese- und Schreibberechtigung für Anwendungen.

Der Benutzer kann die in Policy-1 angegebenen Anwendungen anzeigen. Außerdem kann dieser Benutzer die in Policy-2 angegebenen Anwendungen anzeigen und bearbeiten. Der Bearbeitungszugriff auf Group-1-Anwendungen ist eingeschränkt, da er nicht unter den Autorisierungsbereich von Group-1 fällt.

Einschränkungen

Die folgenden NetScaler Console-Funktionen unterstützen RBAC nicht vollständig:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Analytics** – Die Analysemodule unterstützen RBAC nicht vollständig. Die RBAC-Unterstützung ist auf Instanzebene beschränkt und nicht auf Anwendungsebene in den Analysemodulen Gateway Insight, HDX™ Insight und Security Insight anwendbar.
  - Beispiel 1: Instanzbasiertes RBAC (unterstützt). Ein Administrator, dem einige Instanzen zugewiesen wurden, kann nur diese Instanzen unter **HDX Insight** > **Devices** und nur die entsprechenden virtuellen Server unter **HDX Insight** > **Applications** sehen, da RBAC auf Instanzebene unterstützt wird.
  - Beispiel 2: Anwendungsbasiertes RBAC (nicht unterstützt). Ein Administrator, dem einige Anwendungen zugewiesen wurden, kann alle virtuellen Server unter **HDX Insight** > **Applications** sehen, aber nicht darauf zugreifen, da RBAC auf Anwendungsebene nicht unterstützt wird.
- **StyleBooks** – RBAC wird für StyleBooks nicht vollständig unterstützt.
  - Stellen Sie sich eine Situation vor, in der viele Benutzer Zugriff auf ein einzelnes StyleBook haben, aber Zugriffsberechtigungen für verschiedene NetScaler-Instanzen besitzen. Benutzer können Konfigurationspakete auf ihren eigenen Instanzen erstellen und aktualisieren, da sie keinen Zugriff auf andere Instanzen als ihre eigenen haben. Sie können jedoch weiterhin die Konfigurationspakete und Objekte anzeigen, die auf anderen NetScaler-Instanzen als ihren eigenen erstellt wurden.

Netzwerkprofil für die verwaltete NetScaler-Instanz zuweisen

Wenn Sie Analysen oder Metrik-Collector für die virtuellen Server in NetScaler Console aktivieren, werden die AppFlow- oder Metrikdaten vom NetScaler über die NetScaler-Subnetz-IP-Adresse (SNIP) an NetScaler Console exportiert. In einigen Szenarien kann die SNIP aufgrund der Firewall im Netzwerk blockiert sein. In solchen Szenarien müssen Sie möglicherweise eine andere IP-Adresse verwenden. Weitere Informationen zum Netzwerkprofil finden Sie unter (/de-de/citrix-adc/current-release/load-balancing/load-balancing-manage-clienttraffic/use-specified-srcip.html).

Sie können einer NetScaler-Instanz über NetScaler Console ein Netzwerkprofil zuweisen, um AppFlow-Daten von NetScaler an NetScaler Console zu exportieren.

Voraussetzungen

Stellen Sie sicher, dass:

- Die NetScaler-Instanzversion **13.0-48.4 oder höher** ist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Das Netzwerkprofil in den NetScaler-Instanzen konfiguriert ist.

So weisen Sie ein Netzwerkprofil in NetScaler Console zu:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**.
2. Wählen Sie die Instanz aus und aus der Liste **Aktion auswählen**:
    - Klicken Sie auf **Netzwerkprofile konfigurieren**, um ein Netzwerkprofil für AppFlow zuzuweisen.
    - Klicken Sie auf **Netzwerkprofile für Metrik-Collector konfigurieren**, um ein Netzwerkprofil für den Metrik-Collector zuzuweisen.
3. Wählen Sie ein Netzwerkprofil aus der Liste aus und klicken Sie auf **Anwenden**.

HINWEIS:

- Stellen Sie für AppFlow sicher, dass Sie die Analysen für alle virtuellen Server deaktivieren, bevor Sie ein Netzwerkprofil für die Instanz zuweisen.
- Für den Metrics Collector stellen Sie sicher, dass Sie Metriken für alle virtuellen Server deaktivieren, bevor Sie ein Netzprofil für die Instanz zuweisen.

Verwaltung des Datenspeichers

Es ist wichtig zu wissen, welche Funktionen in NetScaler Console verwendet werden und wie die Datennutzung jeder dieser Funktionen ist. Das Dashboard **Daten-Speicherverwaltung** dient diesem Zweck und fungiert als Visualisierungstool, mit dem Sie den gesamten in der NetScaler Console-Datenbank gespeicherten Datenbestand über verschiedene Funktionen hinweg verstehen können. Das Dashboard zeigt auch an, ob der verbrauchte Speicherplatz innerhalb der angegebenen Grenzen liegt oder ob er den zugewiesenen Speicherplatz überschreitet.

Als Administrator können Sie die folgenden Aufgaben im Dashboard **Daten-Speicherverwaltung** ausführen:

- Anzeigen des Datenspeicherverbrauchs der letzten 30 Tage – Datenspeichertrends werden in der NetScaler Console-Datenbank für die letzten 30 Tage gespeichert. Diese Trends sind in grafischer oder tabellarischer Form verfügbar. Diese Trends zeigen, wie viele Daten eingegangen sind und wie viele Daten nach den geplanten Bereinigungszyklen in NetScaler Console gespeichert werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Anzeigen des Datenerfassungsstatus – Die Datenerfassungsaktivität findet statt, solange der verbrauchte Speicherplatz innerhalb der Grenzen des zugewiesenen Speichers liegt. Wenn der verbrauchte Speicherplatz den zugewiesenen Speicherplatz überschreitet, wird die Datenaktivität angehalten.
- Benachrichtigungen senden – Sie können Benachrichtigungen einrichten, die gesendet werden, wenn der verbrauchte Speicherplatz 75 % oder 100 % des zugewiesenen Speichers erreicht, sodass Benutzer ihren Speicher verwalten können.
- Flexibilität bei der Verwaltung des Datenspeicherplatzes – Sie können mehr Platz innerhalb der gespeicherten Daten schaffen, indem Sie Daten bereinigen, die Sie für die Entfernung oder Reduzierung geeignet halten.

Navigieren Sie zu **Einstellungen > Datenspeicher**, um Ihr Datenspeicher-Dashboard anzuzeigen.

Die folgenden Abschnitte beschreiben, wie Sie das Dashboard **Daten-Speicherverwaltung** für eine effektive Datenspeicherverwaltung verwenden:

- Ihren Datenspeicher verstehen – Dieser Abschnitt hilft Ihnen zu verstehen, wie Sie das Dashboard verwenden können, um Informationen zu Ihrem Datenspeicher anzuzeigen.
- Ihren Datenspeicher verwalten – Dieser Abschnitt enthält Informationen darüber, welche Aktionen Sie im Dashboard ausführen können, um Ihren Datenspeicher zu verwalten.

Ihren Datenspeicher verstehen

Sie können das Dashboard **Daten-Speicherverwaltung** in NetScaler Console verwenden, um Daten und Diagramme anzuzeigen, die Ihnen helfen, Ihre Datenspeicherplatznutzung zu verfolgen.

Um Ihre Datenspeicherplatznutzung zu überwachen, navigieren Sie zu **Einstellungen > Datenspeicher**.

Das Dashboard für die Datenspeicherverwaltung zeigt die folgenden Informationen an:

- Status Ihrer Datenerfassungsaktivität
- Gesamtspeicherverbrauch
- Status der Datenbereinigung
- Trends beim Speicherverbrauch
- Speicherverbrauch nach Funktionen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Status Ihrer Datenerfassungsaktivität

Datenerfassung bezieht sich auf den Prozess des Imports großer und vielfältiger Daten von allen verwalteten NetScaler-Instanzen über verschiedene Funktionen wie Ereignisse, Syslogs, Netzwerkberichterstattung usw. in den NetScaler Console-Speicher.

Der Status der Datenerfassung gibt an, ob NetScaler Console Statistiken von NetScaler-Instanzen sammelt. Die Datenerfassungsaktivität wird fortgesetzt, solange der verbrauchte Speicherplatz innerhalb des zugewiesenen Speichers liegt. Wenn der Verbrauch den zugewiesenen Speicherplatz überschreitet, wird die Datenerfassung angehalten.

Zeigen Sie die Kachel **Datenerfassung** an, um den aktuellen Status der Datenerfassung zu verstehen. Diese Kachel zeigt einen der folgenden zwei Zustände an:

- **Aktiv** – Die Datenerfassungsaktivität ist im Gange.

- **Angehalten** – Die Datenerfassungsaktivität ist angehalten, da der verbrauchte Speicher den berechtigten Speicher überschreitet.

So setzen Sie Ihre angehaltene Datenerfassung fort

Um Ihre Datenerfassungsaktivität fortzusetzen, können Sie eine der folgenden Aktionen ausführen:

- Mehr Datenspeicher hinzufügen.
- Datenbereinigung durchführen.

Gesamtspeicherverbrauch

Für einen schnellen Überblick über Ihren Datenspeicher sehen Sie sich die Kachel **Speicherverbrauch** an.

Die Kachel **Speicherverbrauch** zeigt den gesamten Speicher an, der von allen Funktionen in der Bereitstellung verwendet wird.

Fahren Sie mit der Maus über das Donut-Diagramm, um Folgendes anzuzeigen:

Berechtigter Speicher

Der berechtigte Speicher ist der gesamte Speicher, der Ihnen gemäß Ihrer Lizenz zur Verfügung steht. Wenn Sie eine Express-Lizenz haben, erhalten Sie 500 MB berechtigten Speicher. Wenn Sie

© 1997–2026 Citrix Systems, Inc. All rights reserved.

eine Advanced-Lizenz haben, erhalten Sie die Summe von 500 MB Speicher pro gekauftem VIP und jeglichen zusätzlichen Speicher, der direkt ohne den Kauf von VIPs erworben wurde.

Berücksichtigen Sie die folgenden Szenarien:

- Sie haben 20 VIPs gekauft. Sie erhalten 500 MB kostenlosen Speicherplatz für jeden VIP. Ihr zustehender Speicherplatz beträgt 20*500 = 10 GB.
- Sie haben 20 VIPs und einen zusätzlichen Speicherplatz von 5 GB gekauft. Sie erhalten 500 MB kostenlosen Speicherplatz für jeden VIP. Ihr zustehender Speicherplatz beträgt 20*500 + 5 = 15 GB.

Verbrauchter Speicherplatz

Der verbrauchte Speicherplatz ist der gesamte Speicherplatz, der von allen Funktionen in der Bereitstellung verwendet wird. Die folgenden Farbcodierungskriterien geben die von den Funktionen genutzte Speichermenge an:

- **Grün** – Der verbrauchte Speicherplatz beträgt weniger als 75 % des zustehenden Speicherplatzes.
- **Gelb** – Der verbrauchte Speicherplatz liegt zwischen 75 % und 99 % des zustehenden Speicherplatzes.
- **Rot** – Die Grenze des verbrauchten Speicherplatzes ist erreicht oder überschreitet den aktuell zustehenden Speicherplatz.

Status der Datenbereinigung

Bereinigung ist der Prozess des manuellen Löschens von Daten und des Freigebens von Speicherplatz. Sie dürfen in jedem Kalendermonat 10 Datenbereinigungen durchführen. Sie können Ihre Daten beispielsweise vom 1. bis 31. Juli 10 Mal löschen.

Um zu erfahren, wie viele Datenbereinigungen Sie bereits verwendet haben und wie viele Ihnen noch verbleiben, sehen Sie sich die Kachel **Datenbereinigung** an.

HINWEIS:

Jede Bereinigungsaktivität wird als eine Datenbereinigung gezählt, unabhängig von der Anzahl der ausgewählten Funktionen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Trends beim Speicherverbrauch

Um zu erfahren, wie Daten in den letzten 30 Tagen verbraucht wurden, sehen Sie sich den Abschnitt **Trend des Speicherverbrauchs** an.

Speicherverbrauchstrend bietet Einblicke, welche Funktionen über einen bestimmten Zeitraum den meisten oder geringsten Speicherplatz nutzen, und hilft Ihnen, Ihren Datenspeicherverbrauch effektiv zu verwalten.

Sie können die Speicherdattentrends in einer der folgenden Formen anzeigen:

- **Grafische Ansicht** – Zeigt an, wie der Datenspeicher auf die verschiedenen NetScaler Console-Funktionen verteilt ist. Fahren Sie mit der Maus über die Zeitleiste, um die Datenspeicherinformationen für jeden Tag des Monats anzuzeigen.

  HINWEIS:

  Die **Grafische Ansicht** ist die Standardansicht.

- **Tabellarische Ansicht** – Klicken Sie auf **Tabellarische Ansicht**, um die Datenspeicherinformationen in Tabellenform anzuzeigen.

  HINWEIS:

  Die tabellarische Ansicht ermöglicht es Ihnen, die Daten mithilfe des Suchfelds zu filtern.

Die folgende Tabelle beschreibt die Felder, die im Abschnitt **Speicherverbrauchstrend** angezeigt werden:

FUNKTION	BESCHREIBUNG
Konfiguration	Umfasst alle konfigurierbaren Daten wie Informationen zu Instanzen, Konfigurationsaufträgen, Konfigurationsprüfung und so weiter.
HDX Insight	Bietet End-to-End-Transparenz für ICA-Datenverkehr, der NetScaler durchläuft.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FUNKTION	BESCHREIBUNG
Netzwerkberichterstattung	Zeigt die Netzwerkleistung aller NetScaler-Instanzen an.
Web Insight	Bietet Einblick in Unternehmens-Webanwendungen und ermöglicht eine integrierte Echtzeit-Überwachung von Anwendungen.
Security Insight	Hilft bei der Bewertung des Anwendungssicherheitsstatus und bei der Ergreifung von Korrekturmaßnahmen zur Sicherung der Anwendungen.
Gateway Insight	Bietet Einblick in die Fehler, die allen Benutzern unabhängig vom Zugriffsmodus beim Anmelden am NetScaler Gateway begegnen.
Ereignisse	Überwacht und verwaltet das Auftreten von Ereignissen oder Fehlern auf den NetScaler-Instanzen.
App-Dashboard	Ermöglicht die Anzeige und Verwaltung von Anwendungen.
Bot Insight	Bietet Einblick in Bot-Verletzungen und die daraufhin ergriffenen Maßnahmen.
Syslog	Überwacht Syslog-Ereignisse, die auf NetScaler-Instanzen generiert werden, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Nachrichten an NetScaler Console umgeleitet werden.
Video Insight	Überwacht die Metriken der Videooptimierungstechniken, die von NetScaler-Instanzen verwendet werden.
Detaillierte Transaktionen	Bietet Einblick in Webtransaktionen und zeigt die Metrik der Antwortzeit visuell aufgeteilt nach Client, NetScaler und Server an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Speicherverbrauch nach Funktionen

Um mehr darüber zu erfahren, wie der Datenspeicher auf die verschiedenen Funktionen verteilt ist, sehen Sie sich den Abschnitt **Speicherverbrauch nach Funktionen am *TT MMM*** an.

Speicherverbrauch nach Funktionen am *TT MMM* hilft Ihnen zu verstehen:

- Der von allen verschiedenen Funktionen in NetScaler Console verwendete Speicherplatz
- Der Prozentsatz des Speicherplatzes, den die Funktionen an einem bestimmten Tag verbrauchen

Wenn Sie die Tabelleneinträge sortieren möchten, verwenden Sie die Spaltenüberschriften der Tabelle. NetScaler Console sortiert die Tabelle alphanumerisch von oben nach unten basierend auf den Daten in der ausgewählten Spalte. Um die Tabelle in umgekehrter Reihenfolge zu sortieren, klicken Sie erneut auf die Spaltenüberschrift.

Informationen zum Bereinigen Ihrer Daten, zum Bereinigungsverlauf und zu Speicherereignisprotokollen finden Sie unter Speicherplatz verwalten.

Speicherplatz verwalten

Sie können das Dashboard **Datenspeicherverwaltung** verwenden, um Ihre Datenspeichernutzung zu überwachen und die erforderlichen Maßnahmen zu ergreifen, um Speicherplatz freizugeben oder den Speicher zu erhöhen, wenn Ihr Datenspeicher das lizenzierte Limit überschreitet.

Die Kachel **Aktionen** zeigt die Liste der empfohlenen Schritte an, die Sie zur Verwaltung Ihrer Speicherkapazität unternehmen können:

- Datenaufbewahrungsrichtlinie überprüfen
- Datenbereinigung durchführen
- Bei Überschreitung des Speicherlimits benachrichtigen

Wenn Ihr genutzter Speicher 100 % des lizenzierten Speichers erreicht, wird die Datenerfassungsaktivität angehalten und Daten werden nicht mehr in der NetScaler Console gespeichert.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Datenbereinigung durchführen

Bereinigen Sie Ihre Daten, um Speicherressourcen zu optimieren und mehr Speicherplatz zu erhalten. Neben der Freigabe von Speicherplatz verbessert die Datenbereinigung die Datenqualität und beschleunigt die Verarbeitungszeiten. Wir empfehlen Ihnen, unnötige Daten regelmäßig zu überprüfen und zu löschen. Dieser Prozess stellt sicher, dass Ihre Ressourcen umsichtig genutzt werden und die NetScaler Console agil und reaktionsschnell ist.

So bereinigen Sie Ihre Daten:

1. Scrollen Sie auf der Seite **Datenspeicherverwaltung** zum Abschnitt ***Speicherverbrauch nach Funktionen am JJJJ-MM-TT***.
2. Wählen Sie eine oder mehrere Funktionen aus und klicken Sie auf **Bereinigen**. Sie können **Konfiguration** nicht auswählen, da sie alle Systemkonfigurationen enthält.

   Ein Pop-up-Fenster fordert Sie auf, zu bestätigen, ob Sie alle Daten für die ausgewählten Funktionen löschen möchten. Klicken Sie auf **Ja, bereinigen**.

   HINWEIS:

   Das Pop-up-Fenster zeigt auch Informationen zu Ihrem aktuellen Bereinigungsversuch an.

Bereinigungsverlauf anzeigen

Klicken Sie auf **Bereinigungsverlauf anzeigen**, um Details zu allen Bereinigungsaktivitäten zu erhalten, die Sie in NetScaler Console durchgeführt haben.

Die Seite **Bereinigungsprotokolle: Aufgabenprotokolle** zeigt die Liste aller Bereinigungsaufgaben, einschließlich ihres jeweiligen Status, der Startzeit und der Endzeit.

Um zu verstehen, welche Funktionen bei den einzelnen Bereinigungsvorgängen entfernt wurden, wählen Sie eine Aufgabe aus und klicken Sie auf **Funktionsprotokoll**.

Speicherereignisprotokolle anzeigen

Klicken Sie auf **Speicherereignisprotokolle**, um Einblicke in alle Zeiten zu erhalten, in denen Ihre Daten das lizenzierte Limit überschritten oder 75 % davon erreicht haben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Datenaufbewahrungsrichtlinie überprüfen

Die Datenaufbewahrungsrichtlinie bezieht sich auf eine Reihe von Regeln und Konfigurationen, die festlegen, wie NetScaler Console historische Daten im Laufe der Zeit verwaltet und pflegt. Diese Richtlinie legt fest, wie lange Daten gespeichert werden, bevor sie automatisch gelöscht werden.

Wenn Sie den von allen verschiedenen Funktionen verwendeten Speicherplatz reduzieren möchten, können Sie ändern, wie lange Daten in NetScaler Console aufbewahrt werden.

Verwenden Sie die Seite **Datenaufbewahrungsrichtlinie**, um die Datenspeichereinstellungen zu bearbeiten für:

- Ereignismeldungen
- Syslog-Meldungen
- Netzwerkberichtsdaten

Weitere Informationen zu den Datenspeichereinstellungen finden Sie unter Datenaufbewahrungsrichtlinie.

Benachrichtigung bei Überschreitung des Speicherlimits

Sie können Benachrichtigungen für NetScaler Console einrichten, um Warnungen zu erhalten, wenn Ihre Datenspeicherkapazität die angegebenen Grenzwerte überschreitet.

So zeigen Sie Ihre Systembenachrichtigungen an und konfigurieren sie:

1. Klicken Sie in der Kachel **Aktionen** auf **Benachrichtigung bei Überschreitung des Speicherlimits**.
2. Stellen Sie auf der Seite **Systembenachrichtigungen konfigurieren** unter der **Systemereigniskategorie** sicher, dass die Kategorie **DataStorageExceeded** ausgewählt ist, um Benachrichtigungen zu erhalten.

Sie können verschiedene Parameter festlegen, die sich darauf beziehen, wie und wann Benachrichtigungen an Sie oder andere Benutzer gesendet werden. Wählen Sie die bevorzugte Kommunikationsmethode (z. B. E-Mail-, Slack-, PagerDuty- und ServiceNow-Benachrichtigungen) und definieren Sie die Empfänger für die Benachrichtigungen.

Weitere Informationen zum Einrichten der Profile und zum Senden von Benachrichtigungen finden Sie unter Benachrichtigungen konfigurieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Datenaufbewahrungsrichtlinie

Sie können in NetScaler Console für eine bestimmte Dauer auf Systemereignisse, Syslog-Meldungen und Netzwerkberichtsdaten zugreifen.

1. Navigieren Sie zu **Einstellungen > Datenspeicher > Datenaufbewahrungsrichtlinie**, um die Datenaufbewahrung zu konfigurieren.
2. Klicken Sie auf die Schaltfläche „Bearbeiten“.
3. Geben Sie für jede der folgenden Optionen die Anzahl der Tage ein, die die Daten in NetScaler Console aufbewahrt werden sollen:

OPTIONEN	BESCHREIBUNG
Ereignisse	Ermöglicht es Ihnen, die in NetScaler Console gespeicherten Ereignismeldungen auf bis zu 40 Tage zu begrenzen. Die Ereignisse werden aus NetScaler Console gelöscht, nachdem die Aufbewahrungsrichtlinie abgelaufen ist. Die gelöschten Ereignisse werden nach einem Tag entfernt.
Syslog	Ermöglicht es Ihnen, die Menge der in der Datenbank gespeicherten Syslog-Daten auf bis zu 180 Tage zu begrenzen.
Netzwerkberichterstattung	Ermöglicht es Ihnen, die in NetScaler Console gespeicherten Netzwerkberichtsdaten auf bis zu 30 Tage zu begrenzen.

WICHTIG:

Sie können die Datenaufbewahrungsrichtlinie mit einem Express-Konto nicht bearbeiten.

Wenn Ihr Konto in ein Express-Konto umgewandelt wird, behält die NetScaler Console die Speicherdaten bis zu 500 MB oder die Daten eines Tages, je nachdem, welcher Wert geringer ist. Weitere Informationen finden Sie unter NetScaler Console-Ressourcen mit einem Express-Konto verwalten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Systemalarme konfigurieren und anzeigen

Sie können eine Reihe von Alarmen aktivieren und konfigurieren, um den Zustand Ihrer NetScaler Console-Server zu überwachen. Sie müssen Systemalarme konfigurieren, um sicherzustellen, dass Sie über kritische oder schwerwiegende Systemprobleme informiert sind.

Sie möchten beispielsweise benachrichtigt werden, wenn die CPU-Auslastung hoch ist oder wenn mehrere Anmeldefehler am Server auftreten. Für einige Alarmkategorien, wie z. B. cpuUsageHigh oder memoryUsageHigh, können Sie Schwellenwerte festlegen und den Schweregrad (z. B. Kritisch oder Schwerwiegend) für jede definieren. Für einige Kategorien, wie z. B. inventoryFailed oder loginFailure, können Sie nur den Schweregrad definieren. Wenn der Schwellenwert für eine Alarmkategorie überschritten wird (z. B. memoryUsageHigh) oder wenn ein Ereignis eintritt, das der Alarmkategorie entspricht (z. B. loginFailure), wird eine Meldung im System aufgezeichnet, und Sie können die Meldung als Syslog-Meldung anzeigen. Sie können außerdem Benachrichtigungen einrichten, um eine E-Mail oder SMS entsprechend Ihren Alarmeinstellungen zu erhalten.

Sie können den Schweregrad eines Alarms zuweisen oder ändern. Die Schweregrade, die Sie zuweisen können, sind Kritisch, Schwerwiegend, Geringfügig, Warnung und Informatorisch.

Einen Alarm konfigurieren

Betrachten Sie ein Szenario, in dem Sie einen fehlgeschlagenen Sicherungsversuch überwachen möchten. Sie können den Alarm backupFailed aktivieren und ihm einen Schweregrad, z. B. Schwerwiegend, zuweisen. Immer wenn NetScaler Console versucht, die Systemdateien zu sichern, und der Versuch fehlschlägt, wird ein Alarm ausgelöst. Sie können die Meldung auf der Seite für NetScaler Console-Protokollmeldungen anzeigen oder Benachrichtigungen per E-Mail oder SMS erhalten.

Um den Alarm zu konfigurieren, müssen Sie den Alarm backupFailed auswählen und den Schweregrad als Schwerwiegend festlegen. Der Alarm ist standardmäßig aktiviert.

So konfigurieren und zeigen Sie einen Systemalarm mit NetScaler Console an:

1. Navigieren Sie zu **Einstellungen > SNMP**. Klicken Sie oben rechts auf **Alarme**.

2. Wählen Sie den Alarm aus, den Sie konfigurieren möchten (z. B. cpuUsageHigh), und klicken Sie auf **Bearbeiten**, um dessen Einstellungen zu ändern.

3. Wählen Sie auf der Seite **Alarm konfigurieren** die Option **Alarm aktivieren**, um Warnungen zu erstellen, und geben Sie dann Folgendes an:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Zeit**. Geben Sie die Zeit (in Minuten) ein, nach der der Alarm ausgelöst werden soll.
- **Schweregrad**. Wählen Sie den Schweregrad aus.
- **Alarmschwellenwert**. Geben Sie den Wert ein, bei dem der Alarm ausgelöst und Benachrichtigungen an Sie gesendet werden sollen.

Klicken Sie auf **OK**.

HINWEIS:

Sie können den Schwellenwert für einige Alarme, z. B. backupFailed, nicht festlegen. Wenn der Alarm ausgelöst wird, können Sie das generierte Ereignis als Syslog-Nachricht anzeigen.

So zeigen Sie das durch einen Alarm generierte Ereignis an (z. B. backupFailed):

1. Navigieren Sie zu **Einstellungen** > **Audit-Protokollmeldungen**.
2. Wählen Sie im Suchfeld den Alarmtyp aus. Wählen Sie in diesem Beispiel **Ereignis**, **=** (gleich einem Wert) und dann **BACKUPFAILED**.

   Das für eine fehlgeschlagene Sicherung generierte Ereignis wird angezeigt.

   Sie können auch Benachrichtigungen einrichten, um eine E-Mail oder eine SMS (Short Message Service) zu erhalten, wenn ein Alarm ausgelöst wird.

Schwellenwerte für Festplattenauslastungsalarme hinzufügen

Festplattenauslastungsalarme werden ausgelöst, wenn der auf dem NetScaler Console-Server verwendete Speicherplatz einen vordefinierten Schwellenwert überschreitet.

Als Administrator können Sie bei Erhalt von Warnmeldungen unnötige Daten löschen oder zusätzliche Speicherressourcen zuweisen, um Dienstunterbrechungen oder Leistungseinbußen zu vermeiden.

Ab Release 14.1 Build 25x können Sie auch einen Schwellenwert für die Festplattenauslastung auf niedrigerer Ebene hinzufügen. Mit diesem Schwellenwert können Sie eine Untergrenze festlegen, um Warnmeldungen zu erhalten, bevor eine Obergrenze überschritten wird.

So konfigurieren Sie einen Schwellenwert auf niedrigerer Ebene:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie zu **Einstellungen > SNMP > Alarme**, und geben Sie im Suchfeld diskUtilizationHigh ein, um die Alarme zur Festplattenauslastung anzuzeigen.
2. Wählen Sie den Alarm aus, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie auf der Seite **Alarm konfigurieren** die Option **Schwellenwert auf niedrigerer Ebene konfigurieren** aus. Geben Sie den Schwellenwert auf niedrigerer Ebene ein.

   Alarm bei fehlgeschlagener Sicherung(/en-us/netscaler-console-service/media/snmp-alarms-lower-threshold.png)

Wenn Sie beispielsweise einen unteren Schwellenwert für die Festplattenauslastung von 60 und einen oberen Schwellenwert von 80 festlegen, erhalten Sie eine Warnung, wenn die Festplattennutzung 60 % der Festplattenkapazität überschreitet. Diese Einstellung ermöglicht es Ihnen, Korrekturmaßnahmen zu ergreifen, bevor die Festplattenauslastung 80 % erreicht.

Observability-Integration

Aufgrund der zunehmenden Komplexität moderner Anwendungen stehen Administratoren vor Herausforderungen bei:

- Überwachung und Fehlerbehebung von Anwendungen.
- Gewinnung von Einblicken in das Verhalten von Infrastruktur und Anwendungen.

Observability schließt diese Lücke, indem es diese Einblicke in die gesamte Infrastruktur bietet. Mit der Funktion zur Observability-Integration in NetScaler Console können Sie:

- NetScaler Console in Splunk integrieren.
- NetScaler Console in New Relic integrieren.
- NetScaler Console in Microsoft Sentinel integrieren
- NetScaler-Instanzen für den Export von Einblicken nach Prometheus unter Verwendung des Standardschemas konfigurieren.

Integration mit Splunk

Sie können NetScaler Console jetzt in Splunk integrieren, um Analysen für Folgendes anzuzeigen:

- WAF-Verletzungen
- Bot-Verletzungen
- SSL-Zertifikat-Einblicke
- Gateway-Einblicke

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler® Console Audit-Protokolle

Das Splunk-Add-on ermöglicht Ihnen Folgendes:

- Alle anderen externen Datenquellen kombinieren.
- Eine bessere Sichtbarkeit der Analysen an einem zentralen Ort bieten.

NetScaler Console sammelt Bot-, WAF-, SSL-, Gateway- und Audit-Protokollereignisse und sendet diese regelmäßig an Splunk. Das Splunk Common Information Model (CIM)-Add-on konvertiert die Ereignisse in CIM-kompatible Daten. Als Administrator können Sie die Ereignisse mithilfe der CIM-kompatiblen Daten im Splunk-Dashboard anzeigen.

Für eine erfolgreiche Integration müssen Sie:

- Splunk für den Empfang von Daten von NetScaler Console konfigurieren
- NetScaler Console für den Export von Daten nach Splunk konfigurieren
- Dashboards in Splunk anzeigen

Splunk für den Empfang von Daten von NetScaler Console konfigurieren

In Splunk müssen Sie:

1. Den Splunk HTTP Event Collector-Endpunkt einrichten und ein Token generieren
2. Das Splunk Common Information Model (CIM)-Add-on installieren
3. Den CIM-Normalisierer installieren (nur für WAF- und Bot-Einblicke anwendbar)
4. Ein Beispieldashboard in Splunk vorbereiten

Den Splunk HTTP Event Collector-Endpunkt einrichten und ein Token generieren

Zuerst müssen Sie den HTTP Event Collector in Splunk einrichten. Diese Einrichtung ermöglicht die Integration zwischen der NetScaler Console und Splunk, um WAF- oder Bot-Daten zu senden. Als Nächstes müssen Sie ein Token in Splunk generieren, um:

- Die Authentifizierung zwischen NetScaler Console und Splunk aktivieren.
- Daten über den Event Collector-Endpunkt empfangen.

1. Melden Sie sich bei Splunk an.
2. Navigieren Sie zu **Einstellungen > Dateneingaben > HTTP Event Collector** und klicken Sie auf **Neu hinzufügen**.
3. Geben Sie die folgenden Parameter an:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. **Name**: Geben Sie einen Namen Ihrer Wahl an.

b. **Quellnamenüberschreibung (optional)**: Wenn Sie einen Wert festlegen, überschreibt dieser den Quellwert für den HTTP Event Collector.

c. **Beschreibung (optional)**: Geben Sie eine Beschreibung an.

d. **Ausgabegruppe (optional)**: Standardmäßig ist diese Option als „Keine“ ausgewählt.

e. **Indexer-Bestätigung aktivieren**: NetScaler Console unterstützt diese Option nicht. Wir empfehlen, diese Option nicht auszuwählen.

4. Klicken Sie auf **Weiter**.
5. Optional können Sie auf der Seite **Eingabeeinstellungen** zusätzliche Eingabeparameter festlegen.
6. Klicken Sie auf **Überprüfen**, um die Einträge zu verifizieren, und klicken Sie dann auf **Senden**.

   Ein Token wird generiert. Sie müssen dieses Token verwenden, wenn Sie Details in NetScaler Console hinzufügen.

Installieren des Splunk Common Information Model

In Splunk müssen Sie das Splunk CIM-Add-on installieren. Dieses Add-on stellt sicher, dass die von NetScaler Console empfangenen Daten normalisiert werden und einem gemeinsamen Standard entsprechen, indem dieselben Feldnamen und Ereignis-Tags für äquivalente Ereignisse verwendet werden.

HINWEIS:

Sie können diesen Schritt ignorieren, wenn Sie das Splunk CIM-Add-on bereits installiert haben.

1. Melden Sie sich bei Splunk an.
2. Navigieren Sie zu **Apps > Weitere Apps finden**.

3. Geben Sie **CIM** in die Suchleiste ein und drücken Sie die **Eingabetaste**, um das Add-on **Splunk Common Information Model (CIM)** zu erhalten, und klicken Sie auf **Installieren**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CIM-Normalisierer installieren

Der CIM-Normalisierer ist ein zusätzliches Plug-in, das Sie installieren müssen, um die WAF- und Bot-Erkenntnisse in Splunk anzuzeigen.

1. Navigieren Sie im Splunk-Portal zu **Apps > Weitere Apps finden**.

2. Geben Sie **CIM normalization for ADM service events/data** in die Suchleiste ein und drücken Sie die **Eingabetaste**, um das Add-on zu erhalten, und klicken Sie auf **Installieren**.

Ein Beispieldashboard in Splunk vorbereiten

Nachdem Sie das Splunk CIM installiert haben, müssen Sie ein Beispieldashboard mithilfe einer Vorlage für WAF und Bot sowie SSL Certificate Insights vorbereiten. Sie können die Dashboard-Vorlagendatei (`.tgz`) herunterladen, einen beliebigen Editor (z. B. Notepad) verwenden, um deren Inhalt zu kopieren, und ein Dashboard erstellen, indem Sie die Daten in Splunk einfügen.

HINWEIS:

Das folgende Verfahren zum Erstellen eines Beispieldashboards gilt sowohl für WAF und Bot als auch für SSL Certificate Insights. Sie müssen die erforderliche `json`-Datei verwenden.

1. Melden Sie sich auf der Citrix-Downloadseite an und laden Sie das Beispieldashboard herunter, das unter Observability Integration verfügbar ist.
2. Extrahieren Sie die Datei, öffnen Sie die `json`-Datei mit einem beliebigen Editor und kopieren Sie die Daten aus der Datei.

   HINWEIS:

   Nach dem Extrahieren erhalten Sie zwei `json` Dateien. Verwenden Sie `adm_splunk_security_violations.json`, um das WAF- und Bot-Beispiel-Dashboard zu erstellen, und verwenden Sie `adm_splunk_ssl_certificate.json`, um das SSL-Zertifikat-Einblicks-Beispiel-Dashboard zu erstellen.

3. Navigieren Sie im Splunk-Portal zu **Search & Reporting > Dashboards** und klicken Sie dann auf **Create New Dashboard**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Geben Sie auf der Seite **Create New Dashboard** die folgenden Parameter an:

    a. **Dashboard-Titel** – Geben Sie einen Titel Ihrer Wahl ein.

    b. **Beschreibung** – Optional können Sie eine Beschreibung zu Ihrer Referenz angeben.

    c. **Berechtigung** – Wählen Sie je nach Anforderung **Private** oder **Shared in App** aus.

    d. Wählen Sie **Dashboard Studio** aus.

    e. Wählen Sie ein beliebiges Layout (**Absolute** oder **Grid**) aus und klicken Sie dann auf **Create**.

    Nachdem Sie auf **Create** geklickt haben, wählen Sie das **Source**-Symbol aus dem Layout aus.

5. Löschen Sie die vorhandenen Daten, fügen Sie die in Schritt 2 kopierten Daten ein und klicken Sie auf **Back**.
6. Klicken Sie auf **Save**.

Sie können das folgende Beispieldashboard in Ihrem Splunk anzeigen.

NetScaler Console zum Exportieren von Daten nach Splunk konfigurieren

Sie haben nun alles in Splunk vorbereitet. Der letzte Schritt ist die Konfiguration von NetScaler Console durch Erstellen eines Abonnements und Hinzufügen des Tokens.

Nach Abschluss des folgenden Verfahrens können Sie das aktualisierte Dashboard in Splunk anzeigen, das derzeit in Ihrer NetScaler Console verfügbar ist:

1. Melden Sie sich bei NetScaler Console an.
2. Navigieren Sie zu **Settings > Observability Integration**.
3. Klicken Sie auf der Seite **Integrations** auf **Add**.
4. Geben Sie auf der Seite **Create Subscription** die folgenden Details an:

    a. Geben Sie im Feld **Subscription Name** einen Namen Ihrer Wahl an.

    b. Wählen Sie **NetScaler Console** als **Source** aus und klicken Sie auf **Next**.

    c. Wählen Sie **Splunk** aus und klicken Sie auf **Configure**. Auf der Seite **Configure Endpoint**:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. **End Point URL** – Geben Sie die Splunk-Endpunktdetails an. Der Endpunkt muss im `<https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event>` Format vorliegen.

> **HINWEIS:**
>
> Es wird empfohlen, HTTPS aus Sicherheitsgründen zu verwenden.

- **SPLUNK_PUBLIC_IP** – Eine gültige IP-Adresse, die für Splunk konfiguriert ist.
- **SPLUNK_HEC_PORT** – Bezeichnet die Portnummer, die Sie während der Konfiguration des HTTP-Ereignisendpunkts angegeben haben. Die Standard-Portnummer ist 8088.
- **Services/collector/event** – Bezeichnet den Pfad für die HEC-Anwendung.

ii. **Authentifizierungstoken** – Kopieren Sie das Authentifizierungstoken aus Splunk und fügen Sie es ein.

iii. Klicken Sie auf **Senden**.

d. Klicken Sie auf **Weiter**.

e. Klicken Sie auf **Insights hinzufügen**, und wählen Sie auf der Registerkarte **Feature auswählen** die Features aus, die Sie exportieren möchten, und klicken Sie auf **Ausgewählte hinzufügen**.

> **HINWEIS:**
>
> Wenn Sie **NetScaler Console Audit Logs** ausgewählt haben, können Sie **Täglich** oder **Stündlich** für die Häufigkeit des Exports von Audit-Protokollen nach Splunk auswählen.

f. Klicken Sie auf **Weiter**.

g. Wählen Sie auf der Registerkarte **Instanz auswählen** entweder **Alle Instanzen auswählen** oder **Benutzerdefinierte Auswahl** aus, und klicken Sie dann auf **Weiter**.

- **Alle Instanzen auswählen** – Exportiert Daten von allen NetScaler-Instanzen nach Splunk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Benutzerdefinierte Auswahl** – Ermöglicht Ihnen die Auswahl der NetScaler-Instanzen aus der Liste. Wenn Sie bestimmte Instanzen aus der Liste auswählen, werden die Daten nur von den ausgewählten NetScaler-Instanzen nach Splunk exportiert.

h. Klicken Sie auf **Senden**.

HINWEIS:

Die Daten für die ausgewählten Einblicke werden sofort an Splunk übertragen, nachdem die Verletzungen in NetScaler Console erkannt wurden.

Dashboards in Splunk anzeigen

Nachdem Sie die Konfiguration in NetScaler Console abgeschlossen haben, werden die Ereignisse in Splunk angezeigt.

Sie können das aktualisierte Dashboard in Splunk ohne zusätzliche Schritte anzeigen.

Gehen Sie zu Splunk und klicken Sie auf das Dashboard, das Sie erstellt haben, um das aktualisierte Dashboard anzuzeigen.

Das Folgende ist ein Beispiel für das aktualisierte WAF- und Bot-Dashboard:

Das folgende Dashboard ist ein Beispiel für das aktualisierte SSL Certificate Insights Dashboard.

Abgesehen vom Dashboard können Sie auch Daten in Splunk anzeigen, nachdem Sie das Abonnement erstellt haben.

1. Klicken Sie in Splunk auf **Search & Reporting**.
2. In der Suchleiste:

   - Geben Sie `sourcetype="bot"` oder `sourcetype="waf"` ein und wählen Sie die Dauer aus der Liste aus, um Bot-/WAF-Daten anzuzeigen.
   - Geben Sie `sourcetype="ssl"` ein und wählen Sie die Dauer aus der Liste aus, um die Daten der SSL-Zertifikat-Einblicke anzuzeigen.
   - Geben Sie `sourcetype="gateway_insights"` ein und wählen Sie die Dauer aus der Liste aus, um die Daten der Gateway-Einblicke anzuzeigen.
   - Geben Sie `sourcetype= "audit_logs"` ein und wählen Sie die Dauer aus der Liste aus, um die Audit-Log-Daten anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Integration mit New Relic

Sie können NetScaler Console jetzt in New Relic integrieren, um Analysen für WAF, Bot, SSL, Gateway Insights und NetScaler Console-Überwachungsprotokolle in Ihrem New Relic-Dashboard anzuzeigen. Mit dieser Integration können Sie:

- Alle anderen externen Datenquellen in Ihrem New Relic-Dashboard kombinieren.
- Einblicke in Analysen an einem zentralen Ort erhalten.

NetScaler Console erfasst Bot-, WAF-, SSL-, Gateway Insights- und NetScaler Console-Überwachungsprotokollereignisse und sendet sie sofort an New Relic. Als Administrator können Sie diese Ereignisse auch in Ihrem New Relic-Dashboard anzeigen.

Voraussetzungen

Für eine erfolgreiche Integration müssen Sie:

- Einen New Relic-Ereignisendpunkt im folgenden Format abrufen:

  `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`

  Weitere Informationen zum Konfigurieren eines Ereignisendpunkts finden Sie unter New Relic-Dokumentation.

  Weitere Informationen zum Abrufen einer Konto-ID finden Sie unter New Relic-Dokumentation.
- Einen New Relic-Schlüssel abrufen. Weitere Informationen finden Sie unter New Relic-Dokumentation.
- Die Schlüsseldetails in NetScaler Console hinzufügen

Die Schlüsseldetails in NetScaler Console hinzufügen

Nachdem Sie ein Token generiert haben, müssen Sie Details in NetScaler Console hinzufügen, um die Integration mit New Relic durchzuführen.

1. Melden Sie sich bei NetScaler Console an.
2. Navigieren Sie zu **Einstellungen > Observability Integration**.
3. Klicken Sie auf der Seite **Integrationen** auf **Hinzufügen**.
4. Geben Sie auf der Seite **Abonnement erstellen** die folgenden Details an:

   a. Geben Sie im Feld **Abonnementname** einen Namen Ihrer Wahl an.

   b. Wählen Sie **NetScaler® Console** als **Quelle** aus und klicken Sie auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. Wählen Sie **New Relic** aus und klicken Sie auf **Konfigurieren**. Auf der Seite **Endpunkt konfigurieren**:

   i. **Endpunkt-URL** – Geben Sie die Endpunktdetails von New Relic an. Der Endpunkt muss im `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`-Format vorliegen.

> **HINWEIS:**
>
> Aus Sicherheitsgründen wird die Verwendung von HTTPS empfohlen.

d. **Authentifizierungstoken** – Kopieren Sie das Authentifizierungstoken von New Relic und fügen Sie es ein.

   i. Klicken Sie auf **Senden**.

e. Klicken Sie auf **Weiter**.

f. Klicken Sie auf **Insights hinzufügen** und wählen Sie auf der Registerkarte **Funktion auswählen** die Funktionen aus, die Sie exportieren möchten, und klicken Sie auf **Ausgewählte hinzufügen**.

> **HINWEIS:**
>
> Wenn Sie **NetScaler Console-Audit-Protokolle** ausgewählt haben, können Sie **Täglich** oder **Stündlich** für die Häufigkeit des Exports von Audit-Protokollen nach New Relic auswählen.

g. Klicken Sie auf **Weiter**.

h. Auf der Registerkarte **Instanz auswählen** können Sie entweder **Alle Instanzen auswählen** oder **Benutzerdefinierte Auswahl** wählen und dann auf **Weiter** klicken.

- **Alle Instanzen auswählen** – Exportiert Daten von allen NetScaler-Instanzen nach New Relic.
- **Benutzerdefinierte Auswahl** – Ermöglicht Ihnen die Auswahl der NetScaler-Instanzen aus der Liste. Wenn Sie bestimmte Instanzen aus der Liste auswählen, werden die Daten nur von den ausgewählten NetScaler-Instanzen nach New Relic exportiert.

i. Klicken Sie auf **Senden**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Die Daten für die ausgewählten Einblicke werden unmittelbar nachdem die Verstöße in NetScaler Console erkannt wurden, an New Relic übertragen.

Die Konfiguration ist abgeschlossen. Sie können Details auf der Seite **Abonnements** anzeigen.

New Relic-Dashboard

Wenn die Ereignisse in New Relic exportiert werden, können Sie Ereignisdetails unter **Metriken & Ereignisse** im folgenden JSON-Format anzeigen:

`<subsription_name>_adm_<event name>`, wobei der Ereignisname Bot, WAF usw. sein kann.

Im folgenden Beispiel ist ADMSTAGING der `<subscription_name>` und Bot ist der `<event_name>`.

Sobald die JSON-Daten in Ihr New Relic-Dashboard aufgenommen wurden, können Sie als Administrator die NRQL (New Relic Query Language) verwenden und ein benutzerdefiniertes Dashboard mit Facetten und Widgets nach Ihrer Wahl erstellen, indem Sie Abfragen um die aufgenommenen Daten herum konstruieren. Weitere Informationen finden Sie unter `https://docs.newrelic.com/docs/query-your-data/nrql-new-relic-query-language/get-started/introduction-nrql-new-relics-query-language/`

Im Folgenden sehen Sie ein Beispiel-Dashboard, das mit NRQL erstellt wurde:

Um dieses Dashboard zu erstellen, sind die folgenden Abfragen erforderlich:

- Widget 1: Gesamtzahl der eindeutigen Angriffe in der Ereignistabelle

  `SELECT count(total_attacks) from <event_name> since 30 days ago`

- Widget 2: Eindeutige Transaktions-IDs in der Ereignistabelle

  `SELECT uniqueCount(transaction_id) from <event_name> since 30 days ago`

- Widget 3: Gesamtzahl der eindeutigen Bot-Typen und deren Anzahl

  `SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc) from <event_name> since 30 days ago`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Widget 4: Gesamtzahl der eindeutigen App-Namen mit Bot-Verletzungen

```
SELECT uniques(appname) from <event_name> since 30 days ago
```

Integration mit Microsoft Sentinel

Sie können NetScaler Console in Microsoft Sentinel integrieren, um die folgenden Analysen von NetScaler Console nach Microsoft Sentinel zu exportieren:

- WAF-Verletzungen
- Bot-Verletzungen
- SSL-Zertifikat-Einblicke
- Gateway-Einblicke
- NetScaler® Console-Überwachungsprotokolle

Microsoft Sentinel bietet eine zentralisierte Datenerfassung, die Daten aus verschiedenen Quellen wie Anwendungen, Servern usw. sammelt. Als Administrator können Sie Daten anzeigen und Entscheidungen treffen, nachdem die Einblicke oder Verstöße in Microsoft Sentinel gemeldet wurden.

Stellen Sie für eine erfolgreiche Integration sicher, dass Sie über ein aktives Azure-Abonnement verfügen, und befolgen Sie dann das Verfahren in jedem Abschnitt:

Konfigurieren des Log Analytics Workspace

Ein Log Analytics Workspace ist erforderlich, um die gesammelten Daten zu speichern und zu analysieren.

1. Melden Sie sich bei Azure an.
2. Klicken Sie auf **Ressource erstellen**.

3. Geben Sie in der Suchleiste „log analytics workspace“ ein und klicken Sie unter **Log Analytics Workspace** auf **Erstellen**.

4. Auf der Hauptseite des **Log Analytics-Arbeitsbereichs** klicken Sie auf **Erstellen**.

5. Unter **Log Analytics-Arbeitsbereich erstellen**:

   a. Wählen Sie das aktive Abonnement und die Ressourcengruppe aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Sie können auch auf **Neu erstellen** klicken, um eine Ressourcengruppe hinzuzufügen, wenn Sie die Berechtigung dazu haben.

b. Geben Sie einen Namen Ihrer Wahl an.

c. Wählen Sie Ihre Region aus der Liste aus.

d. Klicken Sie auf **Überprüfen + Erstellen**.

e. Eine Meldung "Validierung erfolgreich" wird angezeigt. Klicken Sie auf **Erstellen**, um den Arbeitsbereich bereitzustellen.

f. Sie sehen die Meldung "Bereitstellung läuft". Nachdem die Meldung "Bereitstellung abgeschlossen" angezeigt wird, klicken Sie auf **Zu Ressource wechseln**.

Der Arbeitsbereich wurde erfolgreich erstellt.

Erstellen einer Microsoft Entra-Anwendung

Sie müssen eine Entra-Anwendung erstellen, die Ihrem Azure-Abonnement zugeordnet ist, um im Namen des Log Analytics-Arbeitsbereichs zu kommunizieren. Nachdem Sie die Anwendung erstellt haben, müssen Sie auch die Berechtigung mit der Rolle **Microsoft Sentinel Contributor** erteilen. Die Anwendung liefert auch Details wie **Client-ID**, **Mandanten-ID** und **Client-Geheimnis**. Wir empfehlen Ihnen, diese Details zu notieren. Diese Details sind erforderlich, wenn Sie ein Abonnement in NetScaler Console erstellen, um den Integrationsprozess abzuschließen.

1. Geben Sie im Azure-Portal das Schlüsselwort in die Suchleiste ein.
2. Klicken Sie auf **Microsoft Entra ID**.

3. Klicken Sie auf **Hinzufügen** und wählen Sie **App-Registrierung**.

4. Geben Sie einen Namen für die App an, wählen Sie die Standardoption unter **Unterstützte Kontotypen** und klicken Sie dann auf **Registrieren**.

5. Nachdem Sie die Anwendung registriert haben:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Notieren Sie sich die **Client-ID** und die **Mandanten-ID**.

b. Erstellen Sie eine geheime ID für Ihre Anwendung. Klicken Sie auf **Zertifikate & Geheimnisse** und klicken Sie unter **Client-Geheimnisse** auf **Neues Client-Geheimnis**. Geben Sie eine Beschreibung und Gültigkeit an und klicken Sie dann auf **Hinzufügen**, um eine geheime ID für Ihre Anwendung zu erstellen.

c. Die Details werden für Ihre Anwendung angezeigt. Stellen Sie sicher, dass Sie die unter **Wert** angezeigte ID sofort nach dem Erstellen des Geheimnisses notieren. Dieser Wert wird ausgeblendet, wenn Sie zu einer anderen GUI-Option navigieren.

Daten an Microsoft Sentinel senden mithilfe des Microsoft Entra ID-Datenkonnektors

Microsoft Entra ID-Protokolle bieten umfassende Informationen über Benutzer, Anwendungen und Netzwerke, die auf Ihren Entra-Mandanten zugreifen. Weitere Informationen finden Sie unter Daten an Microsoft Sentinel senden mithilfe des Microsoft Entra ID-Datenkonnektors.

Datenerfassungsendpunkt konfigurieren

Sie müssen einen Datenerfassungsendpunkt erstellen, um die Endpunkt-URL zu erhalten. Dies ist erforderlich, wenn Sie ein Abonnement in NetScaler Console erstellen.

1. Wählen Sie in Ihrem Azure-Portal unter **Azure-Dienste** die Option **Datenerfassungsendpunkte** aus oder geben Sie das Schlüsselwort in die Suchleiste ein.

2. Klicken Sie auf **Erstellen** auf der Seite **Datenerfassungsendpunkte**.

3. Unter **Datenerfassungsendpunkt erstellen**:

   a. Geben Sie einen Endpunktnamen Ihrer Wahl an

   b. Wählen Sie das **Abonnement, die Ressourcengruppe** und die **Region** aus.

   c. Klicken Sie auf **Überprüfen + Erstellen**.

   d. Nachdem Sie die Meldung „Validierung erfolgreich“ sehen, klicken Sie auf **Erstellen**.

Sie müssen die Endpunkt-URL notieren. Wählen Sie auf der Hauptseite **Datenerfassungsendpunkt** den erstellten Endpunkt aus, klicken Sie auf **JSON-Ansicht**, und notieren Sie die Endpunkt-ID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Tabellen zum Exportieren von Daten erstellen

Sie müssen eine Tabelle erstellen und die JSON-Informationen für jede Insight bereitstellen, die Sie von NetScaler Console nach Microsoft Sentinel exportieren möchten. Die folgenden Details können Sie als Referenz zu den Tabellenanforderungen für jede Insight verwenden:

INSIGHTS	ERFORDERLICHE GESAMTZAHL DER TABELLEN
SSL-Insights	3
WAF	1
Bot	1
Gateway-Insights	5

Für jeden Arbeitsbereich können Sie maximal 10 Tabellen erstellen. Bei mehr als 10 Tabellen müssen Sie einen weiteren Arbeitsbereich erstellen.

1. Navigieren Sie in Ihrem Arbeitsbereich im Azure-Portal und klicken Sie unter **Einstellungen** auf **Tabellen**.
2. Klicken Sie auf **Erstellen** und wählen Sie **Neues benutzerdefiniertes Protokoll (DCR-basiert)**.
3. Unter **Benutzerdefiniertes Protokoll erstellen**:
   a. Geben Sie einen Tabellennamen an. Der Tabellenname muss im Format **console_insightname** vorliegen. Zum Beispiel: **console_ns_sslvserver**, **console_ns_ssl_certkey**. Sie können sich auf Schritt 4 beziehen, um die für jede Insight anwendbaren Tabellennamen zu erhalten.
   b. Geben Sie eine Beschreibung an, um weitere Informationen zum Tabellennamen hinzuzufügen. Dies ist optional.
   c. Erstellen Sie eine neue Datenerfassungsregel und fügen Sie sie hinzu.
   d. Wählen Sie den Datenerfassungsendpunkt aus der Liste aus.
   e. Klicken Sie auf **Weiter**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Auf der Registerkarte **Schema und Transformation** müssen Sie die JSON-Beispielprotokolle für die Insight hochladen, die Sie exportieren möchten. Sie können das folgende JSON-Beispiel für jede Insight verwenden und eine JSON-Datei zum Hochladen erstellen:

INSIGHTS	JSON	ZU VERWENDENDER TABELLENNAME
SSL (1)	{"id": "3eb05733-c326-493c-9aa0-f7db3a6b4277", "ns_ip_address": "10.106.186.141", "name": "zeta_192_168_110_250", "vsvr_ip_address": "", "vsvr_port": -1, "vsvr_type": "", "state": "", "partition_name": "", "display_name": "10.106.186.141", "poll_time": 1716539986, "managed": "f", "ssl2": "f", "ssl3": "t", "tls10": "t", "tls11": "t", "tls12": "t", "dh": "f", "ersa": "t", "sslprofile": "", "tls13": "f", "dhkeyexpsizelimit": "DISABLED", "pushenctriggertimeout": 1, "sessionticket": "", "includesubdomains": "f", "sessionticketkeyrefresh": "", "ssllogprofile": "", "serverauth": "", "ssltriggertimeout":	console_ns_sslvserver

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	ZU VERWENDENDER TABELLENNAME
	100, "ersacount": 0, "strictcachecks": "NO", "dhfile": "", "sessreuse": "ENABLED", "redirectportrewrite": "DISABLED", "skipclientcertpolicycheck": "", "tls13sessionticketsperauthcontext": 1, "cipherredirect": "DISABLED", "dropreqwithnohostheader": "NO", "sessionticketlifetime": -1, "maxage": 0, "pushenctrigger": "Always", "strictsigdigestcheck": "f", "sslredirect": "DISABLED", "sessionkeylifetime": -1, "alpnprotocol": "", "clientauthuseboundcachain": "", "sesstimeout": 120, "clientcert": "", "snihttphostmatch": "CERT", "preload": "NO", "prevsessionkeylifetime": -1, "sessionticketkeydata": "", "encrypttriggerpktcount": 45, "cleartextport": "", "ssliocspcheck": "", "hsts": "f", "sslinterception": "",	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	ZU VERWENDENDER TABELLENNAME
	"commonname": "", "sslireneg": "", "ocspstapling": "DISABLED", "quantumsize": 8192, "insertionencoding": "Unicode", "sslimaxsessperserver": -1, "cipherurl": "", "pushflag": 0, "zerorttearlydata": "DISABLED", "allowextendedmastersecret": "", "dhekeyexchangewithpsk": "NO", "clientauth": "DISABLED", "denysslreneg": "NONSECURE", "sendclosenotify": "YES", "dhcount": 0, "snienable": "DISABLED", "table_name": "ns_sslvserver"}	
SSL (2)	{"id": "a6673ab2-0b59-47b9-b530-bc30fb2b937c", "ssl_certificate": "/nsconfig/ssl/ca-cert.pem", "ssl_key": "/nsconfig/ssl/ca-key.pem", "certkeypair_name": "athul-ca", "cert_format": "PEM", "days_to_expiry": 281, "ns_ip_address":	console_ns_ssl_certkey

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	ZU VERWENDENDER TABELLENNAME
	"10.106.186.141", "status": "Valid", "device_name": "10.106.186.141", "file_location_path": "", "certificate_data": "", "key_data": "", "poll_time": 1717434335, "no_domain_check": "f", "version": 3, "serial_number": "7B34B6A6A1A79E0FF168242D7BCFF78F04C9EE66", "signature_algorithm": "sha256WithRSAEncryption", "issuer": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "valid_from": "Mar 12 08:51:11 2024 GMT", "valid_to": "Mar 12 08:51:11 2025 GMT", "subject": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "public_key_algorithm": "rsaEncryption", "public_key_size": 4096, "no_of_bound_entities": 0, "partition_name": "", "display_name": "10.106.186.141", "hostname": "athulsadc", "key_name": "", "subjaltname": "", "managed_by": "",	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	ZU VERWENDENDER TABELLENNAME
	"certificate_dn": "", "linkcertkeyname": "", "table_name": "ns_ssl_certkey"}	
SSL (3)	{"id": "2baffd1a-7ed6-4035-91e8-ad3a3125bff4", "certkeypair_name": "cert1", "ns_ip_address": "10.106.186.127", "poll_time": 1715671567, "partition_name": "", "display_name": "10.106.186.127", "hostname": "", "entity_name": "secure_gateway", "entity_type": "sslvserver", "table_name": "ns_sslcertkey_binding" }	console_ns_sslcertkey_binding
WAF	[{"ip_address": "10.106.185.156", "ctnsappname": "vserver_1", "severity": 2, "violation_type": 19, "violation_type_desc": "Start URL", "block_flags": 1, "transformed_flags": 0, "not_blocked_flags": 0, "country_code": "-NA-", "region_code": "-NA-",	console_af_threat_exporter_data_l2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	ZU VERWENDENDER TABELLENNAME
	"city": "-NA-", "latitude": 200.0, "longitude": 200.0, "signature_category": "", "attack_category": 2, "attack_category_desc": "Broken Authentication and Session Management", "total_attacks": 1, "rpt_sample_time": 1704783773, "source_ip_address": 174766492, "attack_time": 1704783538, "profile_name": "appfw_cs_lb_prof", "session_id": "", "http_req_url": "https://10.106.192.54/csrf_ffc/ffc.html?field10=asfasd", "violation_name": "-NA-", "violation_value": "-NA-", "violation_location": 4, "violation_threat_index": 5, "app_threat_index": 5, "http_method": 0, "violation_action": 3, "violation_action_desc": "Blocked", "severity_type": 2, "severity_type_desc":	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	ZU VERWENDENDER TABELLENNAME
	"Medium", "iprep_score": 0, "iprep_category": 0, "counter_value": 0, "appname": "vserver_1_10.106.185.156_lb", "violation_category": 12, "violation_category_desc": "Start URL", "source_ipv6_address": "", "true_client_ip": "\\N", "backend_vserver": "", "backend_appname": "", "transactionId": "0", "table_name": "af_threat_exporter_data_l2"}]	
Bot	{"ip_address": "10.106.186.122", "ctnsappname": "secure_gateway", "bot_type": "2", "bot_type_desc": "Bad", "action_type": "6", "action_type_desc": "Log", "country_code": "0.0", "region_code": "0.0", "city": "0.0", "bot_severity": "0", "bot_severity_desc": "Critical", "latitude": "0", "longitude": "0", "bot_detection_mechanism": "6", "bot_detection_mechanis	console_af_bot_attack_details_l2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	ZU VERWENDENDER TABELLENNAME
	m_desc": "BlackList", "bot_category": "0", "bot_category_desc": "Uncategorized", "source_ip_address": "174758625", "bot_signature_category": "Custom Policy Expression", "appname": "secure_gateway_10.106.186.122_lb", "backend_vserver": "", "backend_appname": "", "total_attacks": "2", "rpt_sample_time": "1718783216", "table_name": "af_bot_attack_details_l2"}	
Gateway Insight (1)	{"adc_ip_address": "10.106.186.141", "auth_server": "", "client_ip": 174766732, "epa_method_type": 0, "error_count": 14, "error_details": "Invalid credentials passed", "error_type": 1, "gateway_name": "vpn_vserver_142_6", "req_url": "", "resource": "", "rpt_sample_time": 1713505215, "sso_method_type": 0, "sta_ip": "", "table_name":	console_af_vpn_error_details

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	ZU VERWENDENDER TABELLENNAME
	`"af_vpn_error_details", "username": "John"}`	
Gateway Einblick (2)	`{"adc_ip_address": "10.102.71.166", "display_name": "10.102.71.166", "gateway_name": "firsthop", "ip_address": "10.102.71.168", "rpt_sample_time": "1718812158", "state": "Up", "table_name": "ns_vpnvserver"}`	console_ns_vpnvserver
Gateway Einblick (3)	`{"adc_ip_address": "10.106.186.141", "gateway_name": "vpn_vserver_141_7", "rpt_sample_time": 1702011308, "sessions": 1, "table_name": "af_vpn_session_details", "users": 1}`	console_af_vpn_session_details
Gateway Einblick (4)	`{"active_sessions": 59, "active_users": 1, "adc_ip_address": "10.106.186.136", "gateway_name": "vpnathul2", "rpt_sample_time": 1698919848, "table_name": "af_vpn_active_session_1"}`	console_af_vpn_active_session_1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

INSIGHTS	JSON	ZU VERWENDENDER TABELLENNAME
Gateway Einblick (5)	`{"adc_ip_address": "10.106.186.136", "entity_type": 3, "gateway_name": "vpnathul2", "hits": 3, "rpt_sample_time": 1698052438, "table_name": "af_vpn_error_reports"}`	console_af_vpn_error_reports
Audit-Protokolle	`{"system_gmt_time":1721868291, "source":"X.X.X.X", "severity":"INFO", "module":"DEVICECONFIG", "event_type":"CMD_EXECUTED", "message":"Sample Mesage", "instance_ip":"X.X.X.X", "app_name":""}`	console_syslog_messages

Nach dem Hochladen der JSON-Datei können Sie die folgenden Details anzeigen:

Klicken Sie auf **Transformation editor**, geben Sie die folgende Abfrage ein, die für den entsprechenden Insight anwendbar ist, und klicken Sie auf **Run**, um die Daten ab dem Abfragezeitpunkt in NetScaler Console zu übernehmen.

- **SSL** – `source | extend TimeGenerated = todatetime(poll_time) | project-rename sslvserver_id = id`
- **WAF** und **Bot** – `source | extend TimeGenerated = todatetime(rpt_sample_time)`
- **Gateway Insight** – `source | extend TimeGenerated = todatetime(rpt_sample_time)`

5. Klicken Sie auf **Next** und dann auf **Create**, um den Vorgang abzuschließen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Navigieren Sie zu **Data collection rules** und klicken Sie auf die von Ihnen erstellte DCR.
7. Klicken Sie unter **Configuration** auf **Data sources**, um die erstellte Tabelle anzuzeigen.

   Die DCR (Data collection rule) erfordert Zugriff auf die Rolle **Monitoring Metrics Publisher**.

   a. Navigieren Sie zu Ihrer DCR, auf die Sie über Ihr Azure-Portal unter **Recents** zugreifen können.
   b. Klicken Sie auf Ihrer DCR-Seite auf **Zugriffssteuerung (IAM)** und dann auf **Rollenzuweisung hinzufügen**.
   c. Geben Sie in der Suchleiste das Schlüsselwort „monitor“ ein, um **Monitoring Metrics Publisher** auszuwählen, und klicken Sie auf **Weiter**.
   d. Klicken Sie auf der Registerkarte **Mitglieder** auf **Mitglieder auswählen** und wählen Sie die von Ihnen erstellte Entra-App aus.
   e. Klicken Sie auf **Überprüfen + zuweisen**.

      Sie müssen die ID der Datensammlungsregeln notieren. Navigieren Sie zur Seite „Datensammlungsregeln“, wählen Sie Ihre DCR aus und klicken Sie auf die JSON-Ansicht, um die ID zu notieren.

Ein Abonnement in NetScaler Console erstellen

Sie haben nun alles vorbereitet. Der letzte Schritt besteht darin, NetScaler Console zu konfigurieren, indem Sie ein Abonnement erstellen und die erforderlichen Details hinzufügen. Um ein Abonnement in NetScaler Console zu erstellen, benötigen Sie die folgenden Details, die Sie notiert haben:

- Endpunkt-URL
- ID der Datensammlungsregeln
- Mandanten-ID
- Client-ID
- Client-Geheimnis

1. Melden Sie sich bei NetScaler Console an.
2. Navigieren Sie zu **Einstellungen > Observability Integration**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Klicken Sie auf der Seite **Integrationen** auf **Hinzufügen**.
4. Geben Sie auf der Seite **Abonnement erstellen** die folgenden Details an:
    a. Geben Sie im Feld „Abonnementname“ einen Namen Ihrer Wahl ein.
    b. Wählen Sie **NetScaler Console** als **Quelle** aus und klicken Sie auf **Weiter**.
    c. Wählen Sie **Microsoft Sentinel** aus und klicken Sie auf **Konfigurieren**. Geben Sie auf der Seite **Endpunkt konfigurieren** alle Details ein und klicken Sie auf **Senden**.
    d. Klicken Sie auf **Weiter**.
5. Klicken Sie auf **Insights hinzufügen** und wählen Sie auf der Registerkarte **Funktion auswählen** je nach den Tabellen, die Sie in Microsoft Azure hinzugefügt haben, die Funktionen aus, die Sie exportieren möchten, und klicken Sie auf **Ausgewählte hinzufügen** und dann auf **Weiter**.
6. Auf der Registerkarte **Instanz auswählen** können Sie entweder **Alle Instanzen auswählen** oder **Benutzerdefinierte Auswahl** wählen und dann auf **Weiter** klicken.
    - **Alle Instanzen auswählen** – Exportiert Daten von allen NetScaler-Instanzen nach Microsoft Sentinel.
    - **Benutzerdefinierte Auswahl** – Ermöglicht Ihnen die Auswahl der NetScaler-Instanzen aus der Liste. Wenn Sie bestimmte Instanzen aus der Liste auswählen, werden die Daten nur von den ausgewählten NetScaler-Instanzen nach Microsoft Sentinel exportiert.
7. Klicken Sie auf **Senden**.

Protokolle in Microsoft Azure anzeigen

Nachdem Sie alles konfiguriert haben, empfehlen wir Ihnen, 30 Minuten zu warten, um die Details in Microsoft Azure anzuzeigen.

1. Navigieren Sie in Ihrem Azure-Portal zu Ihrem **Log Analytics Workspace**.
2. Klicken Sie auf **Logs**, geben Sie den Tabellennamen an und klicken Sie auf **Run**, um die Ergebnisse anzuzeigen.

Konfigurieren von NetScaler®-Instanzen für den Export von Einblicken nach Prometheus mithilfe des Standardschemas

NetScaler unterstützt den direkten Export von Metriken nach Prometheus. Sie können den umfangreichen Satz von Metriken nutzen, die von NetScaler-Instanzen bereitgestellt werden, um

© 1997–2026 Citrix Systems, Inc. All rights reserved.

die NetScaler-Integrität und die Anwendungs-Integrität zu überwachen. Sie können beispielsweise Metriken zur CPU- und Speichernutzung erfassen, um die NetScaler-Integrität zu ermitteln. Ebenso können Sie Metriken wie die Anzahl der pro Sekunde empfangenen HTTP-Anfragen oder die Anzahl der aktiven Clients verwenden, um die Anwendungs-Integrität zu überwachen.

Um die Metriken nach Prometheus zu exportieren, müssen Sie ein Analyseprofil mit dem Typ Zeitreihe konfigurieren. Weitere Informationen finden Sie unter NetScaler, Anwendungen und Anwendungssicherheit mit Prometheus überwachen.

Mit der Funktion zur Observability-Integration in NetScaler Console können Sie den Export von Einblicken nach Prometheus mithilfe des Standardschemas konfigurieren.

1. Navigieren Sie zu **Einstellungen > Observability-Integration**.
2. Klicken Sie auf der Seite **Integrationen** auf **Hinzufügen**.
3. Geben Sie auf der Seite **Abonnement erstellen** die folgenden Details an:
    a. Geben Sie im Feld **Abonnementname** einen Namen Ihrer Wahl an.
    b. Wählen Sie **NetScaler** als **Quelle** aus und klicken Sie auf **Weiter**.
    c. Wählen Sie **Prometheus** als Ziel aus.
    d. Wählen Sie **Standard** für die zu exportierenden Standard-Einblicke aus.
    e. Klicken Sie auf **Instanzen hinzufügen** und wählen Sie die Instanzen aus, für die Sie Einblicke nach Prometheus exportieren möchten.
    f. Klicken Sie auf **Senden**.

Protokolle für fehlgeschlagene Konfigurationen anzeigen

Nachdem Sie ein Abonnement erstellt haben, können Sie den Status des erstellten Abonnements unter **Einstellungen > Observability-Integration** anzeigen. Wenn der Status **Fehlgeschlagen** anzeigt, klicken Sie, um Details anzuzeigen.

☐ Klicken Sie unter **Konfigurationsauftragsdetails** auf **Details anzeigen**.

☐ Klicken Sie auf **Protokolle anzeigen**, um die Details des Problems anzuzeigen.

☐

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfigurieren Sie den Export von NetScaler®-Metriken und Audit-Protokollen nach Splunk

NetScaler unterstützt den direkten Export von Metriken nach Splunk im JSON-Format. NetScaler bietet umfangreiche Metriken zur Überwachung der Anwendungs- und Anwendungssicherheitsintegrität. Durch den Export der von NetScaler bereitgestellten Metriken nach Splunk können Sie die Metriken visualisieren und aussagekräftige Erkenntnisse gewinnen.

Die Audit-Protokollierung ermöglicht es Ihnen, die von verschiedenen Modulen in NetScaler gesammelten NetScaler-Zustände und Statusinformationen zu protokollieren. Durch die Überprüfung der Protokolle können Sie Probleme oder Fehler beheben.

Weitere Informationen finden Sie unter:

- Audit-Protokolle direkt von NetScaler nach Splunk exportieren
- Metriken direkt von NetScaler nach Splunk exportieren

So konfigurieren Sie den Export von Metriken und Audit-Protokollen nach Splunk über NetScaler Console:

1. Navigieren Sie zu **Einstellungen > Observability Integration**.
2. Klicken Sie auf der Seite **Integrationen** auf **Hinzufügen**.
3. Geben Sie auf der Seite **Abonnement erstellen** die folgenden Details an:
    a. Geben Sie einen Namen Ihrer Wahl in das Feld **Abonnementname** ein.
    b. Wählen Sie **NetScaler** als **Quelle** aus und klicken Sie auf **Weiter**.
    c. Wählen Sie **Splunk** als **Ziel** aus und klicken Sie auf **Konfigurieren**. Unter Endpunkt konfigurieren:
        - **Endpunkt-URL** – Geben Sie die Splunk-Endpunktdetails an. Der Endpunkt muss im Format `https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event`` vorliegen.
        - **Authentifizierungstoken** – Kopieren Sie das Authentifizierungstoken aus Splunk und fügen Sie es ein.
        - Klicken Sie auf **Senden**.
    d. Klicken Sie auf **Weiter**.
    e. Klicken Sie auf **Insights hinzufügen** und wählen Sie **NetScaler-Metriken** und **NetScaler-Audit-Protokolle** aus, und klicken Sie dann auf **Ausgewählte hinzufügen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

f. Klicken Sie auf **Weiter**.

g. Klicken Sie auf **Instanzen hinzufügen** und wählen Sie die Instanzen aus.

h. Klicken Sie auf **Senden**.

Protokolle für fehlgeschlagene Konfigurationen anzeigen

Nachdem Sie ein Abonnement erstellt haben, können Sie den Status des erstellten Abonnements unter **Einstellungen > Observability Integration** anzeigen. Wenn der Status **Fehlgeschlagen** anzeigt, klicken Sie, um Details anzuzeigen.

Klicken Sie unter **Details zum Konfigurationsauftrag** auf **Details anzeigen**.

Klicken Sie auf **Protokolle anzeigen**, um Details des Problems anzuzeigen.

Analytik-Einstellungen konfigurieren

Bevor Sie die Analytik-Funktion in NetScaler Console nutzen, um Einblicke in Ihre Instanz- und Anwendungsdaten zu erhalten, wird empfohlen, einige Analytik-Einstellungen zu konfigurieren, um eine optimale Nutzung dieser Funktion zu gewährleisten.

Schwellenwerte und Warnmeldungen für Analysen erstellen

Sie können Schwellenwerte und Warnmeldungen festlegen, um die Analytik-Metriken der verwalteten virtuellen Server zu überwachen, die auf den erkannten Instanzen konfiguriert sind. Wenn der Wert einer Metrik den Schwellenwert überschreitet, generiert NetScaler Console ein Ereignis, um eine Schwellenwertüberschreitung anzuzeigen.

Sie können den festgelegten Schwellenwerten auch Aktionen zuordnen. Aktionen umfassen die Anzeige einer Warnmeldung auf der GUI und das Senden von E-Mails wie konfiguriert.

Sie können beispielsweise einen Schwellenwert festlegen, um ein Ereignis für HDX™ Insight zu generieren, wenn der ICA-RTT-Wert eines Benutzers 1 Sekunde überschreitet. Sie können auch Warnmeldungen für das generierte Ereignis aktivieren und die Informationen zur Schwellenwertüberschreitung an eine konfigurierte E-Mail-Liste senden.

So erstellen Sie Schwellenwerte und Warnmeldungen für Analysen:

1. Navigieren Sie zu **Einstellungen** > **Analytik-Einstellungen** > **Schwellenwerte**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Klicken Sie auf dem Bildschirm **Schwellenwerte** auf **Hinzufügen**, um einen neuen Schwellenwert hinzuzufügen und Warnmeldungen für die festgelegten Schwellenwerte zu konfigurieren.
3. Geben Sie auf der Seite **Schwellenwerte und Warnmeldungen erstellen** die folgenden Details an:
    - **Name** – Name für die Konfiguration des Schwellenwerts.
    - **Traffic-Typ** – Art des Analytik-Traffics, für den Sie den Schwellenwert konfigurieren möchten. Zum Beispiel: HDX Insight, Security Insight.
    - **Entität** – Kategorie oder Ressourcentyp, für den Sie den Schwellenwert konfigurieren möchten.
    - **Referenzschlüssel** – Automatisch generierter Wert basierend auf dem ausgewählten Traffic-Typ und der Entität.
    - **Dauer** – Intervall, für das Sie den Schwellenwert konfigurieren möchten.
4. Um E-Mail-Benachrichtigungen zu konfigurieren, aktivieren Sie das Kontrollkästchen für die festgelegten Schwellenwerte.
5. Geben Sie im Abschnitt **Regeln** Folgendes an:
    - **Metrik** – Metrik für den ausgewählten Traffic-Typ, um den Schwellenwert zu konfigurieren.
    - **Vergleichsoperator** – Vergleichsoperator für die ausgewählte Metrik (zum Beispiel: \<, \>=).
    - **Wert** – Wert für die Metrik, um den Schwellenwert festzulegen und Warnmeldungen auszulösen.
6. Klicken Sie auf **Erstellen**.

Benachrichtigungen konfigurieren

Sie können einen Benachrichtigungstyp auswählen, um Benachrichtigungen für die folgenden Funktionen zu erhalten:

- **Ereignisse** – Liste der Ereignisse, die für NetScaler-Instanzen generiert werden. Weitere Informationen finden Sie unter Ereignisregelaktionen hinzufügen.
- **Lizenzen** – Liste der Lizenzen, die derzeit aktiv sind, bald ablaufen usw. Weitere Informationen finden Sie unter Der Ablauf der NetScaler Console-Lizenz.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **SSL-Zertifikate** – Liste der SSL-Zertifikate, die NetScaler-Instanzen hinzugefügt werden. Weitere Informationen finden Sie unter Der Ablauf des SSL-Zertifikats

NetScaler Console unterstützt die folgenden Benachrichtigungstypen:

- E-Mail
- SMS
- Slack
- PagerDuty
- ServiceNow

Für jeden Benachrichtigungstyp zeigt die NetScaler Console-GUI die konfigurierte Verteilerliste oder das Profil an. Die NetScaler Console sendet Benachrichtigungen an die ausgewählte Verteilerliste oder das Profil.

E-Mail-Verteilerliste erstellen

Um E-Mail-Benachrichtigungen für NetScaler Console-Funktionen zu erhalten, müssen Sie einen E-Mail-Server und eine Verteilerliste hinzufügen.

Führen Sie die folgenden Schritte aus, um eine E-Mail-Verteilerliste zu erstellen:

1. Navigieren Sie zu **Einstellungen > Benachrichtigungen**.
2. Klicken Sie unter **E-Mail** auf **Hinzufügen**.
3. Geben Sie unter **E-Mail-Verteilerliste erstellen** die folgenden Details an:
    - **Name** – Geben Sie den Namen der Verteilerliste an.
    - **An** – Geben Sie die E-Mail-Adressen an, an die NetScaler Console Nachrichten senden soll.
    - **Cc** – Geben Sie die E-Mail-Adressen an, an die NetScaler Console Nachrichtenkopien senden soll.
    - **Bcc** – Geben Sie die E-Mail-Adressen an, an die NetScaler Console Nachrichtenkopien senden soll, ohne die Adressen anzuzeigen.

4. Klicken Sie auf **Erstellen**.

Wiederholen Sie diesen Vorgang, um mehrere E-Mail-Verteilerlisten zu erstellen. Die Registerkarte **E-Mail** zeigt alle in NetScaler Console vorhandenen E-Mail-Verteilerlisten an.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Erstellen einer SMS-Verteilerliste

Um SMS-Benachrichtigungen für NetScaler Console-Funktionen zu erhalten, müssen Sie einen SMS-Server und Telefonnummern hinzufügen.

Führen Sie die folgenden Schritte aus, um die SMS-Benachrichtigungseinstellungen zu konfigurieren:

1. Navigieren Sie zu **Einstellungen > Benachrichtigungen**.
2. Klicken Sie unter **SMS** auf **Hinzufügen**.
3. Geben Sie unter **SMS-Verteilerliste erstellen** die folgenden Details an:
    - **Name** – Geben Sie den Namen der Verteilerliste an.
    - **SMS-Server** – Wählen Sie den SMS-Server aus, der SMS-Benachrichtigungen sendet.
    - **An** – Geben Sie die Telefonnummer an, an die NetScaler Console Nachrichten senden soll.
4. Klicken Sie auf **Erstellen**.

Wiederholen Sie diesen Vorgang, um mehrere SMS-Verteilerlisten zu erstellen. Die Registerkarte **SMS** zeigt alle in NetScaler Console vorhandenen SMS-Verteilerlisten an.

Slack-Profil erstellen

Um Slack-Benachrichtigungen für NetScaler Console-Funktionen zu erhalten, müssen Sie ein Slack-Profil erstellen.

Führen Sie die folgenden Schritte aus, um ein Slack-Profil zu erstellen:

1. Navigieren Sie zu **Einstellungen > Benachrichtigungen**.
2. Klicken Sie unter **Slack** auf **Hinzufügen**.
3. Geben Sie unter **Slack-Profil erstellen** die folgenden Details an:
    - **Profilname** – Geben Sie den Profilnamen an. Dieser Name wird in der Slack-Profilliste angezeigt.
    - **Kanalname** – Geben Sie den Slack-Kanalnamen an, an den NetScaler Console Benachrichtigungen senden soll.
    - **Webhook-URL** – Geben Sie die Webhook-URL des Kanals an. Eingehende Webhooks sind eine einfache Möglichkeit, Nachrichten von externen Quellen in Slack zu posten. Die URL ist intern mit dem Kanalnamen verknüpft. Und alle an diese URL gesendeten Ereignisbenachrichtigungen werden auf dem dafür vorgesehenen Slack-Kanal gepostet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ein Beispiel für einen Webhook ist wie folgt: `<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`

4. Klicken Sie auf **Erstellen**.

Wiederholen Sie diesen Vorgang, um mehrere Slack-Profile zu erstellen. Die Registerkarte **Slack** zeigt alle in NetScaler Console vorhandenen Slack-Profile an.

Ein PagerDuty-Profil erstellen

Sie können ein PagerDuty-Profil hinzufügen, um die Vorfallbenachrichtigungen basierend auf den PagerDuty-Konfigurationen zu überwachen. PagerDuty ermöglicht es Ihnen, Benachrichtigungen per E-Mail, SMS, Push-Benachrichtigung und Telefonanruf an eine registrierte Nummer zu konfigurieren.

Bevor Sie ein PagerDuty-Profil in NetScaler Console hinzufügen, stellen Sie sicher, dass Sie die erforderlichen Konfigurationen in PagerDuty abgeschlossen haben. Informationen zu den ersten Schritten mit PagerDuty finden Sie in der PagerDuty-Dokumentation.

Führen Sie die folgenden Schritte aus, um ein PagerDuty-Profil zu erstellen:

1. Navigieren Sie zu **Einstellungen > Benachrichtigungen**.
2. Klicken Sie unter **PagerDuty** auf **Hinzufügen**.
3. Geben Sie unter **PagerDuty-Profil erstellen** die folgenden Details an:
   - **Profilname** – Geben Sie einen Profilnamen Ihrer Wahl an.
   - **Integrationsschlüssel** – Geben Sie den Integrationsschlüssel an. Diesen Schlüssel erhalten Sie über Ihr PagerDuty-Portal.
4. Klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie unter Dienste und Integrationen in der PagerDuty-Dokumentation.

Wiederholen Sie diesen Vorgang, um mehrere PagerDuty-Profile zu erstellen. Die Registerkarte **PagerDuty** zeigt alle in NetScaler Console vorhandenen PagerDuty-Profile an.

ServiceNow-Profil anzeigen

Wenn Sie ServiceNow-Benachrichtigungen für NetScaler-Ereignisse und NetScaler Console-Ereignisse aktivieren möchten, müssen Sie NetScaler Console mithilfe des ITSM-Connectors in

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ServiceNow integrieren. Weitere Informationen finden Sie unter NetScaler Console in die ServiceNow-Instanz integrieren.

Führen Sie die folgenden Schritte aus, um das ServiceNow-Profil anzuzeigen und zu überprüfen:

1. Navigieren Sie zu **Einstellungen > Benachrichtigungen**.
2. Wählen Sie unter **ServiceNow** das Profil **Citrix_Workspace_SN** aus der Liste aus.
3. Klicken Sie auf **Testen**, um ein ServiceNow-Ticket automatisch zu generieren und die Konfiguration zu überprüfen.

   Wenn Sie ServiceNow-Tickets in der NetScaler Console-GUI anzeigen möchten, wählen Sie **ServiceNow-Tickets** aus.

Berichte exportieren oder den Export planen

In NetScaler Console können Sie einen umfassenden Bericht für die ausgewählte NetScaler Console-Funktion exportieren. Dieser Bericht bietet Ihnen einen Überblick über die Zuordnung zwischen den Instanzen, Partitionen und entsprechenden Details.

NetScaler Console zeigt funktionsspezifische geplante Exportberichte unter den einzelnen NetScaler Console-Funktionen an, die Sie anzeigen, bearbeiten oder löschen können. Um beispielsweise die Exportberichte von NetScaler-Instanzen anzuzeigen, navigieren Sie zu **Infrastruktur > Instanzen > NetScaler** und klicken Sie auf das Exportsymbol. Sie können diese Berichte im PDF-, JPEG-, PNG- und CSV-Dateiformat exportieren.

Unter **Berichte exportieren** können Sie die folgenden Aktionen ausführen:

- Einen Bericht auf einen lokalen Computer exportieren
- Exportberichte planen
- Geplante Exportberichte anzeigen, bearbeiten oder löschen

Einen Bericht exportieren

Um einen Bericht von der NetScaler Console auf den lokalen Computer zu exportieren, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf das Exportsymbol in der oberen rechten Ecke der Seite.
2. Wählen Sie **Jetzt exportieren**.
3. Wählen Sie eine der folgenden Exportoptionen aus:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Snapshot** – Diese Option exportiert NetScaler Console-Berichte als Snapshot.
- **Tabellarisch** – Diese Option exportiert NetScaler Console-Berichte in einem tabellarischen Format. Sie können auch auswählen, wie viele Datensätze in einem tabellarischen Format exportiert werden sollen.

4. Wählen Sie das Dateiformat aus, in dem Sie den Bericht auf Ihrem lokalen Computer speichern möchten.
5. Klicken Sie auf **Exportieren**.

Exportbericht planen

Um den Exportbericht in regelmäßigen Abständen zu planen, geben Sie das Wiederholungsintervall an. NetScaler Console sendet den exportierten Bericht an das konfigurierte E-Mail- oder Slack-Profil.

1. Klicken Sie auf das Exportsymbol in der oberen rechten Ecke der Seite.
2. Wählen Sie **Export planen** und geben Sie Folgendes an:
   - **Betreff** – Standardmäßig wird dieses Feld automatisch mit dem Namen der ausgewählten Funktion ausgefüllt. Sie können es jedoch mit einem aussagekräftigen Titel überschreiben.
   - **Exportoption** – Exportieren Sie NetScaler Console-Berichte in einem Snapshot- oder Tabellenformat. Sie können auch auswählen, wie viele Datensätze in einem Tabellenformat exportiert werden sollen.
   - **Format** – Wählen Sie das Dateiformat aus, in dem Sie den Bericht im konfigurierten E-Mail- oder Slack-Profil erhalten möchten.
   - **Wiederholung** – Wählen Sie **Täglich**, **Wöchentlich** oder **Monatlich** aus der Liste aus.
   - **Beschreibung** – Geben Sie eine aussagekräftige Beschreibung für einen Bericht an.
   - **Exportzeit** – Geben Sie an, wann der Bericht exportiert werden soll.
   - **E-Mail** – Aktivieren Sie das Kontrollkästchen und wählen Sie das Profil aus der Liste aus. Wenn Sie ein Profil hinzufügen möchten, klicken Sie auf **Hinzufügen**.
   - **Slack** – Aktivieren Sie das Kontrollkästchen und wählen Sie das Profil aus der Liste aus. Wenn Sie ein Profil hinzufügen möchten, klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **Planen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Geplante Exportberichte anzeigen und bearbeiten

Um die Exportberichte anzuzeigen, führen Sie folgende Schritte aus:

1. Klicken Sie auf das Exportsymbol in der oberen rechten Ecke der Seite.

   Die Seite **Exportbericht** zeigt alle funktionsspezifischen Exportberichte an.
2. Wählen Sie den Bericht aus, den Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.

Globale Einstellungen

Die **globalen Einstellungen** in NetScaler Console ermöglichen Ihnen die Konfiguration systemweiter Optionen, die für Ihre verwalteten NetScaler-Instanzen gelten. Verwenden Sie diese Einstellungen, um Instanzeinstellungen, Systemkonfigurationen, E-Mail-Abonnements zu verwalten und NetScaler Console-Funktionen zu aktivieren oder zu deaktivieren.

Sie können die folgenden globalen Einstellungen konfigurieren:

- Instanzeinstellungen
- Systemkonfigurationen
- E-Mail-Abonnements
- NetScaler Console-Funktionen aktivieren oder deaktivieren

Instanzeinstellungen

Sie können die erkannten Instanzen in NetScaler Console verwalten und die Sicherungseinstellungen für Instanzen konfigurieren.

Instanzkonfiguration verwalten

Unter **Einstellungen > Globale Einstellungen > Instanzeinstellungen > Instanzverwaltung** können Sie die folgenden Instanzkonfigurationen ändern:

- **Kommunikation mit Instanz(en)** – Sie können einen HTTP- oder HTTPS-Kommunikationskanal zwischen NetScaler Console und den erkannten Instanzen auswählen.
- **Zertifikat-Download aktivieren** – Ermöglicht Ihnen das Herunterladen der SSL-Zertifikate von einer erkannten Instanz.
- **Anmeldeinformationen für die Instanzanmeldung anfordern** – Wenn Sie über die NetScaler Console-GUI auf die Instanz zugreifen, wird die Anmeldeseite der Instanz angezeigt. Geben Sie Ihre Anmeldeinformationen ein, um auf eine Instanz zuzugreifen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instanz-Sicherungseinstellungen konfigurieren

Unter **Einstellungen > Globale Einstellungen > Instanzeinstellungen > Instanzsicherung** können Sie die Sicherungseinstellungen für die erkannten NetScaler-Instanzen in NetScaler Console konfigurieren.

Wählen Sie unter **Instanz-Sicherungseinstellungen konfigurieren** die Option **Instanzsicherungen aktivieren**.

- **Anzahl der aufzubewahrenden Sicherungsdateien**: Geben Sie die Anzahl der in der NetScaler Console aufzubewahrenden Sicherungsdateien an. Sie können bis zu 3 Sicherungsdateien pro NetScaler-Instanz aufbewahren. Der Standardwert ist 1 Sicherungsdatei.
- **Einstellungen für die Sicherungsplanung** – Sie können eine Instanzsicherung auf zwei Arten planen:
  - **Intervallbasiert** – Eine Sicherungsdatei wird in NetScaler Console erstellt, nachdem das angegebene Intervall abgelaufen ist. Das Standard-Sicherungsintervall beträgt 12 Stunden.
  - **Zeitbasiert** – Geben Sie die Uhrzeit im `hours:minutes`-Format an, zu der NetScaler Console die Instanzsicherung durchführen soll.
- **NetScaler-Einstellungen** – Mit dieser Option können Sie eine Sicherung basierend auf dem Trap initiieren und GeoDB-Dateien in die Sicherung aufnehmen. Diese Einstellung gilt für MPX-, VPX-, CPX- und BLX-Instanzen.
  - **Instanz-Backup durchführen, wenn NetScalerConfigSave-Trap empfangen wird** – Standardmäßig erstellt NetScaler Console keine Sicherungsdatei, wenn es den „NetScalerConfigSave“-Trap empfängt. Sie können jedoch die Option aktivieren, eine Sicherungsdatei zu erstellen, wann immer eine NetScaler-Instanz einen `NetScalerConfigSave` Trap an NetScaler Console sendet.

    Eine NetScaler-Instanz sendet `NetScalerConfigSave` jedes Mal, wenn die Konfiguration auf der Instanz gespeichert wird.

    Geben Sie die **Backup-Verzögerung bei Trap** in Minuten an. Wenn der empfangene `NetScalerConfigSave` Trap für die angegebene Minutenzahl auf NetScaler Console bestehen bleibt, sichert NetScaler Console die Instanz.
  - **GeoDB-Dateien einschließen** – Standardmäßig sichert NetScaler Console die GeoDatabase-Dateien nicht. Sie können die Option aktivieren, auch eine Sicherung dieser Dateien zu erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **NetScaler SDX-Einstellungen** – Um SDX-Instanzen zu sichern, geben Sie das **Backup-Timeout** in Minuten an. Während eines SDX-Instanz-Backups wird die Verbindung zwischen NetScaler Console und SDX für den angegebenen Zeitraum aufrechterhalten.

  Bei großen SDX-Sicherungsdateien sollte die Verbindung zwischen NetScaler Console und der SDX-Instanz über einen längeren Zeitraum aufrechterhalten werden, um die Sicherung abzuschließen.

  WICHTIG:

  Das Backup schlägt fehl, wenn die Verbindung abbricht.

- **Externer Transfer** – NetScaler Console ermöglicht Ihnen, die NetScaler-Instanz-Sicherungsdateien an einen externen Speicherort zu übertragen:

  a. Geben Sie die IP-Adresse des Speicherorts an.

  b. Geben Sie den Benutzernamen und das Kennwort des externen Servers an, auf den Sie die Sicherungsdateien übertragen möchten.

  c. Geben Sie das Übertragungsprotokoll und die Portnummer an.

  d. Geben Sie den Verzeichnispfad an, in dem die Datei gespeichert werden soll.

  e. Wenn Sie die Sicherungsdatei löschen möchten, nachdem Sie die Datei auf einen externen Server übertragen haben, wählen Sie **Datei nach Übertragung aus Application Delivery Management löschen**.

Benachrichtigungen für verwaltete Geräte deaktivieren

Administratoren können Benachrichtigungen für bestimmte verwaltete Geräte während Wartungs- und Fehlerbehebungsfenstern vorübergehend deaktivieren. Durch das Deaktivieren von Benachrichtigungen können Sie vermeiden, unnötige Warnungen und Benachrichtigungen bezüglich gerätespezifischer Probleme und Statusaktualisierungen während dieser Intervalle zu erhalten.

Administratoren können einzelne Geräte auswählen, einschließlich primärer, sekundärer oder spezifischer Clusterknoten. Wenn eine VPX-Instanz auf SDX ausgeführt wird, werden VPX und SDX für die Benachrichtigungskonfiguration als separate Entitäten behandelt. Wenn das Fenster zum Deaktivieren von Benachrichtigungen für ein Gerät konfiguriert ist, gilt die Konfiguration auch für Gerätepartitionen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Während dieser Intervalle werden Ereignisse zwar verarbeitet, aber es werden keine Benachrichtigungen (E-Mail, Slack, PagerDuty) an Administratoren für die ausgewählten Geräte gesendet. Dieses Verhalten gilt sowohl für gerätespezifische Ereignisse (wie Konfigurationsänderungen, Entity-Down-Warnungen) als auch für von der Konsole generierte Ereignisse (wie Statusabfragen, Schwellenwertüberschreitungen).

Führen Sie die folgenden Schritte aus, um Benachrichtigungen für bestimmte verwaltete Geräte zu deaktivieren:

1. Navigieren Sie zu **Settings > Administration > Instance Settings** und klicken Sie auf **Notification Disable Windows**.
2. Klicken Sie unter **Notification Disable Windows** auf **Add**.
3. Klicken Sie unter **Add Notification Disable Windows** auf **Add Instances** und wählen Sie die erforderlichen Instanzen aus. Klicken Sie auf **Ok**.
4. Wählen Sie Datum und Uhrzeit für **Start Date**, **Start Time**, **End Date** und **End Time** aus.
5. Fügen Sie einen Kommentar hinzu (optional) und klicken Sie auf **Create**. Das Fenster zum Deaktivieren von Benachrichtigungen wird auf der Seite **Notification Disable Windows** angezeigt.

Sie können diese Fenster zum Deaktivieren von Benachrichtigungen auch bearbeiten oder löschen. Sie können auch auf **History** klicken, um die historischen Details der Fenster zum Deaktivieren von Benachrichtigungen anzuzeigen.

Systemkonfigurationen

Sie können das Keep-Alive-Intervall des NetScaler Console-Agenten und die Zeitzone des NetScaler Console-Servers ändern.

Keep-Alive-Intervall des Agenten festlegen

Der NetScaler Console-Server und der Agent halten dieselbe TCP-Verbindung für das angegebene Keep-Alive-Intervall aufrecht. Ein Agent verwendet diese Verbindung, um die Daten der verwalteten Instanzen an den NetScaler Console-Server zu senden.

1. Navigieren Sie zu **Einstellungen > Globale Einstellungen**.
2. Wählen Sie **Agent und Zeitzone** unter **Systemkonfigurationen**.
3. Geben Sie unter **Agent** das Keep-Alive-Intervall zwischen 30 und 120 Sekunden an.
4. Klicken Sie auf **Speichern**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console-Zeitzone festlegen

Sie können die Zeitzone auswählen, in der Sie die Zeit auf der NetScaler Console-Webseite, in Benachrichtigungen und Berichten anzeigen möchten.

1. Navigieren Sie zu **Einstellungen > Globale Einstellungen**.
2. Wählen Sie **Agent und Zeitzone** unter **Systemkonfigurationen**.
3. Wählen Sie unter **Zeitzone** die lokale oder GMT-Zeitzone aus, um die Zeit in NetScaler Console anzuzeigen.
4. Klicken Sie auf **Speichern**.

E-Mail-Abonnements

NetScaler Console sendet E-Mail-Benachrichtigungen an alle inaktiven und neuen Benutzer.

Inaktive Kunden erhalten eine E-Mail-Benachrichtigung, wenn:

- NetScaler-Instanzen nicht konfiguriert sind
- Die Mandantenlizenz in weniger als 30 Tagen abläuft

HINWEIS:

Standardmäßig erhalten alle derartigen inaktiven Kunden eine E-Mail-Benachrichtigung.

Neue Kunden erhalten eine E-Mail von NetScaler Console, in der sie eingeladen werden, die NetScaler-Instanzen in den NetScaler Console-Dienst zu integrieren, wo sie kritische Ereignisse auf NetScaler-Instanzen verwalten und überwachen, Fehler beheben und Aufgaben wie die NetScaler-Konfiguration automatisieren können.

E-Mail-Benachrichtigungen abbestellen

Sie können E-Mail-Benachrichtigungen, die Sie vom NetScaler Console-Dienst erhalten, abonnieren oder abbestellen. So **bestellen Sie E-Mail-Benachrichtigungen ab**:

1. Navigieren Sie in NetScaler Console zu **Einstellungen > Globale Einstellungen > Systemkonfigurationen**, und klicken Sie dann auf **E-Mail-Abonnements**. Das Fenster **E-Mail-Benachrichtigungen abbestellen** wird angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

Standardmäßig befindet sich der Umschalter zum Deaktivieren von E-Mail-Benachrichtigungen in der Aus-Position, und die E-Mail-Benachrichtigungen sind für alle inaktiven Benutzer aktiviert.

2. Aktivieren Sie im Fenster **E-Mail-Benachrichtigungen abbestellen** die Umschalttaste. Klicken Sie auf **OK**.

Sie haben die E-Mail-Benachrichtigungen nun abbestellt und erhalten keine E-Mails mehr zum Onboarding von NetScaler-Instanzen.

Funktionen aktivieren oder deaktivieren

Als Administrator können Sie die folgenden Funktionen auf der Seite **Einstellungen > Globale Einstellungen > Konfigurierbare Funktionen** aktivieren oder deaktivieren:

- **Agent-Failover** – Das Agent-Failover kann an einem Standort auftreten, der zwei oder mehr aktive Agents hat. Wenn ein Agent an diesem Standort inaktiv wird (DOWN-Status), verteilt die NetScaler Console die NetScaler-Instanzen des inaktiven Agents auf andere aktive Agents um. Weitere Informationen finden Sie unter NetScaler-Agent-Agents für die Bereitstellung an mehreren Standorten konfigurieren.
- **Entitäts-Polling-Netzwerkfunktion** – Eine Entität ist entweder eine Richtlinie, ein virtueller Server, ein Dienst oder eine Aktion, die an eine NetScaler-Instanz angehängt ist. Standardmäßig fragt die NetScaler Console konfigurierte Netzwerkfunktionsentitäten alle 60 Minuten automatisch ab. Weitere Informationen finden Sie unter Polling-Übersicht.
- **Instanzsicherung** – Sichern Sie den aktuellen Zustand einer NetScaler-Instanz und verwenden Sie später die gesicherten Dateien, um die NetScaler-Instanz in denselben Zustand wiederherzustellen. Weitere Informationen finden Sie unter Sichern und Wiederherstellen von NetScaler-Instanzen.
- **Instanzkonfigurationsprüfung** – Überwachen Sie Konfigurationsänderungen über verwaltete NetScaler-Instanzen hinweg, beheben Sie Konfigurationsfehler und stellen Sie nicht gespeicherte Konfigurationen wieder her. Weitere Informationen finden Sie unter Audit-Vorlagen erstellen.
- **Instanzereignisse** – Ereignisse stellen das Auftreten von Ereignissen oder Fehlern auf einer verwalteten NetScaler-Instanz dar. In der NetScaler Console empfangene Ereignisse werden auf der Seite **Ereignisübersicht** (**Infrastruktur > Ereignisse**) angezeigt. Und alle aktiven

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ereignisse werden auf der Seite Ereignismeldungen (**Infrastruktur > Ereignisse > Ereignismeldungen**) angezeigt. Weitere Informationen finden Sie unter Ereignisse.

- **Instanz-Netzwerkberichterstattung** – Sie können Berichte für Instanzen auf globaler Ebene generieren. Auch für Entitäten wie virtuelle Server und Netzwerkschnittstellen. Weitere Informationen finden Sie unter Netzwerkberichterstattung.
- **Instanz-SSL-Zertifikate** – Die NetScaler Console bietet eine zentralisierte Ansicht der auf allen verwalteten NetScaler-Instanzen installierten SSL-Zertifikate. Weitere Informationen finden Sie unter SSL-Dashboard.
- **Instanz-Syslog** – Sie können die auf Ihren NetScaler-Instanzen generierten Syslog-Ereignisse überwachen, wenn Sie Ihr Gerät so konfiguriert haben, dass alle Syslog-Meldungen an die NetScaler Console umgeleitet werden. Weitere Informationen finden Sie unter Konfigurieren von Syslog auf Instanzen.

Um eine Funktion zu aktivieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie die Funktion aus der Liste aus, die Sie aktivieren möchten.
2. Klicken Sie auf **Aktivieren**.

WICHTIG:

Wenn eine Funktion deaktiviert ist, kann der Benutzer die mit dieser Funktion verbundenen Vorgänge nicht ausführen.

Eine Aktionsrichtlinie zum Empfangen von Anwendungsereignisbenachrichtigungen konfigurieren

Abgesehen von der bestehenden Analyseansicht von Anwendungsereignissen können Sie eine Aktionsrichtlinie konfigurieren, um Anwendungsereignisbenachrichtigungen über Slack, E-Mail, PagerDuty oder ServiceNow zu erhalten. Die Anwendungsereignisse umfassen Leistungsprobleme, Bot- und WAF-Verletzungen sowie Service-Graph-Verletzungen. Als Administrator können Sie mithilfe der Aktionsrichtlinie Ereignisbenachrichtigungen in Echtzeit erhalten.

Mithilfe der Aktionsrichtlinie können Sie:

- Bestimmte Bedingungen für die Anwendungsereignisse vordefinieren.
- Benachrichtigungen für die folgenden Ereignisse über Slack, E-Mail, PagerDuty und ServiceNow erhalten:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EREIGNISKATEGORIEN	EREIGNISUNTERKATEGORIEN	EREIGNISSE
Sicherheitsverletzungen	Alle Sicherheitsverletzungen	Alle Bot-Verletzungen (Weitere Informationen zur Liste der Bot-Verletzungen finden Sie unter Verletzungskategorien).
		Alle WAF-Verletzungen (WAF-SQL-Verletzungen, WAF-XSS-Verletzungen und WAF-Infer-XML-Verletzungen)
	Alle Sicherheitsverletzungen pro Client	Bot-Verletzungen pro Client
		WAF-Verletzungen pro Client
		Hinweis: Um die WAF-Verletzungsbenachrichtigung zu erhalten, müssen die minimalen Verletzungstransaktionen 20 % betragen. Zum Beispiel müssen von 100 Transaktionen mindestens 20 Verletzungstransaktionen sein.
Anwendungsleistung		Verletzung des App-Scores
		Client-Netzwerklatenz
		Server-Netzwerklatenz
		Server-Verarbeitungszeit
		Antwortzeit
		Anfragen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EREIGNISKATEGORIEN	EREIGNISUNTERKATEGORIEN	EREIGNISSE
		Bandbreite
		Verletzung des Dienstgraphen
Anwendungsnutzung		Anfragen pro Sekunde
		Durchsatz
		Datenvolumen

Eine Aktionsrichtlinie konfigurieren

1. Navigieren Sie zu **Einstellungen > Aktion > Aktionsrichtlinien**.
2. Klicken Sie auf **Hinzufügen**.
3. Auf der Seite **Aktionsrichtlinie erstellen**:

    a. **Richtlinienname** – Geben Sie einen Richtliniennamen Ihrer Wahl ein.

    b. **Aktiviert** – Diese Option ist standardmäßig ausgewählt.

    c. Wenn das **folgende Ereignis eintritt** – Wählen Sie aus der Liste ein Ereignis aus.

    d. **Und die folgende Bedingung erfüllt ist** – Wählen Sie aus der Liste aus, um eine Bedingung zu definieren, für die Sie benachrichtigt werden möchten. Sie können auf **+** klicken, um weitere Bedingungen hinzuzufügen. Um eine Bedingung zu entfernen, klicken Sie auf **–**.

    Sie können die Aktionsrichtlinie mit den folgenden Operatoren konfigurieren. Die Operatoren werden basierend auf den von Ihnen ausgewählten Bedingungen angezeigt.

OPERATOR	BESCHREIBUNG
Gleich	Gleich einem definierten Wert
Ungleich	Ungleich einem definierten Wert
Größer als	Größer als ein definierter Wert

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPERATOR	BESCHREIBUNG
Größer als oder gleich	Größer als oder gleich einem definierten Wert
Kleiner als	Kleiner als ein definierter Wert
Kleiner als oder gleich	Kleiner als oder gleich einem definierten Wert
Enthält	Enthält den definierten Begriff oder Wert
Beginnt mit	Beginnt mit einem definierten Begriff oder Wert
Endet mit	Endet mit einem definierten Begriff oder Wert
IN	Ermöglicht die Auswahl mehrerer Werte

e. **Gehen Sie dann wie folgt vor** – Wählen Sie **Benachrichtigen**. Nachdem Sie **Benachrichtigen** ausgewählt haben, wird die Option Benachrichtigungstyp angezeigt.

f. **Benachrichtigungstyp** – Wählen Sie den Benachrichtigungstyp E-Mail, Slack, PagerDuty oder ServiceNow. Je nach ausgewähltem Benachrichtigungstyp wird die entsprechende Option (Verteilerliste, Slack-Profil, PagerDuty-Profil oder ServiceNow-Profil) angezeigt. Wählen Sie ein Profil aus der Liste aus.

   Wenn Sie ein neues Profil erstellen möchten, klicken Sie auf **Hinzufügen**.

g. Klicken Sie auf **Richtlinie erstellen**.

   Die Richtlinie ist konfiguriert. Sie können die konfigurierten Richtliniendetails anzeigen.

   Nachdem Sie die Richtlinie konfiguriert haben, können Sie die Richtlinie auswählen und klicken auf:

   - **Bearbeiten**, um die Aktionsrichtlinie zu aktualisieren oder zu ändern. Klicken Sie nach der Aktualisierung auf Richtlinie aktualisieren.
   - **Löschen**, um die Aktionsrichtlinie zu entfernen. Sie können mehrere Richtlinien auswählen und auf **Löschen** klicken, um sie zu entfernen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Aktionsverlauf**, um Details wie Uhrzeit, durchgeführte Aktion, Richtlinienname, Warnungstyp und Warnmeldung anzuzeigen.

Die folgende Tabelle beschreibt die Details der Aktionsrichtlinienkonfiguration.

VERLETZUNGSNAME	BEDINGUNG	BESCHREIBUNG
Alle Sicherheitsverletzungen	Instanz-IP	IP-Adresse der NetScaler-Instanz. Wählen Sie die IP-Adresse aus der Liste aus.
	Verstoßanzahl	Die Anzahl der Verstöße, bei der Sie benachrichtigt werden möchten. Wenn Sie beispielsweise die Verstoßanzahl als kleiner oder gleich 10 konfigurieren, werden Sie benachrichtigt, wenn 10 oder weniger Bot-Verstoßtransaktionen empfangen werden.
	Verstoßverhältnis	Dieser Wert gibt die Gesamtanzahl der Verstöße aus bestimmten Transaktionen an, und der Wert muss zwischen 0 und 1 liegen. Wenn beispielsweise von 100 Transaktionen 20 Verstöße sind und Sie für ein solches Szenario benachrichtigt werden möchten, müssen Sie 0,2 eingeben.
Alle Bot-Verstöße	Bot-Profil	Der Bot-Profilname, der für die Konfiguration des Bot-Managements auf der NetScaler-Instanz verwendet wird.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERLETZUNGSNAME	BEDINGUNG	BESCHREIBUNG
	Instanz-IP	IP-Adresse der NetScaler-Instanz. Wählen Sie die IP-Adresse aus der Liste aus.
	Verstoßanzahl	Die Anzahl der Verstöße, bei der Sie benachrichtigt werden möchten. Wenn Sie beispielsweise die Verstoßanzahl als kleiner oder gleich 10 konfigurieren, werden Sie benachrichtigt, wenn 10 oder weniger Bot-Verstoßtransaktionen empfangen werden.
	Verstoßverhältnis	Dieser Wert gibt die Gesamtanzahl der Verstöße aus bestimmten Transaktionen an, und der Wert muss zwischen 0 und 1 liegen. Wenn beispielsweise von 100 Transaktionen 20 Verstöße sind und Sie für ein solches Szenario benachrichtigt werden möchten, müssen Sie 0,2 eingeben.
Alle WAF-Verletzungen, WAF-SQL-Verletzung, WAF-XSS-Verletzung, WAF-Infer-XML-Verletzung	WAF-Profil	Der WAF-Profilname, der für die Konfiguration der WAF-Sicherheitseinstellungen auf der NetScaler-Instanz verwendet wird.
	Instanz-IP	IP-Adresse der NetScaler-Instanz. Wählen Sie die IP-Adresse aus der Liste aus.
	Anzahl der Verletzungen	Die Anzahl der Verletzungen, über die Sie benachrichtigt werden möchten. Die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERLETZUNGSNAME	BEDINGUNG	BESCHREIBUNG
		Mindestanforderung für die Benachrichtigung über WAF-Verletzungen beträgt 20 %.
	Verletzungsverhältnis	Dieser Wert gibt die Gesamtanzahl der Verletzungen aus bestimmten Transaktionen an und muss zwischen 0 und 1 liegen. Wenn beispielsweise von 100 Transaktionen 20 WAF-SQL-Verletzungstransaktionen sind und Sie für ein solches Szenario benachrichtigt werden möchten, müssen Sie 0,2 eingeben.
Alle Sicherheitsverletzungen pro Client	Anwendungsname	Der benutzerdefinierte Anwendungsname. Wählen Sie die Anwendung aus der Liste aus. Wenn Sie diese Bedingung nicht hinzufügen, werden alle Anwendungen der NetScaler-Instanz berücksichtigt.
	Instanz-IP	IP-Adresse der NetScaler-Instanz. Wählen Sie die IP-Adresse aus der Liste aus.
	Client-IP	Die Quelle, von der der Bot stammt. Geben Sie die IP-Adresse an.
	Gesamtzahl der Angriffe	Die Gesamtzahl der Angriffe, über die Sie benachrichtigt werden möchten.
	Anforderungs-URL	Die URL, die Sie zum Blockieren konfigurieren

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERLETZUNGSNAME	BEDINGUNG	BESCHREIBUNG
		möchten. Geben Sie die URL an.
	Vserver-Name	Die zugehörigen Anwendungen, die für benutzerdefinierte Anwendungen konfiguriert sind. Wählen Sie die Anwendung aus der Liste aus. Wenn Sie diese Bedingung nicht hinzufügen, werden alle Anwendungen der NetScaler-Instanz berücksichtigt.
Bot-Verstöße pro Client	Anwendungsname	Der Name der benutzerdefinierten Anwendung. Wählen Sie die Anwendung aus der Liste aus. Wenn Sie diese Bedingung nicht hinzufügen, werden alle Anwendungen der NetScaler-Instanz berücksichtigt.
	Instanz-IP	IP-Adresse der NetScaler-Instanz. Wählen Sie die IP-Adresse aus der Liste aus.
	Client-IP	Die Quelle, von der der Bot stammt. Geben Sie die IP-Adresse an.
	Gesamtzahl der Angriffe	Die Gesamtzahl der Angriffe, über die Sie benachrichtigt werden möchten.
	Verletzungstyp	Wählen Sie die Bot-Verletzung aus der Liste aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERLETZUNGSNAME	BEDINGUNG	BESCHREIBUNG
	Anforderungs-URL	Die URL, die Sie zum Blockieren konfigurieren möchten. Geben Sie die URL an.
	Vserver-Name	Die zugehörigen Anwendungen, die für benutzerdefinierte Anwendungen konfiguriert sind. Wählen Sie die Anwendung aus der Liste aus. Wenn Sie diese Bedingung nicht hinzufügen, werden alle Anwendungen der NetScaler-Instanz berücksichtigt.
WAF-Verletzungen pro Client	Anwendungsname	Der Name der benutzerdefinierten Anwendung. Wählen Sie die Anwendung aus der Liste aus. Wenn Sie diese Bedingung nicht hinzufügen, werden alle Anwendungen der NetScaler-Instanz berücksichtigt.
	Instanz-IP	IP-Adresse der NetScaler-Instanz. Wählen Sie die IP-Adresse aus der Liste aus.
	Client-IP	Die Quelle, von der der Bot stammt. Geben Sie die IP-Adresse an.
	Gesamtzahl der Angriffe	Die Gesamtzahl der Angriffe, für die Sie benachrichtigt werden möchten.
	Verletzungstyp	Wählen Sie die WAF-Verletzung aus der Liste aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERLETZUNGSNAME	BEDINGUNG	BESCHREIBUNG
	Anforderungs-URL	Die URL, die Sie zum Blockieren konfigurieren möchten. Geben Sie die URL an.
	Vserver-Name	Die zugehörigen Anwendungen, die für benutzerdefinierte Anwendungen konfiguriert sind. Wählen Sie die Anwendung aus der Liste aus. Wenn Sie diese Bedingung nicht hinzufügen, werden alle Anwendungen der NetScaler-Instanz berücksichtigt.
App-Score-Verletzung	Leistungsindikator	Die App-Score-Komponenten und ihre Schwellenwerte. Wählen Sie die App-Score-Komponente aus der Liste aus. Weitere Informationen finden Sie unter App-Score-Komponenten auswählen und Schwellenwerte festlegen.
	Anzahl der Verstöße	Die Anzahl der Verstöße, für die Sie benachrichtigt werden möchten. Wenn Sie beispielsweise die Anzahl der Verstöße für die Antwortzeit auf 5 festlegen, werden Sie benachrichtigt, wenn der Schwellenwert für die Antwortzeit 5 Mal überschritten wird.
	Anwendungsname	Klicken Sie auf **Anwendungen auswählen**, um die Anwendungen auszuwählen, für die Sie über

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERLETZUNGSNAME	BEDINGUNG	BESCHREIBUNG
		die Verletzung benachrichtigt werden möchten.
Client-Netzwerklatenz	Durchschnittliche Client-Netzwerklatenz	Geben Sie den Client-Latenzwert (Client zu NetScaler) in Millisekunden an, für den Sie benachrichtigt werden möchten.
	Client-Netzwerklatenz-Anomalien	Geben Sie die Anzahl der Anomalien für die Netzwerklatenz an, über die Sie benachrichtigt werden möchten.
	Anwendungsname	Klicken Sie auf **Anwendungen auswählen**, um die Anwendungen auszuwählen, für die Sie über die Verletzung benachrichtigt werden möchten.
Server-Netzwerklatenz	Durchschnittliche Server-Netzwerklatenz	Geben Sie den Server-Latenzwert (Server zu NetScaler) in Millisekunden an, für den Sie benachrichtigt werden möchten.
	Server-Netzwerklatenz-Anomalien	Geben Sie die Anzahl der Anomalien für die Netzwerklatenz an, über die Sie benachrichtigt werden möchten.
	Anwendungsname	Klicken Sie auf **Anwendungen auswählen**, um die Anwendungen auszuwählen, für die Sie über die Verletzung benachrichtigt werden möchten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERLETZUNGSNAME	BEDINGUNG	BESCHREIBUNG
Antwortzeit	Durchschnittliche Antwortzeit	Geben Sie den Wert (in Millisekunden) an, für den Sie benachrichtigt werden möchten.
	Anomalien der durchschnittlichen Antwortzeit	Geben Sie die Anzahl der Anomalien an, für die Sie benachrichtigt werden möchten.
	Anwendungsname	Klicken Sie auf **Anwendungen auswählen**, um die Anwendungen auszuwählen, für die Sie benachrichtigt werden möchten. Wenn Sie keine Anwendung auswählen, wird dies auf alle Anwendungen angewendet.
Anfragen	Gesamtanfragen	Geben Sie die Gesamtzahl der Anfragen an, für die Sie benachrichtigt werden möchten.
	Anwendungsname	Klicken Sie auf **Anwendungen auswählen**, um die Anwendungen auszuwählen, für die Sie benachrichtigt werden möchten. Wenn Sie keine Anwendung auswählen, wird dies auf alle Anwendungen angewendet.
Bandbreite	Gesamtbandbreite	Geben Sie die Bandbreite (MB) an, für die Sie benachrichtigt werden möchten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERLETZUNGSNAME	BEDINGUNG	BESCHREIBUNG
	Anwendungsname	Klicken Sie auf **Anwendungen auswählen**, um die Anwendungen auszuwählen, für die Sie benachrichtigt werden möchten. Wenn Sie keine Anwendung auswählen, wird dies auf alle Anwendungen angewendet.
Server-Verarbeitungszeit	Durchschnittliche Server-Verarbeitungszeit	Geben Sie den Wert für die Serververarbeitung (Server zu NetScaler) in Millisekunden an, für den Sie benachrichtigt werden möchten.
	Anomalien der Server-Verarbeitungszeit	Geben Sie die Anzahl der Anomalien für die Server-Verarbeitungszeit an, über die Sie benachrichtigt werden möchten.
	Anwendungsname	Klicken Sie auf **Anwendungen auswählen**, um die Anwendungen auszuwählen, für die Sie über die Verletzung benachrichtigt werden möchten.
Service-Graph-Verletzung		Microservices, die die konfigurierten Schwellenwerte überschreiten. Weitere Informationen finden Sie unter Schwellenwerte im Service-Graph konfigurieren.
Anfragen pro Sekunde	Durchschnittliche Anfragen pro Sekunde	Die Anzahl der Anfragen, die die Anwendung pro Sekunde empfängt. Geben Sie den

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERLETZUNGSNAME	BEDINGUNG	BESCHREIBUNG
		Durchschnittswert an, um benachrichtigt zu werden.
	Anomalien des Durchschnitts der Anfragen pro Sekunde	Geben Sie die durchschnittliche Anzahl der Anomalien an, für die Sie benachrichtigt werden möchten.
		Hinweis: Wenn Sie für dieses Ereignis eine UND-Bedingung verwenden, können Sie entweder „Durchschnittliche Anfragen pro Sekunde“ und „Anwendungsname“ oder „Durchschnittliche Anomalien der Anfragen pro Sekunde“ und „Anwendungsname“ konfigurieren.
	Anwendungsname	Klicken Sie auf **Anwendungen auswählen**, um die Anwendungen auszuwählen, für die Sie über die Verletzung benachrichtigt werden möchten.
Durchsatz	Durchschnittlicher Durchsatz	Die über einen bestimmten Zeitraum übermittelten Gesamtdaten. Geben Sie den Durchschnittswert (in MB) an, um benachrichtigt zu werden.
	Durchschnittliche Durchsatzanomalien	Geben Sie die durchschnittliche Anzahl der Anomalien an, für die Sie benachrichtigt werden möchten.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERLETZUNGSNAME	BEDINGUNG	BESCHREIBUNG
		Hinweis: Wenn Sie für dieses Ereignis die UND-Bedingung verwenden, können Sie entweder den durchschnittlichen Durchsatz und den Anwendungsnamen oder die durchschnittliche Durchsatzanomalie und den Anwendungsnamen konfigurieren.
	Anwendungsname	Klicken Sie auf **Anwendungen auswählen**, um die Anwendungen auszuwählen, für die Sie über die Verletzung benachrichtigt werden möchten.
Datenvolumen	Gesamtdatenvolumen	Die Gesamtdaten, die in einer bestimmten Dauer übertragen werden sollen. Geben Sie den Wert (in MB) an, um benachrichtigt zu werden.
	Datenvolumenanomalien	Geben Sie die Anzahl der Anomalien an, für die Sie benachrichtigt werden möchten.
		Hinweis: Wenn Sie für dieses Ereignis die UND-Bedingung verwenden, können Sie entweder „Gesamtdatenvolumen“ und „Anwendungsname“ oder „Datenvolumenanomalien“ und „Anwendungsname“ konfigurieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VERLETZUNGSNAME	BEDINGUNG	BESCHREIBUNG
	Anwendungsname	Klicken Sie auf **Anwendungen auswählen**, um die Anwendungen auszuwählen, für die Sie über Verstöße benachrichtigt werden möchten.

Suchleiste verwenden

Mit der Suchleiste können Sie Ergebnisse filtern. Wenn Sie auf die Suchleiste klicken, erhalten Sie eine Liste mit Suchvorschlägen. Sie können die Komponente auswählen und die Ergebnisse basierend auf Ihren Anforderungen filtern.

Option „Audit-Protokolle“ verwenden

Klicken Sie auf **Audit-Protokolle** und wählen Sie die Dauer aus der Liste aus, um die Aktionsrichtlinien anzuzeigen, die für die ausgewählte Dauer erstellt, geändert und gelöscht wurden, und klicken Sie auf **Suchen**.

HINWEIS

Die Datenspeicherrichtlinien werden voraussichtlich in den kommenden Versionen geändert. Mit diesen Änderungen können Sie keine historischen Daten mehr speichern, nachdem die Speichergrenze überschritten wurde. Vorerst wird empfohlen, mehr Speicherplatz hinzuzufügen oder den Speicherplatz innerhalb der Lizenzberechtigungsgrenzen zu halten.

Audit-Protokolle zur Verwaltung und Überwachung Ihrer Infrastruktur verwenden

Sie können die NetScaler Console verwenden, um alle Ereignisse auf der NetScaler Console und Syslog-Ereignisse, die auf den NetScaler-Instanzen generiert werden, zu verfolgen. Diese Meldungen können Ihnen helfen, Ihre Infrastruktur zu verwalten und zu überwachen. Protokollmeldungen sind jedoch nur dann eine große Informationsquelle, wenn Sie sie überprüfen, und die NetScaler Console vereinfacht die Überprüfung von Protokollmeldungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können Filter verwenden, um NetScaler Console Syslog- und Audit-Protokollmeldungen zu durchsuchen. Die Filter helfen Ihnen, Ihre Ergebnisse einzugrenzen und genau das zu finden, wonach Sie suchen, und das in Echtzeit. Die integrierte Suchhilfe führt Sie durch die Filterung der Protokolle. Eine weitere Möglichkeit, Protokollmeldungen anzuzeigen, besteht darin, sie in den Formaten PDF, CSV, PNG und JPEG zu exportieren. Sie können den Export dieser Berichte in bestimmten Intervallen an angegebene E-Mail-Adressen planen.

Sie können die folgenden Arten von Protokollmeldungen über die NetScaler Console GUI überprüfen:

- NetScaler-Instanzbezogene Audit-Protokolle
- NetScaler Console-bezogene Audit-Protokolle
- Anwendungs-Audit-Protokolle

NetScaler-Instanzbezogene Audit-Protokolle

Bevor Sie NetScaler-instanzbezogene Syslog-Meldungen von der NetScaler Console anzeigen können, konfigurieren Sie die NetScaler Console als Syslog-Server für Ihre NetScaler-Instanz. Nach Abschluss der Konfiguration werden alle Syslog-Meldungen von der Instanz an die NetScaler Console umgeleitet.

NetScaler Console als Syslog-Server konfigurieren

Führen Sie die folgenden Schritte aus, um die NetScaler Console als Syslog-Server zu konfigurieren:

1. Navigieren Sie in der NetScaler Console GUI zu **Infrastruktur > Instanzen**.
2. Wählen Sie die NetScaler-Instanz aus, von der die Syslog-Meldungen gesammelt und in der NetScaler Console angezeigt werden sollen.
3. Wählen Sie in der Liste **Aktion auswählen** die Option **Syslog konfigurieren**.
4. Klicken Sie auf **Aktivieren**.
5. Wählen Sie in der Dropdown-Liste **Facility** eine lokale oder benutzerdefinierte Facility aus.
6. Wählen Sie die erforderliche Protokollstufe für die Syslog-Meldungen.
7. Klicken Sie auf **OK**.

Diese Schritte konfigurieren alle Syslog-Befehle in der NetScaler-Instanz, und NetScaler Console beginnt, die Syslog-Meldungen zu empfangen. Sie können die Meldungen anzeigen, indem Sie zu **Infrastructure > Events > Syslog Messages** navigieren. Klicken Sie auf **Need Help?**, um die

© 1997–2026 Citrix Systems, Inc. All rights reserved.

integrierte Suchhilfe zu öffnen. Weitere Informationen finden Sie unter Syslog-Meldungen anzeigen und exportieren.

Um die Protokollmeldungen zu exportieren, klicken Sie auf das Pfeilsymbol in der oberen rechten Ecke.

Klicken Sie anschließend auf **Export Now** oder **Schedule Export**. Weitere Informationen finden Sie unter Syslog-Meldungen exportieren.

NetScaler Console-bezogene Audit-Protokolle

Basierend auf vorkonfigurierten Regeln generiert NetScaler Console Audit-Protokollmeldungen für alle Ereignisse, die Ihnen helfen, den Zustand Ihrer Infrastruktur zu überwachen. Um alle in der NetScaler Console vorhandenen Audit-Protokollmeldungen anzuzeigen, navigieren Sie zu **Settings->Audit Log Messages**.

Um die Protokollmeldungen zu exportieren, klicken Sie auf das Pfeilsymbol in der oberen rechten Ecke.

Anwendungsbezogene Audit-Protokolle

Sie können die Audit-Protokollmeldungen für alle NetScaler Console-Anwendungen oder für eine bestimmte Anwendung anzeigen.

- Um alle Audit-Protokollmeldungen für alle in der NetScaler Console vorhandenen Anwendungen anzuzeigen, navigieren Sie zu **Infrastructure > Network Functions > Auditing**.
- Um Audit-Protokollmeldungen für eine bestimmte Anwendung in der NetScaler Console anzuzeigen, navigieren Sie zu **Applications > Dashboard > Doppelklicken Sie auf den virtuellen Server > Audit Log**.

Hinweis

Sie können NetScaler Console-Überwachungsprotokollmeldungen an einen externen Server weiterleiten. Weitere Informationen finden Sie unter Überwachungsinformationen anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IP-Adressverwaltung (IPAM) konfigurieren

NetScaler Console IPAM ermöglicht Ihnen die automatische Zuweisung und Freigabe von IP-Adressen in von NetScaler Console verwalteten Konfigurationen. Sie können IPs aus Netzwerken oder IP-Bereichen zuweisen, die mit den folgenden IP-Anbietern definiert wurden:

- Integrierter IPAM-Anbieter von NetScaler Console.
- Infoblox IPAM-Lösung.

Sie können NetScaler Console IPAM verwenden in:

- **StyleBooks**: IPs automatisch virtuellen Servern zuweisen, wenn Sie Konfigurationen erstellen.
- **API-Gateway**: Eine IP-Adresse automatisch dem API-Proxy zuweisen.

Sie können auch die IP-Adressen in jedem Netzwerk oder dem IP-Bereich verfolgen, die von NetScaler Console verwaltet werden.

Wenn der folgende Fehler beim Hinzufügen eines externen IPAM-Anbieters auftritt, weist dies darauf hin, dass die NetScaler Console das SSL-Zertifikat für den externen IPAM-Anbieter aufgrund eines fehlenden oder nicht erkannten Zertifizierungsstellen-Zertifikats (CA-Zertifikat) nicht überprüfen kann:

`certificate verify failed: unable to get local issuer certificate`

Um dieses Problem zu beheben, können Sie das erforderliche CA-Zertifikat manuell zum NetScaler Console-Agent hinzufügen, der für den Zugriff auf den externen IPAM-Anbieter verwendet wird. Das Hinzufügen des erforderlichen CA-Zertifikats stellt sicher, dass sichere Verbindungen zum externen IPAM-Anbieter ordnungsgemäß validiert werden.

Melden Sie sich beim NetScaler Console-Agent an, der für den Zugriff auf den externen IPAM-Anbieter verwendet wird, und fügen Sie Ihr CA-Zertifikat zum vertrauenswürdigen Zertifikatspaket `/var/mps/ca_certs/cacert.pem` hinzu.

Einen externen IP-Adressanbieter hinzufügen

NetScaler Console verfügt über einen integrierten IPAM-Anbieter zur Verwaltung von IPs und IP-Bereichen. Sie können auch einen externen IP-Adressanbieter in NetScaler Console verwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WICHTIG:

Stellen Sie vorab sicher, dass die folgenden Berechtigungen im externen IP-Adressanbieter aktiviert sind:

- Möglichkeit, im Anbieter vorhandene Netzwerke abzufragen.
- Eine IP-Adresse im Netzwerk reservieren.
- Eine IP-Adresse aus dem Netzwerk freigeben.
- Die verwendeten IP-Adressen aus einem Netzwerk abrufen.
- Verfügbare IP-Adressen aus einem Netzwerk abrufen.

Führen Sie die folgenden Schritte aus, um eine externe IPAM-Anbieterlösung in NetScaler Console hinzuzufügen:

1. Navigieren Sie zu **Einstellungen > IPAM**.
2. Klicken Sie unter **Anbieter** auf **Hinzufügen**.
3. Geben Sie die folgenden Details an, um einen IPAM-Anbieter hinzuzufügen:
   - **Name** – Geben Sie den Namen des IP-Anbieters an, der in NetScaler Console verwendet werden soll.
   - **Anbieter** – Wählen Sie einen IPAM-Anbieter aus der Liste aus.
   - **URL** – Geben Sie die URL der IPAM-Lösung an, die IP-Adressen in einer NetScaler Console-Umgebung zuweist. Stellen Sie sicher, dass die URL im folgenden Format angegeben wird:

     ```
     https://<host name>
     ```

     Beispiel: `https://myinfoblox.example.com`
   - **Ist es ein privater Endpunkt?** – Wenn der Infoblox DDI privat gehostet wird, aktivieren Sie dieses Kontrollkästchen und wählen Sie dann einen **Agenten** aus.
   - **Benutzername** – Geben Sie den Benutzernamen ein, um sich bei der IPAM-Lösung anzumelden.
   - **Passwort** – Geben Sie das Passwort ein, um sich bei der IPAM-Lösung anzumelden.
4. Klicken Sie auf **Hinzufügen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infoblox DDI als externer Anbieter

Derzeit unterstützt NetScaler Console Infoblox DDI als externen Anbieter. Das Infoblox DDI kann entweder öffentlich zugänglich oder privat gehostet werden, wobei es nur innerhalb des internen Netzwerks eines Unternehmens zugänglich ist. Im Falle eines privat gehosteten Infoblox DDI müssen Sie während des Konfigurationsprozesses einen NetScaler-Agenten auswählen. Der NetScaler-Agent fungiert als Proxy, um auf den Anbieter zuzugreifen, der sich im Intranet des Unternehmens befindet.

Sie können NetScaler Console IPAM mit dem Infoblox-Anbieter für die folgenden Aktionen verwenden:

- IPAM-Netzwerke auflisten
- IPAM-Netzwerke erstellen, aktualisieren und löschen
- Eine IP-Adresse aus IPAM-Netzwerken reservieren und freigeben

Ein IPAM-Netzwerk erstellen

Um ein NetScaler Console IPAM-Netzwerk mit dem Infoblox-Anbieter zu erstellen, muss ein Netzwerk mit demselben CIDR-IP-Bereich auf Infoblox vorhanden sein.

Wenn Sie ein IPAM-Netzwerk innerhalb der NetScaler Console erstellen, registrieren Sie lediglich die Nutzung des Infoblox-Netzwerks innerhalb der NetScaler Console. Die NetScaler Console arbeitet dann mit Infoblox zusammen, um die aus dem Netzwerk zugewiesenen IP-Adressen zu verwalten. Das InfoBlox-Netzwerk kann weiterhin außerhalb der NetScaler Console verwendet werden.

Wenn Sie das NetScaler Console IPAM-Netzwerk löschen, hebt die NetScaler Console die Registrierung des Infoblox-Netzwerks auf. Dies bedeutet, dass die NetScaler Console für die IP-Adressverwaltung in diesem Netzwerk nicht mehr mit Infoblox interagiert.

Infoblox DDI-APIs

NetScaler Console IPAM verwendet die folgenden Infoblox-APIs, um die jeweiligen Aktionen auszuführen:

- (/network) – Listet alle verfügbaren Infoblox-Netzwerke auf
- (/network?network={id}) – Ruft Details eines bestimmten Infoblox-Netzwerks ab
- (/ipv4address) – Listet alle IPs in einem Infoblox-Netzwerk auf
- (/record:host) – Ruft Details einer bestimmten IP-Adresse ab
- (/{IP}) – Reserviert und gibt IPs in einem Infoblox-Netzwerk frei

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS:

- Die IP und der Port des Infoblox DNS-, DHCP- und IP-Adressmanagement (DDI)-Servers müssen über das öffentliche Netzwerk zugänglich sein, damit der NetScaler Console-Dienst den Infoblox-Server erreichen und sich mit ihm verbinden kann.
- Das in NetScaler Console konfigurierte Infoblox-Benutzerkonto muss über die erforderlichen Berechtigungen verfügen, um die Infoblox-APIs zu verwenden.

Weitere Informationen zu den Infoblox-APIs finden Sie im Infoblox REST API-Referenzhandbuch, das unter Infoblox DDI verfügbar ist.

Netzwerk hinzufügen

Fügen Sie ein Netzwerk hinzu, um IPAM mit von NetScaler Console verwalteten Konfigurationen zu verwenden.

1. Navigieren Sie zu **Einstellungen > IPAM**.
2. Klicken Sie unter **Netzwerke** auf **Hinzufügen**.
3. Geben Sie die folgenden Details an:

   - **Netzwerkname** – Geben Sie den Netzwerknamen an, um das Netzwerk in NetScaler Console zu identifizieren.
   - **Anbieter** – Wählen Sie den Anbieter aus der Liste aus.

     Diese Liste zeigt die in NetScaler Console hinzugefügten Anbieter an.
   - **Netzwerktyp** – Wählen Sie je nach Anforderung **IP-Bereich** oder **CIDR** aus der Liste aus.
   - **Netzwerkwert** – Geben Sie den Netzwerkwert an.

     HINWEIS:

     NetScaler Console IPAM unterstützt nur IPv4-Adressen.

     Geben Sie für den **IP-Bereich** den Netzwerkwert im folgenden Format an:

     ```
     <first-IP-address>-<last-IP-address>
     ```

     Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
10.0.0.20-10.0.0.100
```

Geben Sie für **CIDR** den Netzwerkwert im folgenden Format an:

```
<IP-address>/<subnet-mask>
```

Beispiel:

```
10.70.124.0/24
```

4. Klicken Sie auf **Erstellen**.

Zugewiesene IP-Adressen anzeigen

Um weitere Details zu zugewiesenen IP-Adressen aus dem IPAM-Netzwerk anzuzeigen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Einstellungen > IPAM**.
2. Klicken Sie auf der Registerkarte **Netzwerke** auf **Alle zugewiesenen IPs anzeigen**.

   Dieser Bereich zeigt IP-Adresse, Anbietername, Anbieter-Hersteller und Beschreibung an. Er zeigt auch die Ressourcendetails an, die diese IP-Adresse reserviert haben:

   - **Modul**: Zeigt das NetScaler Console-Modul an, das die IP-Adresse reserviert hat. Wenn beispielsweise StyleBooks die IP-Adresse reserviert hat, wird in dieser Spalte StyleBooks als Modul angezeigt.
   - **Ressourcentyp**: Zeigt den Ressourcentyp in diesem Modul an. Für das StyleBooks-Modul verwendet nur der Ressourcentyp Konfigurationen das IPAM-Netzwerk. Daher wird in dieser Spalte Konfigurationen angezeigt.
   - **Ressourcen-ID**: Zeigt die genaue Ressourcen-ID mit einem Link an. Klicken Sie auf diesen Link, um auf die Ressource zuzugreifen, die die IP-Adresse verwendet. Für den Konfigurationsressourcentyp wird die Konfigurationspaket-ID als Ressourcen-ID angezeigt.

HINWEIS:

Wenn Sie die IP-Adresse freigeben möchten, wählen Sie die IP-Adresse aus, die Sie freigeben möchten, und klicken Sie auf **Zugewiesene IPs freigeben**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How-to-Artikel

Die „How-to-Artikel“ von NetScaler Console sind einfache, relevante und leicht umzusetzende Artikel zu den im Dienst verfügbaren Funktionen. Diese Artikel enthalten Informationen zu einigen der beliebtesten NetScaler Console-Funktionen wie Instanzverwaltung, Konfigurationsverwaltung, Ereignisverwaltung, Anwendungsverwaltung, StyleBooks und Zertifikatsverwaltung.

Klicken Sie in der folgenden Tabelle auf einen Funktionsnamen, um die Liste der Anleitungen für diese Funktion anzuzeigen.

THEMEN		
Instanzverwaltung	Konfigurationsverwaltung	Zertifikatsverwaltung
StyleBooks	Ereignisverwaltung	

Instanzverwaltung

So überwachen Sie global verteilte Sites

So verwalten Sie Administratorpartitionen von NetScaler-Instanzen

So fügen Sie Instanzen zu NetScaler Console hinzu

So erstellen Sie Instanzgruppen in NetScaler Console

So fragen Sie NetScaler-Instanzen und -Entitäten in NetScaler Console ab

So konfigurieren Sie Sites für Geomaps in NetScaler Console

So erzwingen Sie ein Failover auf die sekundäre NetScaler-Instanz

So erzwingen Sie, dass eine sekundäre NetScaler-Instanz sekundär bleibt

So ändern Sie ein NetScaler MPX- oder VPX-Root-Passwort

So ändern Sie ein NetScaler SDX-Root-Passwort

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Konfigurationsverwaltung

So verwenden Sie den SCP-Befehl (put) in Konfigurationsaufträgen

So aktualisieren Sie NetScaler SDX-Instanzen mit NetScaler Console

So planen Sie Aufträge, die mit integrierten Vorlagen in NetScaler Console erstellt wurden

So planen Sie Aufträge neu, die mit integrierten Vorlagen in NetScaler Console konfiguriert wurden

Konfigurationsaufträge wiederverwenden

So aktualisieren Sie NetScaler-Instanzen mit NetScaler Console

So erstellen Sie einen Konfigurationsauftrag in NetScaler Console

So verwenden Sie Variablen in Konfigurationsaufträgen in NetScaler Console

So verwenden Sie Konfigurationsvorlagen zum Erstellen von Audit-Vorlagen in NetScaler Console

So erstellen Sie Konfigurationsaufträge aus Korrekturbefehlen in NetScaler Console

So replizieren Sie ausgeführte und gespeicherte Konfigurationsbefehle von einer NetScaler-Instanz auf eine andere in NetScaler Console

So verwenden Sie Konfigurationsaufträge, um die Konfiguration von einer Instanz auf mehrere Instanzen zu replizieren

So verwenden Sie die Master-Konfigurationsvorlage in NetScaler Console

Zertifikatsverwaltung

So konfigurieren Sie eine Unternehmensrichtlinie in NetScaler Console

So installieren Sie SSL-Zertifikate auf einer NetScaler-Instanz über NetScaler Console

So aktualisieren Sie ein installiertes Zertifikat über NetScaler Console

So verknüpfen und entknüpfen Sie SSL-Zertifikate mithilfe von NetScaler Console

So erstellen Sie eine Zertifikatsignierungsanforderung (CSR) mithilfe von NetScaler Console

So richten Sie Benachrichtigungen für den Ablauf von SSL-Zertifikaten über NetScaler Console ein

So verwenden Sie das SSL-Dashboard in NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

So verwenden Sie Standard-StyleBooks in NetScaler Console

So erstellen Sie eigene StyleBooks

So verwenden Sie benutzerdefinierte StyleBooks in NetScaler Console

So verwenden Sie die API zum Erstellen von Konfigurationen aus StyleBooks

So aktivieren Sie Analysen und konfigurieren Alarme auf einem in einem StyleBook definierten virtuellen Server

So erstellen Sie ein StyleBook zum Hochladen von SSL-Zertifikats- und Zertifikatsschlüsseldateien in NetScaler Console

So verwenden Sie das Microsoft Skype for Business StyleBook in Unternehmen

So verwenden Sie das Microsoft Exchange StyleBook in Unternehmen

So verwenden Sie das Microsoft SharePoint StyleBook in Unternehmen

So verwenden Sie das Microsoft ADFS Proxy StyleBook

So verwenden Sie das Oracle E-Business StyleBook

So verwenden Sie das SSO Office 365 StyleBook

So verwenden Sie das SSO Google Apps StyleBook

Ereignisverwaltung

So legen Sie das Ereignisalter für Ereignisse in NetScaler Console fest

So planen Sie einen Ereignisfilter mithilfe von NetScaler Console

So legen Sie wiederholte E-Mail-Benachrichtigungen für Ereignisse von NetScaler Console fest

So unterdrücken Sie Ereignisse mit NetScaler Console

So verwenden Sie das Ereignis-Dashboard, um Ereignisse zu überwachen

So erstellen Sie Ereignisregeln auf NetScaler Console

So ändern Sie den gemeldeten Schweregrad von Ereignissen, die auf NetScaler-Instanzen auftreten

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So zeigen Sie die Ereigniszusammenfassung in NetScaler Console an

So zeigen Sie Ereignisschweregrade und Abweichungen von SNMP-Traps auf NetScaler Console an

So exportieren Sie Syslog-Nachrichten mit NetScaler Console

So unterdrücken Sie Syslog-Nachrichten in NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FAQs

Wie viele Agents muss ich installieren?

Die Anzahl der Agents hängt von der Anzahl der verwalteten Instanzen in einem Rechenzentrum und dem Gesamtdurchsatz ab. Citrix empfiehlt, dass Sie mindestens einen Agent pro Rechenzentrum installieren.

Wie kann ich mehrere Agents installieren?

Sie können nur einen Agent installieren, wenn Sie sich zum ersten Mal beim Dienst anmelden. Um mehrere Agents hinzuzufügen, schließen Sie zuerst die Ersteinrichtung ab und navigieren Sie dann zu **Einstellungen** > **Agents einrichten**.

Unterstützt der NetScaler Agent AMD-Prozessoren?

Ja.

Kann ich von einem integrierten Agent zu einem externen Agent wechseln?

Ja, das können Sie. Weitere Informationen finden Sie unter Wechsel von einem integrierten Agent zu einem externen Agent.

Wie erhalte ich einen neuen Aktivierungscode, wenn ich ihn verloren habe?

Wenn Sie sich zum ersten Mal anmelden, rufen Sie die Dienst-GUI auf, navigieren Sie zum Bildschirm **Agent einrichten** und klicken Sie auf **Aktivierungscode generieren**.

Wenn Sie versuchen, einen zweiten Agent zu installieren, um einen neuen Aktivierungscode zu generieren, navigieren Sie zu **Infrastruktur > Instanzen > Agents > Aktivierungscode generieren.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Wie melde ich mich bei der Agent-VM an? Was sind die Standardanmeldeinformationen?

Wenn Ihr Agent auf einem Hypervisor oder in der Microsoft Azure Cloud installiert ist, lauten die Standardanmeldeinformationen für den Agent `nsrecover/nsroot`, wodurch die Shell-Eingabeaufforderung des Agent geöffnet wird.

Wenn Ihr Agent auf AWS installiert ist, lauten die Standardanmeldeinformationen für die Anmeldung beim Agent `nsrecover/instance id`.

Welche Ressourcenanforderungen gelten für die Installation eines Agents auf einem lokalen Hypervisor?

32 GB RAM, 8 virtuelle CPUs, 500 GB Speicher, 1 virtuelle Netzwerkschnittstelle, 1 Gbit/s Durchsatz

Muss ich dem Agenten bei der Bereitstellung eine zusätzliche Festplatte zuweisen?

Nein, Sie müssen keine zusätzliche Festplatte hinzufügen. Der Agent wird nur als Vermittler zwischen der NetScaler Console und den Instanzen in Ihrem Unternehmensrechenzentrum oder in der Cloud verwendet. Er speichert keine Bestands- oder Analysedaten, die eine zusätzliche Festplatte erfordern würden.

Kann ich meinen Aktivierungscode mit mehreren Agenten wiederverwenden?

Nein, das können Sie nicht.

Wie führe ich die Netzwerkeinstellungen erneut aus, wenn ich einen falschen Wert eingegeben habe?

Greifen Sie auf die Agentenkonsole auf Ihrem Hypervisor zu, melden Sie sich mit den Anmeldeinformationen nsrecover/nsroot an der Shell-Eingabeaufforderung an und führen Sie dann den Befehl `networkconfig` aus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Was mache ich, wenn die Agentenregistrierung fehlschlägt?

Stellen Sie sicher, dass:

- Ihr Agent Zugriff auf das Internet hat (DNS konfigurieren).
- Sie den Aktivierungscode korrekt kopiert haben.
- Sie die Dienst-URL korrekt eingegeben haben.
- Sie die erforderlichen Ports geöffnet haben.

Die Registrierung war erfolgreich, aber woher weiß ich, ob der Agent ordnungsgemäß funktioniert?

Nachdem der Agent erfolgreich registriert wurde, greifen Sie auf NetScaler Console zu und navigieren Sie zum Bildschirm **Agent einrichten**. Sie können den erkannten Agenten auf dem Bildschirm sehen. Wenn der Agent ordnungsgemäß ausgeführt wird, wird ein grünes Symbol angezeigt. Wenn er nicht ausgeführt wird, wird ein rotes Symbol angezeigt.

Wie kann ich Agenten über einen Proxy-Server mit NetScaler Console verbinden?

Sie können Agenten über einen Proxy-Server mit NetScaler Console verbinden. Das Skript ist im Ordner `/mps` des Agenten verfügbar. Die Agenten leiten alle ihre Daten an den Proxy-Server weiter, der die Daten dann über das Internet an die NetScaler Console sendet.

Um Daten über den Proxy-Server weiterzuleiten, geben Sie die Details des Proxy-Servers auf dem Agenten mit dem folgenden Skript ein: `proxy_input.py`, und folgen Sie den Anweisungen des Skripts, um weitere Informationen einzugeben. Der Agent ruft diese Informationen ab, während er sich über den Proxy-Server mit NetScaler Console verbindet.

Sie können Ihren Proxy-Server authentifizieren, indem Sie Ihre Benutzername- und Kennwortinformationen angeben. Wenn der Agent die Daten sendet, authentifiziert der Proxy-Server die Benutzeranmeldeinformationen, bevor er sie an NetScaler Console weiterleitet.

Weitere Informationen finden Sie unter NetScaler Console als API-Proxy-Server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

NetScaler Console unterstützt Proxy-Server mit aktivierter Basisauthentifizierung. NetScaler Console unterstützt auch Proxy-Server, bei denen die Authentifizierung deaktiviert ist.

Ich sehe meine Analysereports nicht

Aktivieren Sie Insight auf Ihren virtuellen Servern, um die Analysereports anzuzeigen. Details finden Sie unter Analysen aktivieren.

Welche Versionen von NetScaler-Instanzen werden in NetScaler Console unterstützt?

Für Verwaltungs- und Überwachungsfunktionen werden NetScaler-Instanzen ab Version 10.5 unterstützt. Einige Funktionen werden nur auf bestimmten NetScaler-Versionen unterstützt. Details finden Sie unter Systemanforderungen.

Wie exportiere ich Dashboard-Berichte in NetScaler Console?

Um den Bericht eines Dashboards in NetScaler Console zu exportieren, klicken Sie auf das Symbol **Exportieren** oben rechts auf dieser Seite. Auf der Seite **Exportieren** können Sie eine der folgenden Aktionen ausführen:

1. Wählen Sie die Registerkarte **Jetzt exportieren**. Um den Bericht im PDF-, JPEG-, PNG- oder CSV-Format anzuzeigen und zu speichern. Der Bericht wird auf Ihr System heruntergeladen.
2. Wählen Sie **Bericht planen**, um Zeitpläne für die Generierung und den Export von Berichten in regelmäßigen Abständen einzurichten. Geben Sie die Wiederholungseinstellungen für die Berichtsgenerierung an und erstellen Sie ein E-Mail-Profil, an das der Bericht exportiert werden soll.

    a. **Wiederholung** – Wählen Sie **Täglich**, **Wöchentlich** oder **Monatlich** aus der Dropdown-Liste.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

- Wenn Sie die Wiederholung **Wöchentlich** auswählen, stellen Sie sicher, dass Sie die Wochentage auswählen, an denen der Bericht geplant werden soll.
- Wenn Sie die Wiederholung **Monatlich** auswählen, stellen Sie sicher, dass Sie alle Tage, an denen der Bericht geplant werden soll, durch Kommas getrennt eingeben.

b. **Wiederholungszeit** – Geben Sie die Zeit als `Hour: Minute` im 24-Stunden-Format ein.

c. **E-Mail** – Aktivieren Sie das Kontrollkästchen und wählen Sie dann das Profil aus der Dropdown-Liste aus, oder klicken Sie auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

d. **Slack** – Aktivieren Sie das Kontrollkästchen und wählen Sie dann das Profil aus der Dropdown-Liste aus, oder klicken Sie auf **Hinzufügen**, um ein E-Mail-Profil zu erstellen.

Klicken Sie auf **Zeitplan aktivieren**, um Ihren Bericht zu planen, und klicken Sie dann auf **OK**. Durch Aktivieren des Kontrollkästchens **Zeitplan aktivieren** können Sie die ausgewählten Berichte generieren.

Was bewirkt die Aktivierung clientseitiger Messungen?

Bei aktivierten clientseitigen Messungen erfasst NetScaler Console Ladezeit- und Renderzeitmetriken für HTML-Seiten durch HTML-Injektion. Mithilfe dieser Metriken können Administratoren L7-Latenzprobleme identifizieren.

Wird der SSL-Datenverkehr vom Agent zum NetScaler Console-Dienst einer SSL-Inspektion unterzogen?

Wir empfehlen Ihnen, die SSL-Inspektion für den SSL-Datenverkehr vom Agent zum NetScaler Console-Dienst zu umgehen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

index

- Analysen
- Dashboards
- WAF Insight
- Lernprofil konfigurieren
- Details zu Netzwerkverstößen
- Zusammenfassung der WAF-Lernaktionen anzeigen
- Entspannungsregeln, Leerlauf- und Ablehnungsregeln anzeigen
- SSL Insight
- Analysen für Web-Transaktionen anzeigen
- Detaillierte Verfahren zur Einrichtung einer Dual-Tier- oder Service-Mesh-Lite-Topologie
- Detaillierte Verfahren zum Einrichten der Service-Mesh-Topologie
- Detaillierte Verfahren zur Einrichtung einer einstufigen oder vereinheitlichten Ingress-Topologie
- Datengovernance für das NetScaler®-Telemetrieprogramm
- So ändern Sie das Root-Passwort von NetScaler MPX und VPX
- Vorherige Releases

Analysen

NetScaler Console-Analysen bieten eine einfache und skalierbare Möglichkeit, die verschiedenen Einblicke in die Daten der NetScaler-Instanzen zu untersuchen, um die Anwendungsleistung zu beschreiben, vorherzusagen und zu verbessern. Sie können eine oder mehrere Analysefunktionen gleichzeitig in NetScaler Console verwenden. Die folgende Tabelle beschreibt die verschiedenen Analysefunktionen, die in NetScaler Console unterstützt werden:

ANALYSEFUNKTIONEN	BESCHREIBUNGEN
Web Insight	Web Insight ermöglicht die Sichtbarkeit von Webanwendungen im Unternehmen und erlaubt IT-Administratoren, alle von NetScaler bereitgestellten Webanwendungen durch

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ANALYSEFUNKTIONEN	BESCHREIBUNGEN
	integrierte Echtzeitüberwachung von Anwendungen zu überwachen.
HDX Insight	HDX Insight bietet End-to-End-Transparenz für ICA-Datenverkehr, der NetScaler durchläuft. HDX Insight ermöglicht Administratoren, Client- und Netzwerklatenzmetriken in Echtzeit, historische Berichte, End-to-End-Leistungsdaten anzuzeigen und Leistungsprobleme zu beheben.
Gateway Insight	Gateway Insight bietet Einblick in die Fehler, die allen Benutzern, unabhängig vom Zugriffsmodus, beim Anmelden bei NetScaler Gateway begegnen.
Security Insight	Security Insight bietet eine Single-Pane-Lösung, die Ihnen hilft, den Sicherheitsstatus Ihrer Anwendungen zu bewerten und Korrekturmaßnahmen zur Sicherung Ihrer Anwendungen zu ergreifen.
SSL Insight	SSL Insight bietet Einblick in sichere Webtransaktionen (HTTPS) und ermöglicht IT-Administratoren, alle von NetScaler bereitgestellten sicheren Webanwendungen durch integrierte Echtzeit- und historische Überwachung sicherer Webtransaktionen zu überwachen.

Dashboards

NetScaler Console bietet zwei Dashboards: das **Dashboard für ausgehenden Datenverkehr** und das **Benutzer-Dashboard**. Diese Dashboards zeigen mehrere Diagramme an, die die von Ihrem Unternehmensnetzwerk aus aufgerufenen Websites oder Anwendungen sowie die von den Benutzern in Ihrem Netzwerk ausgeführten Aktivitäten zusammenfassen.

Dashboard für ausgehenden Datenverkehr

Das **Dashboard für ausgehenden Datenverkehr** bietet eine Zusammenfassung der von Ihrem Netzwerk aus aufgerufenen URLs oder Domänen. Es bietet eine ganzheitliche Ansicht aller URLs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

oder Domänen nach der Anzahl der Transaktionen oder dem von den URLs oder Domänen verbrauchten Datenvolumen. Es enthält auch Details wie die folgenden:

1. Menge der Bandbreite, die von den von Ihrem Netzwerk aus aufgerufenen URLs oder Domänen verbraucht wird.
2. Anzahl der Transaktionen, die beim Zugriff auf die URLs und Domänen von Ihrem Netzwerk aus aufgetreten sind.
3. Anzahl der SSL-Verbindungen, die von der NetScaler Appliance während der Transaktionen abgefangen wurden.
4. Anzahl der SSL-Verbindungen, die von der NetScaler Appliance während der Transaktionen nicht abgefangen wurden.
5. Anzahl der SSL-Verbindungen, die von der NetScaler Appliance während der Transaktionen zurückgesetzt wurden.
6. Menge des übertragenen Web-Datenverkehrs, basierend auf dem zum Übertragen des Datenverkehrs verwendeten Port, dem vom Web-Datenverkehr verwendeten Protokoll und den zum Übertragen des Datenverkehrs verwendeten Client-Betriebssystemen.

Um auf das Dashboard für ausgehenden Datenverkehr zuzugreifen, navigieren Sie zu **Security > Users & Endpoints > Outbound Traffic Dashboard**.

Ausgehenden Datenverkehr aus dem Netzwerk anzeigen

Das **Dashboard für ausgehenden Datenverkehr** enthält einen Bereich **Übersicht über ausgehenden Datenverkehr**. Im Bereich **Übersicht über ausgehenden Datenverkehr** gruppiert NetScaler Console die aufgerufenen URLs oder Domänen in Kategorien wie Shopping, Nachrichten, soziale Netzwerke usw. Der Bereich **Übersicht über ausgehenden Datenverkehr** zeigt die von Ihrem Netzwerk aus aufgerufenen URLs oder Domänen als Knoten in den URL-Kategorien an. Die Größe der Knoten richtet sich nach dem Datenvolumen, das beim Zugriff auf die URL oder Domäne verbraucht wird. Die Farbe des Knotens gibt die Anzahl der Transaktionen an, die beim Zugriff auf die URL oder Domäne aufgetreten sind.

Sie können auf eine Kategorie klicken, um die Diagramme so zu filtern, dass Details zu dieser Kategorie für den angegebenen Zeitraum angezeigt werden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benutzer-Dashboard

Das **Benutzer-Dashboard** zeigt eine Zusammenfassung der von den Benutzern in Ihrem Unternehmen ausgeführten Aktivitäten an. Es bietet wichtige Metriken, die Sie verwenden können, um Folgendes zu bestimmen:

1. Surfverhalten der Benutzer in Ihrem Unternehmen.
2. Von den Benutzern in Ihrem Unternehmen aufgerufene URL-Kategorien.
3. Die fünf wichtigsten Benutzer, basierend auf ihren Risikobewertungen und der von ihnen verbrauchten Bandbreite. Weitere Informationen zur Risikobewertung finden Sie unter Risikobewertung.
4. Browser, die für den Zugriff auf die URLs oder Domänen verwendet werden.
5. Menge des von den Benutzern generierten Web-Traffics, basierend auf der Traffic-Reputationsbewertung.

Um auf das **Benutzer-Dashboard** zuzugreifen, navigieren Sie zu **Benutzer > Dashboard**.

Sie können im Bereich **Top-Benutzer** auf einen Benutzer klicken, um die Diagramme so zu filtern, dass Details der vom Benutzer im angegebenen Zeitraum ausgeführten Webaktivität angezeigt werden.

Benutzeraktivitäts-Untersuchung

Das **Benutzer-Dashboard** enthält einen Bereich **Benutzeraktivitäts-Untersuchung**, der verschiedene von den Benutzern ausgeführte Webaktivitäten anzeigt. Es zeigt die von den Benutzern im ausgewählten Zeitraum aufgerufenen URL-Kategorien und verschiedene pro URL-Kategorie ausgelöste Ereignisse an. Sie können auf die Ereignisse klicken, um die Details auf Transaktionsebene abzurufen.

Die **Benutzeraktivitäts-Untersuchung** zeigt wichtige Informationen wie das Surfverhalten des Benutzers, risikoreiche Aktivitäten des Benutzers und ausgelöste Ereignisse pro URL-Kategorie an. Die Ereignisse werden als rechteckige Legenden im Diagramm angezeigt. Jede der Legenden wird in Ein-Minuten-Intervallen aggregiert, wenn die ausgewählte Dauer eine Stunde beträgt, und in Ein-Stunden-Intervallen, wenn die ausgewählte Dauer ein Tag beträgt.

Diese Legenden werden aggregiert und sind farblich nach der Anzahl der aufgetretenen Ereignisse kodiert. Sie können den Mauszeiger über eine Legende bewegen, um Details wie die Uhrzeit und

© 1997–2026 Citrix Systems, Inc. All rights reserved.

die Anzahl der für die ausgewählte Legende aggregierten Ereignisse anzuzeigen. Sie können den Zeitraum des Diagramms anpassen, indem Sie eine Zeit aus der Zeitraumsliste auswählen.

Sie können auf die Ereignisse klicken, um weitere Details der Transaktionen aufzurufen.

Benutzertransaktionen

Die Seite Benutzertransaktionen zeigt die Details der Benutzertransaktionen in Ihrem Netzwerk an. Sie bietet transaktionsebene Details wie:

1. Zeitpunkt, zu dem die Transaktion stattfand
2. Für die Transaktion verwendetes Protokoll
3. Benutzername
4. Vom Benutzer aufgerufene Domäne
5. URL-Kategorie
6. Proxy-Server, der zum Abfangen der Transaktion verwendet wurde
7. Details zum Client-Port
8. Eingehende Bytes
9. Ausgehende Bytes

ÜBERSICHTSBEREICH

Das **Zusammenfassungsfenster** zeigt alle Metriken der Transaktionen an, die im Bereich **Transaktionsdetails** sichtbar sind. Dieses Fenster ermöglicht es Ihnen, die Transaktionen im Bereich **Transaktionsdetails** durch Auswählen oder Abwählen der Metriken zu sortieren und anzuzeigen. Das **Zusammenfassungsfenster** zeigt die folgenden Metriken an:

METRIKEN	BESCHREIBUNG
Protokolle	In den Transaktionen verwendete Protokolle
Ports	Für die Transaktionen verwendete Ports
URL-Reputation	URL-Reputationswert
Browser	Für die Transaktionen verwendete Browser
Betriebssystem	Für die Transaktionen verwendetes Betriebssystem

© 1997–2026 Citrix Systems, Inc. All rights reserved.

METRIKEN	BESCHREIBUNG
Eingehende Bytes	Datenmenge, die über die NetScaler Appliance empfangen wurde.
Bytes ausgehend	Datenmenge, die über die NetScaler Appliance gesendet wurde.

Risikobewertung

Die Risikobewertung ist ein Bewertungssystem, das in NetScaler Console verwendet wird, um die mit Benutzern in Ihrem Unternehmen verbundenen Risiken zu bestimmen. NetScaler Console weist eine Risikobewertung basierend auf der URL-Reputationsbewertung zu, die von der NetScaler Appliance für die von den Benutzern in Ihrem Netzwerk aufgerufenen URLs zugewiesen wird. Informationen zur URL-Reputationsbewertung finden Sie unter URL-Reputationsbewertung. Die folgende Tabelle beschreibt die von NetScaler Console zugewiesenen Risikobewertungen.

RISIKOBEWERTUNG	BESCHREIBUNG
1	Die Webaktivität des Benutzers weist keine wahrgenommene Bedrohung auf oder ist nicht abnormal.
2	Die Webaktivität des Benutzers weist keine wahrgenommene Bedrohung auf oder ist nicht abnormal, aber der Benutzer greift auf „unbekannte Websites“ zu, die keine URL-Reputationsbewertungen haben.
3	Es wird keine Bedrohung in der Webaktivität des Benutzers erkannt, aber der Benutzer hat versucht, auf potenziell anfällige Websites oder mit potenziell anfälligen Websites verbundene Websites zuzugreifen.
4	Potenziell kompromittierter Benutzer.
5	Die Web-Aktivität des Benutzers ist ungewöhnlich, und der Benutzer hat bekannte bösartige Websites aufgerufen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF Insight

Web- und Webdienstanwendungen, die dem Internet ausgesetzt sind, sind zunehmend anfällig für Angriffe geworden. Um Anwendungen vor Angriffen zu schützen, benötigen Sie Einblick in die Art und das Ausmaß vergangener, gegenwärtiger und bevorstehender Bedrohungen, umsetzbare Echtzeitdaten zu Angriffen und Empfehlungen für Gegenmaßnahmen. WAF Insight bietet eine zentrale Lösung, die Ihnen hilft, den Sicherheitsstatus Ihrer Anwendungen zu bewerten und Korrekturmaßnahmen zur Sicherung Ihrer Anwendungen zu ergreifen.

HINWEIS

WAF Insight wird auf NetScaler Console mit allen NetScaler Appliances unterstützt, die unter Version 11.0 Build 65.31 und höher ausgeführt werden.

So funktioniert WAF Insight

WAF Insight ist eine intuitive, Dashboard-basierte Sicherheitsanalyse-Lösung, die Ihnen volle Transparenz über die Bedrohungslandschaft Ihrer Anwendungen bietet. Security Insight ist in NetScaler Console enthalten und generiert regelmäßig Berichte basierend auf Ihren Application Firewall- und NetScaler-Systemsicherheitskonfigurationen. Die Berichte enthalten die folgenden Informationen für jede Anwendung:

- **Bedrohungsindex.** Ein einstelliges Bewertungssystem, das die Kritikalität von Angriffen auf die Anwendung angibt, unabhängig davon, ob die Anwendung durch eine NetScaler Appliance geschützt ist. Je kritischer die Angriffe auf eine Anwendung sind, desto höher ist der Bedrohungsindex für diese Anwendung. Die Werte reichen von 1 bis 7.

  Der Bedrohungsindex basiert auf Angriffsinformationen. Die angriffsbezogenen Informationen, wie z. B. Verletzungstyp, Angriffskategorie, Standort und Clientdetails, geben Ihnen Einblick in die Angriffe auf die Anwendung. Verletzungsinformationen werden nur dann an NetScaler Console gesendet, wenn eine Verletzung oder ein Angriff auftritt. Viele Verstöße und Schwachstellen führen zu einem hohen Bedrohungsindexwert.
- **Sicherheitsindex.** Ein einstelliges Bewertungssystem, das angibt, wie sicher Sie die NetScaler-Instanzen konfiguriert haben, um Anwendungen vor externen Bedrohungen und Schwachstellen zu schützen. Je geringer die Sicherheitsrisiken für eine Anwendung, desto höher der Sicherheitsindex. Die Werte reichen von 1 bis 7.

  Der Sicherheitsindex berücksichtigt sowohl die Application Firewall-Konfiguration als auch die NetScaler-Systemsicherheitskonfiguration. Für einen hohen Sicherheitsindexwert müssen beide Konfigurationen stark sein. Wenn beispielsweise strenge Application Firewall-Prüfungen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

vorhanden sind, aber NetScaler-Systemsicherheitsmaßnahmen, wie ein starkes Kennwort für den `nsroot`-Benutzer, nicht übernommen wurden, erhalten Anwendungen einen niedrigen Sicherheitsindexwert.

- **Verwertbare Informationen.** Die Informationen, die Sie benötigen, um den Bedrohungsindex zu senken und den Sicherheitsindex zu erhöhen, was die Anwendungssicherheit erheblich verbessert. Sie können beispielsweise Informationen zu Verstößen, vorhandenen und fehlenden Sicherheitskonfigurationen für die Application Firewall und andere Sicherheitsfunktionen sowie die Häufigkeit, mit der die Anwendungen angegriffen werden, überprüfen.

WAF Insight konfigurieren

HINWEIS:

Sie können mit der Konfiguration von Schutzmaßnahmen über das Dashboard **Unified Security** beginnen. Weitere Informationen finden Sie unter Unified Security-Dashboard

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler** und wählen Sie den Instanztyp aus. Zum Beispiel VPX.
2. Wählen Sie die Instanz aus und wählen Sie aus der Liste **Aktion auswählen** die Option **Analytics konfigurieren**.
3. Im Fenster **Analytics auf virtuellem Server konfigurieren**:

   a. Wählen Sie die virtuellen Server aus, für die Sie Security Insight aktivieren möchten, und klicken Sie auf **Sicherheit & Analytics aktivieren**.

   Das Fenster **Sicherheit & Analytics aktivieren** wird angezeigt.

   b. Wählen Sie **WAF-Sicherheitsverletzungen**

   c. Wählen Sie unter **Erweiterte Optionen** entweder **Logstream** oder **IPFIX** als Transportmodus aus.

   HINWEIS

   Für NetScaler 12.0 oder früher ist **IPFIX** die Standardoption für den Transportmodus. Für NetScaler 12.0 oder höher können Sie entweder **Logstream** oder **IPFIX** als Transportmodus auswählen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen zu **IPFIX** und **Logstream** finden Sie unter **Logstream-Übersicht**.

d. Der Ausdruck ist standardmäßig wahr.

e. Klicken Sie auf **OK**

HINWEIS

- Wenn Sie keine Flexed-Lizenz verwenden und virtuelle Server auswählen, die nicht lizenziert sind, lizenziert NetScaler Console diese virtuellen Server zuerst und aktiviert dann Analytics.

Nachdem Sie auf **OK** geklickt haben, beginnt NetScaler Console mit der Aktivierung von Analytics auf den ausgewählten virtuellen Servern.

HINWEIS

Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, der Gruppe Zugriff auf Anwendungsebene gewähren und Benutzer der Gruppe zuweisen. NetScaler Console Analytics unterstützt jetzt die Autorisierung basierend auf virtuellen IP-Adressen. Ihre Benutzer können jetzt Berichte für alle Insights nur für die Anwendungen (virtuelle Server) sehen, für die sie autorisiert sind. Weitere Informationen zu Gruppen und zum Zuweisen von Benutzern zu Gruppen finden Sie unter Konfigurieren von Gruppen in NetScaler Console.

Geostandorte für Sicherheits-Insight-Berichte konfigurieren

Wenn Sie Geostandorte in NetScaler Console konfigurieren, enthalten WAF Insight-Berichte die genauen geografischen Standorte, von denen Clientanfragen stammen. Um Geostandorte zu aktivieren, geben Sie für jeden geografischen Standort in Ihrer Organisation einen privaten IP-Block oder einen Bereich von IP-Adressen an. Fügen Sie diese Informationen in der Geo-Datenbankdatei zusammen mit dem Namen der Stadt/des Bundeslandes/des Landes und den Breiten- und Längengradkoordinaten jedes Standorts hinzu. Wenden Sie sich an Ihren NetScaler-Vertreter, um die Geo-Datenbankdatei zu erhalten, und laden Sie die Datei dann auf die NetScaler-Instanz hoch.

So konfigurieren Sie Geostandorte:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Kopieren Sie die Geo-Datenbankdatei Citrix_Netscaler_InBuilt_GeoIP_DB.csv an einen beliebigen Speicherort auf der NetScaler Appliance.
2. Öffnen Sie die Geo-Datenbankdatei mit einem Texteditor, z. B. dem vi-Editor, und fügen Sie einen Eintrag für jeden Standort in Ihrer Organisation hinzu.

   Der Eintrag muss das folgende Format haben:

   ```
   <start IP\>,<end IP\>,,<country\>,<state\>,,<city\>,,longitude,latitude
   ```

   Zum Beispiel,

   ```
   4.17.142.224,4.17.142.239,,US,New York,,Harrison,,73.7304,41.0568
   ```
3. Führen Sie die folgenden Befehle aus, um die Geostandortprotokollierung und die Protokollierung im CEF-Format zu aktivieren:

   - **add locationFile** <Vollständiger Pfad mit DB-Datei\>
   - **Appfw-Einstellungen festlegen** -GeoStandortProtokollierung AN
   - **Appfw-Einstellungen festlegen** -CEFProtokollierung AN

IP-Reputation überwachen

Die IP-Reputationsfunktion bietet angriffsbezogene Informationen über bösartige IP-Adressen. Zum Beispiel meldet sie den IP-Reputations-Score, die IP-Reputationskategorie, die IP-Reputations-Angriffszeit, die Geräte-IP und Details zur Client-IP-Adresse.

Der IP-Reputations-Score gibt das mit einer IP-Adresse verbundene Risiko an. Der Score hat die folgenden Bereiche:

IP-REPUTATIONS-SCORE	RISIKOSTUFE
1–20	Hohes Risiko
21–40	Verdächtig
41–60	Moderates Risiko
61–80	Geringes Risiko
81–100	Vertrauenswürdig

So überwachen Sie die IP-Reputation:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Navigieren Sie zu **Security > Security Violations**, und wählen Sie unter **WAF** die Anwendung aus, die Sie überwachen möchten.
2. Die Werte für **Threat Index** und **Safety Index** werden angezeigt. Klicken Sie auf **Details anzeigen**.
3. Unter „Application Firewall Configuration“ können Sie den Safety Index-Wert der IP-Reputation anzeigen.

Schwellenwerte

Sie können Schwellenwerte für den Safety Index und den Threat Index von Anwendungen in WAF Insight festlegen und anzeigen.

So legen Sie einen Schwellenwert fest:

1. Navigieren Sie zu **Settings > Analytics Settings > Thresholds**, und wählen Sie **Add**.
2. Wählen Sie im Feld „Traffic Type“ den Traffic-Typ als **Security** aus und geben Sie die erforderlichen Informationen in die anderen entsprechenden Felder wie Name, Dauer und Entität ein.
3. Verwenden Sie im Abschnitt **Rule** die Felder „Metric“, „Comparator“ und „Value“, um einen Schwellenwert festzulegen.

   Zum Beispiel: „Threat Index“ „>“ „5“
4. Klicken Sie auf **Create**.

WAF Insight-Anwendungsfälle

Die folgenden Anwendungsfälle beschreiben, wie Sie Security Insight verwenden können, um die Bedrohungsgefährdung von Anwendungen zu bewerten und Sicherheitsmaßnahmen zu verbessern.

Einen Überblick über die Bedrohungslandschaft erhalten

In diesem Anwendungsfall verfügen Sie über eine Reihe von Anwendungen, die Angriffen ausgesetzt sind, und Sie haben NetScaler Console so konfiguriert, dass es die Bedrohungsumgebung überwacht. Sie müssen den Bedrohungsindex, den Sicherheitsindex sowie Art und Schweregrad aller Angriffe überprüfen, denen die Anwendungen möglicherweise ausgesetzt waren, um sich zuerst auf die kritischen Anwendungen zu konzentrieren. Das Security Insight-Dashboard bietet eine Zusammenfassung der Bedrohungen, denen Ihre Anwendungen über einen von Ihnen gewählten Zeitraum und für ein ausgewähltes NetScaler-Gerät ausgesetzt

© 1997–2026 Citrix Systems, Inc. All rights reserved.

waren. Es zeigt die Liste der Anwendungen, deren Bedrohungs- und Sicherheitsindizes sowie die Gesamtzahl der Angriffe für den gewählten Zeitraum an.

Um eine Zusammenfassung der Bedrohungsumgebung zu erhalten, melden Sie sich bei NetScaler Console an und navigieren Sie dann zu **Security > Security Violation**. Unter **WAF** werden die fünf wichtigsten Anwendungen basierend auf der Gesamtzahl der betroffenen Verstöße angezeigt. Um alle Anwendungen anzuzeigen, können Sie auf **Alle anzeigen** klicken.

Vorhandene und fehlende Sicherheitskonfiguration für eine Anwendung ermitteln

Nachdem Sie die Bedrohungsgefährdung einer Anwendung überprüft haben, möchten Sie feststellen, welche Anwendungssicherheitskonfigurationen vorhanden sind und welche für diese Anwendung fehlen. Diese Informationen erhalten Sie, indem Sie die Anwendungszusammenfassung detailliert untersuchen.

Die Zusammenfassung gibt Ihnen Aufschluss über die Wirksamkeit der folgenden Sicherheitskonfigurationen:

- **Anwendungs-Firewall-Konfiguration.** Zeigt an, wie viele Signatur- und Sicherheitsentitäten nicht konfiguriert sind.
- **NetScaler Console Systemsicherheit.** Zeigt an, wie viele Systemsicherheitseinstellungen nicht konfiguriert sind.

Im Knoten **Anwendungs-Firewall-Konfiguration** überprüfen Sie die Informationen zur Sicherheitsprüfung und Sicherheitsverletzung.

Klicken Sie auf den Knoten **NetScaler Console Systemsicherheit** und überprüfen Sie die Systemsicherheitseinstellungen und Citrix-Empfehlungen zur Verbesserung des Anwendungssicherheitsindex.

Anwendungen identifizieren, die sofortige Aufmerksamkeit erfordern

Die Anwendungen, die sofortige Aufmerksamkeit erfordern, sind diejenigen mit einem hohen Bedrohungsindex und einem niedrigen Sicherheitsindex.

Anzahl der Angriffe in einem bestimmten Zeitraum ermitteln

Möglicherweise möchten Sie ermitteln, wie viele Angriffe auf eine bestimmte Anwendung zu einem bestimmten Zeitpunkt aufgetreten sind, oder Sie möchten die Angriffsrate für einen bestimmten Zeitraum untersuchen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Klicken Sie unter **WAF** auf eine beliebige Anwendung, um die insgesamt erkannten WAF-Verletzungen für die ausgewählte Dauer anzuzeigen.

Klicken Sie auf **Protokolle**, um Details zu Angriffen basierend auf Schweregrad und ergriffenen Maßnahmen anzuzeigen. Die Protokollseite enthält die folgenden Details:

- Angriffszeit
- IP-Adresse des Clients, von dem der Angriff ausging
- Schweregrad
- Kategorie der Verletzung
- URL, von der der Angriff ausging, und weitere Details.

Lernprofil konfigurieren

Sie müssen ein Lernprofil in NetScaler Console konfigurieren und die **NetScaler-Profile** auswählen, um die Liste der Entspannungsregeln zu generieren. Abhängig vom Datenverkehr können Sie Profile auf NetScaler-Instanzen konfigurieren und ein Lernprofil in NetScaler Console konfigurieren.

HINWEIS

Derzeit können Sie nur 25 Profile konfigurieren.

Sie können Lernprofile konfigurieren, um die Liste der Entspannungsregeln für die ausgewählten Elemente zu generieren:

- **Webanwendungen** – Ermöglicht Ihnen die Auswahl der Anwendung, für die Sie die Entspannungsregeln erstellen möchten.
- **Profilnamen** – Ermöglicht Ihnen die Auswahl des WAF-Profils, für das Sie die Entspannungsregeln erstellen möchten.

Nachdem Sie das Lernprofil erstellt haben, können Sie, wenn NetScaler keinen eingehenden Datenverkehr für die konfigurierten Sicherheitsprüfungen empfängt, auch konfigurieren, die Entspannungsregeln aus NetScaler Console zu entfernen.

So konfigurieren Sie ein Lernprofil:

1. Navigieren Sie zu **Sicherheit** > **WAF-Lernen** > **Lernprofile**
2. Klicken Sie auf **Hinzufügen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Auf der Seite **Profilkonfiguration hinzufügen** geben Sie die folgenden Parameter an:

   a. **Lernprofilname** – Geben Sie einen Namen Ihrer Wahl an.

      Wählen Sie die Option **Aktivieren** aus. Standardmäßig ist diese Option ausgewählt. Wenn Sie diese Option deaktivieren, ist das Profil nicht aktiv.

   b. **Lernverhalten** – Wählen Sie das Lernverhalten aus, um Regeln zu generieren, Regeln zu entfernen oder beides.

      i. **Regeln lernen** – Generiert die Ausnahmeregel und ermöglicht dem Administrator, diese entweder bereitzustellen oder zu überspringen.

      ii. **Inaktive Regeln entfernen** – Entfernt die Ausnahmeregel, wenn die konfigurierte Leerlaufzeit den Schwellenwert überschreitet.

      iii. **Regeln lernen & inaktive Regeln entfernen** – Generiert die Ausnahmeregeln und entfernt diese auch, wenn kein eingehender Datenverkehr vorhanden ist.

      HINWEIS

      - Die Option zum Entfernen von Regeln wird nur für die Sicherheitsprüfungen **Start-URL**, **Deny-URL**, **HTML Cross-Site Scripting** und **HTML SQL Injection** unterstützt.
      - Wenn Sie die Option **Regel entfernen** auswählen, werden die unterstützten Sicherheitsprüfungsoptionen angezeigt.

   c. **Lerngruppe** – Wählen Sie entweder **Profilbasiert** oder **Anwendungsbasiert**.

   d. **WAF-Profil auswählen** – Diese Option wird angezeigt, wenn Sie **Profilbasiert** auswählen. Wählen Sie die erforderlichen WAF-Profile basierend auf Anwendungen oder Profilnamen aus.

   e. **Anwendungen auswählen** – Diese Option wird angezeigt, wenn Sie **Anwendungsbasiert** auswählen. Wählen Sie die Anwendungen aus der Liste aus und fügen Sie sie hinzu.

   f. Unter **Sicherheitsprüfung** wählen Sie die Optionen für Sicherheitsprüfungen aus, für die Sie Maßnahmen bei den in NetScaler Console gemeldeten Verstößen ergreifen möchten. Wenn Sie eine Option auswählen, müssen Sie die folgenden Informationen angeben:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. **Mindestanzahl von Sitzungen** – Geben Sie die Sitzungen an. NetScaler Console überwacht die angegebenen Sitzungen, die auf der NetScaler-Instanz auftreten sollen, um sie in der Ausnahmeliste zu melden.

ii. **Automatische Bereitstellung** – Diese Option ermöglicht es den Administratoren, eine Aktion (Bereitstellen oder Überspringen) durchzuführen. Sie müssen die Karenzzeit (Format: Tage, Stunden und Minuten) angeben, für die NetScaler Console diese Verstöße in der Liste der Ausnahmeregeln behält.

Die maximale Karenzzeit, die Sie angeben können, beträgt 30 Tage.

iii. Wenn Sie die Option **Regel entfernen** ausgewählt haben, geben Sie die **Leerlaufzeit (Tag)** in Tagen und Stunden an. Wenn NetScaler nach diesem Zeitraum keinen eingehenden Datenverkehr für diese Sicherheitsprüfung empfängt, wird die Regel automatisch entfernt.

Standardmäßig beträgt die Leerlaufzeit 7 Tage, Sie können diese Zeit jedoch auf nicht weniger als 23 Stunden konfigurieren.

g. Wählen Sie unter **Benachrichtigungseinstellungen** die Benachrichtigungsoptionen aus, über die Sie über Verstöße informiert werden möchten. Die verfügbaren Benachrichtigungsoptionen sind E-Mail, SMS, Slack und ServiceNow.

Nachdem Sie die Benachrichtigungsoptionen ausgewählt haben, können Sie entweder aus dem vorhandenen verteilten Profil auswählen oder ein Profil erstellen.

h. Klicken Sie auf **Erstellen**.

Details zu Netzwerkverstößen

HTTP Slow Loris

Slow Loris ist ein Denial-of-Service-Angriff, der HTTP-Header so langsam wie möglich an die Zielanwendung senden kann. Die Zielanwendung ist gezwungen, auf das Eintreffen der Header zu warten und kann auch schnell nicht mehr verfügbar sein, um Anfragen zu bearbeiten, wenn mehrere ähnliche Verbindungen geöffnet werden. Wenn eine NetScaler-Instanz ein hohes Volumen an HTTP-Anfragen empfängt, erhöht sich der HTTP-Header und es dauert lange, die Anfragen abzuschließen. Dieser Prozess kann die Ressourcen des Anwendungsservers erschöpfen und zu einem **HTTP Slow Loris**-Angriff führen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mithilfe des Indikators **HTTP Slow Loris** können Sie die Anfragen analysieren, die zu einem **HTTP Slow Loris**-Angriff geführt haben.

Die **Empfohlenen Aktionen** zur Behebung des Problems:

- Erwägen Sie, die Konfiguration für die unvollständige Header-Verzögerung (incompHdrDelay) auf einen kleineren Wert einzustellen.
- Standardmäßig verwirft die NetScaler-Instanz diese unvollständigen Anfragen.

Unter **Ereignisdetails** können Sie Folgendes anzeigen:

- Die betroffene Anwendung. Sie können die Anwendung auch aus der Liste auswählen, wenn zwei oder mehr Anwendungen von Verstößen betroffen sind.
- Das Diagramm, das alle Verstöße anzeigt
- Die Uhrzeit des Auftretens des Verstoßes
- Die Erkennungsmeldung, die die gesamten unvollständigen Anfragen als **Slow Loris**-Angriff anzeigt

DNS Slow Loris

Der Indikator **DNS Slow Loris** erkennt, wenn ein NetScaler eine hohe Anzahl von DNS-Anfragen empfängt, die sich über mehr als ein Paket erstrecken. Dieser Prozess kann die DNS-Serverressourcen erschöpfen und zu einem **DNS Slow Loris**-Angriff führen. Standardmäßig verwirft die NetScaler-Instanz diese **DNS Slow Loris**-Anfragen, und es sind keine weiteren Maßnahmen zur Behebung dieses Problems erforderlich.

Unter **Ereignisdetails** können Sie Folgendes anzeigen:

- Die betroffene Anwendung. Sie können die Anwendung auch aus der Liste auswählen, wenn zwei oder mehr Anwendungen von Verstößen betroffen sind.
- Das Diagramm, das alle Verstöße anzeigt
- Die Uhrzeit des Auftretens des Verstoßes
- Die Erkennungsmeldung, die die gesamten DNS-Anfragen als **Slow Loris**-Angriff anzeigt

HTTP Slow Post

Der **Slow Post** ist ein Denial-of-Service-Angriff, der HTTP-POST-Header an eine Zielanwendung senden kann. In den Headern sind die Größen der Nachrichtentexte korrekt angegeben, aber der Nachrichtentext wird mit geringer Geschwindigkeit gesendet. Die Zielanwendung wird zum Warten

© 1997–2026 Citrix Systems, Inc. All rights reserved.

gezwungen und kann auch schnell nicht mehr in der Lage sein, Anfragen zu bearbeiten, wenn mehrere ähnliche Verbindungen geöffnet werden.

Dieser Prozess kann die Ressourcen des Anwendungsservers erschöpfen und zu einem **HTTP Slow Post**-Angriff führen.

Mithilfe des **HTTP Slow Post**-Indikators können Sie die Anfragen analysieren, die zu einem Slow Post-Angriff geführt haben.

Die **empfohlene Maßnahme** zur Behebung dieses Problems besteht darin, das Anforderungs-Timeout im NetScaler HTTP-Profil zu aktivieren und zu konfigurieren. Weitere Informationen finden Sie unter HTTP-Konfigurationen.

Unter **Ereignisdetails** können Sie Folgendes anzeigen:

- Die betroffene Anwendung. Sie können die Anwendung auch aus der Liste auswählen, wenn zwei oder mehr Anwendungen von Verstößen betroffen sind.
- Das Diagramm, das alle Verstöße anzeigt
- Die Zeit des Auftretens des Verstoßes
- Die Erkennungsmeldung, die die gesamten POST-Anfragen als **Slow-Loris**-Angriff anzeigt

NXDOMAIN-Flood-Angriff

Der **NXDOMAIN-Flood-Angriff** ist ein Distributed-Denial-of-Service (DDoS)-Angriff, der auf einen DNS-Server oder eine NetScaler-Instanz (die als DNS-Proxyserver konfiguriert ist) abzielen und eine große Menge nicht existierender oder ungültiger Anfragen senden kann. Dieser Angriff kann den DNS-Server oder die NetScaler-Instanz beeinträchtigen, was zu einer Verlangsamung oder dazu führt, dass Anfragen keine Antwort erhalten.

Mithilfe des Indikators **NXDOMAIN-Flood-Angriff** können Sie analysieren, ob die Anfragen zu einem NXDOMAIN-Angriff geführt haben.

Die **empfohlenen Maßnahmen** zur Behebung des Problems:

- Prüfen Sie auf ungewöhnlich hohen Ressourcenverbrauch sowohl auf dem DNS-Server als auch auf dem DNS-Proxyserver.
- Erzwingen Sie eine Begrenzung der Anfragerate auf der NetScaler-Instanz.
- Verdächtige Client-IP-Adressen isolieren und blockieren

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wenn die meisten Namen zu NXDOMAIN führen, folgen Sie einem identifizierbaren Muster und konfigurieren Sie DNS-Richtlinien, um solche Anfragen zu verwerfen.
- Um Speicher für echte DNS-Einträge zu sparen, konfigurieren Sie ein Limit für negative Einträge auf der NetScaler-Instanz. Weitere Informationen finden Sie unter DNS-DDoS-Angriffe mindern.

Unter **Ereignisdetails** können Sie Folgendes anzeigen:

- Die betroffene Anwendung. Sie können die Anwendung auch aus der Liste auswählen, wenn zwei oder mehr Anwendungen von Verstößen betroffen sind.
- Das Diagramm, das alle Verstöße anzeigt

HTTP-Desync-Angriff

Bei einem HTTP-Desync-Angriff wird eine einzelne HTTP-Anfrage interpretiert als:

- Eine einzelne Anfrage an den Front-End-Server (virtueller Server)
- 2 Anfragen an den Back-End-Server

In diesem Szenario interpretiert der Back-End-Server die zweite Anfrage als von einem anderen Client stammend. Die Verbindung zwischen dem virtuellen Server und dem Back-End-Server wird für verschiedene Anfragen wiederverwendet. Wenn die erste Client-Anfrage von einem bösartigen Client mit bösartigen Daten verarbeitet wird, kann die nächste Client-Anfrage eine angepasste Anfrage sein. Diese Aktivität kann einen Angriff verursachen, indem die Kombination zweier Header missbraucht wird: Content-Length und Transfer-Encoding.

Mithilfe des Indikators **HTTP-Desync-Angriff** können Sie analysieren, ob die NetScaler-Instanz möglicherweise einem HTTP-Desync-Angriff ausgesetzt ist, der aufgrund des Vorhandenseins von Folgendem aufgetreten ist:

- Content-Length- und Transfer-Encoding-Header in einer einzelnen HTTP-Transaktion
- Mehrere Content-Length-Header mit unterschiedlichen Werten in einer einzelnen HTTP-Transaktion

Die **Empfohlene Aktion** schlägt vor, ungültige HTTP-Transaktionen zu verwerfen.

Unter **Ereignisdetails** können Sie Folgendes anzeigen:

- Die betroffene Anwendung. Sie können die Anwendung auch aus der Liste auswählen, wenn zwei oder mehr Anwendungen von dieser Verletzung betroffen sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Das Diagramm mit den Details zur Verletzung. Bewegen Sie den Mauszeiger über das Balkendiagramm, um die Gesamtzahl der ungültigen Anfragen/Antworten anzuzeigen.
- Die Erkennungsmeldung für die Verletzung, die die Gesamtzahl der Anfragen/Antworten angibt:
  - Die mehrere Content-Length-Header mit unterschiedlichen Werten enthalten
  - Enthält sowohl Content-Length- als auch Transfer-Encoding-Header

Bleichenbacher-Angriff

Die NetScaler-Instanz erkennt, ob eine gegebene Byte-Sequenz einer verschlüsselten Nachricht nach der Entschlüsselung das korrekte Padding-Format aufweist.

Mithilfe des Indikators **Bleichenbacher-Angriff** können Sie analysieren, ob die NetScaler-Instanz SSL/TLS-Handshake-Verbindungen mit fehlerhaften verschlüsselten Daten empfängt.

Die **Empfohlene Aktion** zeigt an, dass keine weiteren Maßnahmen erforderlich sind, da die NetScaler-Instanz die Handshake-Verbindungen beendet und diesen Angriff abwehrt.

Unter **Ereignisdetails** können Sie Folgendes anzeigen:

- Die betroffene Anwendung. Sie können die Anwendung auch aus der Liste auswählen, wenn zwei oder mehr Anwendungen von dieser Verletzung betroffen sind.
- Das Diagramm mit den Details zur Verletzung. Bewegen Sie den Mauszeiger über das Balkendiagramm, um die insgesamt erkannten fehlerhaften Handshake-Verbindungen anzuzeigen.
- Die Erkennungsmeldung für die Verletzung, die die Gesamtzahl der Handshake-Verbindungen auf dem virtuellen Server mit fehlerhaften verschlüsselten Daten angibt.

Segment-Smack-Angriff

Ein **Segment-Smack-Angriff** ist ein Denial-of-Service (DoS)-Angriff, bei dem der Angreifer ungeordnete kleine Pakete während einer TCP-Sitzung senden kann. Diese angepassten TCP-Pakete können CPU und Arbeitsspeicher beeinträchtigen und zu einem Denial of Service auf der NetScaler-Instanz führen.

Mithilfe des Indikators **Segment-Smack-Angriff** können Sie analysieren, ob eine NetScaler-Instanz eine größere Anzahl von TCP-Paketen als das konfigurierte Warteschlangenlimit empfangen hat. Weitere Informationen finden Sie unter TCP-Konfiguration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Als Administrator sind keine weiteren Maßnahmen erforderlich, da die NetScaler-Instanz diesen Angriff abwehrt, indem sie alle überschüssigen TCP-Pakete verwirft.

Unter **Ereignisdetails** können Sie Folgendes anzeigen:

- Die betroffene NetScaler-Instanz
- Das Diagramm mit den Details zur Verletzung. Bewegen Sie den Mauszeiger über das Balkendiagramm, um die Gesamtzahl der erkannten fehlerhaften Clientverbindungen anzuzeigen.
- Die Erkennungsmeldung für die Verletzung, die die Gesamtzahl der abgebrochenen Clientverbindungen angibt.

SYN-Flood-Angriff

Ein SYN-Flood-Angriff ist ein Denial-of-Service (DoS)-Angriff, der das Zielsystem beeinträchtigen kann, indem Tausende von Verbindungsanfragen mit gefälschten IP-Adressen gesendet werden. Wenn eine NetScaler-Instanz einem **SYN-Flood**-Angriff ausgesetzt ist, versucht die Instanz, für jede bösartige Anfrage eine Verbindung zu öffnen und wartet dann auf ein Bestätigungspaket, das niemals ankommt.

Der **SYNCOOKIE** im TCP-Profil verhindert SYN-Angriffe auf die NetScaler-Appliance. Standardmäßig ist der **SYNCOOKIE** auf der NetScaler-Instanz aktiviert. Die Wahrscheinlichkeit, dass die NetScaler-Instanz einem SYN-Flood-Angriff ausgesetzt ist, ist nur dann hoch, wenn `SYNCOOKIE` deaktiviert ist. Weitere Informationen finden Sie unter Layer 3–4 SYN Denial-of-Service protection.

Mithilfe des Indikators **SYN-Flood-Angriff** können Sie analysieren, ob die NetScaler-Instanz einem SYN-Angriff ausgesetzt ist.

Als Administrator empfiehlt die **Empfohlene Aktion**, `SYN COOKIE` im TCP-Profil zu aktivieren.

Unter **Ereignisdetails** können Sie Folgendes anzeigen:

- Die betroffene Anwendung. Sie können die Anwendung auch aus der Liste auswählen, wenn zwei oder mehr Anwendungen von dieser Verletzung betroffen sind.
- Das Diagramm mit den Details zum SYN-Angriff
- Die Erkennungsmeldung, die angibt, wie oft die Anwendung mit dem SYN-Angriff erkannt wurde.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Small Window Attack

Ein **Small Window Attack** ist ein Denial-of-Service (DoS)-Angriff, der die Zielmaschine beeinträchtigen kann, indem er Tausende von TCP-Paketen mit entweder kleinerer Fenstergröße oder Fenstergröße 0 sendet. Die Fenstergröße 0 zeigt an, dass die Zielmaschine keine weiteren Daten senden soll, bis sie eine weitere Benachrichtigung erhält. Durch das Senden von so vielen ähnlichen Verbindungen an die Zielmaschine wird der Speicher der Zielmaschine maximal ausgelastet und reagiert nicht mehr.

Mithilfe des Indikators **Small Window Attack** können Sie analysieren, ob die NetScaler-Instanz einem Sockstress-Angriff ausgesetzt ist.

Standardmäßig entschärft die NetScaler-Instanz diesen Angriff, indem sie alle derartigen TCP-Small-Window-Pakete verwirft. Daher ist als Administrator keine weitere Aktion erforderlich.

Unter **Ereignisdetails** können Sie Folgendes anzeigen:

- Die betroffene Anwendung. Sie können die Anwendung auch aus der Liste auswählen, wenn zwei oder mehr Anwendungen von dieser Verletzung betroffen sind.
- Das Diagramm, das die Angriffsdetails anzeigt. Bewegen Sie den Mauszeiger auf das Balkendiagramm, um die Gesamtzahl der erkannten TCP-Small-Window-Pakete anzuzeigen.
- Die Erkennungsmeldung, die die Gesamtzahl der verworfenen TCP-Small-Window-Pakete angibt.

Zusammenfassung der WAF-Lernaktionen anzeigen

Auf der Seite **Zusammenfassung der Aktionen** des WAF-Lernens können Sie alle bereitgestellten Regeln anzeigen.

1 – Wählen Sie **Gelernte Regeln** oder **Inaktive Regeln** aus der Liste aus, um Details im Dashboard anzuzeigen.

2 – Eine erweiterte Suchleiste, mit der Sie das Ergebnis basierend auf den Vorschlägen und Operatoren anzeigen können.

3 – Liste der Zeitdauern, für die Sie das Ergebnis anzeigen möchten

4 – Ein Ergebnis im Diagrammformat, mit dem Sie das Diagramm ziehen und auswählen können, um die Ergebnisse zu filtern

5 – Die Details der bereitgestellten oder entfernten Regeln

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Klicken Sie auf **>** , um die Details anzuzeigen.

Fehlgeschlagene Regeln anzeigen

Wenn eine bereitgestellte Lernregel fehlgeschlagen ist, können Sie den Grund für den Fehler anzeigen.

Erweiterte Suche

Die erweiterte Suchleiste ermöglicht es Ihnen, die Ergebnisse nach Ihren Anforderungen anzuzeigen. Wenn Sie auf das Suchfeld klicken, erhalten Sie eine Liste mit Suchvorschlägen. Sie können auch Operatoren in Ihren Suchanfragen verwenden, um den Fokus Ihrer Suche einzugrenzen.

Die folgenden Vorschläge werden angezeigt, wenn Sie den Mauszeiger auf das Suchfeld bewegen:

- **Learn-Profile-Name** – Gibt den Namen des Lernprofils an, das Sie konfiguriert haben.
- **Rule-Type** – Gibt den Regeltyp an (Verweigern oder Zulassen).
- **Violation-Name** – Gibt den Namen der Verletzung an, z. B. Start-URL, Cross-Site-Script und so weiter.
- **URL** – Gibt die URL der Webanwendung an.
- **Status** – Gibt den Status der bereitgestellten Regel an.
- **Field-Name** – Gibt den Feldnamen an, der in den Webformularen für die Sicherheitsprüfung von Formularfeldern aktualisiert wurde.
- **Violation-String** – Gibt die mögliche Zeichenfolge an, von der die Verletzung ausgegangen ist.
- **Value-Type** – Gibt die bei den Sicherheitsprüfungen verwendeten Datentypen an. Zum Beispiel Schlüsselwort.

Ergebnisse filtern

In der **Aktionsübersicht** können Sie die Ergebnisse filtern, indem Sie die folgenden Optionen auswählen:

- **Learn Profile Name** – Filtern nach dem Namen des Lernprofils.
- **Violation Name** – Filtern nach dem Namen der Verletzung, z. B. Start-URL, HTML-Cross-Site-Scripting, Inhaltstyp und so weiter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Status** – Filtern nach dem Status der bereitgestellten oder inaktiven Regeln.
- **Action By** – Filtern nach dem Benutzer.

Entspannungsregeln, Leerlauf- und Ablehnungsregeln anzeigen

Nachdem Sie das Lernprofil konfiguriert haben, beginnt NetScaler Console, eine Liste von Entspannungs-, Leerlauf- und Ablehnungsregeln abzurufen.

1. Navigieren Sie zu **Security** > **WAF Learning** > **Learn Profiles**.

   Die Seite **Learn Profiles** zeigt den Namen des WAF-Lernprofils, die insgesamt zugeordnete NetScaler-Instanz, das auf der Instanz erstellte WAF-Profil, die insgesamt gelernten Regeln, die insgesamt bereitgestellten Regeln und den Status an.

2. Wählen Sie den Profilnamen aus und klicken Sie auf **Manage Relaxation Rules**.

   Sie können die Gesamtzahl der Regeln, die insgesamt gelernten Regeln, die insgesamt bereitgestellten Regeln und die insgesamt inaktiven Regeln für das ausgewählte Profil anzeigen.

   - Auf der Registerkarte **Learned Rules** können Sie die gelockerten Regeln anzeigen. Wählen Sie die Regel aus, validieren Sie sie und klicken Sie auf **Add & Deploy**, **Deploy**, **Edit & Deploy**, **Delete** oder **Deploy as Deny**.
     - **Add & Deploy** – Ermöglicht das Erstellen einer neuen Regel mit den Sicherheitsprüfungsoptionen. Nachdem Sie die Regel erstellt haben, klicken Sie auf **Deploy**.
     - **Deploy** – Ermöglicht die Bereitstellung der gelockerten Regel.
     - **Edit & Deploy** – Ermöglicht das Bearbeiten der Regel, bevor Sie sie bereitstellen möchten. Für die SQL-Sicherheitsprüfung können Sie die Regel bearbeiten und den **Rule Type** in **Deny** ändern und dann bereitstellen.

       Weitere Informationen finden Sie unter Entspannungs- und Ablehnungsregeln für die Behandlung von HTML-SQL-Injection-Angriffen.
     - **Delete** – Ermöglicht das Löschen der Regel ohne weitere Aktion.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - **Als Ablehnung bereitstellen** – Für die SQL-Sicherheitsprüfung können Sie diese Option verwenden, um Anfragen abzulehnen.

- Klicken Sie auf die Registerkarte **Bereitgestellte Regeln**, um die bereitgestellten Regeln anzuzeigen. Wählen Sie eine Regel aus und entscheiden Sie, ob Sie die Regel löschen, aktivieren oder deaktivieren möchten.
- Klicken Sie auf die Registerkarte **Inaktive Regeln**, um die inaktiven Regeln anzuzeigen, die keinen Datenverkehr aufweisen. Klicken Sie auf **Löschen**, wenn Sie die Regel löschen möchten.

HINWEIS

Die Verletzungsliste ist bis zur konfigurierten Kulanzdauer verfügbar. Nach dem Kulanzzeitraum stellt NetScaler Console die verfügbaren Verletzungen automatisch bereit.

Für jedes konfigurierte Lernprofil können Sie bis zu 1 Million gelernte Regeln anzeigen.

Ablehnungsregeln verwalten

Zusätzlich zum Relaxationsmodus (Zulassen) können Sie auch die Ablehnungsregeln für die Sicherheitsprüfung von HTML-SQL-Injection-Angriffen konfigurieren und verwenden. Wenn Sie die HTML-SQL-Injection-Sicherheitsprüfung im Ablehnungsmodus konfigurieren, werden die erkannten Verletzungen blockiert.

Auf der Registerkarte **Ablehnungsregeln verwalten** können Sie die abgelehnten Regeln für HTML-SQL-Injection-Prüfungen anzeigen. Wählen Sie die Regel aus, validieren Sie sie und klicken Sie auf **Hinzufügen & Bereitstellen**, **Bereitstellen**, **Bearbeiten & Bereitstellen**, **Löschen** oder **Als Relaxation bereitstellen**.

- **Hinzufügen & Bereitstellen** – Ermöglicht Ihnen, eine neue Regel mit den Sicherheitsprüfungsoptionen zu erstellen. Nachdem Sie die Regel erstellt haben, klicken Sie auf **Bereitstellen**.
- **Bereitstellen** – Ermöglicht Ihnen, die abgelehnte Regel bereitzustellen.
- **Bearbeiten & Bereitstellen** – Ermöglicht Ihnen, die Regel zu bearbeiten, bevor Sie sie bereitstellen möchten.
- **Löschen** – Ermöglicht Ihnen, die Regel ohne weitere Aktion zu löschen.
- **Als Relaxation bereitstellen** – Erlaubt den Datenverkehr.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL Insight

SSL Insight bietet Einblick in sichere Webtransaktionen (HTTPS) und ermöglicht IT-Administratoren, alle sicheren Webanwendungen, die vom NetScaler bereitgestellt werden, zu überwachen, indem es eine integrierte Echtzeit- und historische Überwachung sicherer Webtransaktionen bietet. Mit dieser Transparenz kann der Administrator Folgendes bewerten:

- **Auswirkungen von Konfigurationsänderungen auf die Kundennutzung ermitteln**. Der Administrator kann die Auswirkungen auf Clients verstehen, wenn eine Konfigurationsänderung vorgenommen wird, z. B. das Deaktivieren von SSLv3 oder das Entfernen einer Chiffre wie RC4-MD5. Dies kann durch die Bewertung der historischen Transaktionsdaten zu diesem Protokoll und dieser Chiffre erfolgen.
- **Clientleistung quantifizieren**. Der Administrator kann die Auswirkungen auf die Anwendungsantwortzeit basierend auf den verwendeten SSL-Chiffren/Protokollen oder den ausgehandelten Zertifikaten verstehen.
- **Anwendungssicherheit**. Beurteilen Sie, ob Transaktionen einer der Anwendungen mit Protokollen, Chiffren oder einer Schlüsselschwäche mit geringer Sicherheit ausgeführt werden.

Wenn SSL Analytics auf einer NetScaler-Instanz aktiviert ist, werden SSL-Statistiken für jede SSL-Transaktion aufgezeichnet und protokolliert. Die Statistiken zeigen die Details des SSL-Flusses. Außerdem wird jede erfolgreiche Verbindung von NetScaler Console protokolliert und angezeigt.

SSL Insight bietet die folgenden kritischen Informationen, die von NetScaler Console Analytics angezeigt werden:

- Ausgehandelte SSL-Protokollversion
- Ausgehandelte Chiffre und die Chiffrierstärke
- Signatur-Hash-Algorithmus des verwendeten Zertifikats
- Zertifikatstyp und -größe
- SSL-Frontend- und Backend-Fehler

HINWEIS

Bei erfolgreichen SSL-Verbindungen erfolgt die SSL AppFlow®-Protokollierung am Ende jeder Transaktion.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Voraussetzungen

- Die NetScaler-Instanz, auf der Sie SSL Insight konfigurieren möchten, muss NetScaler Software Release 11.1 51.21 oder höher ausführen. Führen Sie die folgenden Befehle auf der NetScaler-Instanz mit 11.1 51.21 aus, um **Logstream** als Transporttyp für SSL Insight zu aktivieren.

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the NetScaler Console>`

   Wählen Sie für NetScaler-Instanzen ab Version 12.0 **Logstream** als Transporttyp aus, während Sie AppFlow über die NetScaler Console aktivieren.

- Die Version und der Build der NetScaler Console müssen gleich oder höher sein als die Version und der Build des NetScaler. Wenn Sie beispielsweise NetScaler Console 11.1 Build 61.7 installiert haben, stellen Sie sicher, dass Sie NetScaler 11.1 Build 60.14 oder früher installiert haben.

SSL Insight konfigurieren

SSL Insight-Metriken sind in Web Insight-Berichten enthalten, wenn Sie die folgenden Elemente aktivieren:

- AppFlow für Web Insight auf jeder NetScaler-Instanz aktivieren.
- ULFD-Modus auf jeder NetScaler-Instanz aktivieren.
- Erforderliche AppFlow-Parameter auf jeder NetScaler-Instanz aktivieren.

Das Insight aktivieren

HINWEIS

Sie können die AppFlow-Funktion entweder über die NetScaler Console oder von jeder NetScaler-Instanz aus aktivieren.

AppFlow-Funktion über die NetScaler Console aktivieren

1. Navigieren Sie zu **Infrastructure > Instances**, und wählen Sie die NetScaler-Instanz aus, auf der Sie die Analyse aktivieren möchten.
2. Wählen Sie in der Liste **Aktion auswählen** die Option **Analytics konfigurieren**.
3. Auf der Seite **Analytics auf virtuellen Servern konfigurieren**:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. Wählen Sie die virtuellen Server aus, für die Sie Web Insight aktivieren möchten, und klicken Sie auf **Sicherheit & Analytics aktivieren**.

   Das Fenster **Sicherheit & Analytics aktivieren** wird angezeigt.

b. Wählen Sie **Web Insight** aus.

c. Wählen Sie unter **Erweiterte Optionen** entweder **Logstream** oder **IPFIX** als Transportmodus aus.

   HINWEIS

   Für NetScaler 12.0 oder früher ist **IPFIX** die Standardoption für den Transportmodus. Für NetScaler 12.0 oder höher können Sie entweder **Logstream** oder **IPFIX** als Transportmodus auswählen.

   Weitere Informationen zu **IPFIX** und **Logstream** finden Sie unter **Logstream-Übersicht**.

d. Der Ausdruck ist standardmäßig wahr.

e. Klicken Sie auf **OK**.

HINWEIS

Sie können die Datenerfassung auf einem virtuellen Server nicht aktivieren, wenn der Betriebsstatus des virtuellen Servers nicht UP ist.

Aktivieren Sie die AppFlow-Funktion mithilfe der NetScaler-GUI

Navigieren Sie in der GUI einer NetScaler-Instanz zu **Configuration** > **System** > **Settings**, klicken Sie auf **Configure Advanced Features** und wählen Sie **AppFlow**.

ULFD-Modus aktivieren

Nachdem Sie den ULFD-Modus auf den NetScaler-Instanzen aktiviert haben, auf denen die virtuellen Server konfiguriert sind, streamt der ULFD-Server die Analysedaten von den NetScaler-Instanzen an NetScaler Console.

SSL Insight-Parameter aktivieren

Auf jeder NetScaler-Instanz müssen Sie einige HTTP-Parameter aktivieren, um SSL Insight-Datensätze in NetScaler Console anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL Insight-Parameter über das NetScaler-Konfigurationsdienstprogramm aktivieren

1. Navigieren Sie zu **Configuration** > **System** > **AppFlow** und klicken Sie auf **Change AppFlowSettings**.
2. Aktivieren Sie die folgenden Kontrollkästchen: **HTTP Domain**, **HTTP Host**, **HTTP Method**, **HTTP URL**, **HTTP User-Agent**, **HTTP Content-Type**.
3. Klicken Sie auf **OK**.

SSL Insight-Metriken anzeigen

SSL Insight-Metriken in NetScaler Console bieten eine detaillierte Ansicht der Leistung der von den NetScaler-Instanzen bereitgestellten SSL-Transaktionen. Sie können die SSL Insight-Metriken auf Client-, Server- oder Anwendungsebene sowie die Metriken für erfolgreiche und fehlgeschlagene SSL-Transaktionen anzeigen. Mithilfe dieser Metriken können Sie Ihre NetScaler HTTPS-Einstellungen und SSL-Zertifikatseinstellungen analysieren und optimieren sowie Leistungsprobleme verfolgen.

HINWEIS

Wenn Sie eine Gruppe erstellen, können Sie der Gruppe Rollen zuweisen, der Gruppe Zugriff auf Anwendungsebene gewähren und Benutzer der Gruppe zuweisen. NetScaler Console Analytics unterstützt jetzt die virtuelle IP-adressbasierte Autorisierung. Ihre Benutzer können jetzt Berichte für alle Insights nur für die Anwendungen (virtuellen Server) sehen, für die sie autorisiert sind. Weitere Informationen zu Gruppen und dem Zuweisen von Benutzern zu Gruppen finden Sie unter Konfigurieren von Gruppen in NetScaler Console.

SSL Insight-Metriken in NetScaler Console überwachen

Als Administrator können Sie SSL-Metriken anzeigen für:

- Eine Anwendung. Navigieren Sie zu **Applications > Dashboard**, klicken Sie auf eine Anwendung und wählen Sie die Registerkarte **Web Insight**, um die detaillierten Metriken anzuzeigen. Weitere Informationen finden Sie unter Application Usage Analytics.
- Alle Anwendungen. Navigieren Sie zu **Applications > Web Insight** und klicken Sie auf die Registerkarten **Applications** und **Clients**, um die SSL-Metriken anzuzeigen.

Anwendungsfall: Überblick über die SSL-Transaktionen erhalten

Der folgende Anwendungsfall beschreibt, wie Sie SSL Insight verwenden können, um die Nutzung verschiedener SSL-Parameter zu bewerten und Sicherheitsmaßnahmen zu verbessern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Angenommen, Sie haben eine Reihe von Anwendungen, die SSL-Transaktionen (HTTPS) für die Kommunikation verwenden, und Sie haben NetScaler Console so konfiguriert, dass die SSL-Komponenten überwacht werden. Möglicherweise müssen Sie die Anwendungen häufig überprüfen, damit Sie sich zuerst auf die Anwendungen konzentrieren können, die die meiste Aufmerksamkeit benötigen. Das **Web Insight**-Dashboard für eine Anwendung oder alle Anwendungen bietet eine Zusammenfassung der folgenden SSL-Parameter unter **SSL Errors** und **SSL Usage**:

- SSL-Zertifikate
- SSL-Protokolle
- SSL-Chiffre
- SSL-Schlüsselstärke
- SSL-Fehler – Frontend
- SSL-Fehler – Backend

Sie können auf jede Registerkarte klicken, um Details anzuzeigen.

Anwendungsfall: SSL-Metriken für Clients

Sie können eine Liste der Clients (identifiziert durch ihre IP-Adressen) und die Gesamtzahl der Vorkommen pro Client sehen. Navigieren Sie zu **Applications > Web Insight** und wählen Sie die Registerkarte **Clients**, um die Details unter **SSL Usage** anzuzeigen.

Klicken Sie auf eine Metrik, um Details anzuzeigen, und klicken Sie unter **Clients** auf eine beliebige Client-IP-Adresse, um die SSL-Metriken für den ausgewählten Client anzuzeigen.

Analysen für Web-Transaktionen anzeigen

Web-Transaktionsanalysen ermöglichen die Anzeige detaillierter Transaktionen für:

- Antwortzeit > 500 ms
- 5xx-Fehler

HINWEIS:

Sie können nur einige Beispiel-2xx-Transaktionen für die ausgewählte Anwendung anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Voraussetzungen

Um die Web-Transaktionsanalysen anzuzeigen, müssen Sie:

1. Navigieren Sie zu **Einstellungen > Analyse-Einstellungen > Funktionen für Analysen aktivieren**, und wählen Sie eine der folgenden Optionen aus:

   - **Keine** – Es werden keine Daten angezeigt.
   - **Alle** – Zeigt alle HTTP-Transaktionen an. Wenn Sie diese Option auswählen, verbraucht NetScaler Console mehr Speicherplatz. Stellen Sie sicher, dass Sie diese Option nur für kritische Anwendungen verwenden.
   - **Anomal** – Zeigt Transaktionen mit 5xx-Fehler und einer Antwortzeit > 500 ms an.

2. Wählen Sie **Detaillierte Web-Transaktionen** unter **Web Insight** aus, wenn Sie Analysen für die virtuellen Server aktivieren.

   HINWEIS:

   Ab Build 14.1-44.x ist **Web Transaction Analytics** auf der Ebene des virtuellen Servers verfügbar.

Detaillierte Webtransaktionen

Diese Funktion ermöglicht es Ihnen nicht nur, detaillierte Transaktionen zu untersuchen, sondern auch die Metriken (wie Client-RTT, Server-Antwortzeit und SSL-Metriken) visuell aufgeteilt nach Client, NetScaler und Server zu verstehen.

HINWEIS:

In einigen Szenarien ist NetScaler möglicherweise nicht in der Lage, die RTT-Werte für bestimmte Transaktionen zu berechnen. Für solche Transaktionen zeigt NetScaler Console die RTT-Werte wie folgt an:

- **NA** – Wird angezeigt, wenn die NetScaler-Instanz den RTT nicht berechnen kann.
- **< 1ms** – Wird angezeigt, wenn die NetScaler-Instanz den RTT in Dezimalwerten zwischen 0 ms und 1 ms berechnet. Zum Beispiel 0,22 ms.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sie können die detaillierten Transaktionen für Folgendes anzeigen:

- **Anwendungen** – Navigieren Sie zu **Applications > Dashboard**, wählen Sie eine Anwendung aus und klicken Sie auf **Transaction Log**.

- **Kubernetes-Anwendungen** – Navigieren Sie zu **Applications** > **Service Graph**. Klicken Sie auf einen Dienst und wählen Sie dann **Transaction Logs**.

  HINWEIS:

  Sie können die Fehler anzeigen, indem Sie den Mauszeiger über einen fehlerhaften Dienst bewegen und auf die Anzahl der Probleme klicken.

Die detaillierte Transaktion mit der **Transaktionsübersicht** für die ausgewählte Anwendung wird angezeigt.

Fahren Sie mit dem Mauszeiger über **App-Antwort**, um Details wie RTT und Verarbeitungszeit von der NetScaler-Instanz und dem Server anzuzeigen.

Das folgende Beispiel hilft Ihnen zu analysieren, dass das Problem vom Server kommt. Die Server-Antwortzeit beträgt 10 Sekunden.

Sie können auch ziehen und auswählen, um die Transaktionen für einen bestimmten Zeitraum anzuzeigen.

Ausgewählte Transaktion(/en-us/netscaler-console-service/media/select-transaction.png)

Ereignisse anzeigen

Sie können die detaillierten Informationen zu einem bestimmten Ereignis anzeigen. Im Bereich **Transaktionsübersicht** können Sie die Ergebnisse filtern, indem Sie die Optionen aus jeder Metrik auswählen.

Nehmen wir zum Beispiel an, Sie möchten 4xx-Transaktionen anzeigen.

Klicken Sie im Panel **Transaktionsübersicht** auf **Antwortcode**, und wählen Sie **404** aus, um das Ergebnis anzuzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Klicken Sie auf eine Transaktion, um die Details anzuzeigen, die die Metrikinformationen vom Client zum Server darstellen.

Für Transaktionen mit SSL-Fehlern werden die Details sowohl für Client als auch für Server angezeigt. Die folgenden SSL-Metriken werden angezeigt:

- SSL-Protokollversion
- SSL-Frontend-Fehler
- SSL-Chiffrierstärke
- SSL-Schlüsselstärke
- SSL-Zertifikatstyp

Sie können auch auf die SSL-Frontend- und SSL-Backend-Metriken im Bereich **Transaktionsübersicht** klicken, um die Ergebnisse zu filtern.

Um die Ergebnisse zu filtern, wählen Sie die unter **Transaktionsübersicht** verfügbaren Optionen aus.

- **Browser**: Die von den Clients verwendeten Browsertypen. Zum Beispiel: Chrome, Firefox.
- **Client-Betriebssystem**: Das Client-Betriebssystem basierend auf den User-Agent-Details des Browsers. Zum Beispiel: Windows
- **Gerät**: Die Geräte basierend auf den User-Agent-Details des Browsers. Zum Beispiel: Tablet, Mobiltelefon.
- **Anforderungstyp**: Der Transaktionsanforderungstyp. Zum Beispiel: GET.
- **Antwortcode**: Der vom Server empfangene Antwortcode. Zum Beispiel: 501, 404, 200.
- **Antwort-Inhaltstyp**: Der Transaktions-Inhaltstyp. Wenn die Client-Anfrage für text/html ist, muss die Antwort vom Server text/html sein.
- **Frontend-SSL-Protokollversion**: Die von den Clients verwendete SSL-Protokollversion. Zum Beispiel: SSLv3.
- **Frontend-SSL-Chiffrierstärke**: Die Chiffrierstärke basierend auf der Schlüsselgröße des SSL-Zertifikats, z. B. hoch, mittel und niedrig.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Frontend-SSL-Schlüsselstärke**: Die SSL-Chiffrierstärke wird aus der Schlüsselgröße des SSL-Zertifikats berechnet. Die Schlüssellänge definiert die Sicherheit des SSL-Algorithmus. Zum Beispiel: 2048
- **Frontend-SSL-Fehler**: Die Fehlermeldung des Frontend-SSL-Handshakes. Zum Beispiel: SSL CLIENTAUTH FAILURE
- **Frontend-SSL-Zertifikatstyp**: Der vom Client verwendete Zertifikatstyp. Zum Beispiel: RSA, DSA, ECDSA, DH.
- **Backend-SSL-Protokollversion**: Die vom Server verwendeten SSL-Protokolle. Zum Beispiel: SSLv3
- **Backend-SSL-Chiffrierstärke**: Die Chiffrierstärke basierend auf der Schlüsselgröße des SSL-Zertifikats, z. B. hoch, mittel und niedrig.
- **Backend-SSL-Schlüsselstärke**: Die SSL-Chiffrierstärke wird aus der Schlüsselgröße des SSL-Zertifikats berechnet. Die Schlüssellänge definiert die Sicherheit des SSL-Algorithmus. Zum Beispiel: 2048
- **Backend-SSL-Zertifikatstyp**: Der vom Server verwendete Zertifikatstyp. Zum Beispiel: RSA, DSA, ECDSA, DH.

Spalten in der Ereignisliste hinzufügen

Sie können auf die Schaltfläche

klicken, um die Liste der Optionen auszuwählen, und auf **Spalten hinzufügen** klicken, um die Details anzuzeigen.

Erweiterte Suche

Die **Transaktionsübersicht** verfügt auch über ein Suchtextfeld und eine Zeitdauerliste, in der Sie die Ereignisse nach Ihren Anforderungen anzeigen können. Wenn Sie den Cursor in das Suchfeld setzen, bietet Ihnen das Suchfeld eine Liste von Suchvorschlägen. Sie können auch Operatoren in Ihren Suchanfragen verwenden, um den Fokus Ihrer Suche einzugrenzen.

Im Folgenden sind die Operatoren aufgeführt, die Sie für Ihre Suchanfragen verwenden können:

OPERATOREN	BESCHREIBUNG	BEISPIEL	AUSGABE
=	Gleich einem Wert	Virtueller Server = test	Zeigt das Ereignis für den virtuellen Server

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPERATOREN	BESCHREIBUNG	BEISPIEL	AUSGABE
			mit dem Namen „test“ an
>	Größer als ein Wert	App-Response-Time > 500	Zeigt die Ereignisse für Anwendungen an, deren App-Antwortzeit mehr als 500 ms beträgt
<	Kleiner als ein Wert	App-Response-Time < 300	Zeigt die Ereignisse für die Anwendungen an, deren App-Antwortzeit weniger als 300 ms beträgt.
>=	Größer oder gleich einem bestimmten Wert	Total-Bytes >= 1024	Zeigt die Ereignisse für Transaktionen an, die größer oder gleich 1 KB sind.
<=	Kleiner oder gleich einem bestimmten Wert	Total-Bytes <= 1024	Zeigt die Ereignisse für Transaktionen an, die kleiner oder gleich 1 KB sind.
!=	Nicht gleich einem bestimmten Wert	Response-code != 200	Zeigt die Ereignisse mit allen Transaktionen an, außer den fehlgeschlagenen Transaktionen.
~	Enthält einen Wert	Virtueller Server ~ mas	Zeigt die Ereignisse für die virtuellen Server an, die den Namen mas haben.

Betrachten Sie beispielsweise ein Szenario, in dem Sie Ereignisse für Gesamtbytes generieren möchten, die kleiner als 300 Bytes sind. Geben Sie die Suchanfragen wie folgt an:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Geben Sie das gewünschte Wort in das Suchfeld ein, um die entsprechenden Vorschläge zu erhalten.

2. Wählen Sie **Total-Bytes** aus und klicken Sie erneut auf das Suchtextfeld, und wählen Sie **\<** aus.

3. Geben Sie den Wert 300 ein.

4. Wählen Sie den Zeitraum aus und klicken Sie auf **Suchen**, um die Ereignisse basierend auf Ihrer Suchanfrage anzuzeigen.

   Das Suchergebnis wird angezeigt.

Suche speichern

Nachdem Sie die Vorschläge und Operatoren verwendet haben, können Sie die Suchanfrage speichern. Sie können sie dann später aus der Liste verwenden, anstatt die Vorschläge und Operatoren erneut zu verwenden.

- Um eine Suchabfrage zu speichern, klicken Sie auf das Lesezeichensymbol, geben Sie einen Namen Ihrer Wahl an und klicken Sie dann auf **Speichern**.

- Um die Suchabfrage aus der Liste zu verwenden, klicken Sie auf das Symbol und wählen Sie die Suchabfrage aus der Liste aus, um die Ergebnisse anzuzeigen.

- Um die Suchabfrage zu entfernen, klicken Sie auf das Symbol, bewegen Sie den Mauszeiger über die gespeicherte Suchabfrage und klicken Sie auf **Entfernen**.

  Sie können auch auf das Lesezeichensymbol klicken und auf **Entfernen** klicken.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Daten exportieren

Sie können die Webtransaktionsanalysedaten für den ausgewählten Zeitraum exportieren, indem Sie auf das Symbol **Exportieren** klicken. Sie können im PDF-, PNG-, JPEG- und CSV-Format exportieren. Die Option **Exportieren** ermöglicht Ihnen Folgendes:

- Wählen Sie **Jetzt exportieren**, um den Bericht im PDF-, JPEG-, PNG- oder CSV-Format anzuzeigen und zu exportieren.
- Wählen Sie die Registerkarte **Export planen**, um den Bericht täglich, wöchentlich oder monatlich zu planen und den Bericht per E-Mail oder Slack-Nachricht zu senden.

Detaillierte Verfahren zur Einrichtung einer Dual-Tier- oder Service-Mesh-Lite-Topologie

Die Voraussetzungen für die Bereitstellung der Dual-Tier- oder Service-Mesh-Lite-Topologie finden Sie unter Einrichten des Service-Graphen.

Einen NetScaler-Agent konfigurieren

Um die Kommunikation zwischen dem Kubernetes-Cluster und der NetScaler Console zu ermöglichen, müssen Sie einen Agent installieren und konfigurieren. Sie können einen Agenten über einen Hypervisor, öffentliche Cloud-Dienste (wie Microsoft Azure, AWS) oder einen integrierten Agenten auf NetScaler-Instanzen (ideal für HA-Bereitstellungen) konfigurieren.

Befolgen Sie das Verfahren, um einen Agenten zu konfigurieren.

HINWEIS

- Sie können auch einen vorhandenen Agenten verwenden.
- Die Agenten werden standardmäßig automatisch auf die neueste Version der NetScaler Console aktualisiert. Sie können die Agentendetails auf der Seite **Infrastruktur > Instanzen > Agenten** anzeigen. Sie können auch den Zeitpunkt festlegen, zu dem die Agenten-Upgrades erfolgen sollen. Weitere Informationen finden Sie unter Konfigurieren der Agenten-Upgrade-Einstellungen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Statische Routen im Agenten konfigurieren

Innerhalb des Kubernetes-Clusters verwenden alle containerisierten Pods ein Overlay-Netzwerk. Eine direkte Kommunikation über diese privaten IP-Adressen ist nicht möglich. Um die Kommunikation von der NetScaler Console zum Kubernetes-Cluster zu ermöglichen, müssen Sie statisches Routing im Agenten konfigurieren.

Angenommen, Sie haben die folgenden IP-Adressen für Ihren Kubernetes-Cluster:

- Kubernetes Master – 101.xx.xx.112
- Kubernetes Worker 1 – 101.xx.xx.111
- Kubernetes Worker 2 – 101.xx.xx.110

Führen Sie auf dem Kubernetes Master den folgenden Befehl aus, um das Pod-Netzwerk für das statische Routing zu identifizieren:

```
kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}{.status.addresses[0].address}{'\n'}{end}"
```

Das Folgende ist eine Beispielausgabe, nachdem Sie den Befehl ausgeführt haben:

Nachdem Sie einen Agenten erfolgreich konfiguriert haben:

1. Melden Sie sich mit einem SSH-Client beim Agenten an
2. Geben Sie `shell` ein und drücken Sie die **Eingabetaste**, um zu `bash` zu wechseln
3. Konfigurieren Sie das statische Routing mit dem Befehl `route add -net <public IP address range> <Kubernetes IP address>`

   Zum Beispiel:

   `route add -net 192.168.0.0/24 101.xx.xx.112`

   `route add -net 192.168.1.0/24 101.xx.xx.111`

   `route add -net 192.168.2.0/24 101.xx.xx.110`
4. Überprüfen Sie die Konfiguration mit `netstat -rn`

5. Fügen Sie diese Routenbefehle in die Datei `/mpsconfig/svm.conf` ein.

   a. Greifen Sie im NetScaler-Agenten mit dem folgenden Befehl auf die Datei **svm.conf** zu:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`vim /mpsconfig/svm.conf`

b. Fügen Sie die statischen Routen in der Datei **svm.conf** hinzu.

Zum Beispiel, `route add -net 192.168.0.0/24 101.xx.xx.112`.

Beispiel-Bereitstellungsdateien von GitHub herunterladen

1. Verwenden Sie den Befehl **git clone** `https://github.com/citrix/citrix-k8s-ingress-controller.git`, um das GitHub-Repository im Master-Knoten zu klonen.
2. Um auf die YAMLs zuzugreifen:

`cd citrix-k8s-ingress-controller/example/servicegraph-demo/`

Parameter in der CPX-YAML-Datei hinzufügen

HINWEIS

Wenn Sie CPX 58.x oder höher verwenden, müssen Sie bei der Registrierung beim Agenten das Nicht-nsroot-Passwort verwenden. Um die Sicherheit zu gewährleisten, erfordern NetScaler Agent 61.x oder spätere Versionen eine obligatorische Passwortänderung. Wenn Ihr NetScaler Agent auf 61.x oder die neueste Version aktualisiert wird, müssen Sie sicherstellen, dass Sie den Build **CPX 58.x oder höher** verwenden.

Sie müssen die folgenden Parameter in die Datei `cpx.yaml` aufnehmen, um die CPX-Registrierung bei NetScaler Console sicherzustellen:

```
- name: "NS_MGMT_SERVER"

  value: "xx.xx.xx.xx"

- name: "NS_MGMT_FINGER_PRINT"

  value: "xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx"

- name: "NS_HTTP_PORT"

  value: "9080"

- name: "NS_HTTPS_PORT"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  value: 9443"

- name: "NS_MGMT_USER"

  value: "nsroot"

- name: "NS_MGMT_PASS"

  value: <your password>

- name: "LOGSTREAM_COLLECTOR_IP"

  value: "xx.xx.xx.xx"
```

- **NS_MGMT_SERVER** – Gibt die IP-Adresse des Agenten an
- **NS_MGMT_FINGER_PRINT** – Gibt die Authentifizierung für CPX im Agenten an. Um den Fingerabdruck zu erhalten:

  a. Navigieren Sie in NetScaler Console zu **Infrastructure > Instances > Agents**

  b. Wählen Sie den Agenten aus und klicken Sie dann auf **Fingerabdruck anzeigen**.

- **NS_HTTP_PORT** – Gibt den HTTP-Port für die Kommunikation an
- **NS_HTTPS_PORT** – Gibt den HTTPS-Port für die Kommunikation an
- **NS_MGMT_USER** – Gibt den Benutzernamen an
- **NS_MGMT_PASS** – Gibt das Kennwort an. Geben Sie ein Kennwort Ihrer Wahl ein
- **LOGSTREAM_COLLECTOR_IP** – Gibt die IP-Adresse des Agenten an, auf der das **Logstream**-Protokoll aktiviert sein muss, um Protokolldaten von CPX an NetScaler Console zu übertragen

VPX- oder SDX- oder MPX- oder BLX-Instanz in NetScaler Console hinzufügen

Um die Analysen der Tier-1-NetScaler-Instanz im Service-Graph zu erhalten, müssen Sie die VPX-/SDX-/MPX-/BLX-Instanz in NetScaler Console hinzufügen und **Web Insight** aktivieren. Sie

© 1997–2026 Citrix Systems, Inc. All rights reserved.

müssen **Web Insight** aktivieren, damit NetScaler Console die Webtransaktionsdetails von der VPX-/SDX-/MPX-/BLX-Instanz anzeigen kann.

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler**
2. Klicken Sie auf die Option **Hinzufügen**, um die Instanz hinzuzufügen. Weitere Informationen finden Sie unter Instanzen in NetScaler Console hinzufügen
3. Nach dem Hinzufügen der Instanz wählen Sie den virtuellen Server aus und aktivieren **Web Insight**. Weitere Informationen finden Sie unter Lizenzierung verwalten und Analysen auf virtuellen Servern aktivieren

Kubernetes-Cluster in NetScaler Console hinzufügen

So fügen Sie den Kubernetes-Cluster hinzu:

1. Melden Sie sich mit Administratoranmeldeinformationen bei NetScaler Console an.
2. Navigieren Sie zu **Infrastruktur > Orchestrierung > Kubernetes > Cluster**. Die Seite „Cluster“ wird angezeigt.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie auf der Seite **Cluster hinzufügen** die folgenden Parameter an:
    a. **Name** – Geben Sie einen Namen Ihrer Wahl an.
    b. **API-Server-URL** – Sie können die Details der API-Server-URL vom Kubernetes-Masterknoten abrufen.
        i. Führen Sie auf dem Kubernetes-Masterknoten den Befehl `kubectl cluster-info` aus.
        ii. Geben Sie die URL ein, die für **„Kubernetes master is running at.“** angezeigt wird.
    c. **Authentifizierungstoken** – Geben Sie das Authentifizierungstoken an. Das Authentifizierungstoken ist erforderlich, um den Zugriff für die Kommunikation zwischen dem Kubernetes-Cluster und der NetScaler Console zu validieren. So generieren Sie ein Authentifizierungstoken:

        Auf dem Kubernetes-Masterknoten:

        i. Verwenden Sie die folgende YAML-Datei, um ein Dienstkonto zu erstellen:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
apiVersion: v1

kind: ServiceAccount

metadata:

  name: <name>

  namespace: <namespace>
```

ii. Führen Sie `kubectl create -f <yaml file>` aus.

Das Dienstkonto wird erstellt.

iii. Führen Sie `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` aus, um die Clusterrolle an das Dienstkonto zu binden.

Das Dienstkonto hat nun clusterweiten Zugriff.

Ein Token wird beim Erstellen des Dienstkontos automatisch generiert.

iv. Führen Sie `kubectl describe sa <name>` aus, um das Token anzuzeigen.

v. Um die geheime Zeichenfolge zu erhalten, führen Sie `kubectl describe secret <token-name>` aus.

d. Wählen Sie den Agenten aus der Liste aus.

Hinweis

> Stellen Sie sicher, dass Sie denselben Agenten auswählen, den Sie in der CPX-YAML-Datei hinzugefügt haben.

e. Klicken Sie auf **Erstellen**.

Bereitstellen einer Beispiel-Microservice-Anwendung

Auf dem Masterknoten:

1. Führen Sie `kubectl create -f namespace.yaml` aus, um einen Namespace zu erstellen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Stellen Sie `hotdrink` Microservices, Ingress und Secrets mit den folgenden Befehlen bereit:

   `kubectl create -f team_hotdrink.yaml -n sg-demo`

   `kubectl create -f hotdrink-secret.yaml -n sg-demo`

CPX bereitstellen und in NetScaler Console registrieren

1. Führen Sie `kubectl create -f rbac.yaml` aus, um die Clusterrolle und die Clusterbindung bereitzustellen.
2. Führen Sie `kubectl create -f cpx.yaml -n sg-demo` aus, um CPX bereitzustellen.

Nach der Bereitstellung erfolgt die CPX-Registrierung automatisch.

Automatische Auswahl virtueller Server für die Lizenzierung aktivieren

Hinweis

> Stellen Sie sicher, dass Sie über ausreichende Lizenzen für virtuelle Server verfügen. Weitere Informationen finden Sie unter Lizenzierung

Nachdem Sie den Kubernetes-Cluster in NetScaler Console hinzugefügt haben, müssen Sie sicherstellen, dass virtuelle Server für die Lizenzierung automatisch ausgewählt werden. CPX-virtuelle Server müssen lizenziert sein, um Daten im Service-Graph anzuzeigen. So wählen Sie virtuelle Server automatisch aus:

1. Navigieren Sie zu **Einstellungen > NetScaler Console Lizenzierungs- und Analysekonfiguration**.
2. Aktivieren Sie unter **Zusammenfassung der virtuellen Serverlizenzen** die Optionen **Virtuelle Server automatisch auswählen** und **Nicht adressierbare virtuelle Server automatisch auswählen**.

Web-Transaktions- und TCP-Transaktionseinstellungen aktivieren

Nachdem Sie den Kubernetes-Cluster hinzugefügt und die automatische Auswahl virtueller Server aktiviert haben, ändern Sie die **Web-Transaktionseinstellungen** und **TCP-Transaktionseinstellungen** in **Alle**.

1. Navigieren Sie zu **Einstellungen > Analyseeinstellungen**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie auf **Funktionen für Analysen aktivieren**.
3. Wählen Sie unter **Web-Transaktionseinstellungen** die Option **Alle**.

4. Wählen Sie unter **TCP-Transaktionseinstellungen** die Option **Alle**.

5. Klicken Sie auf **OK**.

Datenverkehr an Microservices senden

Als Nächstes müssen Sie Datenverkehr an Microservices senden, damit der Service-Graph in NetScaler Console gefüllt wird.

1. Führen Sie `kubectl get svc -n sg-demo` aus, um CPX über NodePort verfügbar zu machen.

2. Bearbeiten Sie die Datei **etc/host** und erstellen Sie einen Domänen-IP-Eintrag für `hotdrink.beverages.com`.

   Sie können jetzt über `https://hotdrink.beverages.com` auf den Microservice zugreifen.

Detaillierte Verfahren zum Einrichten der Service-Mesh-Topologie

Die Voraussetzungen für die Bereitstellung der Service-Mesh-Topologie finden Sie unter Einrichten des Service-Graphen.

NetScaler-Agent konfigurieren

Um die Kommunikation zwischen Kubernetes-Cluster und NetScaler Console zu ermöglichen, müssen Sie einen Agenten installieren und konfigurieren. Sie können einen Agenten über einen Hypervisor, öffentliche Cloud-Dienste (wie Microsoft Azure, AWS) oder einen integrierten Agenten konfigurieren, der auf NetScaler-Instanzen verfügbar ist (ideal für HA-Bereitstellungen).

Befolgen Sie das Verfahren, um einen Agenten zu konfigurieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HINWEIS

- Sie können auch einen vorhandenen Agenten verwenden.
- Die Agenten werden standardmäßig automatisch auf die neueste NetScaler Console-Build-Version aktualisiert. Sie können die Agentendetails auf der Seite **Infrastruktur > Instanzen > Agenten** anzeigen. Sie können auch den Zeitpunkt festlegen, zu dem die Agenten-Upgrades erfolgen sollen. Weitere Informationen finden Sie unter Konfigurieren der Agenten-Upgrade-Einstellungen.

Statische Routen im Agenten konfigurieren

Innerhalb des Kubernetes-Clusters verwenden alle containerisierten Pods ein Overlay-Netzwerk. Eine direkte Kommunikation über diese privaten IP-Adressen ist nicht möglich. Um die Kommunikation von NetScaler Console zum Kubernetes-Cluster zu ermöglichen, müssen Sie statisches Routing im Agenten konfigurieren.

Angenommen, Sie haben die folgenden IP-Adressen für Ihren Kubernetes-Cluster:

- Kubernetes-Master – 101.xx.xx.112
- Kubernetes-Worker 1 – 101.xx.xx.111
- Kubernetes-Worker 2 – 101.xx.xx.110

Führen Sie auf dem Kubernetes-Master den folgenden Befehl aus, um das Pod-Netzwerk für das statische Routing zu identifizieren:

```
kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}{.status.addresses[0].address}{'\n'}{end}"
```

Das Folgende ist eine Beispielausgabe, nachdem Sie den Befehl ausgeführt haben:

Nach erfolgreicher Konfiguration eines Agenten:

1. Melden Sie sich mit einem SSH-Client beim Agenten an
2. Geben Sie `shell` ein und drücken Sie die **Eingabetaste**, um zu `bash` zu wechseln
3. Konfigurieren Sie das statische Routing mit dem Befehl `route add -net <public IP address range> <Kubernetes IP address>`

   Zum Beispiel:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
route add -net 192.168.0.0/24 101.xx.xx.112
```

```
route add -net 192.168.1.0/24 101.xx.xx.111
```

```
route add -net 192.168.2.0/24 101.xx.xx.110
```

4. Überprüfen Sie die Konfiguration mit `netstat -rn`

5. Fügen Sie diese Routenbefehle in die Datei `/mpsconfig/svm.conf` ein.

   a. Greifen Sie im Agenten mit dem folgenden Befehl auf die Datei **svm.conf** zu:

      ```
      vim /mpsconfig/svm.conf
      ```

   b. Fügen Sie die statischen Routen in der Datei **svm.conf** hinzu.

      Zum Beispiel, `route add -net 192.168.0.0/24 101.xx.xx.112`.

Erforderliche Parameter konfigurieren

Im Kubernetes-Master:

1. Erstellen Sie ein Secret mit den Agent-Anmeldeinformationen in jedem Namespace, in dem CPX als Ingress-Gateway / Sidecar bereitgestellt wird.

   ```
   kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n <namespace>
   ```

2. `helm repo add citrix https://citrix.github.io/citrix-helm-charts/`
3. NetScaler CPX als Ingress-Gateway bereitstellen

   ```
   helm install citrix-adc-istio-ingress-gateway citrix/citrix-adc-istio-ingress-gateway --version 1.2.1 --namespace <namespace> --set ingressGateway.EULA=YES,citrixCPX=true,ADMSettings.ADMFingerPrint=XX:00:X1:00:XX:0X:X0,A
   ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30
   ```

   Die folgende Tabelle listet die konfigurierbaren Parameter im Helm-Chart und deren Standardwerte auf:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	BESCHREIBUNG	STANDARD	OPTIONAL/ OBLIGATORISCH (HELM)
citrixCPX	NetScaler CPX	FALSCH	Obligatorisch für NetScaler CPX
xDSAdaptor.image	Image des Citrix xDS-Adapter-Containers	quay.io/citrix/citrix-istio-adaptor:1.2.1	Obligatorisch
ADMSettings.ADMIP	IP-Adresse der NetScaler Console	Keine Angabe	Obligatorisch für NetScaler CPX
ADMSettings.ADMFingerPrint	Der NetScaler Console Fingerprint. Navigieren Sie zu **Infrastruktur > Instanzen > Agents**, wählen Sie den Agenten aus und klicken Sie auf **Fingerprint anzeigen**.	Keine Angabe	Optional
ingressGateway.EULA	Nutzungsbedingungen (EULA). Wenn ja, stimmt der Benutzer den EULA-Bedingungen zu.	NEIN	Obligatorisch für NetScaler CPX
ingressGateway.image	Image von NetScaler CPX, das als Ingress Gateway ausgeführt werden soll	quay.io/citrix/citrix-k8s-cpx-ingress:13.0–58.30	Obligatorisch für NetScaler CPX

4. Stellen Sie den Citrix SideCar Injector bereit.

```
helm install cpx-sidecar-injector citrix/citrix-cpx-istio-sidecar-injector --version 1.2.1 --namespace <namespace> set
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
cpxProxy.EULA=YES,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSettings.ADMIP=<xx.xx.xx.xx
citrix/citrix-k8s-cpx-ingress,cpxProxy.tag=13.0-58.30
```

Die folgende Tabelle listet die konfigurierbaren Parameter im Helm-Chart und deren Standardwerte auf:

PARAMETER	BESCHREIBUNG	STANDARDWERT
ADMSettings.ADMIP	Die NetScaler Console IP-Adresse	NIL
cpxProxy.image	NetScaler CPX-Image, das als Sidecar-Proxy verwendet wird	quay.io/citrix/citrix-k8s-cpx-ingress:13.0–58.30
cpxProxy.imagePullPolicy	Image-Pull-Richtlinie für NetScaler	IfNotPresent
cpxProxy.EULA	Endbenutzer-Lizenzvertrag (EULA) Bedingungen. Wenn ja, stimmt der Benutzer den EULA-Bedingungen zu.	NEIN
cpxProxy.cpxSidecarMode	Umgebungsvariable für NetScaler CPX. Sie gibt an, ob NetScaler CPX im Sidecar-Modus ausgeführt wird oder nicht.	JA

5. Legen Sie das Label für jeden Namespace fest, der eine CPX Sidecar Injection benötigt.

   ```
   kubectl label namespace <app-namespace> cpx-injection=enabled
   ```

   Nach Ausführung von Schritt 3 und 5 können Sie sehen, dass der NetScaler CPX in der NetScaler Console registriert ist.

Beispielanwendung bereitstellen

Angenommen, Sie möchten die folgenden Anwendungen bereitstellen:

- [ ]

Führen Sie das folgende Verfahren aus, um eine Beispielanwendung bereitzustellen:

1. `kubectl create namespace citrix-system`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. `kubectl create namespace bookinfo`
3. `kubectl label namespace bookinfo cpx-injection=enabled`
4. `kubectl create secret generic admlogin --from-literal=username=<uername> --from-literal=password=<password> -n citrix-system`

   Hinweis

   Sie können einen Benutzernamen und ein Kennwort Ihrer Wahl eingeben.

5. `kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n bookinfo`

   Hinweis

   Sie können einen Benutzernamen und ein Passwort Ihrer Wahl eingeben.

6. `helm install citrix-adc-istio-ingress-gateway citrix/citrix-adc-istio-ingress-gateway --version 1.2.1 --namespace citrix-system --set ingressGateway.EULA=YES,citrixCPX=true,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSetting agent IP address>,ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30`

   Hinweis

   Sie müssen Ihren NetScaler Console-Fingerabdruck und die Agent-IP-Adresse angeben.

7. `helm install cpx-sidecar-injector citrix/citrix-cpx-istio-sidecar-injector --namespace citrix-system --set cpxProxy.EULA=YES,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSettings.ADMIP=<ADM agent IP address>,cpxProxy.image=quay.io/citrix/citrix-k8s-cpx-ingress,cpxProxy.tag=13.0-58.30`

   Hinweis

   Sie müssen Ihren NetScaler Console-Fingerabdruck und die Agent-IP-Adresse angeben.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. `helm install bookinfo bookinfo/ --namespace bookinfo --set citrixIngressGateway.namespace=citrix-system`

Kubernetes-Cluster in NetScaler Console hinzufügen

So fügen Sie den Kubernetes-Cluster hinzu:

1. Melden Sie sich mit Administratoranmeldeinformationen bei NetScaler Console an.
2. Navigieren Sie zu **Infrastructure > Orchestration > Kubernetes > Cluster**. Die Seite „Cluster“ wird angezeigt.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie auf der Seite **Cluster hinzufügen** die folgenden Parameter an:
   a. **Name** – Geben Sie einen Namen Ihrer Wahl an.
   b. **API-Server-URL** – Sie können die Details der API-Server-URL vom Kubernetes-Masterknoten abrufen.
      i. Führen Sie auf dem Kubernetes-Masterknoten den Befehl `kubectl cluster-info` aus.

      ii. Geben Sie die URL ein, die für **„Kubernetes master is running at.“** angezeigt wird.
   c. **Authentifizierungstoken** – Geben Sie das Authentifizierungstoken an. Das Authentifizierungstoken ist erforderlich, um den Zugriff für die Kommunikation zwischen dem Kubernetes-Cluster und der NetScaler Console zu validieren. So generieren Sie ein Authentifizierungstoken:

      Auf dem Kubernetes-Masterknoten:

      i. Verwenden Sie die folgende YAML-Datei, um ein Dienstkonto zu erstellen:

```
apiVersion: v1

kind: ServiceAccount

metadata:

  name: <name>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
namespace: <namespace>
```

ii. Führen Sie `kubectl create -f <yaml file>` aus.

Das Dienstkonto wird erstellt.

iii. Führen Sie `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` aus, um die Clusterrolle an das Dienstkonto zu binden.

Das Dienstkonto verfügt nun über den clusterweiten Zugriff.

Ein Token wird automatisch generiert, wenn das Dienstkonto erstellt wird.

iv. Führen Sie `kubectl describe sa <name>` aus, um das Token anzuzeigen.

v. Um die geheime Zeichenfolge zu erhalten, führen Sie `kubectl describe secret <token-name>` aus.

d. Wählen Sie den Agenten aus der Liste aus.

Hinweis

> Stellen Sie sicher, dass Sie denselben Agenten auswählen, den Sie in der CPX-YAML-Datei hinzugefügt haben.

e. Klicken Sie auf **Erstellen**.

Automatische Auswahl virtueller Server für die Lizenzierung aktivieren

Hinweis

> Stellen Sie sicher, dass Sie über ausreichende Lizenzen für virtuelle Server verfügen. Weitere Informationen finden Sie unter Lizenzierung

Nachdem Sie den Kubernetes-Cluster in der NetScaler Console hinzugefügt haben, müssen Sie sicherstellen, dass virtuelle Server für die Lizenzierung automatisch ausgewählt werden. Virtuelle

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Server müssen lizenziert sein, um Daten im Service Graph anzuzeigen. So wählen Sie virtuelle Server automatisch aus:

1. Navigieren Sie zu **Einstellungen > NetScaler Console Lizenzierungs- und Analysekonfiguration**.
2. Aktivieren Sie unter **Zusammenfassung der virtuellen Serverlizenzen** die Optionen **Virtuelle Server automatisch auswählen** und **Nicht adressierbare virtuelle Server automatisch auswählen**.

Web-Transaktions- und TCP-Transaktionseinstellungen aktivieren

Nachdem Sie den Kubernetes-Cluster hinzugefügt und die automatische Auswahl virtueller Server aktiviert haben, ändern Sie die **Web-Transaktionseinstellungen** und **TCP-Transaktionseinstellungen** in **Alle**.

1. Navigieren Sie zu **Einstellungen** > **Analyseeinstellungen**.

   Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie auf **Funktionen für Analysen aktivieren**.
3. Wählen Sie unter **Web-Transaktionseinstellungen Alle** aus.

4. Wählen Sie unter **TCP-Transaktionseinstellungen Alle** aus.

5. Klicken Sie auf **OK**.

Datenverkehr an Microservices senden

Als Nächstes müssen Sie Datenverkehr an Microservices senden, damit der Service-Graph in NetScaler Console gefüllt wird.

1. Bestimmen Sie die Ingress-IP und den Port

```
export INGRESS_HOST=$(kubectl get pods -l app=citrix-ingressgateway -n citrix-system -o 'jsonpath={.items[0].status.hostIP}')
```

```
export INGRESS_PORT=$(kubectl -n citrix-system get service citrix-ingressgateway -o jsonpath='{.spec.ports[?(@.name=="http2")].nodePort}')
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
export SECURE_INGRESS_PORT=$(kubectl -n citrix-system get service citrix-ingressgateway -o jsonpath='{.spec.ports[?(@.name=="https")].nodePort}')
```

2. Greifen Sie mit curl auf die Bookinfo-Frontend-Anwendung zu. Der `productpage` Dienst muss eine 200 OK-Antwort zurückgeben.

   ```
   curl -kv https://$INGRESS_HOST:$SECURE_INGRESS_PORT/productpage
   ```

   ```
   curl -v http://$INGRESS_HOST:$INGRESS_PORT/productpage
   ```

3. Besuchen Sie `https://$INGRESS_HOST:$SECURE_INGRESS_PORT/productpage` über einen Browser.

   Die Seite **Bookinfo** wird angezeigt.

4. Stellen Sie sicher, dass $INGRESS_HOST und $SECURE_INGRESS_PORT durch eine IP-Adresse und einen Portwert ersetzt werden.

Nachdem Sie Datenverkehr an Mikroservices gesendet haben, wird der Dienstgraph innerhalb von etwa 10 Minuten gefüllt.

Mithilfe des Dienstgraphen können Sie verschiedene Dienstdetails wie Metriken, Fehler usw. analysieren. Weitere Informationen finden Sie unter Dienstgraph.

Detaillierte Verfahren zur Einrichtung einer einstufigen oder vereinheitlichten Ingress-Topologie

Die Voraussetzungen für die Bereitstellung der einstufigen oder vereinheitlichten Ingress-Topologie finden Sie unter Einrichten des Service-Graphen.

VPX-, SDX-, MPX- oder BLX-Instanz in NetScaler Console hinzufügen

Um die Analysen der Tier-1 NetScaler-Instanz im Service-Graphen zu erhalten, müssen Sie die VPX/SDX/MPX/BLX-Instanz in NetScaler Console hinzufügen und **Web Insight** aktivieren. Sie müssen **Web Insight** aktivieren, damit NetScaler Console die Webtransaktionsdetails von der VPX/SDX/MPX/BLX-Instanz anzeigen kann.

1. Navigieren Sie zu **Infrastructure > Instances > NetScaler**
2. Klicken Sie auf die Option **Hinzufügen**, um die Instanz hinzuzufügen. Weitere Informationen finden Sie unter Instanzen in NetScaler Console hinzufügen

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Nachdem Sie die Instanz hinzugefügt haben, wählen Sie den virtuellen Server aus und aktivieren Sie **Web Insight**, um die Webtransaktionsdetails anzuzeigen. Weitere Informationen finden Sie unter Lizenzierung verwalten und Analysen auf virtuellen Servern aktivieren

Kubernetes-Cluster in NetScaler Console hinzufügen

So fügen Sie den Kubernetes-Cluster hinzu:

1. Melden Sie sich mit Administratoranmeldeinformationen bei NetScaler Console an.
2. Navigieren Sie zu **Infrastructure > Orchestration > Kubernetes > Cluster**. Die Seite „Cluster“ wird angezeigt.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie auf der Seite **Cluster hinzufügen** die folgenden Parameter an:

    a. **Name** – Geben Sie einen Namen Ihrer Wahl an.

    b. **API-Server-URL** – Sie können die Details der API-Server-URL vom Kubernetes-Masterknoten abrufen.

        i. Führen Sie auf dem Kubernetes-Masterknoten den Befehl `kubectl cluster-info` aus.

        ii. Geben Sie die URL ein, die für **„Kubernetes-Master läuft unter.“** angezeigt wird.

    c. **Authentifizierungstoken** – Geben Sie das Authentifizierungstoken an. Das Authentifizierungstoken ist erforderlich, um den Zugriff für die Kommunikation zwischen dem Kubernetes-Cluster und der NetScaler Console zu validieren. So generieren Sie ein Authentifizierungstoken:

    Auf dem Kubernetes-Masterknoten:

        i. Erstellen Sie ein Dienstkonto mithilfe der YAML-Datei.

        ```
        kubectl create -f adm_svc_account.yaml
        ```

        Das Dienstkonto wird erstellt.

        ii. Führen Sie `kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole=cluster-admin --serviceaccount=default:citrixadm-sa` aus, um die Clusterrolle an das Dienstkonto zu binden.

        Das Dienstkonto verfügt nun über den clusterweiten Zugriff.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ein Token wird automatisch während der Erstellung des Dienstkontos generiert.

iii. Führen Sie `kubectl describe sa citrixadm-sa` aus, um das Token anzuzeigen.

iv. Um die geheime Zeichenfolge zu erhalten, führen Sie `kubectl describe secret <token-name>` aus.

d. Wählen Sie den Agenten aus der Liste aus.

Hinweis

Stellen Sie sicher, dass Sie denselben Agenten auswählen, den Sie in der CPX YAML hinzugefügt haben.

e. Klicken Sie auf **Erstellen**.

Datengovernance für das NetScaler®-Telemetrieprogramm

Alle bestehenden NetScaler Console-Kunden müssen die Anforderungen des NetScaler-Telemetrieprogramms erfüllen, indem sie die erforderlichen Telemetriedaten hochladen. Das NetScaler-Telemetrieprogramm ist ab Build **14.1-28.x** aktiviert, und die Telemetriedaten werden automatisch hochgeladen. Weitere Informationen finden Sie unter NetScaler-Telemetrieprogramm. Citrix erfasst grundlegende Lizenz-Telemetriedaten sowie Telemetriedaten zur NetScaler-Bereitstellung und Funktionsnutzung für seine berechtigten Interessen, einschließlich der Lizenzkonformität. NetScaler Console-Konfigurations- und Funktionsnutzungsdaten werden ebenfalls erfasst, um Citrix-Produkte und -Dienste zu verwalten, zu messen und zu verbessern.

HINWEISE:

- Der Telemetrie-Upload erfolgt automatisch alle 24 Stunden.
- Um die Telemetrie-Metriken in Ihren NetScaler-Instanzen zu erfassen und zu speichern, wurde die folgende Konfiguration über NetScaler Console an Ihre NetScaler-Instanzen übertragen, als Teil des am 18. Juni 2024 veröffentlichten NetScaler-Telemetrieprogramms.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
enable ns feature AppFlow

add analytics profile telemetry_metrics_profile -type timeseries
-outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "./
telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300
```

- Die `/nsconfig/.telemetry.conf`-Datei wird mit dem folgenden Befehl für die Gateway-Telemetrie aktualisiert. NetScaler Console prüft stündlich auf diesen Befehl und fügt ihn hinzu, falls er fehlt. Dieser Befehl wird nur an NetScaler-Instanzen übertragen, die über eine VPN-Virtual-Server-Konfiguration verfügen:

```
ns_telemetry_server,&lt;Console IP>,5140
```

- Einige Telemetrieparameter werden über Skripte erfasst, die von NetScaler Console an NetScaler-Instanzen übertragen werden. Diese Skripte sind schreibgeschützt und ändern nichts in NetScaler.

Die folgende Tabelle enthält die erforderlichen Parameterdetails, die im Rahmen des NetScaler-Telemetrieprogramms erfasst werden:

KATEGORIEN	BESCHREIBUNG	WOFÜR VERWENDEN WIR ES?
Lizenz- sowie NetScaler-Bereitstellungs- und Nutzungs-Telemetrie	Informationen zu Lizenzberechtigungen, Nutzung und übergeordnete NetScaler-Bereitstellungsdaten sowie NetScaler-Funktionsnutzung.	Lizenzkonformität und zur Verwaltung, Messung und Verbesserung des Dienstes.
NetScaler Console-Bereitstellungs- und Funktionsnutzungs-Telemetrie	Informationen zur Console-Bereitstellung und Funktionsnutzung.	Zur Verwaltung, Messung und Verbesserung des Dienstes.

Erforderliche Telemetriedaten

Die im Rahmen des NetScaler-Telemetrieprogramms gesammelten Daten sind im Telemetriedaten-Governance Dokument aufgeführt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

*Die durch Telemetrie gesammelten Informationen, wie E-Mail-Adressen, Benutzernamen und IP-Adressen, werden durch Hashing der Informationen an der Quelle mithilfe von Einweg-Hashing-Algorithmen sicher pseudonymisiert. Daher kann Citrix auf diese Werte nicht zugreifen oder sie lesen. Diese Telemetriedaten werden ausschließlich für logische Asset-Matching-Zwecke verwendet.

So ändern Sie das Root-Passwort von NetScaler MPX und VPX

Gelegentlich müssen Sie das Root-Passwort der NetScaler Appliance aus Sicherheitsgründen oder zur Einhaltung der Passwortrotationsrichtlinie ändern.

Dieses Dokument beschreibt die Schritte, die erforderlich sind, um das Root-Passwort der NetScaler MPX- und VPX-Appliances zu ändern, die über NetScaler Console Cloud verwaltet werden.

Wenn Sie das NetScaler-Passwort ändern, müssen Sie das NetScaler Console-Administratorprofil ändern, das mit dem NetScaler verknüpft ist. Ein NetScaler Console-Administratorprofil verwaltet die NetScaler-Anmeldeinformationen für die REST-API-, SSH-, SCP- oder SNMP-basierte Kommunikation mit der NetScaler-Appliance. Über Administratorprofile verwaltet NetScaler Console NetScaler MPX- und VPX-Appliances.

Weitere Informationen zum Ändern des NetScaler-`nsroot`-Passworts auf einer einzelnen Appliance finden Sie im Artikel CTX224027.

Passwort ändern mit der Funktion Konfigurationsaufträge

Mithilfe der NetScaler Console-Funktion für Konfigurationsaufträge können Sie den wiederholten Passwortänderungsprozess vereinfachen und die Änderungen auf die NetScaler-Appliances anwenden, ohne auf die einzelnen Instanzen zugreifen zu müssen.

Führen Sie die folgenden Schritte aus, um das Passwort zu ändern:

Schritt 1. Erstellen Sie eine Konfigurationsvorlage. Schritt 2. Erstellen Sie einen Konfigurationsauftrag. Schritt 3. Erstellen und ändern Sie ein Administratorprofil.

Hinweis: Wenn die NetScaler-Appliances auch von anderen Tools verwaltet werden, müssen Sie die Anmeldeinformationen auch in diesen Tools ändern.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Schritt 1. Erstellen Sie eine Konfigurationsvorlage

1. Navigieren Sie in der NetScaler Console-GUI zu **Infrastruktur > Konfigurationsaufträge > Konfigurationsvorlagen**.
2. Wählen Sie **Hinzufügen**. Erstellen Sie eine Konfigurationsvorlage, indem Sie den SSH-Befehl `set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$` eingeben.

3. Wählen Sie die Variable `$ROOT_USER_NAME$` aus und wählen Sie **Textfeld als Typ**.
4. Geben Sie optional den Standardwert für den Root-Benutzernamen an. Wählen Sie **Fertig**, um die Variableneinstellungen zu speichern.

5. Wählen Sie die Variable `$ROOT_USER_PASSWORD$` aus, und wählen Sie **Passwortfeld als Typ**. Wählen Sie **Fertig**, um die Variableneinstellungen zu speichern.
6. Wählen Sie **OK**, um die Konfigurationsvorlage zu speichern.
7. Die neue Konfigurationsvorlage wird unter **Konfigurationsvorlagen** angezeigt.

Konfigurationsauftrag erstellen

1. Navigieren Sie in der NetScaler Console-GUI zu **Infrastruktur > Konfigurationsaufträge**.
2. Wählen Sie **Auftrag erstellen** und klicken Sie auf das „+“-Symbol der neuen Konfigurationsvorlage. Wählen Sie **Weiter**.

3. Wählen Sie die NetScaler-Instanz oder -Instanzen aus, für die das Kennwort geändert werden muss.

4. Wählen Sie im Bereich **Instanzen auswählen** die Instanzen aus, und klicken Sie auf **Weiter**.
5. Geben Sie im Bereich **Variablenwerte angeben** Werte für Benutzername und Kennwort ein, und klicken Sie auf **Weiter**.
6. Überprüfen Sie unter **Auftragsvorschau** die tatsächlichen CLI-Befehle, die die NetScaler Console auf den NetScaler-Instanzen ausführen wird. Wenn die Vorschau in Ordnung ist, klicken Sie auf **Weiter**.

7. Im Bereich **Ausführen** haben Sie die Wahl, den Job sofort auszuführen oder für später zu planen. Sie können den Job auch parallel auf allen ausgewählten Instanzen ausführen oder

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nacheinander. Wählen Sie **Fertig stellen**, nachdem Sie die Ausführungsdetails angegeben haben.

8. Die Seite **Jobs** zeigt an, ob die Ausführung erfolgreich war oder fehlgeschlagen ist.
9. Wählen Sie den **Job** aus und klicken Sie auf **Details**. Die Ausführungsdetails zeigen den Status auf Ebene der einzelnen Instanzen an.

Administratorprofil ändern

Nachdem Sie die NetScaler-Passwörter geändert haben, müssen Sie die Administratorprofile der Instanzen hinzufügen und ändern. Gehen Sie dazu wie folgt vor:

1. Navigieren Sie zu **Infrastruktur > Instanzen > NetScaler**.
2. Klicken Sie auf **Aktion auswählen > Profile**, um alle Administratorprofile anzuzeigen.
3. Wählen Sie **Hinzufügen**, um ein Administratorprofil zu erstellen und neue NetScaler-Anmeldeinformationen anzugeben.

4. Das neu erstellte Profil wird unter **Administratorprofile** angezeigt.
5. Gehen Sie zu **Netzwerk > Instanzen > NetScaler**. Wählen Sie die NetScaler-Instanz aus, für die das Passwort geändert wurde, und wählen Sie dann **Bearbeiten**.
6. Wählen Sie den neu erstellten Profilnamen aus und klicken Sie auf **OK**.

7. Wählen Sie die Instanz erneut aus, klicken Sie mit der rechten Maustaste und wählen Sie **Neu erkennen**.

Diese Schritte schließen den Prozess zum Zurücksetzen des Kennworts in NetScaler Console ab.

Vorherige Releases

Dieses Thema ist die Liste der früheren Releases für NetScaler Application Delivery Management (NetScaler Console).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

December 13, 2023

Infrastruktur

Umbenennung des NetScaler® ADM-Dienstes

Der NetScaler Application Delivery Management Service (ADM Service) wurde in NetScaler Console Service umbenannt.

Weitere umbenannte Terminologien sind die folgenden:

- Der ADM-Agent wurde in NetScaler-Agent umbenannt
- ADM Service Connect wurde in Console Advisory Connect umbenannt

HINWEIS:

Die Benutzeroberfläche und die Dokumentation unseres NetScaler Console Service-Produkts werden derzeit aktualisiert, um diese Änderungen widerzuspiegeln. Während dieser Zeit können Sie auf die früheren und die umbenannten Namen stoßen, die austauschbar verwendet werden. Wir danken Ihnen für Ihr Verständnis während dieses Übergangs.

Lizenzierung

NetScaler Flexed-Lizenzierung

Die NetScaler Flexed-Lizenzierung ist das neue Lizenzierungsframework, das darauf abzielt, den Lizenzverwaltungsprozess zu vereinfachen. Ihre Flexed-Lizenz umfasst Software-Instanzlizenzen (VPX/CPX/BLX, SDX, MPX und VPX FIPS) und Bandbreitenkapazitätslizenzen. Sie müssen die Flexed-Lizenzen auf dem NetScaler Console Service oder NetScaler ADM On-Prem anwenden. Sie müssen auch die MPX Z-Cap- und SDX Z-Cap-Lizenz auf NetScaler MPX-Hardware bzw. NetScaler SDX-Hardware anwenden. Sie können sie dann auf alle NetScaler-Formfaktoren verteilen, die in der Cloud oder On-Prem bereitgestellt werden.

HINWEIS:

Stellen Sie sicher, dass Ihre NetScaler-Agenten Version 16.x oder höher ausführen.

Weitere Informationen finden Sie unter Flexed-Lizenz.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analysen

Flexed-Lizenz – Metrics Collector standardmäßig deaktiviert für neue NetScaler-Instanzen, die in NetScaler Console hinzugefügt wurden

Wenn Sie die Flexed-Lizenz verwenden, ist der Metrics Collector für die neuen NetScaler-Instanzen, die in NetScaler Console hinzugefügt wurden, jetzt standardmäßig deaktiviert. Sie müssen diese Option manuell aktivieren, um die NetScaler-Metriken und Zählerdaten an die Konsole zu übertragen. Die Konfiguration des Metrics Collectors für die bestehenden verwalteten Instanzen bleibt unverändert.

HINWEIS:

Der Metrics Collector muss aktiviert sein, damit die Daten im Anwendungs-Dashboard und den zugehörigen Registerkarten wie Leistung, SSL und Schlüsselmetriken für alle lizenzierten virtuellen Server auf dieser Instanz angezeigt werden.

Weitere Informationen finden Sie unter Intelligent App Analytics konfigurieren.

Veralten der Video- und TCP-Insight-Funktionen

Mit der neuesten Version sind die Berichtsdaten von **Video Insight** und **TCP Insight** in der NetScaler Console nicht mehr zur Visualisierung verfügbar.

Infrastruktur

Dateien für Batch-Konfigurationsaufträge herunterladen

Die Konfigurationsaufträge ermöglichen Ihnen jetzt, Dateien aus einem Verzeichnis auf einer NetScaler-Instanz in ein Verzeichnis auf Ihrem lokalen Computer mithilfe der NetScaler ADM GUI herunterzuladen.

Um diese Funktion zu nutzen, navigieren Sie zu **Infrastructure > Configuration > Configuration Jobs**, wählen Sie einen Auftrag aus und klicken Sie auf **Download Result Files**.

Die Schaltfläche **Download Result Files** ist nur verfügbar, wenn die folgenden Bedingungen erfüllt sind:

- Der erstellte Konfigurationsauftrag ist ein Batch-Konfigurationsauftrag. Um einen Batch-Konfigurationsauftrag zu erstellen, gehen Sie zu **Create Job > Select Configuration** und

© 1997–2026 Citrix Systems, Inc. All rights reserved.

wählen Sie im **Configuration Editor** die Option **Configuration Source > Batch Configuration**.

- Ein `scp get` Befehl wird im **Configuration Editor** verwendet

Für mehrere NetScaler-Instanzen sind die heruntergeladenen Ergebnisdateien in separaten Ordnern verfügbar, wobei jeder Ordner einer einzelnen Instanz entspricht.

Anhalten und Fortsetzen eines geplanten Upgrade-Auftrags

NetScaler ADM bietet jetzt die Möglichkeit, Ihren geplanten Upgrade-Auftrag anzuhalten. Um diese Funktion zu nutzen, navigieren Sie zu **Infrastructure > Upgrade Jobs**, wählen Sie einen vorhandenen geplanten Upgrade-Auftrag aus und klicken Sie auf **Stop**, um den Auftrag anzuhalten. Um den geplanten Upgrade-Auftrag fortzusetzen, klicken Sie auf **Resume**.

HINWEIS:

Wenn die geplante Zeit für den Upgrade-Auftrag verstrichen ist, nachdem Sie sich entschieden haben, ihn fortzusetzen, müssen Sie den Upgrade-Auftrag erneut erstellen.

Weitere Informationen finden Sie unter Upgrade-Aufträge

Behobene Probleme

Die Probleme, die in Build December 13, 2023 behoben wurden.

Analysen

- Unter **Anwendungen > Dashboard** zeigt der Export von Transaktionsprotokolldaten in das Tabellen- oder CSV-Format keine Daten an. Dieses Problem tritt auf, wenn NetScaler ADM mit Nicht-UTC-Zeitzonen konfiguriert ist.

- Unter **Sicherheit > Sicherheitsverletzungen > Verletzungsdetails** erkennt der Suchfilter die Abfrage „Client-IP !=“ nicht.

- Geplante Snapshot-Berichte, die aus **Sicherheit > Sicherheitsverletzungen > Berichte exportieren > Export planen** exportiert werden, wobei das Dateiformat als JPEG ausgewählt ist, zeigen den folgenden Fehler an:

  „Bitte geben Sie Abfrageparameter im Berichtskontext oder in csv_export_arr an.“

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastruktur

- Bestimmte Benutzer sehen auf den Karten auf der Seite **Infrastruktur > Instanzen** das Wasserzeichen „Nur für Entwicklungszwecke“.

Verwaltung und Überwachung

- Der NetScaler ADM-Agent generiert „netScalerLoginFailure“-SNMP-Traps. Dieses Problem tritt auf, weil die Anmeldeinformationen, die der ADM-Agent für die Anmeldung bei NetScaler verwendet, aufgrund eines Zeilenumbruchzeichens abgeschnitten werden.

Sicherheit

- Nach dem Konfigurieren von Schutzmaßnahmen im Unified Security Dashboard (**Security > Security Dashboard > Manage Application**) werden die Schutzmaßnahmen nicht auf dem Content Switching Virtual Server bereitgestellt.

November 29, 2023

Infrastruktur

Tags verwenden, um Instanzen für Benutzergruppen zu autorisieren

Als Administrator können Sie Benutzer jetzt basierend auf zugeordneten Tags für bestimmte Instanzen autorisieren. Navigieren Sie beim Erstellen von Benutzergruppen zu **Settings > Users & Roles > Add > Authorization Settings > Select Tags** und autorisieren Sie dann Benutzer für Instanzen anhand von Tags.

Weitere Informationen finden Sie unter Konfigurieren der rollenbasierten Zugriffssteuerung.

Behobene Probleme

Die Probleme, die in Build November 29, 2023 behoben wurden.

- Wenn Sie eine VPX-Instanz auf SDX unter **Infrastructure > Instances > NetScaler > SDX > Select Action > Provision VPX** bereitstellen, wird die Option **Manage through network** nicht angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

November 09, 2023

Analysen

Gateway-Sitzungs-Timeout konfigurieren

Unter **Einstellungen > Analyse-Einstellungen > ICA/Gateway-Sitzungs-Timeout konfigurieren** können Sie jetzt das Timeout für Gateway Insight-Sitzungen konfigurieren. Standardmäßig beträgt der Wert 30 Minuten. Mit dieser Konfiguration wird die Sitzung als beendet aufgezeichnet, wenn NetScaler ADM innerhalb der konfigurierten Dauer keinen Sitzungsbeendigungsdatensatz erhält.

Update im NetScaler-Sicherungsprozess und Firewall-Zugriff

NetScaler-Instanz-Backups werden jetzt direkt vom NetScaler-Agenten zum NetScaler ADM Service und dann zu Amazon S3 hochgeladen. Daher müssen Sie den Zugriff auf S3-URLs in Ihrer Firewall für den NetScaler-Backup-Dienst nicht mehr zulassen.

Vereinheitlichtes Sicherheits-Dashboard

In NetScaler ADM können Sie jetzt ein Single-Pane-Dashboard verwenden, um Schutzmaßnahmen zu konfigurieren, Analysen zu aktivieren und diese auf Ihren Anwendungen bereitzustellen. Navigieren Sie zu **Sicherheit > Sicherheits-Dashboard** und klicken Sie dann auf **Anwendung verwalten**, um:

- Alle gesicherten und ungesicherten Anwendungen anzeigen.
- Eine ungesicherte Anwendung auswählen, Schutzmaßnahmen aus verschiedenen Vorlagenoptionen konfigurieren, Analysen für die Schutzmaßnahmen aktivieren und diese auf Ihrer Anwendung bereitstellen, um die Anwendung zu sichern.

Zuvor mussten Sie alle Schutzmaßnahmen in den NetScaler-Instanzen konfigurieren und konnten nur Analysen für die konfigurierten Schutzmaßnahmen in NetScaler ADM anzeigen. Als Administrator ermöglicht Ihnen dieses Single-Pane-Dashboard, Schutzmaßnahmen für die Anwendung in einem einzigen Workflow zu konfigurieren.

Weitere Informationen finden Sie unter Vereinheitlichtes Sicherheits-Dashboard.

Behobene Probleme

Die in Build Nov 09, 2023 behobenen Probleme.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastruktur

- Beim Einrichten des integrierten NetScaler-Agenten zur Verwaltung von Instanzen bleibt die Konfiguration auf der Seite **Instanzen hinzufügen** hängen, obwohl die Registrierung erfolgreich war und der Agent auf der Seite **Instanz-Dashboard** angezeigt werden kann.

StyleBooks

- Wenn Konfigurationspakete mit Sonderzeichen in ihren Parametern aktualisiert oder gelöscht werden, zeigt NetScaler ADM eine Erfolgsmeldung an, obwohl die Aktualisierungs- oder Löschvorgänge auf NetScaler unvollständig sind. Mit dieser Korrektur zeigt NetScaler ADM nun Fehler für alle unvollständigen Konfigurationen, die aufgrund von Sonderzeichen in der Konfigurationspaketdefinition entstehen, korrekt an.

October 25, 2023

Analysen

Benutzerdefinierte Dashboards erstellen, um wichtige Instanzmetrikdetails anzuzeigen

Ähnlich wie beim vereinheitlichten Dashboard (**Übersicht > Dashboard**) können Sie jetzt Instanzmetrikdetails nach Ihrer Wahl anzeigen, indem Sie benutzerdefinierte Dashboards erstellen. Wenn Sie beispielsweise die Schlüsselmetriken für Anwendungen und Anwendungssicherheit überwachen möchten, können Sie ein benutzerdefiniertes Dashboard erstellen, indem Sie nur diese beiden Kategorien auswählen. Sie können bis zu 20 Dashboards mit einem eindeutigen Namen für jedes Dashboard erstellen. Als Administrator ermöglicht Ihnen diese Verbesserung, mehrere Dashboards zu erstellen und nur die erforderlichen Instanzinformationen zu überwachen.

Navigieren Sie zum Starten zu **Übersicht > Benutzerdefiniertes Dashboard**.

Weitere Informationen finden Sie unter Benutzerdefinierte Dashboards erstellen, um wichtige Instanzmetrikdetails anzuzeigen.

Umsetzbare Aufgaben und Empfehlungen

Die folgenden Verbesserungen wurden der **Aufgaben**-Funktion hinzugefügt:

- Eine neue Registerkarte **Aufgaben** wurde eingeführt, auf der Sie umsetzbare Aufgaben anzeigen können, die Ihre sofortige Aufmerksamkeit erfordern. Diese Aufgaben werden basierend auf Ihrer aktuellen Auslastung angezeigt. Als Administrator stellt die Erledigung dieser umsetzbaren Aufgaben sicher, dass Ihre NetScaler-Bereitstellung sicher, konform und

© 1997–2026 Citrix Systems, Inc. All rights reserved.

effizient ist. Sie können diese umsetzbaren Aufgaben auch basierend auf dem Schweregrad der Probleme (Kritisch und Mittel) anzeigen.

- Die Registerkarte **To Do** wurde in **Empfehlungen** umbenannt. Unter **Empfehlungen** können Sie weiterhin die vorhandenen Aufgaben überprüfen und auf **Guide Me** klicken, um die Aufgabe abzuschließen.
- Die Registerkarte **Archiv** ist nicht mehr verfügbar. Stattdessen können Sie eine Empfehlung aus der Liste **Verwerfen**.

Weitere Informationen finden Sie unter Umsetzbare Aufgaben und Empfehlungen.

Infrastruktur

Zertifikatsspeicher zum Aktualisieren von SSL-Zertifikaten verwenden

Wenn Sie ein SSL-Zertifikat unter **Infrastruktur > SSL-Dashboard > Aktualisieren** aktualisieren, können Sie das Zertifikat jetzt aus dem Zertifikatsspeicher auswählen. Zuvor mussten Sie die Zertifikatsdatei und die Schlüsseldatei hochladen, um ein SSL-Zertifikat zu aktualisieren.

Aktualisierte Liste der SNMP-Traps

Die Liste der SNMP-Traps wurde jetzt um neue Traps sowie um einige zuvor fehlende Traps erweitert. Um die vollständige Liste anzuzeigen, navigieren Sie zu **Infrastruktur > Ereignisse > Ereigniseinstellungen > NetScaler**.

Behobene Probleme

Die Probleme, die in Build Oct 25, 2023 behoben wurden.

- Wenn Sie eine VPX-Instanz auf SDX unter **Infrastruktur > Instanzen > NetScaler > SDX > Aktion auswählen > VPX bereitstellen** bereitstellen, wird die Option **Über Netzwerk verwalten** nicht angezeigt.

October 10, 2023

Verwaltung und Überwachung

Unterstützung bei der Identifizierung und Behebung von CVE-2023-4966 und CVE-2023-4967

NetScaler Console Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2023-4966 und CVE-2023-4967.

- Die Identifizierung erfordert eine Kombination aus Versions- und Konfigurationsscan.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die Behebung erfordert ein Upgrade der anfälligen NetScaler-Instanzen auf einen empfohlenen Build, der den Fix enthält.

HINWEIS:

Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

Weitere Informationen zur Verwendung von NetScaler ADM zum Upgrade von NetScaler-Instanzen finden Sie unter Verwenden von Aufträgen zum Upgrade von NetScaler-Instanzen.

Weitere Informationen finden Sie unter Sicherheitsbulletin.

September 26, 2023

Analysen

Daten nur von ausgewählten Instanzen nach Splunk und New Relic exportieren

Wenn Sie ein Abonnement zum Exportieren von Daten nach Splunk und New Relic erstellen, können Sie jetzt die NetScaler-Instanzen auswählen. Wenn Sie ein Abonnement mit bestimmten Instanzen erstellen, werden die Daten nur von den ausgewählten NetScaler-Instanzen nach Splunk und New Relic exportiert.

Weitere Informationen finden Sie unter Integration mit Splunk und Integration mit New Relic.

Infrastruktur

ADM On-Prem-Instanzen, die über Cloud Connector mit dem ADM-Dienst verbunden sind

Unter **Einstellungen** können Sie jetzt eine neue Option namens **ADM On-Prem** anzeigen. Auf dieser Seite können Sie Details der ADM On-Prem-Instanzen anzeigen, die über den ADM On-Prem Cloud Connector mit dem ADM-Dienst-Mandanten verbunden sind.

Weitere Informationen finden Sie unter ADM On-Prem-Instanzen, die über Cloud Connector mit dem ADM-Dienst verbunden sind.

Behobene Probleme

Die Probleme, die in Build Sep 26, 2023 behoben wurden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analysen

- Die regelmäßige Bereinigung der App-Dashboard-Daten funktionierte nicht wie erwartet. Infolgedessen belegte NetScaler Console mehr Speicherplatz.

September 13, 2023

Infrastruktur

Authentifizierungstoken zum Hochladen des technischen Support-Pakets

Sie benötigen jetzt ein Authentifizierungstoken, um das auf Ihrem NetScaler generierte technische Support-Paket auf den technischen Support-Server von Citrix hochzuladen. Zuvor haben Sie das technische Support-Paket unter Verwendung des Citrix Benutzernamens und Passworts hochgeladen. Weitere Informationen finden Sie unter So generieren Sie ein technisches Support-Paket für eine NetScaler-Instanz.

Behobene Probleme

Die Probleme, die in Build Sep 13, 2023 behoben wurden.

Analysen

- Wenn NetScaler Console die Lizenzen für virtuelle Server verliert, wird erwartet, dass der Analysestatus für die virtuellen Server, die diese Lizenzen verwenden, deaktiviert wird. Dieses Szenario funktionierte für die virtuellen VPN-Server nicht wie erwartet.

Infrastruktur

- In **Gateway > HDX™ Insight** und **Gateway > Gateway Insight** zeigt die X-Achse des Diagramms Daten anstelle von Uhrzeiten an.

Verwaltung und Überwachung

- Berichte, die aus **Infrastruktur > Netzwerkberichterstattung > Export** exportiert wurden, erscheinen abgeschnitten oder unvollständig.

- Azure Active Directory (AD)-Benutzer, die vielen Azure-Gruppen angehören, können nicht auf NetScaler Console zugreifen, selbst wenn die AD-Gruppen ADM-Gruppen zugeordnet sind.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

August 31, 2023

Infrastruktur

Anzeigen der Seite „Zertifikatsspeicher“ unter „SSL-Dashboard“

Sie können jetzt zu **Infrastruktur > SSL-Dashboard > Zertifikatsspeicher** navigieren, um die Seite **Zertifikatsspeicher** anzuzeigen.

Unterstützung der SNMP-Funktionalität für die Agents

Unter **Infrastruktur > Agents > Aktionen > SNMP verwalten** können Sie jetzt SNMP-Manager, SNMP-Benutzer und SNMP-Ansichten für Agents erstellen.

Weitere Informationen zu SNMP-Managern und -Benutzern finden Sie unter SNMP-Manager und -Benutzer für NetScaler ADM Agent erstellen.

Verbesserungen der Benutzerfreundlichkeit und Funktionalität für das Dashboard zur Datenspeicherverwaltung

Um die Benutzerfreundlichkeit zu verbessern und die Datenspeicherverwaltung effizienter zu gestalten, sind die folgenden Verbesserungen für das Dashboard zur **Datenspeicherverwaltung** verfügbar:

- Neues UI-Design für das Dashboard:
  - Kacheln für **Datenerfassung**, **Speicherverbrauch**, **Datenbereinigung** und **Aktionen** hinzugefügt
  - Die Kachel **Aktionen** bietet Optionen zum Hinzufügen von mehr Speicher, zum Überprüfen der Datenaufbewahrungsrichtlinie, zum Durchführen der Datenbereinigung und zum Überprüfen Ihrer Systembenachrichtigungen.
- Suchfunktion im Abschnitt **Speicherverbrauchstrends**:

  Zusätzlich zur Anzeige der Speichertrends können Sie jetzt nach bestimmten Funktionen und Trends suchen.
- Datenbereinigung durchführen:
  - Sie können jetzt eine oder mehrere Funktionen auswählen und deren Daten bereinigen, um Speicherplatz freizugeben.
  - Sie sind zu 10 Datenbereinigungen pro Monat berechtigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen zum Dashboard für die Datenspeicherverwaltung finden Sie unter Datenspeicherverwaltung.

Sicherheit

API Gateway umbenannt in API Security

API Gateway wurde in **API Security** umbenannt. Die Änderungen können auf den folgenden Seiten angezeigt werden:

- **Sicherheit > API Security**
- **Sicherheit > API Security > API Analytics > Hilfe erhalten > API Security-Dokumente**
- **Einstellungen > Benutzer & Rollen > Gruppen > Autorisierungseinstellungen > API Security**
- **Einstellungen > Benutzer & Rollen > Zugriffsrichtlinien > Berechtigungen > Sicherheit > API Security**

Behobene Probleme

Die Probleme, die in Build August 31, 2023 behoben wurden.

Verwaltung und Überwachung

- Unter **Infrastruktur > Netzwerkberichterstattung** zeigt das Dashboard für die Netzwerkberichterstattung keine historischen Daten in den Berichten der virtuellen Server an. Dieses Problem tritt auf, wenn Sie ein NetScaler HA-Paar unter **Entitäten auswählen** bei der Erstellung des Dashboards auswählen.

August 11, 2023

Verwaltung und Überwachung

Sicherheitshinweis – Überwachung der Dateintegrität

Der NetScaler Console Sicherheitshinweis ermöglicht es Ihnen nun, die NetScaler Build-Dateien zu scannen und die Ergebnisse von Änderungen oder Ergänzungen an den ursprünglichen NetScaler Build-Dateien anzuzeigen.

Im Sicherheitshinweis (**Infrastruktur > Instanzhinweis > Sicherheitshinweis**) können Sie mit der Option **Jetzt scannen** die Optionen **CVEs scannen**, **Dateien scannen** oder **Beide scannen** auswählen. Nachdem Sie **Dateien scannen** oder **Beide scannen** ausgewählt haben, vergleicht

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console den binären Hash für verwaltete NetScaler Build-Dateien mit den ursprünglichen binären Hash-Werten und hebt im Tab **Dateintegritätsüberwachung** hervor, ob Dateiveränderungen oder Dateiergänzungen vorliegen.

Die Scan-Ergebnisse zeigen die NetScaler-Instanzen an, bei denen potenzielle Änderungen an den Originaldateien und/oder andere Dateiergänzungen vorliegen. Für weitere Untersuchungen der Scan-Ergebnisse können Sie die digitale Forensik Ihrer Organisation kontaktieren.

Weitere Informationen finden Sie unter Sicherheitshinweis.

August 09, 2023

Infrastruktur

Virtualisierungsplattformdetails für NetScaler VPX™ anzeigen

Unter **Infrastructure > Instances > NetScaler > VPX** können Sie jetzt die Plattform anzeigen, auf der NetScaler VPX gehostet wird, indem Sie **Settings > Cloud Platform** auswählen.

Fehlgeschlagene Upgrade-Aufträge wiederholen

Unter **Infrastructure > Upgrade Jobs** können Sie jetzt den fehlgeschlagenen Upgrade-Auftrag auswählen und eine der folgenden Aktionen ausführen:

- Klicken Sie auf **Retry** neben dem fehlgeschlagenen Upgrade-Auftrag
- Gehen Sie zu **Select Action > Retry Upgrade Job**

Weitere Informationen finden Sie unter Fehlgeschlagene Upgrade-Aufträge wiederholen.

Sicherheit

Eine vorhandene API-Definition aktualisieren

Unter **Security > API Gateway > API Discovery** können Sie jetzt eine vorhandene API-Definition mit ausgewählten API-Ressourcen aktualisieren.

Weitere Informationen finden Sie unter Eine vorhandene API-Definition mit erkannten API-Endpunkten aktualisieren.

Behobene Probleme

Die Probleme, die in Build August 09, 2023 behoben wurden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Bereitstellung

- Die NetScaler VPX-Bereitstellung auf VMware vCenter (**Infrastructure > Instance > Citrix ADC > VPX > Provision**) schlägt fehl, da derselbe Name verwendet wurde, der in der zuvor gelöschten VPX-Instanz verwendet wurde.

StyleBooks

- Wenn Sie versuchen, eine ADC-Konfiguration von einer Quell-ADC-Instanz zu einer Zielinstanz unter **Applications > Configuration > Config Packs > Migrate ADC > Get Started > Specify Configuration** zu migrieren und auf **Next** klicken, wird zeitweise die folgende Fehlermeldung angezeigt:

  Kein Job gefunden.

- Wenn Sie ein Configpack aus einer StyleBook-Definition erstellen, die einen virtuellen Authentifizierungsserver und integrierte Cache-Richtlinienbindungen enthält, und das Configpack anschließend löschen, ist die Löschung erfolgreich. Wenn Sie jedoch versuchen, das Configpack erneut mit denselben Parametern zu erstellen, wird die folgende Fehlermeldung angezeigt:

  Ressource existiert bereits.

July 26, 2023

Analysen

Unterstützung zum Konfigurieren des Exports von Metriken von NetScaler nach Prometheus über StyleBook

Um Metriken von NetScaler nach Prometheus zu exportieren, müssen Sie ein Analyseprofil in NetScaler erstellen und die Schemadatei angeben. Weitere Informationen finden Sie unter Überwachung von NetScaler Console, Anwendungen und Anwendungssicherheit mit Prometheus.

Unter **Applications > Configuration > Stylebooks > Default Stylebook** können Sie jetzt das StyleBook **Prometheus TimeSeries Analytics Configuration** verwenden und die Konfiguration für alle verwalteten Instanzen ausführen.

Weitere Informationen finden Sie unter Prometheus Analytics StyleBook.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Zuweisen eines Netzprofils für die verwalteten NetScaler-Instanzen von NetScaler Console

Wenn Sie Analysen für die virtuellen Server in NetScaler Console aktivieren, werden die AppFlow-Daten vom NetScaler über die NetScaler-Subnetz-IP-Adresse (SNIP) an NetScaler Console exportiert. In einigen Szenarien kann die SNIP aufgrund der Firewall im Netzwerk blockiert sein. In solchen Szenarien müssen Sie möglicherweise eine andere IP-Adresse als die SNIP verwenden. Weitere Informationen zum Netzprofil finden Sie unter Verwenden einer angegebenen Quell-IP für die Back-End-Kommunikation.

Sie können jetzt NetScaler-Instanzen über NetScaler Console Netzprofile zuweisen. Navigieren Sie zu **Infrastructure > Instances > Citrix ADC**, wählen Sie die Instanz aus und klicken Sie in der Liste **Select Action** auf **Configure Net Profiles**, um der Instanz ein Netzprofil zuzuweisen.

HINWEIS:

Stellen Sie sicher, dass Sie die Analyse in allen virtuellen Servern deaktiviert haben, bevor Sie der Instanz ein Netzprofil zuweisen.

Mit dieser Erweiterung können Sie ein Netzprofil für den Export von AppFlow-Daten von NetScaler an NetScaler Console zuweisen.

Infrastruktur

Verbesserte Benutzerfreundlichkeit bei der Verwendung der CLI zur Konfiguration des NetScaler-Agenten als Proxy

Wenn Sie versuchen, einen NetScaler-Agenten beim NetScaler Console-Dienst zu registrieren, werden Sie in der CLI jetzt mit (y/n)-Fragen zur Proxy-Nutzung aufgefordert.

Sie haben auch die Möglichkeit, den Proxy bei Bedarf im selben Skript zu konfigurieren.

CLI-Unterstützung zum Anzeigen von Endpunkt-URLs bei der Registrierung eines NetScaler-Agenten

Nachdem Sie eine Dienst-URL in der CLI eingegeben haben, während Sie einen NetScaler-Agenten beim NetScaler Console-Dienst registrieren, können Sie die Liste aller Endpunkt-URLs anzeigen, denen der Zugriff gestattet werden muss.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StyleBooks

Unterstützung für zusätzliche Attribute in StyleBooks-Analysen

Der Abschnitt StyleBooks-Analysen wurde nun erweitert, um:

- Parameter zur Konfiguration des Transportmodus akzeptieren (`transport-mode`)
- HDX Insight für verschiedene Arten von Datenverkehr konfigurieren (`enable-hdxinsight-for`)
  - HTTP X-Forwarded-For-Option aktivieren (`http-x-forwarded-for`)
  - Clientseitige Messungen aktivieren (`client-side-measurements`)

Weitere Informationen finden Sie unter StyleBooks Analytics.

July 18, 2023

Verwaltung und Überwachung

Unterstützung bei der Identifizierung und Behebung von CVE-2023-3519, CVE-2023-3466 und CVE-2023-3467

NetScaler Console Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2023-3519, CVE-2023-3466 und CVE-2023-3467.

Identifizierung von:

- CVE-2023-3519 erfordert eine Kombination aus Versions- und Konfigurationsscan.
- CVE-2023-3466 und CVE-2023-3467 erfordern einen Versionsscan.

Die Behebung für CVE-2023-3519, CVE-2023-3466 und CVE-2023-3467 erfordert ein Upgrade der anfälligen NetScaler-Instanz auf eine Version und einen Build, der den Fix enthält.

HINWEIS:

Security Advisory unterstützt keine NetScaler-Builds, die das End of Life (EOL) erreicht haben. Wir empfehlen Ihnen, auf die von NetScaler unterstützten Builds oder Versionen zu aktualisieren.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von NetScaler-Instanzen finden Sie unter Aufträge zum Upgrade von NetScaler-Instanzen verwenden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen zur Behebung von CVE-2023-3519, CVE-2023-3466 und CVE-2023-3467 finden Sie unter Sicherheitsbulletin.

HINWEIS:

Es kann einige Stunden dauern, bis der Scan des Sicherheitshinweissystems abgeschlossen ist und die Auswirkungen von CVE-2023-3519, CVE-2023-3466 und CVE-2023-3467 im Sicherheitshinweismodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, können Sie einen On-Demand-Scan starten, indem Sie auf **Jetzt scannen** klicken.

July 12, 2023

Behobene Probleme

Die Probleme, die in Build July 12, 2023 behoben wurden.

- Wenn Sie eine NetScaler-Instanz sichern oder wiederherstellen, wird das Verzeichnis `/var/metrics_conf` nicht gesichert.
- Die Bereitstellung von Konfigurationspaketen kann fehlschlagen, wenn die StyleBook-Definition den Abschnitt `operations` enthält.

July 03, 2023

Analysen

Konfigurationsauftrag – Unterstützung zum Erstellen eines Auftrags zur Konfiguration des Exports von Metriken von NetScaler nach Prometheus

Um Metriken von NetScaler nach Prometheus zu exportieren, müssen Sie ein Analyseprofil in NetScaler erstellen und die Schemadatei angeben. Weitere Informationen finden Sie unter Überwachung von NetScaler, Anwendungen und Anwendungssicherheit mit Prometheus.

In **Konfigurationsauftrag** können Sie jetzt einen Auftrag mithilfe der Vorlage `NSConfigurePrometheusAnalyticsProfile` aus der **integrierten Vorlage** erstellen, die erforderlichen Parameter angeben und den Auftrag für alle verwalteten Instanzen ausführen.

Weitere Informationen finden Sie unter Planen eines Auftrags zur Konfiguration des Exports von Metriken von NetScaler nach Prometheus.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Infrastruktur

NetScaler-Agent speichert NetScaler-Images zwischen

Die für das NetScaler-Upgrade benötigte Zeit wird jetzt erheblich reduziert, da die NetScaler-Images nach dem Herunterladen im NetScaler-Agent zwischengespeichert werden. Daher müssen die Images für nachfolgende Upgrade-Aufträge nicht erneut heruntergeladen werden.

HINWEIS:

Dies gilt nur für NetScaler, die über den NetScaler-Agent hinzugefügt werden.

Weitere Informationen finden Sie unter ADC-Upgrade-Job erstellen.

Behobene Probleme

- In Web Insight bleibt das Diagramm in der vorherigen Ansicht, wenn Sie eine Metrik aufschlüsseln, um Details anzuzeigen, und dann eine weitere Metrik aufschlüsseln, aber alle anderen Details werden wie erwartet angezeigt.

  Dies führt zu der Annahme, dass die weitere Aufschlüsselung nicht wie erwartet funktioniert.

- Wenn Sie versuchen, eine ADC-Konfiguration von einer Quell-ADC-Instanz zu einer Zielinstanz unter **Applications > Configuration > Config Packs > Migrate ADC > Get Started > Specify Configuration** zu migrieren und auf **Next** klicken, wird zeitweise die folgende Fehlermeldung angezeigt:

  „Kein Job gefunden“.

- Im **App-Dashboard** wird beim Auswählen einer Anwendung und Navigieren zur Registerkarte **SSL** zum Binden eines Zertifikats die Fehlermeldung „**Zertifikat nicht in Datenbank gefunden**“ angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

June 14, 2023

Sicherheit

Unterstützung zum Erstellen einer API-Definition ohne Auswahl von Endpunkten

Auf der Seite **Security > API Gateway > API Discovery** > **Vserver** können Sie jetzt eine API-Definition erstellen, ohne einen Endpunkt auszuwählen. Wenn Sie auf **API-Definition erstellen** klicken, wird ein Pop-up-Fenster angezeigt, in dem Sie bestätigen können, ob eine API-Definition für alle erkannten Endpunkte erstellt werden soll. Klicken Sie auf **Ja**, um die API-Definition mit allen Endpunkten zu erstellen, andernfalls klicken Sie auf **Nein**.

Weitere Informationen finden Sie unter API-Endpunkte ermitteln.

StyleBooks

Unterstützung für zusätzliche Argumenttypen in der Funktion replace()

Die integrierte Funktion `replace()` kann auch eine Liste der folgenden integrierten Typen akzeptieren:

- `string`
- `ipaddress`
- `tcp-port`
- `number`
- `boolean`

Weitere Informationen finden Sie unter replace().

Behobene Probleme

Die Probleme, die in Build June 14, 2023 behoben wurden.

- In Upgrade-Aufträgen (**Infrastruktur > Upgrade-Aufträge**) wird eine Fehlermeldung angezeigt, wenn Sie die Instanz auswählen, bei der die Vor-Upgrade-Validierung fehlgeschlagen ist, und auf **Neu validieren** klicken.

- MPX-Instanzen fehlen auf der Seite **Infrastruktur > Citrix ADC-Bestand > Citrix ADC (MPX/VPX/CPX/BLX)**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Wenn Sie die SSL-Ablaufberichte für wöchentlich, 30 Tage oder 90 Tage aus **Infrastruktur > SSL-Dashboard > SSL-Zertifikate > Berichte exportieren** exportieren und **Tabellarisch** auswählen, zeigt der resultierende Bericht eine leere Domänenspalte an.

- Unter **Infrastruktur > SSL-Dashboard > SSL-Zertifikate** zeigt das NetScaler-Hochverfügbarkeitspaar nicht den hochgestellten Buchstaben „P“ und „S“ für die primären und sekundären Geräte an.

- In NetScaler-Version 13.1 und höher werden die ISSU-Befehle während des NetScaler-Upgrades nicht ausgeführt.

- Bei mehreren Cluster-IP-Adressen (CLIPs) in einem Cluster schlägt die Konfiguration fehl und der CLIP wird nicht zur NetScaler Console hinzugefügt, wenn Sie einen CLIP in Klammern unter **Infrastruktur > Instanzen > Citrix ADC > Hinzufügen** hinzufügen.

May 31, 2023

Analysen

Empfehlungen für gepoolte Lizenzen in der Funktion „Aufgaben“

Unter **Aufgaben** können Sie jetzt Empfehlungen und Guide Me-Workflows für gepoolte Lizenzberechtigungen anzeigen. Als Administrator stellen diese Empfehlungen für gepoolte Lizenzen sicher, dass Sie alle Funktionen von NetScaler Console nutzen.

Weitere Informationen finden Sie unter Empfehlungen anzeigen und Ihre ADCs und Anwendungen effizient verwalten.

SSL-Einblicksdaten nach Splunk und New Relic exportieren

Wenn Sie unter **Einstellungen > Ökosystemintegration** ein neues Abonnement für die Integration von Citrix ADM mit Splunk und New Relic erstellen, können Sie jetzt die Option **SSL-Zertifikat-Einblicke** auswählen. Nachdem Sie das Abonnement mit der Option **SSL-Zertifikat-Einblicke** konfiguriert haben, können Sie die SSL-Daten (SSL-vServer- und SSL-Zertifikat-bezogene Daten) im Splunk- und New Relic-Dashboard anzeigen.

Weitere Informationen finden Sie unter Integration mit Splunk und Integration mit New Relic.

Behobene Probleme

Die Probleme, die in Build May 31, 2023 behoben wurden.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Unter **Gateway > HDX Insight > Instanzen** war beim Auswählen einer Instanz und Exportieren der Daten die Benutzername-Information für Desktop-Benutzer nicht verfügbar. Mit dieser Korrektur sind die Benutzername-Informationen auch im Bericht verfügbar.

- Wenn Sie unter **Infrastruktur > Instanzen > Citrix ADC > SDX** die Option **SNMP konfigurieren** für eine SDX-Instanz auswählen, wird eine Fehlermeldung angezeigt. Dieses Problem tritt auf, wenn das SDX-Profil mit SNMP v3 und **NoAuthNoPriv** als Sicherheitsstufe konfiguriert ist.

- Unter **Infrastruktur > Konfiguration > Konfigurationsaufträge > Auftrag erstellen > Konfiguration auswählen** wird die Seite nicht geladen, wenn Sie eine Passwortvariable ($password$) eingeben und den **Typ** als **Textfeld** anstelle von **Passwortfeld** beibehalten und auf **Weiter** klicken.

- In Web Insight werden die Diagramme im Bericht leer angezeigt, wenn Sie Daten über die Snapshot-Option exportieren.

- Analysen sind in HDX Insight nicht sichtbar. Selbst wenn Citrix ADM neu gestartet wird, sind die Analysen nur für kurze Zeit sichtbar und werden später unsichtbar.

- Für eine SDX-Instanz unter **Infrastructure > Instances > Citrix ADC > SDX > Dasboard** zeigt das Diagramm **System Resource Utilization** einen leeren Bereich und leere Wertefelder an, wenn die belegten und freien Werte für eine Ressource null sind.

  Mit diesem Fix wird die Zahl Null neben dem Ressourcennamen angezeigt, wenn die belegten und freien Werte null sind.

May 18, 2023

Analysen

Unterstützung für den Export aus jedem Widget in Web Insight

In **Web Insight** ist die Exportoption jetzt in allen Widgets verfügbar und ermöglicht Ihnen den Export von Daten im Tabellenformat. Mit dieser Verbesserung können Sie:

- Die erforderlichen Daten einzeln aus jedem Widget exportieren.
- Jede Metrik aufschlüsseln und die erforderlichen Daten aus jedem Widget exportieren.

Zuvor lieferten die Exportdaten nur den konsolidierten Bericht.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Hinweis

Sie können auch weiterhin die vorhandene Exportoption verwenden, um den konsolidierten Bericht zu generieren.

Infrastruktur

Vollständige Zertifikatskette anzeigen

Sie können jetzt die vollständige Kette von Links für ein Zertifikat anzeigen, einschließlich der Zwischenzertifikate bis zum Root-CA-Zertifikat.

Um die Zertifikatskette anzuzeigen, navigieren Sie zu **Infrastructure > SSL Dashboard**, wählen Sie ein SSL-Zertifikat aus und klicken Sie auf **Details**.

Unterstützung für die Protokollierung von Ereignissen unabhängig vom Ereignisalter

NetScaler Console ermöglicht Ihnen jetzt die Aufzeichnung aller Ereignisse, unabhängig vom Ereignisalter, das Sie in den Ereignisregeln festgelegt haben.

Um diese Option festzulegen, navigieren Sie zu **Infrastructure > Rules > Add > Configure Event Age** und aktivieren Sie das Kontrollkästchen **Log events instantly irrespective of event age duration**.

Behobene Probleme

Die in Build May 18, 2023 behobenen Probleme.

- Wenn Sie unter **Infrastructure > Upgrade Jobs > Add > Schedule Task** die Option **Perform two stage upgrade for nodes in HA** auswählen und in den beiden Feldern **Start Time** dieselbe Zeit auswählen, wird beim Fortfahren die folgende Fehlermeldung angezeigt:

  "common.date_diff_error:Zwischen den Upgrade-Zeiten sollte ein Unterschied von mindestens 1 Stunde liegen"

  Auch wenn Sie die Startzeit in den Feldern ändern, zeigt die Registerkarte **Auftrag erstellen** eine leere Seite an.

- Unter **Infrastruktur > Instanzberatung > Upgrade-Beratung** sind die Details zu End of Maintenance (EOM) und End of Life (EOL) für Release 13.0 falsch.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Die E-Mail-Benachrichtigung für jedes Ereignis zeigte die Region fälschlicherweise an. Mit dieser Korrektur wird die Region in den E-Mail-Benachrichtigungen für Ereignisse nicht mehr angezeigt.

May 09, 2023

Verwaltung und Überwachung

Unterstützung bei der Identifizierung und Behebung von CVE-2023-24488 und CVE-2023-24487

NetScaler Console Security Advisory unterstützt jetzt die Identifizierung und Behebung von CVE-2023-24488 und CVE-2023-24487.

Identifizierung von:

- CVE-2023-24488 erfordert eine Kombination aus Versions- und Konfigurationsscan.
- CVE-2023-24487 erfordert einen Versionsscan.

Die Behebung für CVE-2023-24487 und CVE-2023-24488 erfordert ein Upgrade der anfälligen ADC-Instanz auf ein Release und einen Build, der die Korrektur enthält.

Weitere Informationen zu den Details der behobenen Build-Version für CVE-2023-24487 und CVE-2023-24488 finden Sie unter Sicherheitsbulletin.

HINWEIS:

ADC Build 13.1–45.63 ersetzt Build 13.1–45.61.

Weitere Informationen zur Verwendung von NetScaler Console zum Upgrade von ADC-Instanzen finden Sie unter ADC-Upgrade-Job erstellen.

HINWEIS:

Es kann ein paar Stunden dauern, bis der Scan des Sicherheitshinweissystems abgeschlossen ist und die Auswirkungen von CVE-2023-24488 und CVE-2023-24487 im Sicherheitshinweismodul widergespiegelt werden. Um die Auswirkungen früher zu sehen, können Sie einen On-Demand-Scan starten, indem Sie auf **Jetzt scannen** klicken.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

April 25, 2023

Die Verbesserungen und Änderungen, die im Build April 25, 2023 verfügbar sind.

Analysen

Web Insight – Unterstützung zur Anzeige von Nullwerten in Diagrammen

In **Web Insight** bietet die Analyseansicht beim Drilldown einer Metrik unter Anwendungen, Clients, URLs oder Instanzen jetzt die Sichtbarkeit von Nullwerten (z. B. 0 ms und 0 Anfragen) im Diagramm für die ausgewählte Dauer.

Zuvor, wenn für die ausgewählte Dauer kein Datenverkehr oder keine Transaktionen empfangen wurden, zeigte Web Insight die Diagramme an, indem diese Nullwerte übersprungen wurden. Als Administrator können Sie nun das vollständige Diagramm mit diesen Nullwerten anzeigen.

StyleBooks

Benutzergruppenzugriff auf Konfigurationspakete festlegen

Als Administrator können Sie jetzt Benutzergruppen den Zugriff auf Konfigurationspakete verwehren, die von anderen Benutzergruppen erstellt wurden. Um diese Option auszuwählen, navigieren Sie zu **Einstellungen > Benutzer & Rollen > Gruppen > Autorisierungseinstellungen > Konfigurationspakete > Alle Konfigurationen, die von der Benutzergruppe erstellt wurden**.

Behobene Probleme

Die Probleme, die in Build April 25, 2023 behoben werden.

- In **Anwendungen > Konfiguration > Konfigurationspakete** wird, wenn Sie eine Suchanfrage unter Verwendung der Suchkriterien **Eigenschaften > Anzeigeschlüssel** eingeben, das Suchergebnis angezeigt, aber die Suchleiste zeigt die Indexnummer des Ergebnisses an.

  Mit diesem Fix zeigt die Suchleiste die Suchanfrage als Text anstelle einer Zahl an.

Analysen

- Die Bandbreitendaten in **HDX Insight** und **Gateway Insight** werden fälschlicherweise in Bytes pro Sekunde anstelle von Bits pro Sekunde angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

April 13, 2023

Die Verbesserungen und Änderungen, die in Build April 13, 2023 verfügbar sind.

Analysen

Benachrichtigung über integrierten Cache in Web Insight

Nachdem Sie den integrierten Cache in der NetScaler-Instanz aktiviert haben, werden die berechtigten Anfragen verarbeitet, ohne dass ein Roundtrip zu einem Ursprungsserver erforderlich ist. In **Web Insight** sind diese Anfragen des integrierten Caches derzeit unter **Server** mit der IP-Adresse des virtuellen Servers anstelle der tatsächlichen IP-Adresse des Servers sichtbar.

Für eine bessere Sichtbarkeit dieser Integrated Cache-Anfragen können Sie jetzt eine IC-Benachrichtigung neben der IP-Adresse des virtuellen ADC-Servers unter **Server** anzeigen.

Für Anfragen, die nicht mit Integrated Cache verarbeitet werden, ist die tatsächliche IP-Adresse des Ursprungsservers sichtbar.

Als Administrator ermöglicht Ihnen diese Benachrichtigung, schnell zu erkennen, dass die ADC-Instanz die Integrated Cache-Anfragen verarbeitet hat.

Diagramm für Integrated Cache-Treffer und -Fehler in Web Insight

In **Web Insight** zeigen die **Servermetriken** jetzt, wenn Sie einen Server aufschlüsseln, die Registerkarten **Integrated Cache-Treffer** und **Integrated Cache-Fehler** an.

Als Administrator die Diagrammansicht in:

- Die Registerkarte **Integrated Cache-Treffer** ermöglicht Ihnen, die Gesamtzahl der Antworten anzuzeigen, die die NetScaler-Appliance aus dem Cache bereitstellt.
- Die Registerkarte **Integrated Cache-Fehler** ermöglicht Ihnen, die Gesamtzahl der Antworten anzuzeigen, die die NetScaler-Appliance vom Ursprungsserver bereitstellt.

Web Insight – Anzeige von Durchschnitts- und Maximalwerten in Diagrammen

Ab Version 13.1 45.47 oder höher wird **Web Insight** in NetScaler Console mit der Sichtbarkeit von maximalen Latenzwerten unter **Server** und **Clients** unterstützt.

Zusätzlich zu dieser Unterstützung können Sie, wenn Sie einen Server oder einen Client aufschlüsseln, jetzt sowohl Durchschnitts- als auch Maximalwerte im Übersichtsfenster anzeigen und auch, indem Sie den Mauszeiger über das Zeitreihen-Analyse-Diagramm in **Server-Netzwerklatenz**, **Server-Antwortzeit** und **Client-Netzwerklatenz** bewegen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Als Administrator ermöglicht Ihnen diese Verbesserung, die maximale Latenz in Diagrammen für die ausgewählte Dauer zu visualisieren.

Infrastruktur

Datenspeichertrends in der NetScaler Console GUI anzeigen

Unter **Einstellungen > Datenspeicher** können Sie jetzt die Datenspeicherinformationen für die verschiedenen Funktionen in Ihrer aktuellen Bereitstellung anzeigen. Das Dashboard **Datenspeicherverwaltung** hilft Ihnen, zu visualisieren, wie die Daten gespeichert werden und ob die Funktionen innerhalb ihres Speicheranspruchs arbeiten.

HINWEIS

Die Datenspeicherrichtlinien werden sich in den kommenden Versionen voraussichtlich ändern. Mit diesen Änderungen können Sie keine historischen Daten mehr speichern, nachdem sie das Speicherlimit überschritten haben.

Weitere Informationen finden Sie unter Datenspeicher verwalten.

Behobene Probleme

Die Probleme, die in Build April 12, 2023 behoben wurden.

Infrastruktur

- In Hochverfügbarkeitsbereitstellungen gibt es keine Option, Build-Image-Dateien nur auf den sekundären Knoten hochzuladen.

  Als Teil der Korrektur können Sie jetzt Build-Image-Dateien auf den sekundären Knoten hochladen, und zwar unter **Infrastruktur > Upgrade-Aufträge** > Registerkarte **Auftrag erstellen** > **Nur auf sekundären Knoten hochladen**.

- Die aus **Infrastruktur > Instanzen > NetScaler** exportierten Berichte zeigen die Seriennummer der sekundären Knoten nicht an.

  Die Berichte zeigen jetzt die Seriennummern sowohl der primären als auch der sekundären Knoten der NetScaler-Instanzen an. Sie können die Berichte auch unter **Infrastruktur > NetScaler-Bestand** anzeigen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

April 05, 2023

Die Verbesserungen und Änderungen, die in Build April 05, 2023 verfügbar sind.

Sicherheit

API-Definitionen aus erkannten API-Endpunkten in der NetScaler Console GUI erstellen

Sie können jetzt API-Definitionen aus erkannten API-Endpunkten unter **Sicherheit > API-Gateway > API-Erkennung** erstellen.

Vereinheitlichtes Dashboard – Wichtige API-Analysemetriken anzeigen

Im vereinheitlichten Dashboard (**Übersicht > Dashboard**) können Sie jetzt wichtige Metriken für die über NetScaler Console konfigurierten API-Endpunkte anzeigen.

Weitere Informationen finden Sie unter Ein vereinheitlichtes Dashboard zur Anzeige wichtiger Metrikdetails der Instanz.

Behobene Probleme

Die Probleme, die in Build April 05, 2023 behoben wurden.

- Die Option **Appliance auswählen** für die Felder **Zertifikatsdatei** und **Schlüsseldatei** wird für die folgenden Seiten angezeigt:
  - **Infrastruktur > SSL-Dashboard > Zertifikatsspeicher verwalten > Hinzufügen**
  - **Infrastruktur > SSL-Dashboard > SSL-Zertifikate > Aktualisieren**

  Als Korrektur wurde die Option **Appliance auswählen** nun entfernt.

- Wenn NetScaler eine lokale NetScaler Console als Lizenzserver hat und ein Agent in **Infrastruktur > Instanzen > Agents** geändert wird, tritt das folgende Problem auf:

  `The IP address of the license server on NetScaler changes from the IP address of the on-premises NetScaler Console to the IP address of one of the NetScaler agents`.

- Wenn Sie das Kennwort für ein mit SNMPv3 konfiguriertes SDX-Administratorprofil unter **Infrastruktur > Instanzen > NetScaler > SDX-Registerkarte > Profil** bearbeiten, wird die folgende Fehlermeldung angezeigt:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`Please provide valid authentication protocol. The possible values are MD5, SHA`.

March 14, 2023

Behobene Probleme

Das folgende Problem wird in Build March 14, 2023 behoben:

Unter **Infrastruktur > SSL-Dashboard > Zertifikate installieren** schlägt die Zertifikatsinstallation fehl, wenn Sie eine Zertifikatskette hochladen, die dasselbe Stammzertifikat wie eine vorhandene Zertifikatskette hat. Der folgende Text wird unter **Infrastruktur > SSL-Dashboard > SSL-Audit-Protokolle > Geräteprotokoll > Befehlsprotokoll** angezeigt:

`Resource Already Exists`

Wenn Sie eine E-Mail-Verteilerliste aus **Einstellungen > Benachrichtigungen > E-Mail** löschen, wird der folgende Fehler angezeigt:

`Error: Bad Gateway`

Dieses Problem tritt auf, weil der Name der E-Mail-Verteilerliste ein Leerzeichen enthält.

Im Rahmen der Fehlerbehebung ermöglicht NetScaler Console Ihnen jetzt das Löschen von E-Mail-Verteilerlisten mit Leerzeichen.

March 02, 2023

Analysen

Verbesserungen an Web Insight

In Web Insight können Sie jetzt die folgenden Verbesserungen unter **Anwendungsmetriken** anzeigen:

- Eine neue Registerkarte **Zusammenfassung** wird eingeführt, die es Ihnen ermöglicht, eine Übersicht über die Anwendungsleistung zu visualisieren, wie z. B. Antwortzeit, Anfragen und Bandbreite. Als Administrator erhalten Sie dadurch einen Einblick in die Anwendungsleistung für den ausgewählten Zeitraum. Sie können die Umschaltoption verwenden und die Ansicht anpassen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Auf der Registerkarte **Anfragen** können Sie neben den bestehenden Gesamtanfragen auch Anfragen von den Top-5-Clients basierend auf den Gesamtanfragen anzeigen. Als Administrator erhalten Sie dadurch einen Einblick in die Clients, die auf die Anwendung für den ausgewählten Zeitraum zugreifen.
- Auf der Registerkarte **Bandbreite** können Sie den Bandbreitenverbrauch der Top-5-Server basierend auf dem gesamten Bandbreitenverbrauch anzeigen. Als Administrator erhalten Sie dadurch einen Einblick in die Server, die im ausgewählten Zeitraum mehr Bandbreite verbrauchen.
- Auf der Registerkarte **Antwortzeit** können Sie auch Client-Netzwerklatenz, Server-Netzwerklatenz und Server-Verarbeitungszeit im selben Diagramm anzeigen. Als Administrator erhalten Sie dadurch einen Einblick in die Latenz, die vom Client, Server und der Anwendung für den ausgewählten Zeitraum auftritt. Sie können die Umschaltoption verwenden und die Ansicht anpassen.

Infrastruktur

Löschen inaktiver NetScaler Console Express-Konten

Wenn Ihr NetScaler Console Express-Konto 45 Tage lang inaktiv bleibt, wird das Konto gelöscht. Citrix sendet nach 30 Tagen Inaktivität eine Erinnerung.

Verwaltung und Überwachung

Änderung der Ausführungszusammenfassung für das NetScaler Hochverfügbarkeits-Upgrade

In der NetScaler Console GUI zeigt die Ausführungszusammenfassung unter **Infrastructure > Upgrade Jobs > Execution Summary** keine Befehle mehr an, die sich auf die Hochverfügbarkeitssynchronisierung beziehen.

Dies liegt daran, dass NetScaler während des NetScaler Hochverfügbarkeits-Upgrades, wenn die primären und sekundären NetScaler-Knoten unterschiedliche Versionen haben, die Deaktivierung der Hochverfügbarkeitssynchronisierung zwischen den Knoten durchführt. NetScaler Console führt diesen Vorgang nicht aus.

Schwellenwert für einzelne Entitäten in Netzwerkberichten festlegen

Unter **Infrastructure > Network Reporting > Thresholds** können Sie jetzt beim Konfigurieren des Schwellenwerts den Schwellenwert für bestimmte Entitäten festlegen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Weitere Informationen finden Sie unter Netzwerkberichterstellung.

Unterstützung für die Planung individueller Agenten-Upgrades

Unter **Infrastructure > Instances > Agents > Settings** können Sie jetzt das Upgrade jedes NetScaler-Agenten planen. Sie können entweder einen Agenten automatisch auf den nächsten Build aktualisieren lassen oder eine Uhrzeit und Zeitzone für die Planung eines Upgrades festlegen.

Weitere Informationen finden Sie unter Agent-Upgrade-Einstellungen.

Verbesserungen beim Upgrade von NetScaler-Instanzen

Die folgenden Änderungen sind jetzt auf der Registerkarte **Pre-upgrade validation** verfügbar:

- Abschnitt **Instances blocked from upgrade** – Dieser neue Abschnitt listet die Instanzen auf, deren Upgrade aufgrund von Validierungsfehlern vor dem Upgrade blockiert ist.
- Schaltfläche **Quick Cleanup** – Diese Schaltfläche ist im Bereich **Disk Space Details** verfügbar und ermöglicht es Ihnen, den Speicherplatz von mehreren Ordnern schnell freizugeben.

Weitere Informationen finden Sie unter How to upgrade an ADC instance.

NetScaler BLX-Images jetzt in der Image-Bibliothek verfügbar

Beim Upgrade von NetScaler BLX über **Infrastructure > Upgrade jobs > Upgrade NetScaler BLX > Select Image** können Sie jetzt die **NetScaler BLX images** aus der Image-Bibliothek auswählen.

Sicherheit

Anzeigen der Versionen von NetScaler Web App Firewall und Bot-Signaturen für eine NetScaler-Instanz

Sie können jetzt die Versionen von NetScaler Web App Firewall und Bot-Signaturen für eine NetScaler-Instanz anzeigen. Die neuesten Signaturversionen schützen Ihre Instanz vor den CVEs. Weitere Informationen finden Sie unter Signature Alert Articles und Bot signature alert articles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Analyse der Anwendungsleistung

Verbesserungen an Web Insight

In **Web Insight** können Sie jetzt die maximalen Netzwerklatenzwerte sowohl in **Server** als auch in **Client** anzeigen. Als Administrator ermöglicht Ihnen diese Verbesserung, den genauen Server oder Client zu identifizieren, der mit maximaler Latenz arbeitet.

Zuvor lieferte Web Insight den Maximalwert nur basierend auf den durchschnittlichen Latenzwerten über alle Server und Clients hinweg.

Sonstiges

Filter im vereinheitlichten Dashboard erstellen und anwenden

Im vereinheitlichten Dashboard (**Übersicht > Dashboard**) können Sie jetzt Filter erstellen und anwenden in:

- Anwendungen
- ADC-Infrastruktur
- Anwendungssicherheit

Als Administrator können Sie Filter anwenden und Einblicke nur für die ausgewählten Instanzen oder Anwendungen anzeigen.

Weitere Informationen finden Sie unter Ein vereinheitlichtes Dashboard zur Anzeige wichtiger Metrikdetails von Instanzen.

Behobene Probleme

Die Probleme, die in Build Mar 02, 2023 behoben wurden.

- Unter **Infrastructure > Upgrade Jobs** wird, wenn Sie einen abgeschlossenen Auftrag auswählen, dessen Skriptdateiname vor oder nach dem Upgrade Sonderzeichen enthält, und dann die Ausgabeskripte aus der Liste **Aktion auswählen** herunterladen, die Fehlermeldung **Datei nicht gefunden** angezeigt.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

February 07, 2023

Analysen

Sicherheitsverletzungen zeigen OWASP-Tags an

In der NetScaler Console GUI werden Sicherheitsverletzungen jetzt mit OWASP-Tags angezeigt. Es werden die OWASP 2017- und OWASP 2021-Listen unterstützt. Diese Tags helfen Ihnen festzustellen, ob die Verletzung zur OWASP Top 10-Liste gehört.

Wählen Sie eine Verletzung aus, um weitere Details anzuzeigen. Die Details enthalten jetzt die Spalten OWASP 2017 und OWASP 2021. Diese Spalten zeigen die OWASP-Codes an, und Sie können sie verwenden, um weitere Informationen über die Verletzung von der OWASP-Website zu erhalten.

Verwaltung und Überwachung

Unterstützung für die Änderung des Agent-Passworts ohne aktuelles Passwort

Als Superadministrator können Sie jetzt zulassen, dass Agent-Passwörter ohne deren aktuelle Passwörter geändert werden.

Navigieren Sie zu **Einstellungen** > **Globale Einstellungen** > **Systemkonfigurationen** > **Agent und Zeitzone > Agent** und aktivieren Sie das Kontrollkästchen **Voraussetzung für aktuelles Passwort für Agent-Passwortänderung entfernen**. Die Seite **Agent-Passwort ändern** enthält dann nicht mehr das Feld **Aktuelles Passwort**.

Um das Feld **Aktuelles Passwort** wieder anzuzeigen, deaktivieren Sie das Kontrollkästchen **Voraussetzung für aktuelles Passwort für Agent-Passwortänderung entfernen**.

Visualisierungsintervall für Zeitreihendaten für NetScaler Console Express-Konten wurde überarbeitet

Für virtuelle Server, die mit dem Express-Konto verwaltet werden, wurde die Zeitreihen-Datenvisualisierung in Analyse-Diagrammen und Netzwerkberichts-Diagrammen für die Dauer von **Letzte 1 Stunde** nun überarbeitet.

FUNKTION	VORHANDENES DATENVISUALISIERUNGSINTERVALL	NEUES DATENVISUALISIERUNGSINTERVALL
Anwendungs-Dashboard	1 Minute	5 Minuten

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FUNKTION	VORHANDENES DATENVISUALISIERUNGSINTERVALL	NEUES DATENVISUALISIERUNGSINTERVALL
Netzwerkberichterstattung	5 Minuten	10 Minuten
Web Insight, HDX Insight, Gateway Insight, Security Insights, BOT Insights, Detaillierte Transaktionen	1 Minute	5 Minuten

Behobene Probleme

Die folgenden Probleme werden in Build February 07, 2023 behoben.

Wenn Sie die Syslog-Einstellungen für die ADC-Instanz aktivieren oder deaktivieren, speichert ADM die Konfiguration nicht in der ADC-Instanz. Daher werden Ereignisse von Konfigurationsänderungen nicht in NetScaler Console gespeichert.

Unter **Infrastructure > Instances > Agent** schlägt die Verbindung zum Agenten auf Port 443 fehl, nachdem Sie das SSL-Zertifikat mit einem passwortverschlüsselten Schlüssel installiert haben.

January 24, 2023

Behobene Probleme

Die folgenden Probleme werden in Build January 24, 2023 behoben.

Eine Fehlermeldung wird angezeigt, wenn Sie SNMP v3 auf einer NetScaler SDX-Instanz über die NetScaler Console GUI aktivieren, indem Sie zu **Infrastructure > Instances > NetScaler > SDX > Select Action > Configure SNMP** navigieren.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 10, 2023

Verwaltung und Überwachung

Empfehlungen anzeigen und Ihre ADCs und Anwendungen effizient als umsetzbare Aufgaben mit Guide Me-Workflows verwalten

In der NetScaler Console GUI wird eine neue Option **Aufgabe** eingeführt, wo Sie jetzt Empfehlungen basierend auf Ihrem Abonnement und Ihrer aktuellen Auslastung anzeigen können. Als Administrator können Sie:

- **To-Do**-Aufgaben als umsetzbare Empfehlungen für Lizenzierung, Analysen, Ereignisse, SSL-Zertifikate und vieles mehr anzeigen
- Erledigen Sie die Aufgabe mithilfe der Option **Guide Me**, die Anleitungshinweise bereitstellt, um die Aufgabe erfolgreich abzuschließen.
- Bestätigen Sie die Aufgaben und verschieben Sie sie ins Archiv.
- Gehen Sie zu **Archivierte Aufgaben** und verwenden Sie die geführten Hinweise für wiederkehrende Anforderungen.

Diese Empfehlungen stellen sicher, dass Sie alle Funktionen von NetScaler Console nutzen, die Produktentdeckung und vom Produkt empfohlene Funktionalitäten für eine effiziente Verwaltung der Bereitstellung ermöglichen.

Weitere Informationen finden Sie unter Empfehlungen anzeigen und Ihre ADCs und Anwendungen effizient verwalten.

StyleBooks

Netzmaskenlänge in der StyleBook-Konfigurations-GUI aktivieren oder deaktivieren

Wenn Sie ein Konfigurationspaket aus StyleBooks mit dem `type: ipnetwork` Attribut erstellen, zeigt die StyleBook-Konfigurations-GUI jetzt die Schaltfläche **Netzmaskenlänge** neben dem Feld **IP-Adresse** an.

Sie können eine der folgenden Aktionen ausführen:

- Aktivieren, um die Netzmaskenlänge einzugeben
- Deaktivieren, um die Netzmasken-IP-Adresse einzugeben

© 1997–2026 Citrix Systems, Inc. All rights reserved.

fix

This is the content for the sample heading topic. It is hidden from the main table of contents but remains accessible via links.

© 1997–2026 Citrix Systems, Inc. All rights reserved.