# NetScaler VPX 14.1

cloud SOFTWARE GROUP

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

# Contents

NetScaler VPX Support-Matrix 32
VPX-Instanz auf VMware ESX Hypervisor 32
VPX-Instanz auf XenServer oder Citrix Hypervisor™ 34
VPX-Instanz auf Microsoft Hyper-V 35
VPX-Instanz auf Azure Local 35
VPX-Instanz auf Red Hat® OpenShift® Virtualization (RHOCPV) 35
VPX-Instanz auf Nutanix AHV 36
Einstellung von Citrix Ready® VPX (KVM) auf Nutanix AHV 36
VPX-Instanz auf generischem KVM 37
VPX-Instanz in öffentlichen Clouds 38
VPX-Funktionen, die auf Hypervisoren unterstützt werden 38
VPX-Funktionen, die in öffentlichen Clouds unterstützt werden 41
Unterstützte Browser 43
Unterstützte Prozessoren für NetScaler VPX™ 43
Unterstützte NICs für NetScaler® VPX 44
Weitere Referenzen 45
Optimieren der NetScaler VPX-Leistung auf VMware ESX, Linux KVM und Citrix Hypervisoren 46
NetScaler VPX-Instanz auf VMware ESX-Hypervisoren 46
Empfohlene Konfiguration auf ESX-Hosts 46
NetScaler VPX mit E1000-Netzwerkschnittstellen 47
Zwei vNICs pro pNIC-Bereitstellung 48
NetScaler VPX mit VMXNET3-Netzwerkschnittstellen 49
Konfigurieren Sie Multi-Queue- und RSS-Unterstützung auf VMware ESX für VMXNET3-Geräte 50
NetScaler VPX mit SR-IOV- und PCI-Passthrough-Netzwerkschnittstellen 51
Nutzungsrichtlinien für VMware ESXi Hypervisor 51

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

Befehle zur Steuerung der CPU-Auslastung der Paket-Engine 53
NetScaler VPX-Instanz auf der Linux-KVM-Plattform 54
Leistungseinstellungen für KVM 55
NetScaler VPX mit PV-Netzwerkschnittstellen 59
NetScaler VPX mit SR-IOV- und Fortville-PCIe-Passthrough-Netzwerkschnittstellen 61
NetScaler VPX-Instanz auf Citrix Hypervisors 62
Leistungseinstellungen für Citrix Hypervisors 62
NetScaler VPX mit SR-IOV-Netzwerkschnittstellen 63
NetScaler VPX mit paravirtualisierten Schnittstellen 63
Unterstützung für die Erhöhung des NetScaler VPX-Festplattenspeichers 65
Primäre Festplattengröße auf NetScaler VPX dynamisch erhöhen 65
Sekundäre Festplatte hinzufügen 66
Manuelles Erhöhen der primären Festplattengröße auf NetScaler VPX 67
Zusätzlichen Management-CPU-Kern auf NetScaler VPX konfigurieren 69
Zusätzlichen Management-CPU-Kern über die CLI konfigurieren 69
Zusätzlichen Management-CPU-Kern über die GUI konfigurieren 70
Statistiken und Überwachung 71
Fehlerbehebung bei zusätzlicher Management-CPU 71
Anwenden von NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance in der Cloud 73
Was sind Benutzerdaten 73
So stellen Sie Preboot-Benutzerdaten in der Cloud-Instanz bereit 73
Bereitstellen von Preboot-Benutzerdaten über die AWS-Konsole 74
Preboot-Benutzerdaten mithilfe der AWS CLI bereitstellen 74
Preboot-Benutzerdaten mithilfe der Azure-Konsole bereitstellen 75
Preboot-Benutzerdaten mithilfe der Azure CLI bereitstellen 75
Preboot-Benutzerdaten mithilfe der GCP-Konsole bereitstellen 75
Preboot-Benutzerdaten mithilfe der gcloud CLI bereitstellen 76

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

Format der Preboot-Benutzerdaten 76
NetScaler-Konfigurationen 77
Benutzerskripte 79
Lizenzierung 82
Bootstrapping 83
Standard-Bootstrap-Konfiguration 83
Bootstrap-Konfiguration anpassen 84
Methode 1: Benutzerdefiniertes Bootstrap durch Angabe nur der Schnittstellendetails 85
Benutzerdefiniertes Bootstrap-Beispiel für AWS 85
Benutzerdefiniertes Bootstrap-Beispiel für Azure 85
Benutzerdefinierte Bootstrap-Beispiele für GCP 86
Methode 2: Benutzerdefinierter Bootstrap durch Angabe der Schnittstellen, IP-Adressen und Subnetzmasken 87
Benutzerdefinierte Bootstrap-Beispiele für AWS 87
Benutzerdefiniertes Bootstrap-Beispiel für Azure 87
Beispiel für benutzerdefinierten Bootstrap für GCP 88
Methode 3: Benutzerdefinierter Bootstrap durch Bereitstellung von Bootstrap-bezogenen Befehlen im Abschnitt `<NS-CONFIG>` 88
Beispiel für benutzerdefinierten Bootstrap für AWS 89
Benutzerdefiniertes Bootstrap-Beispiel für Azure 90
Benutzerdefiniertes Bootstrap-Beispiel für GCP 93
Auswirkungen des Anhängens und Entfernens von NICs in AWS und Azure 94
Verbessern der SSL-TPS-Leistung auf öffentlichen Cloud-Plattformen 96
Konfigurieren des PE-Modus über die NetScaler CLI 96
Anwenden der PE-Modus-Konfiguration beim ersten Start der NetScaler Appliance in der Cloud 97
Gleichzeitiges Multithreading für NetScaler VPX in öffentlichen Clouds konfigurieren 98
SMT-Unterstützungsmatrix 99
Einschränkungen 99

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

SMT konfigurieren 100
Fehlerbehebung 101
NetScaler Sanity Checker Tool 103
NetScaler Sanity Checker Tool für AWS 103
Ausführen des Sanity Checker Tools mithilfe der NetScaler CLI 104
Installieren einer NetScaler VPX-Instanz auf einem Bare-Metal-Server 106
Voraussetzungen für die Installation einer NetScaler VPX-Instanz auf Bare-Metal-Servern 106
Installieren der NetScaler VPX-Instanz auf Bare-Metal-Servern 106
Installieren einer NetScaler VPX-Instanz auf Citrix Hypervisor/XenServer 108
Voraussetzungen für die Installation einer NetScaler VPX-Instanz auf dem Hypervisor 108
Hardwareanforderungen für den Hypervisor 108
XenCenter-Systemanforderungen 110
NetScaler VPX-Instanzen auf Hypervisor mit XenCenter installieren 110
Konfigurieren von VPX-Instanzen zur Verwendung von Single Root I/O Virtualization (SR-IOV)-Netzwerkschnittstellen 112
Einschränkungen 112
Einschränkungen für Intel 82599 NIC 112
Einschränkungen für Intel X710 10G und Intel XL710 40G NICs 112
Voraussetzungen für Intel 82599 NIC 113
Zuweisen von Intel 82599 SR-IOV VFs zur NetScaler VPX-Instanz über den Citrix Hypervisor-Host 114
Zuweisung von Intel 82599 SR-IOV VFs zur NetScaler VPX-Instanz über den Citrix Hypervisor-Host aufheben 114
Zuweisen von Intel X710/XL710 SR-IOV VFs zur NetScaler VPX-Instanz mithilfe des Citrix Hypervisor-Hosts 115
Entfernen von Intel X710/XL710 SR-IOV VFs aus der NetScaler-Instanz mithilfe des Citrix Hypervisor-Hosts 117
Link-Aggregation auf der SR-IOV-Schnittstelle konfigurieren 118
VLAN auf der SR-IOV-Schnittstelle konfigurieren 118

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

Weitere Verweise 118
Installieren einer NetScaler VPX-Instanz auf VMware ESX 119
Voraussetzungen 119
Hardwareanforderungen für VMware ESX 120
Systemanforderungen für den VMware vSphere Client 122
Systemanforderungen für OVF Tool 1.0 122
Herunterladen der NetScaler VPX-Setup-Dateien 123
Installieren einer NetScaler VPX-Instanz auf VMware ESX 123
Migrieren einer NetScaler VPX-Instanz mit VMware vMotion 124
Konfigurieren einer NetScaler VPX-Instanz zur Verwendung der VMXNET3-Netzwerkschnittstelle 125
Empfangsringgröße für die VMXNET3-Netzwerkschnittstelle festlegen 129
So legen Sie die Ringgröße auf einer VMXNET3-Netzwerkschnittstelle fest 129
Konfigurieren einer NetScaler VPX-Instanz zur Verwendung der SR-IOV-Netzwerkschnittstelle 129
Einschränkungen 130
Voraussetzung 130
Konfigurieren einer NetScaler VPX auf dem ESX-Hypervisor zur Verwendung von Intel QAT für die SSL-Beschleunigung im SR-IOV-Modus 136
Voraussetzungen 136
Einschränkungen 136
Einrichten der Hostumgebung für die Verwendung von Intel QAT 137
Hinweise 137
QAT-VFs mit dem vSphere Web Client VPX zuweisen 138
Informationen zur Bereitstellung 138
Migration der NetScaler VPX von E1000 auf SR-IOV- oder VMXNET3-Netzwerkschnittstellen 138
Eine NetScaler VPX-Instanz zur Verwendung von PCI-Passthrough-Netzwerkschnittstellen konfigurieren 139
Übersicht 139

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

Voraussetzungen 139

Passthrough-Geräte auf einem Host konfigurieren 139

Konfigurieren von Passthrough-Geräten auf einer NetScaler VPX-Instanz 140

NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance auf dem VMware ESX-Hypervisor anwenden 141

Bereitstellen von Preboot-Benutzerdaten auf dem ESX-Hypervisor 142

Benutzerdaten mithilfe von CD/DVD-ISO bereitstellen 142

Benutzerdaten mithilfe der OVF-Eigenschaft über den ESX-Webclient bereitstellen 145

Benutzerdaten mithilfe der OVF-Eigenschaft über den ESX vSphere Client bereitstellen 148

Installieren einer NetScaler VPX-Instanz in der VMware Cloud auf AWS 152

Voraussetzungen 152

Hardwareanforderungen für VMware Cloud 152

OVF Tool 1.0 Systemanforderungen 153

Herunterladen der NetScaler VPX-Setup-Dateien 154

Installieren einer NetScaler VPX-Instanz in der VMware Cloud 154

Installieren einer NetScaler VPX-Instanz auf einem Microsoft Hyper-V-Server 156

Voraussetzungen für die Installation der NetScaler VPX-Instanz auf Microsoft-Servern 156

Hardwareanforderungen für Microsoft-Server 157

Herunterladen der NetScaler VPX-Setup-Dateien 157

Installieren der NetScaler VPX-Instanz auf Microsoft-Servern 158

Automatische Bereitstellung einer NetScaler VPX-Instanz auf Hyper-V 159

Installieren einer NetScaler VPX-Instanz auf der Linux-KVM-Plattform 164

Einschränkungen und Nutzungsrichtlinien 164

Allgemeine Empfehlungen 164

Einschränkungen 164

Voraussetzungen für die Installation einer NetScaler VPX-Instanz auf der Linux-KVM-Plattform 165

Softwareanforderungen 165

Hardwareanforderungen für Gast-VM 166

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

Netzwerkanforderungen 166
Quellschnittstelle und Modi 166
Eigenschaften der Quellschnittstellen 167
Promiskuitiver Modus 170
Erforderliches Modul 171
Bereitstellen der NetScaler VPX-Instanz mit dem Virtual Machine Manager 171
Voraussetzungen für die automatische Bereitstellung einer NetScaler VPX-Instanz prüfen 172
Bereitstellen der NetScaler VPX-Instanz mithilfe eines RAW-Images 175
Bereitstellen der NetScaler VPX-Instanz mithilfe eines QCOW2-Images 176
Automatische Bereitstellung durch Anschließen eines CD-ROM-Laufwerks aktivieren 177
Weitere Schnittstellen zur NetScaler VPX-Instanz mithilfe des Virtual Machine Managers hinzufügen 177
Konfigurieren einer NetScaler VPX-Instanz zur Verwendung von SR-IOV-Netzwerkschnittstellen 179
Einschränkungen 179
Voraussetzungen 180
Konfigurieren einer NetScaler VPX-Instanz zur Verwendung der SR-IOV-Netzwerkschnittstelle 182
Statische LA/LACP auf der SR-IOV-Schnittstelle konfigurieren 183
VLAN auf der SR-IOV-Schnittstelle konfigurieren 184
Konfigurieren Sie eine NetScaler VPX auf dem KVM-Hypervisor zur Verwendung von Intel QAT für die SSL-Beschleunigung im SR-IOV-Modus 184
Voraussetzungen 185
Einschränkungen 185
Richten Sie die Host-Umgebung für die Verwendung von Intel QAT ein 185
Wichtige Hinweise 187
Zuweisen von QAT-VFs zu NetScaler VPX, das auf dem Linux KVM-Hypervisor bereitgestellt wird 187
Informationen zur Bereitstellung 188

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

Konfigurieren Sie eine NetScaler VPX-Instanz zur Verwendung von PCI-Passthrough-Netzwerkschnittstellen 188

Voraussetzungen 188

NetScaler VPX-Instanz mithilfe des `virsh`-Programms bereitstellen 189

Weitere Schnittstellen zur NetScaler VPX-Instanz mit dem `virsh`-Programm hinzufügen 192

Verwalten der NetScaler VPX Gast-VMs 194

Verwalten der VPX Gast-VMs mithilfe des Virtual Machine Managers 194

Verwalten der NetScaler VPX Gast-VMs mithilfe des `virsh` Programms 196

Konfigurieren einer NetScaler VPX-Instanz auf KVM zur Verwendung von OVS DPDK-basierten Host-Schnittstellen 198

Voraussetzungen 198

DPDK installieren 199

OVS erstellen und installieren 199

Eine OVS-Bridge erstellen 199

Physische Schnittstelle an die OVS-Bridge anbinden 199

`vhost-user`-Ports an den OVS-Datenpfad anbinden 200

Eine KVM-VPX mit OVS-DPDK-basierten `vhost-user`-Ports bereitstellen 201

Hinweise 217

NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance auf dem KVM-Hypervisor anwenden 218

So stellen Sie Preboot-Benutzerdaten auf dem KVM-Hypervisor bereit 220

Benutzerdaten mithilfe einer CD-ROM-ISO-Datei bereitstellen 220

NetScaler VPX auf Red Hat OpenShift Virtualization installieren 223

Systemanforderungen 223

NetScaler VPX-Instanzen auf OpenShift Virtualization installieren 223

Upgrade von NetScaler VPX auf OpenShift Virtualization 229

Nicht unterstützte Funktionen und Einschränkungen 229

Installieren von NetScaler VPX auf dem Nutanix Acropolis Hypervisor 231

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

Systemanforderungen 231
Installieren von NetScaler VPX-Instanzen auf Nutanix AHV mit Prism 232
NetScaler VPX™ auf Nutanix AHV aktualisieren 233
Nicht unterstützte Funktionen und Einschränkungen 234
Migration von Citrix Ready KVM VPX zu offiziell unterstütztem NetScaler VPX™ auf Nutanix AHV 234
Voraussetzung 234
Direktes Upgrade von Citrix Ready KVM VPX auf offiziell unterstütztes NetScaler VPX auf Nutanix AHV 235
Voraussetzungen 235
Wichtige Überlegungen vor dem Upgrade 235
Datensicherung und -erhaltung während des Upgrades 236
Upgrade-Verfahren 237
Validierung nach dem Upgrade 237
Migration mithilfe der Node-by-Node-Hochverfügbarkeits- (HA) Ersatzmethode 238
Wichtige Überlegungen 240
NetScaler VPX™ auf Nutanix Acropolis Hypervisor – FAQs 241
Einschränkungen für NetScaler VPX-Bereitstellungen auf Red Hat OpenShift Virtualization und Nutanix AHV 247
NetScaler VPX auf AWS 249
Erste Schritte 249
Bereitstellen einer NetScaler VPX-Instanz auf AWS 249
Hybride Bereitstellungen 250
Lizenzierung 250
Automatisierung 250
Blogs 250
Videos 250
Kundenreferenzen 251

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

Lösungen 251
Support 251
Weitere Referenzen 251
AWS-Terminologie 252
AWS-VPX Support-Matrix 254
Unterstützte VPX-Angebote auf AWS 254
Unterstützte AWS-Regionen 255
Unterstützte AWS-Instanztypen 255
Unterstützte AWS-Dienste 256
Einschränkungen und Nutzungsrichtlinien 257
Voraussetzungen 259
AWS IAM-Rollen auf NetScaler VPX-Instanz konfigurieren 263
Eine IAM-Rolle erstellen 267
IAM-Richtlinien mit dem IAM-Richtliniensimulator testen 270
Weitere Referenzen 271
Wie eine NetScaler VPX-Instanz auf AWS funktioniert 271
Bereitstellen einer eigenständigen NetScaler VPX-Instanz in AWS 272
Bereitstellen einer NetScaler VPX-Instanz in AWS mithilfe der AWS-Webkonsole 273
Konfigurieren einer NetScaler VPX-Instanz mithilfe der Citrix CloudFormation-Vorlage 277
Konfigurieren einer NetScaler VPX-Instanz mithilfe der AWS CLI 278
Szenario: eigenständige Instanz 278
NetScaler VPX-Lizenz herunterladen 284
So migrieren Sie das AWS-Abonnement zu BYOL 284
Einschränkungen 287
Lastverteilung von Servern in verschiedenen Verfügbarkeitszonen 287
So funktioniert Hochverfügbarkeit auf AWS 288
Hochverfügbarkeit innerhalb derselben Zonen 289
Hochverfügbarkeit über verschiedene Zonen hinweg 290

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

Vor Beginn Ihrer Bereitstellung 291

Fehlerbehebung 291

Bereitstellen eines VPX HA-Paares in derselben AWS-Verfügbarkeitszone 291

So stellen Sie ein VPX HA-Paar in derselben Zone bereit 292

Schritt 1. Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) unter Verwendung desselben VPC, jede mit drei NICs (Ethernet 0, Ethernet 1, Ethernet 2) 292

Schritt 2. Weisen Sie auf dem primären Knoten private IP-Adressen für Ethernet 1 (Client-IP oder VIP) und Ethernet 2 (Back-End-Server-IP oder SNIP) zu 293

Schritt 3. Konfigurieren Sie VIP und SNIP auf dem primären Knoten unter Verwendung sekundärer privater IP-Adressen 294

Schritt 4: HA auf beiden Instanzen konfigurieren 294

Migrieren eines älteren HA-Paares zu einem neuen HA-Paar basierend auf der Migration sekundärer privater IP-Adressen 295

Bereitstellen eines Hochverfügbarkeitspaars mithilfe der Citrix CloudFormation-Vorlage 296

Überwachen Sie Ihre Instanzen mit Amazon CloudWatch 298

Hinweise 298

So zeigen Sie CloudWatch-Metriken an 299

Konfigurieren von SR-IOV in einer Hochverfügbarkeitskonfiguration 299

Verwandte Ressourcen 299

Hochverfügbarkeit über verschiedene AWS-Verfügbarkeitszonen hinweg 300

Hinweise 300

Weitere Referenzen 301

Bereitstellen eines VPX-Hochverfügbarkeitspaares mit elastischen IP-Adressen über verschiedene AWS-Zonen hinweg 301

So funktioniert HA mit EIP-Adressen über verschiedene AWS-Zonen hinweg 301

So stellen Sie ein VPX-Hochverfügbarkeitspaar mit elastischen IP-Adressen über verschiedene AWS-Zonen hinweg bereit 302

Hochverfügbarkeit mithilfe der CLI konfigurieren 302

Hochverfügbarkeit über die GUI konfigurieren 303

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

Szenario 304

Bereitstellen eines VPX-Hochverfügbarkeitspaares mit privaten IP-Adressen über verschiedene AWS-Zonen hinweg 306

Hochverfügbarkeitspaar mit privaten IP-Adressen unter Verwendung einer nicht freigegebenen AWS VPC 306

Voraussetzungen 306

Bereitstellen eines VPX HA-Paares mit privaten IP-Adressen unter Verwendung einer nicht freigegebenen AWS VPC 307

Hochverfügbarkeit mithilfe der CLI konfigurieren 309

Hochverfügbarkeit über die GUI konfigurieren 310

Bereitstellen eines VPX HA-Paares mit privaten IP-Adressen unter Verwendung von AWS Shared VPC 310

Voraussetzungen 311

Kontoübergreifende IAM-Rolle erstellen 313

Cross-Account-IAM-Rolle mithilfe der NetScaler CLI festlegen 313

Cross-Account-IAM-Rolle mithilfe der NetScaler GUI festlegen 313

Szenario 314

AWS Transit Gateway-Konfiguration für HA-Lösung mit privater IP 315

Fehlerbehebung 315

Bereitstellen einer NetScaler VPX-Instanz auf AWS Outposts 316

So funktioniert AWS Outposts 317

Voraussetzung 317

Bereitstellen einer NetScaler VPX-Instanz auf AWS Outposts mithilfe der AWS-Webkonsole 317

Bereitstellen einer NetScaler VPX-Instanz in einer Hybrid Cloud mit AWS Outposts 318

Referenzen 319

AWS API Gateway mithilfe der NetScaler Web App Firewall schützen 319

NetScaler Appliance vor dem AWS API Gateway bereitstellen 320

NetScaler Appliance mit aktiviertem WAF konfigurieren 320

NetScaler-Funktionen und -Möglichkeiten 322

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

Back-End-AWS-Autoscaling-Dienst hinzufügen 323
Bevor Sie beginnen 325
Den AWS Autoscaling-Dienst zu einer NetScaler VPX-Instanz hinzufügen 327
NetScaler GSLB auf AWS bereitstellen 328
DBS-Übersicht 329
DBS mit ELB 329
AWS-Komponenten konfigurieren 329
Sicherheitsgruppen 329
Konfigurieren von Domainnamen-basierten Diensten für den globalen Server-Lastausgleich 331
Bereitstellungstypen 331
CFT-Bereitstellung 332
Bereitstellungsschritte 332
NetScaler Global Server Load Balancing für Hybrid- und Multi-Cloud-Bereitstellungen 333
Konfiguration der Sicherheitsgruppen 335
Funktionen der hybriden und Multi-Cloud-GSLB-Lösung von NetScaler 335
Kompatibilität mit anderen Lastenausgleichslösungen 335
GSLB-Methoden 336
GSLB-Topologien 336
IPv6-Unterstützung 337
Überwachung 337
Persistenz 337
Konfiguration mithilfe von NetScaler ADM StyleBooks 338
Workflow der NetScaler Hybrid- und Multi-Cloud-GSLB-Lösungskonfiguration 338
Verwenden von StyleBooks zur Konfiguration von GSLB auf NetScaler-Lastverteilungsknoten 340
Konfigurieren einer untergeordneten Site in einer Parent-Child-Topologie mithilfe des Multi-Cloud-GSLB-StyleBooks für LB-Knoten 341
Bereitstellung der CloudFormation-Vorlage 343

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

CFT-Bereitstellung mit drei NICs 343

**Notfallwiederherstellung (DR)** 345

Weitere Ressourcen 345

Bereitstellen von NetScaler Web App Firewall auf AWS 346

Architektur für NetScaler Web App Firewall auf AWS für die Produktionsbereitstellung 346

Kosten und Lizenzierung 347

Bereitstellungsoptionen 349

AWS Quick Start 349

Schritt 1: Beim AWS-Benutzerkonto anmelden 349

Schritt 2: NetScaler Web App Firewall AMI abonnieren 350

Schritt 3: AWS Quick Start starten 351

Parameter zur Bereitstellung von NetScaler Web App Firewall in einem neuen VPC 353

Schritt 4: Bereitstellung testen 363

Verbindung zu NetScaler Web App Firewall HA-Paar mithilfe eines Bastion-Hosts herstellen 364

NetScaler Console 365

Bereitstellen von NetScaler VPX-Instanzen auf AWS mit NetScaler Console 365

NetScaler Web App Firewall und OWASP Top 10 – 2017 365

NetScaler Web App Firewall 367

Web App Firewall Bereitstellungsstrategie 367

NetScaler-Konsole 368

NetScaler Console Anwendungsanalyse- und Verwaltungsfunktionen 368

Voraussetzungen 368

Einschränkungen und Nutzungsrichtlinien 368

Technische Anforderungen 369

Ressourcen 369

Regionen 370

Schlüsselpaar 370

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

Referenzen 370
NetScaler VPX-Instanz zur Verwendung der SR-IOV-Netzwerkschnittstelle konfigurieren 371
Schnittstellentyp in SR-IOV ändern 371
So ändern Sie den Schnittstellentyp in SR-IOV 372
SR-IOV in einem Hochverfügbarkeits-Setup konfigurieren 372
Konfigurieren einer NetScaler VPX-Instanz zur Verwendung von Enhanced Networking mit AWS ENA 373
Eine NetScaler VPX-Instanz auf AWS aktualisieren 374
Change the EC2 instance type of a NetScaler VPX instance on AWS 374
Aktualisieren des Durchsatzes oder der Software-Edition einer NetScaler VPX-Instanz auf AWS 375
Verwenden einer Kundenlizenz (Bring-Your-Own-License) 375
Verwenden einer Utility-Lizenz (Utility-Lizenz mit stündlicher Gebühr) 375
Aktualisieren der Systemsoftware einer NetScaler VPX-Instanz auf AWS 375
Upgrade auf eine neue NetScaler AMI-Instanz mithilfe einer NetScaler Hochverfügbarkeitskonfiguration 376
Voraussetzungen und zu berücksichtigende Punkte 376
Fehlerbehebung bei einer VPX-Instanz auf AWS 380
AWS FAQs 381
Bereitstellen einer NetScaler VPX-Instanz in Microsoft Azure 385
Voraussetzung 385
So funktioniert eine NetScaler VPX-Instanz in Azure 386
Multi-NIC-Multi-IP-Architektur 386
Einzel-NIC-Multi-IP-Architektur 387
Einzel-NIC-Einzel-IP 387
NetScaler VPX-Lizenzierung 387
VPX-Leistung und empfohlene Azure-Instanztypen 388
Wichtige Hinweise 389

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

IPv6-Unterstützung für NetScaler VPX-Instanz in Azure 389
Einschränkungen 390
Azure-Terminologie 390
Netzwerkarchitektur für NetScaler VPX-Instanzen auf Microsoft Azure 393
Datenfluss durch Netzwerkadressübersetzung 394
Richtlinien zur Portnutzung 395
Eine NetScaler VPX Standalone-Instanz konfigurieren 396
Bevor Sie beginnen 396
Zusammenfassung der Konfigurationsschritte 397
Ressourcengruppe konfigurieren 397
Netzwerksicherheitsgruppe konfigurieren 397
Ein virtuelles Netzwerk und Subnetze konfigurieren 398
Zweites Subnetz konfigurieren 399
Speicherkonto konfigurieren 399
Eine Verfügbarkeitsgruppe konfigurieren 400
Eine NetScaler VPX-Instanz konfigurieren 400
Mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz konfigurieren 403
Anwendungsfall 403
Bevor Sie beginnen 404
Schritt 2: NetScaler-eigene IP-Adressen konfigurieren 406
Konfigurieren einer Hochverfügbarkeits-Einrichtung mit mehreren IP-Adressen und NICs 406
Hochverfügbarkeit unter Verwendung eines Availability Sets 407
HA-INC-Knoten mithilfe der NetScaler®-Hochverfügbarkeitsvorlage konfigurieren 408
Hochverfügbarkeit mithilfe von Verfügbarkeitszonen 410
Überwachen Sie Ihre Instanzen mithilfe von Metriken in Azure Monitor 411
Hinweise 411
So zeigen Sie Metriken in Azure Monitor an 412

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

Konfigurieren Sie ein Hochverfügbarkeits-Setup mit mehreren IP-Adressen und NICs mithilfe von PowerShell-Befehlen 412

HA-INC-Knoten mithilfe von PowerShell-Befehlen konfigurieren 414

Szenario: HA-INC PowerShell-Bereitstellung 414

Parametereinstellungen 414

Bereitstellen eines NetScaler-Hochverfügbarkeitspaars auf Azure mit ALB im Floating-IP-deaktivierten Modus 432

HA-Bereitstellungsarchitektur mit ALB im Floating-IP-deaktivierten Modus 433

Voraussetzungen 433

Bereitstellen eines VPX HA-Paares in Azure mit deaktivierter ALB Floating IP 433

Bereitstellen eines NetScaler® für eine private Azure DNS-Zone 441

Übersicht über Azure DNS 441

Warum NetScaler GSLB für private Azure DNS-Zonen? 442

Anwendungsfall 442

Lösung des Anwendungsfalls 442

Topologie 443

Konfigurieren von NetScaler für eine private Azure DNS-Zone 443

Voraussetzungen 443

Lösungsbeschreibung 444

Azure- und lokale Einrichtung konfigurieren 444

Private Azure DNS-Zone 444

Virtuelle Azure-Netzwerke (VNet A, VNet B) im Hub-and-Spoke-Modell 445

VNet A-zu-VNet B-Peering 445

VNet B-zu-VNet A-Peering 445

Bereitstellen von App-Server, DNS-Forwarder, Windows 10 Pro-Client, NetScaler in VNet A 446

App-Server und DNS-Forwarder bereitstellen, wenn sich Clients in VNet B befinden 448

App-Server, DNS-Forwarder und Windows 10 Pro-Client lokal bereitstellen 448

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

NetScaler im virtuellen Azure-Netzwerk konfigurieren 449
NetScaler GSLB konfigurieren 449
ADNS-Dienst hinzufügen 449
GSLB-Sites hinzufügen 449
GSLB-Dienste hinzufügen 450
Virtuellen GSLB-Server hinzufügen 450
Konfigurieren einer NetScaler VPX-Instanz für Azure Accelerated Networking 451
Voraussetzungen 452
Einschränkungen 452
Für beschleunigtes Netzwerk unterstützte NICs 452
So aktivieren Sie beschleunigtes Netzwerk auf einer NetScaler VPX-Instanz über die Azure-Konsole 453
Beschleunigtes Netzwerk mit Azure PowerShell aktivieren 454
So überprüfen Sie Accelerated Networking auf einer Schnittstelle mithilfe der FreeBSD-Shell von NetScaler 455
So überprüfen Sie die beschleunigte Netzwerkanbindung auf einer Schnittstelle mithilfe der ADC-CLI 456
Wichtige Hinweise in NetScaler 457
Ein VLAN für eine PV-Schnittstelle konfigurieren 457
HA-INC-Knoten mithilfe der NetScaler® Hochverfügbarkeitsvorlage mit Azure ILB konfigurieren 459
Beispielkonfiguration 462
HA-INC-Knoten mithilfe der NetScaler® Hochverfügbarkeitsvorlage für internetorientierte Anwendungen konfigurieren 463
Beispielkonfiguration 466
Konfigurieren eines Hochverfügbarkeits-Setups mit externen und internen Azure Load Balancern gleichzeitig 467
Bereitstellen eines NetScaler VPX HA-Paars in Azure unter Verwendung der sekundären IP-Konfigurationen 470

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

Voraussetzungen für die Bereitstellung eines NetScaler VPX™ HA-Paars unter Verwendung von Azure sekundären IP-Konfigurationen 471

Bereitstellen eines NetScaler VPX HA-Paares mithilfe sekundärer Azure IP-Konfigurationen 471

Bereitstellen eines NetScaler VPX HA-Paares in Azure mithilfe von Lösungsvorlagen 475

Hauptmerkmale der NetScaler VPX Azure-Lösungsbereitstellung 476

Voraussetzungen 476

Marketplace-Angebotsinformationen (Eigene Lizenz mitbringen – BYOL) 476

Bereitstellen eines NetScaler VPX HA-Paares in Azure mithilfe von Lösungsvorlagen 477

Installieren einer NetScaler VPX-Instanz in Azure VMware Solution 479

Voraussetzungen 480

VMware Cloud-Hardwareanforderungen 481

OVF Tool 1.0 Systemanforderungen 481

Herunterladen der NetScaler VPX-Setup-Dateien 482

Azure VMware Solution bereitstellen 483

Verbinden mit einer virtuellen Azure-Maschine unter Windows 484

Zugriff auf Ihr Private Cloud vCenter-Portal 484

Ein NSX-T-Segment im Azure-Portal erstellen 485

Installieren einer NetScaler VPX-Instanz in der VMware Cloud 486

NetScaler VPX-Standalone-Instanz in Azure VMware Solution konfigurieren 487

Voraussetzungen 487

Konfigurieren einer NetScaler VPX-Standalone-Instanz in AVS mithilfe des NetScaler Load Balancers 488

NetScaler VPX Standalone-Instanz auf AVS mit dem Azure Load Balancer konfigurieren 489

Konfigurieren einer NetScaler VPX Hochverfügbarkeits-Einrichtung in der Azure VMware Solution 490

Voraussetzungen 490

Konfigurationsschritte 491

Azure Route Server mit NetScaler VPX HA-Paar konfigurieren 491

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

Voraussetzungen 492
So konfigurieren Sie einen Azure Route Server mit einem NetScaler VPX HA-Paar 493
Back-End Azure Autoscaling-Dienst hinzufügen 496
Bevor Sie beginnen 496
Konfigurieren einer verwalteten Identität auf einer virtuellen Maschine 498
VMSS zu einer NetScaler VPX-Instanz hinzufügen 499
Hinweise zur Erstellung eines Cloud-Profils 500
Migration von nicht verwalteten Datenträgern zu verwalteten Datenträgern in Azure 500
Referenzen 501
Azure-Tags für die NetScaler VPX-Bereitstellung 501
Wie Azure-Tags für die VPX-Bereitstellung funktionieren 501
Bevor Sie beginnen 501
So fügen Sie Azure-Tag-Einstellungen über die VPX-GUI hinzu 502
So fügen Sie Azure-Tag-Einstellungen mithilfe der VPX-CLI hinzu 503
Fehlerbehebung 504
GSLB auf NetScaler VPX-Instanzen konfigurieren 505
Szenario 506
Parameter 506
Eine VM erstellen 509
Ressourcengruppe erstellen 510
Speicherkonto erstellen 510
Verfügbarkeitsgruppe erstellen 510
Virtuelles Netzwerk erstellen 510
Öffentliche IP-Adresse erstellen 511
NICs erstellen 511
VM-Konfigurationsobjekt erstellen 512
Anmeldeinformationen abrufen und Betriebssystemeigenschaften festlegen 512
NICs hinzufügen 512

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

Betriebssystemdatenträger angeben und VM erstellen 513
Details zur IP-Konfiguration 513
GSLB-Sites und andere Einstellungen konfigurieren 515
Notfallwiederherstellung 516
Multi-NIC Multi-IP (Drei-NIC)-Bereitstellung für die Notfallwiederherstellung 517
Single-NIC Multi-IP (Ein-NIC)-Bereitstellung für die Notfallwiederherstellung 517
GSLB in einer Aktiv-Standby-Hochverfügbarkeitskonfiguration konfigurieren 517
Szenario 518
Parametereinstellungen 519
ALB mit der Frontend-IP-Adresse und Regeln konfigurieren, um GSLB- und DNS-Traffic zuzulassen 520
GSLB auf jedem Hochverfügbarkeitspaar aktivieren 521
NetScaler GSLB in Azure bereitstellen 523
DBS-Übersicht 523
Domänennamenbasierte Dienste mit Azure Load Balancer (ALB) 523
Azure GSLB-Voraussetzungen 524
Azure-Komponenten konfigurieren 524
NetScaler GSLB-domänenbasierten Dienst konfigurieren 525
Konfigurationen für die Datenverkehrsverwaltung 525
GSLB-Konfigurationen 525
Weitere Ressourcen 528
Eine NetScaler VPX-Instanz auf Azure Local bereitstellen 528
Voraussetzungen für die Bereitstellung einer NetScaler VPX-Instanz auf Azure Local 528
Eine NetScaler VPX-Instanz auf Azure Local mithilfe eines VM-Dateipakets aus dem Windows Admin Center bereitstellen 528
Bereitstellen einer NetScaler VPX-Instanz auf Azure Local mithilfe von VHD aus dem Windows Admin Center 530
Bereitstellen von NetScaler® Web App Firewall in Azure 532

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

NetScaler Web App Firewall Bereitstellungsstrategie 533
Konfigurieren der Web Application Firewall 534
SQL-Injection 535
Cross-Site-Scripting 535
Pufferüberlaufprüfung 535
Virtuelles Patching/Signaturen 535
Anwendungssicherheitsanalyse 536
Zentralisiertes Lernen auf ADM 536
StyleBooks 538
Security Insight-Analysen 538
Detaillierte Informationen zu Sicherheitsverletzungen abrufen 538
Details der Protokollausdrücke anzeigen 539
Sicherheitsverletzungen 540
Details zu Anwendungssicherheitsverletzungen anzeigen 540
Verletzungskategorien 541
Einrichtung 541
Erweiterte Sicherheitsanalysen aktivieren 541
Webtransaktionseinstellungen aktivieren 542
Dashboard für Sicherheitsverletzungen 542
Bot-Einblicke 542
Bots anzeigen 542
CAPTCHA-Bots anzeigen 544
Bot-Fallen anzeigen 544
Bot-Details anzeigen 544
Erweiterte Suche 545
**Ungewöhnlich hohe Anfragerate** 546
Bot-Erkennung 546
IP-Reputation 547

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

NetScaler Web App Firewall und OWASP Top Ten–2021 547
A1:2021 Fehlerhafte Zugriffskontrolle 548
NetScaler Web App Firewall-Schutzfunktionen 548
A2:2021 – Kryptografische Fehler 549
NetScaler Web App Firewall-Schutzfunktionen 549
A3:2021 – Injection 549
NetScaler Web App Firewall-Schutzfunktionen 550
A5:2021 – Sicherheitsfehlkonfiguration 551
NetScaler Web App Firewall-Schutzfunktionen 551
A6:2021 – Anfällige und veraltete Komponenten 552
NetScaler Web App Firewall Schutzmaßnahmen 552
A7:2021 – Fehlerhafte Authentifizierung 552
NetScaler Web App Firewall-Schutzmaßnahmen 552
A8:2021 – Fehler bei der Software- und Datenintegrität 553
NetScaler Web App Firewall-Schutzmaßnahmen 553
A9:2021 – Fehler bei der Sicherheits-Protokollierung und -Überwachung 553
NetScaler Web App Firewall-Schutzmaßnahmen 553
Referenzen 553
Intranet-IP-Adresspools für eine NetScaler Gateway Appliance konfigurieren 554
Eine private IP-Adresse im Azure-Portal registrieren 555
Adresspools in der NetScaler Gateway Appliance konfigurieren 555
Konfigurieren Sie mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz mithilfe von PowerShell-Befehlen 556
Anwendungsfall 556
Skript 558
Parameter 558
1. Ressourcengruppe erstellen 560
2. Speicherkonto erstellen 561

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

3. Verfügbarkeitsgruppe erstellen 561
4. Netzwerksicherheitsgruppe erstellen 561
5. Virtuelles Netzwerk erstellen 561
6. Öffentliche IP-Adresse erstellen 562
7. IP-Konfiguration zuweisen 562
8. NIC erstellen 563
9. NetScaler VPX-Instanz erstellen 563
10. NIC-Konfigurationen überprüfen 564
11. VPX-seitige Konfigurationen überprüfen 564
Zusätzliche PowerShell-Skripte für die Azure-Bereitstellung 564
Bereitstellen einer NetScaler VPX Standalone-Instanz 565
Bereitstellen eines NetScaler VPX-Paares in einer Hochverfügbarkeitskonfiguration mit einem externen Azure Load Balancer 571
Bereitstellen eines NetScaler VPX-Paares in einer Hochverfügbarkeitskonfiguration mit Azure Internal Load Balancer 581
Ein Support-Ticket für die VPX-Instanz in Azure erstellen 589
Azure-FAQs 590
Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform 591
Unterstützte GCP-Maschinentypfamilien 591
Unterstützte Funktionen 591
Einschränkung 592
Hardware-Anforderungen 592
Hinweise 592
Szenario: Bereitstellen einer Multi-NIC-, Multi-IP-Standalone-NetScaler-VPX-Instanz 592
Zusammenfassung der Bereitstellungsschritte 593
Szenario: Bereitstellen einer eigenständigen VPX-Instanz mit einer einzelnen NIC 594
Zusammenfassung der Bereitstellungsschritte 595
Hinweise nach der Bereitstellung der VPX-Instanz auf GCP 598

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

NetScaler VPX-Lizenzierung 599
Unterstützte NetScaler VPX-Angebote auf GCP 599
GDM-Vorlagen zur Bereitstellung einer NetScaler VPX-Instanz 599
Ressourcen 600
Zugehörige Informationen 600
Bereitstellen eines VPX-Hochverfügbarkeitspaares auf der Google Cloud Platform 600
GDM-Vorlagen zur Bereitstellung eines VPX-Hochverfügbarkeitspaares auf GCP 601
Unterstützung von Weiterleitungsregeln für ein VPX-Hochverfügbarkeitspaar auf GCP 601
Voraussetzungen 601
Einschränkungen 601
Bereitstellen eines VPX-Hochverfügbarkeitspaares mit externer statischer IP-Adresse auf der Google Cloud Platform 601
Bevor Sie beginnen 602
So stellen Sie ein VPX-HA-Paar auf der Google Cloud Platform bereit 603
Schritt 1. VPC-Netzwerke erstellen 604
Schritt 2. Zwei VPX-Instanzen erstellen 604
Schritt 3. Hochverfügbarkeit konfigurieren 604
Bereitstellen eines VPX-Hochverfügbarkeitspaares mit einer einzelnen NIC und privater IP-Adresse auf der Google Cloud Platform 611
Bevor Sie beginnen 611
So stellen Sie ein VPX-Hochverfügbarkeitspaar auf der Google Cloud Platform bereit 613
Schritt 1. Ein VPC-Netzwerk erstellen 613
Schritt 2. Zwei VPX-Instanzen erstellen 613
Schritt 3. Hochverfügbarkeit konfigurieren 614
Hochverfügbarkeit über die GUI konfigurieren 614
Hochverfügbarkeit mit der CLI konfigurieren 617
Bereitstellen eines VPX-Hochverfügbarkeitspaares mit privater IP-Adresse auf Google Cloud Platform 619

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

Bevor Sie beginnen 619
So stellen Sie ein VPX-Hochverfügbarkeitspaar auf Google Cloud Platform bereit 621
Schritt 1. VPC-Netzwerke erstellen 621
Schritt 2. Zwei VPX-Instanzen erstellen 621
Schritt 3. Hochverfügbarkeit konfigurieren 622
Hochverfügbarkeit über die GUI konfigurieren 622
Hochverfügbarkeit mithilfe der CLI konfigurieren 625
Installieren einer NetScaler VPX-Instanz auf Google Cloud VMware Engine 627
Voraussetzungen 628
Hardwareanforderungen für VMware Cloud 628
OVF Tool 1.0 Systemanforderungen 629
Herunterladen der NetScaler VPX-Setup-Dateien 630
Google Cloud VMware Engine bereitstellen 630
Zugriff auf Ihr Private Cloud vCenter-Portal 631
Ein NSX-T-Segment im GCVE NSX-T-Portal erstellen 631
Installieren einer NetScaler VPX-Instanz in der VMware Cloud 633
Einer NetScaler VPX-Instanz in der VMware Cloud eine öffentliche IP-Adresse zuweisen 635
Backend-GCP-Autoscaling-Dienst hinzufügen 636
Bevor Sie beginnen 636
Hinzufügen des GCP-Autoskalierungsdienstes zu einer NetScaler VPX-Instanz 638
VIP-Skalierungsunterstützung für NetScaler VPX-Instanz auf GCP 639
Hinweise 640
Bevor Sie beginnen 641
Konfigurieren externer IP-Adressen für die VIP-Skalierung auf der NetScaler VPX-Instanz 643
Einrichten eines virtuellen Lastausgleichsservers mit externer IP-Adresse auf einer NetScaler VPX-Instanz 645
Fehlerbehebung bei einer VPX-Instanz auf GCP 646
Jumbo-Frames auf NetScaler VPX-Instanzen 647

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

Jumbo-Frames für eine VPX-Instanz konfigurieren, die auf VMware ESX ausgeführt wird 648
Jumbo-Frames für eine auf einem Linux-KVM-Server ausgeführte VPX-Instanz konfigurieren 648
Jumbo-Frames für eine auf Citrix XenServer ausgeführte VPX-Instanz konfigurieren 648
Jumbo-Frames für eine auf AWS ausgeführte VPX-Instanz konfigurieren 649
FAQs 650
Funktionen und Funktionalität 650
Was ist NetScaler VPX? 650
Umfasst NetScaler VPX alle Funktionen zur Webanwendungsoptimierung wie ADC-Appliances? 650
Gibt es Einschränkungen bei der Citrix Application Firewall, wenn sie auf NetScaler VPX verwendet wird? 650
Gibt es Unterschiede zwischen NetScaler Gateway auf NetScaler VPX und NetScaler Gateway auf NetScaler Appliances? 651
Abgesehen vom offensichtlichen Unterschied, dass NetScaler VPX auf einem Hypervisor laufen kann, wie unterscheidet es sich von physischen NetScaler Appliances? 651
Welche Rolle spielt NetScaler VPX auf dem Markt für Anwendungsbereitstellung? 651
Wie passt NetScaler VPX in unsere Citrix Delivery Center-Strategie? 652
Verschlüsselung 652
Unterstützt NetScaler VPX SSL-Offload? 652
Beschleunigen SSL-Karten von Drittanbietern, die auf dem Server installiert sind, der NetScaler VPX hostet, die SSL-Verschlüsselung oder -Entschlüsselung? 652
Unterstützt NetScaler VPX die gleichen Verschlüsselungs-Ciphers wie physische NetScaler Appliances? 653
Wie hoch ist der SSL-Transaktionsdurchsatz von NetScaler VPX? 653
Preise und Pakete 653
Wie wird NetScaler VPX verpackt? 653
Ist NetScaler VPX für alle Hypervisoren gleich bepreist? 653
Werden dieselben NetScaler SKUs für VPX auf allen Hypervisoren verwendet? 653

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

Kann eine NetScaler VPX-Lizenz von einem Hypervisor auf einen anderen verschoben werden (z. B. von VMware zu Hyper-V)? 653

Können NetScaler VPX-Instanzen aktualisiert werden? 653

Wenn ich NetScaler VPX in einem Hochverfügbarkeitspaar bereitstellen möchte, wie viele Lizenzen benötige ich? 654

NetScaler® VPX Express und 90-Tage-Testversion 654

Umfasst NetScaler VPX Express alle NetScaler-Standardfunktionen? Umfasst es NetScaler Gateway und Lastausgleich für Citrix Virtual Apps (ehemals XenApp) Web Interface und XML-Broker? 654

Benötigt NetScaler VPX Express eine Lizenz? 654

Läuft die NetScaler VPX Express-Lizenz ab? 654

Unterstützt NetScaler VPX Express dieselben Verschlüsselungs-Ciphers wie NetScaler MPX-Appliances? 654

Kann ich technische Supportfälle für NetScaler VPX Express einreichen? 655

Kann NetScaler VPX Express auf eine Einzelhandelsversion aktualisiert werden? 655

Hypervisor 655

Welche VMware-Versionen unterstützt NetScaler VPX? 655

Wie viele virtuelle Netzwerkschnittstellen können Sie einem VPX in VMware zuweisen? 655

Wie können wir über vSphere auf die NetScaler VPX-Befehlszeile zugreifen? 655

Wie können Sie auf die NetScaler VPX-GUI zugreifen? 655

Können zwei NetScaler VPX-Instanzen, die auf demselben VMware ESX installiert sind, in einer Hochverfügbarkeitskonfiguration eingerichtet werden? 656

Können zwei NetScaler VPX-Instanzen, die auf zwei verschiedenen VMware ESX-Systemen ausgeführt werden, in einer Hochverfügbarkeitskonfiguration eingerichtet werden? 656

Werden für VMware schnittstellenbezogene Ereignisse auf NetScaler VPX unterstützt? 656

Werden für VMware getaggte VLANs auf NetScaler VPX unterstützt? 656

Werden für VMware Link-Aggregation und LACP auf NetScaler VPX unterstützt? 656

Wie greifen wir auf die NetScaler VPX-Dokumentation zu? 656

Kapazitätsplanung oder Dimensionierung 656

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

Welche Leistung kann ich von NetScaler VPX erwarten? 656

Angesichts der Tatsache, dass die CPU-Leistung des Servers variiert, wie können wir die maximale Leistung einer NetScaler-Instanz abschätzen? 657

Gelten die Bandbreiten- oder Durchsatzgrenzen von NetScaler VPX nur für eingehenden Datenverkehr oder für eingehenden und ausgehenden Datenverkehr? 657

Können mehrere Instanzen von NetScaler VPX auf demselben Server ausgeführt werden? 657

Wenn mehr als eine Instanz von NetScaler VPX auf einem physischen Server ausgeführt wird, wie lauten die Mindestanforderungen an die Hardware pro NetScaler VPX-Instanz? 657

Kann ich NetScaler VPX und andere Anwendungen auf demselben Server hosten? 658

Erhöht das Hinzufügen von CPU-Kernen zu einer einzelnen NetScaler VPX-Instanz die Leistung dieser Instanz? 658

Warum scheint NetScaler VPX mehr als 90 % der CPU zu verbrauchen, obwohl es im Leerlauf ist? 658

Systemanforderungen 659

Was sind die Mindestanforderungen an die Hardware für NetScaler VPX? 659

Was ist Intel VT-x? 660

Wie verbreitet ist VT-x? 660

Gibt es eine Hardware-Kompatibilitätsliste (HCL) für NetScaler VPX? 660

Auf welcher Version von NetScaler OS basiert NetScaler VPX? 660

Da NetScaler VPX auf BSD läuft, kann es nativ auf einem Server mit installiertem BSD Unix ausgeführt werden? 661

Weitere technische FAQs 661

Funktioniert Link-Aggregation auf einem physischen Server mit mehreren NICs? 661

Wird MAC-basiertes Forwarding (MBF) auf VPX unterstützt? Gibt es Änderungen gegenüber der Implementierung der NetScaler Appliance? 661

Wie wird der NetScaler VPX Upgrade-Prozess durchgeführt? 661

Wie werden Flash- und Festplattenspeicher zugewiesen? Können wir das ändern? 661

Können wir eine neue Festplatte hinzufügen, um den Speicherplatz auf der NetScaler VPX-Instanz zu erhöhen? 662

Kann ich die Größe der primären Festplatte auf NetScaler VPX erhöhen? 663

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

Wie erhöhe ich manuell die Größe der primären Festplatte auf NetScaler VPX? 663

Was ist hinsichtlich der NetScaler VPX Build-Nummerierung und der Interoperabilität mit anderen Builds zu erwarten? 664

Kann der NetScaler VPX Teil eines Hochverfügbarkeits-Setups mit einer NetScaler Appliance sein? 664

Sind alle in NetScaler VPX sichtbaren Schnittstellen direkt mit der Anzahl der Schnittstellen auf dem Hypervisor verbunden? 664

Warum wird eine paravirtuelle (PV) Schnittstelle auf NetScaler VPX als 1G-Schnittstelle (`1/x`) angezeigt, obwohl die zugrunde liegende physische Schnittstelle 10G ist? Bedeutet dies, dass der maximale Durchsatz auf 1 Gbit/s begrenzt ist? 665

Können Citrix Hypervisor XenMotion oder VMware vMotion oder Hyper-V Live-Migration verwendet werden, um aktive Instanzen von NetScaler VPX zu verschieben? 665

_fix_ 666

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

# NetScaler VPX Support-Matrix

Dieses Dokument listet die verschiedenen Hypervisoren und Funktionen auf, die sowohl auf NetScaler VPX- als auch auf VPX FIPS-Instanzen unterstützt werden, es sei denn, ein bestimmter Hypervisor wird ausdrücklich als auf VPX FIPS nicht unterstützt angegeben. Das Dokument beschreibt auch deren Nutzungsrichtlinien und bekannte Einschränkungen.

## VPX-Instanz auf VMware ESX Hypervisor

| ESXI-VERSION | ESXI VERÖFFENTLICHUNGSDATUM (JJJJ/MM/TT) | ESXI BUILD-NUMMER | NETSCALER VPX-VERSION | LEISTUNGSBEREICH |
|---|---|---|---|---|
| ESXi 9.0.2 | 2026/01/20 | 25148076 | 14.1-66.x und höhere Builds | 10 Mbit/s bis 100 Gbit/s |
| ESXi 8.0 Update 3k | 2026/07/29 | 25595708 | 14.1-73.x und höhere Builds | |
| ESXi 8.0 Update 3j | 2026/05/27 | 25429389 | 14.1-72.x und höhere Builds | |
| ESXi 8.0 Update 3g | 2025/07/29 | 24859861 | 14.1-47.x und höhere Builds | |
| ESXi 8.0 Update 3f | 2025/07/15 | 24784735 | 14.1-47.x und höhere Builds | |
| ESXi 8.0 Update 3e | 2025/04/10 | 24674464 | 14.1-43.x und höhere Builds | |
| ESXi 8.0 Update 3d | 2025/03/04 | 24585383 | 14.1-38.x und höhere Builds | |
| ESXi 8.0 Update 3c | 2025/01/23 | 24414501 | 14.1-29.x und höhere Builds | |

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

| ESXI-VERSION | ESXI VERÖFFENTLICHUNGSDATUM (JJJJ/MM/TT) | ESXI BUILD-NUMMER | NETSCALER VPX-VERSION | LEISTUNGSBEREICH |
|---|---|---|---|---|
| ESXi 8.0 Update 3b | 2024/09/17 | 24280767 | 14.1-21.x und höhere Builds | |
| ESXi 8.0 Update 3 | 2024/06/25 | 24022510 | 14.1-21.x und höhere Builds | |
| ESXi 8.0 Update 2c | 2024/05/21 | 23825572 | 14.1-21.x und höhere Builds | |
| ESXi 8.0 Update 2b | 2024/02/29 | 23305546 | 14.1-17.x und höhere Builds | |
| ESXi 8.0 Update 2 | 2023/09/21 | 22380479 | 14.1-17.x und höhere Builds | |
| ESXi 8.0 Update 1 | 2023/04/18 | 21495797 | 14.1-4.x und höhere Builds | |
| ESXi 8.0c | 2023/03/30 | 21493926 | 14.1-4.x und höhere Builds | |
| ESXi 8.0 | 2022/10/11 | 20513097 | 14.1-4.x und höhere Builds | |
| ESXi 7.0 Update 3w | 2025/07/15 | 24784741 | 14.1-47.x und höhere Builds | |
| ESXi 7.0 Update 3s | 2025/03/04 | 24585291 | 14.1-29.x und höhere Builds | |
| ESXi 7.0 Update 3r | 2024/12/12 | 24411414 | 14.1-29.x und höhere Builds | |
| ESXi 7.0 Update 3q | 2024/05/21 | 23794027 | 14.1-21.x und höhere Builds | |
| ESXi 7.0 Update 3p | 2024/04/11 | 23307199 | 14.1-17.x und höhere Builds | |

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

| ESXI-VERSION | ESXI VERÖFFENTLICHUNGSDATUM (JJJJ/MM/TT) | ESXI BUILD-NUMMER | NETSCALER VPX-VERSION | LEISTUNGSBEREICH |
|---|---|---|---|---|
| ESXi 7.0 Update 3o | 2023/09/28 | 22348816 | 14.1-12.x und höhere Builds | |
| ESXi 7.0 Update 3n | 2023/07/06 | 21930508 | 14.1-8.x und höhere Builds | |
| ESXi 7.0 Update 3m | 2023/05/03 | 21686933 | 14.1-4.x und höhere Builds | |

**HINWEIS:**

Die Unterstützung jedes ESXi-Patches wird für die in der vorhergehenden Tabelle angegebene NetScaler VPX-Version validiert und gilt für alle höheren Builds der NetScaler VPX 14.1-Version.

Weitere Informationen zu den Nutzungsrichtlinien finden Sie unter Nutzungsrichtlinien für VMware ESXi-Hypervisor.

## VPX-Instanz auf XenServer oder Citrix Hypervisor™

| XENSERVER- ODER CITRIX HYPERVISOR-VERSION | SYSID | LEISTUNGSBEREICH |
|---|---|---|
| 8.4, unterstützt ab NetScaler VPX Version 14.1 Build 17.x | 450000 | 10 Mbit/s bis 40 Gbit/s |
| 8.2, unterstützt ab NetScaler VPX Version 13.0 Build 64.x | | |
| 8.0, 7.6, 7.1 | | |

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

## VPX-Instanz auf Microsoft Hyper-V

| HYPER-V-VERSION | SYSID | NETSCALER VPX-VERSION | LEISTUNGSBEREICH |
|---|---|---|---|
| 2016, 2019 | 450020 | ab 14.1-4.x | 10 Mbit/s bis 3 Gbit/s |
| 2022 | | ab 14.1-47.x | |
| 2025 | | ab 14.1-51.x | |

## VPX-Instanz auf Azure Local

| KOMPONENTE | UNTERSTÜTZTE VERSIONEN / BUILDS | SYSID |
|---|---|---|
| NetScaler VPX | 14.1-60.x und höher | 450020 |
| Azure Lokaler OS Build | 25398.1965, 26100.7171 und 20349.3692 | |

Weitere Informationen zu Azure Local Release-Versionen finden Sie in der Microsoft-Dokumentation.

## VPX-Instanz auf Red Hat® OpenShift® Virtualization (RHOCPV)

| RHOCPV-VERSION | SYSID | NETSCALER VPX-VERSION | LEISTUNGSBEREICH |
|---|---|---|---|
| 4.20.5 Baremetal Single-Node OpenShift (SNO)-Cluster | 450070 | 14.1-66.64 und höher | 10 Mbit/s bis 2 Gbit/s |

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

**HINWEIS:**

- Die NetScaler VPX-Instanz auf RHOCPV wird ab NetScaler Release 14.1-66.64 unterstützt. Weitere Informationen finden Sie unter Install NetScaler VPX on Red Hat OpenShift Virtualization.
- NetScaler VPX FIPS auf RHOCPV wird ab NetScaler Release 14.1-72.x unterstützt.

# VPX-Instanz auf Nutanix AHV

**HINWEIS:**

Die NetScaler VPX-Instanz auf Nutanix AHV wird ab NetScaler Release 14.1-51.x unterstützt. Weitere Informationen finden Sie unter Install a NetScaler VPX on Nutanix Acropolis hypervisor.

| NUTANIX-VERSION | SYSID | LEISTUNGSBEREICH |
|---|---|---|
| AOS 7.3, AHV 10.0.1, Prism Central 7.3 | 450070 | 10 Mbit/s bis 5 Gbit/s |

Informationen zu unterstützten NetScaler-Versionen und validierten Konfigurationen für Nutanix AHV-Bereitstellungen finden Sie unter Nutanix Compatibility and Interoperability Matrix.

**HINWEIS:**

Citrix hat Nutanix AHV unter Verwendung von AOS 6.0.1 CE qualifiziert.

## Einstellung von Citrix Ready® VPX (KVM) auf Nutanix AHV

Citrix unterstützte zuvor ältere NetScaler VPX (KVM)-Bereitstellungen auf Nutanix AHV über das Citrix Ready-Partnerschafts-Programm.

Ab NetScaler-Release 14.1-66.x bietet Citrix keine Unterstützung mehr für die älteren NetScaler VPX (KVM)-Bereitstellungen auf Nutanix AHV.

**Wichtige Überlegungen:**

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

- Upgrades von früheren NetScaler-Versionen auf 14.1-66.x und spätere Releases werden für Citrix Ready® VPX (KVM) auf Nutanix AHV nicht unterstützt.
- Kunden, die Citrix Ready VPX (KVM)-Images verwenden, müssen auf offiziell unterstützte NetScaler VPX-Images und Upgrade-Bundles migrieren, um weiterhin Support und Zugriff auf die neuesten Funktionen zu gewährleisten. Weitere Informationen finden Sie unter Migration von Citrix Ready KVM VPX zu offiziell unterstütztem NetScaler VPX™ auf Nutanix AHV.

## VPX-Instanz auf generischem KVM

| GENERISCHE KVM-VERSION | SYSID | LEISTUNGSBEREICH |
|---|---|---|
| RHEL 7.6, RHEL 8.0, RHEL 9.3 | 450070 | 10 Mbit/s bis 100 Gbit/s |
| Ubuntu 16.04, Ubuntu 18.04, Ubuntu 22.04 | | |

**Zu beachten:**

Beachten Sie die folgenden Punkte bei der Verwendung von KVM-Hypervisoren.

- Die VPX-Instanz ist für die in Tabelle 1–4 genannten Hypervisor-Release-Versionen qualifiziert, nicht jedoch für Patch-Releases innerhalb einer Version. Es wird jedoch erwartet, dass die VPX-Instanz nahtlos mit Patch-Releases einer unterstützten Version funktioniert. Sollte dies nicht der Fall sein, eröffnen Sie einen Support-Fall zur Fehlerbehebung und Diagnose.
- Führen Sie vor der Verwendung von RHEL 7.6 die folgenden Schritte auf dem KVM-Host aus:
  a. Bearbeiten Sie /etc/default/grub und fügen Sie `"kvm_intel.preemption_timer=0"` zur Variablen `GRUB_CMDLINE_LINUX` hinzu.
  b. Generieren Sie grub.cfg mit dem Befehl `"# grub2-mkconfig -o /boot/grub2/grub.cfg"` neu.
  c. Starten Sie die Hostmaschine neu.
- Führen Sie vor der Verwendung von Ubuntu 18.04 die folgenden Schritte auf dem KVM-Host aus:
  a. Bearbeiten Sie /etc/default/grub und fügen Sie `"kvm_intel.preemption_timer=0"` zur Variablen `GRUB_CMDLINE_LINUX` hinzu.

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

b. Generieren Sie grub.cfg mit dem Befehl `"# grub-mkconfig -o /boot/grub/grub.cfg "` neu.

c. Starten Sie die Hostmaschine neu.

## VPX-Instanz in öffentlichen Clouds

| ÖFFENTLICHE CLOUD | SYSID | LEISTUNGSBEREICH |
|---|---|---|
| AWS | 450040 | 10 Mbit/s bis 30 Gbit/s |
| Azure | 450020 | 10 Mbit/s bis 10 Gbit/s |
| GCP | 450070 | 10 Mbit/s bis 10 Gbit/s |

## VPX-Funktionen, die auf Hypervisoren unterstützt werden

| HYPERVISOR → FUNKTIONEN ↓ | VPX AUF XENSERVER | VPX AUF VMWARE ESX | VPX AUF MICROSOFT HYPER-V | VPX AUF GENERISCH KVM | VPX AUF NUTANIX AHV |
|---|---|---|---|---|---|
| **Schnittstellen →** | **PV** | **SR-IOV** | **PV** | **SR-IOV** | **Emuliert** | **PCI-Passthrough** | **PV** | **PV** | **SR-IOV** | **PCI-Passthrough** | **PV** |
| **Multi-PE-Unterstütz** | Ja | Ja | Ja | Ja | Ja | Ja | Ja | Ja | Ja | Ja | Ja |

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

| HYPERVISOR → FUNKTIONEN ↓ | VPX AUF XENSERVER | VPX AUF VMWARE ESX | VPX AUF MICROSOFT HYPER-V | VPX AUF GENERISCHEM KVM | VPX AUF NUTANIX AHV | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **ung** | | | | | | | | | | | |
| **Clustering-Unterstützung** | Ja | Ja[1] | Ja | Ja[1] | Ja | Ja | Ja | Ja | Ja[1] | Ja | Ja |
| **VLAN-Tagging** | Ja | Ja | Ja | Ja | Ja | Ja | Ja (nur auf 2012R2) | Ja | Ja | Ja | Ja |
| **Erkennung von Link-Ereignissen/** | Nein[2] | Ja[3] | Nein[2] | Ja[3] | Nein[2] | Ja[3] | Nein[2] | Nein[2] | Ja[3] | Ja[3] | Nein[2] |

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

| HYPERVISOR → FUNKTIONEN ↓ | VPX AUF XENSERVER | VPX AUF VMWARE ESX | VPX AUF MICROSOFT HYPER-V | VPX AUF GENERISCH KVM | VPX AUF NUTANIX AHV |
|---|---|---|---|---|---|
| **HA Mon** | | | | | |
| **Schnittstellenparameterkonfiguration** | Nein | Nein | Nein | Nein | Nein |
| **Statisches LA** | Ja[2] | Ja[3] | Ja[2] | Nein | Ja[2] |
| **LACP** | Nein | Ja[3] | Ja[2] | Nein | Ja[2] |
| **Statisches CLAG** | Nein | Nein | Nein | Nein | Nein |

| HYPERVISOR → FUNKTIONEN ↓ | VPX AUF AZURE | VPX AUF GOOGLE CLOUD | VPX AUF AWS | VPX AUF OCI | VPX AUF ALIBABA CLOUD |
|---|---|---|---|---|---|
| **HA Mon** | | | | | |
| **Schnittstellenparameterkonfiguration** | Ja | Nein | Nein | Ja | Nein |
| **Statisches LA** | Ja[3] | Ja[2] | Ja[2] | Ja[3] | Nein[2] |
| **LACP** | Ja[3] | Nein | Ja[2] | Ja[3] | Nein[2] |
| **Statisches CLAG** | Nein | Nein | Nein | Nein | Nein |

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

| HYPERVISOR → FUNKTIONEN ↓ | VPX AUF XENSERVER | VPX AUF VMWARE ESX | VPX AUF MICROSOFT HYPER-V | VPX AUF GENERISCH KVM | VPX AUF NUTANIX AHV | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **LACP CLAG** | Nein | Nein | Ja[2] | Nein | Ja[2] | Ja[3] | Nein | Ja[2] | Ja[3] | Ja[3] | Nein[2] |
| **Hot-Plug** | Nein | Nein | Nein | Nein | Nein | Nein | Nein | Nein | Nein | Nein | Nein |

## VPX-Funktionen, die in öffentlichen Clouds unterstützt werden

| ÖFFENTLICHE CLOUDS → FUNKTIONEN ↓ | VPX UNTER AWS | VPX UNTER AZURE | VPX UNTER GCP |
|---|---|---|---|
| **Multi-PE-Unterstützung** | Ja | Ja | Ja |
| **Clustering-Unterstützung** | Nein | Nein | Nein |
| **VLAN-Tagging** | Nein | Nein | Nein |
| **Erkennung von Link-Ereignissen/ HAMon** | Nein[2] | Nein[2] | Nein[2] |

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

| ÖFFENTLICHE CLOUDS → FUNKTIONEN ↓ | VPX UNTER AWS | VPX UNTER AZURE | VPX UNTER GCP |
|---|---|---|---|
| **Konfiguration der Schnittstellenparameter** | Nein | Nein | Nein |
| **Statische LA** | Nein | Nein | Nein |
| **LACP** | Nein | Nein | Nein |
| **Statische CLAG** | Nein | Nein | Nein |
| **LACP CLAG** | Nein | Nein | Nein |
| **Hot-Plug** | Ja | Nein | Nein |

Die hochgestellten Zahlen (1, 2, 3) in den beiden vorangegangenen Tabellen beziehen sich auf die folgenden Punkte mit entsprechender Nummerierung:

1. Clustering-Unterstützung ist auf SRIOV für clientseitige und serverseitige Schnittstellen verfügbar, jedoch nicht für die Backplane.
2. Schnittstellen-DOWN-Ereignisse werden in NetScaler VPX-Instanzen nicht aufgezeichnet.
3. Bei Static LA kann der Datenverkehr weiterhin über die Schnittstelle gesendet werden, deren physischer Status DOWN ist.

Die folgenden Punkte gelten für die jeweiligen Funktionen, die in den beiden vorangegangenen Tabellen aufgeführt sind:

- Bei LACP erkennt das Peer-Gerät das Schnittstellen-DOWN-Ereignis basierend auf dem LACP-Timeout-Mechanismus.
    - Kurzer Timeout: 3 Sekunden
    - Langer Timeout: 90 Sekunden
- Für LACP dürfen Schnittstellen nicht über VMs hinweg gemeinsam genutzt werden.

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

- Beim dynamischen Routing hängt die Konvergenzzeit vom Routing-Protokoll ab, da Link-Ereignisse nicht erkannt werden.
- Die Funktionalität überwachter statischer Routen schlägt fehl, wenn Sie keine Monitore an statische Routen binden, da der Routenstatus vom VLAN-Status abhängt. Der VLAN-Status hängt vom Link-Status ab.
- Eine teilweise Fehlererkennung findet bei Hochverfügbarkeit nicht statt, wenn ein Link-Fehler vorliegt. Eine Split-Brain-Bedingung bei Hochverfügbarkeit kann auftreten, wenn ein Link-Fehler vorliegt.
    - Wenn ein Link-Ereignis (Deaktivieren, Aktivieren, Zurücksetzen) von einer VPX-Instanz generiert wird, ändert sich der physische Status des Links nicht. Bei statischem LA wird jeglicher vom Peer initiierter Datenverkehr auf der Instanz verworfen.
    - Damit die VLAN-Tagging-Funktion auf VMware ESX funktioniert, setzen Sie die VLAN-ID der Portgruppe auf 1–4095 auf dem vSwitch des VMware ESX-Servers.
- Hot-Plug wird auf VPX-Instanzen mit ENA-Schnittstellen nicht unterstützt, und das Verhalten der Instanzen kann unvorhersehbar sein, wenn Hot-Plugging versucht wird. Hot-Adding wird nur für PV- und SRIOV-Schnittstellen mit NetScaler auf AWS unterstützt.
- Das Hot-Entfernen über die AWS-Webkonsole oder die AWS-CLI-Schnittstelle wird mit den PV-, SRIOV- und ENA-Schnittstellen für NetScaler nicht unterstützt. Das Verhalten der Instanzen kann unvorhersehbar sein, wenn ein Hot-Entfernen versucht wird.

## Unterstützte Browser

Informationen zu unterstützten Browsern für den Zugriff auf NetScaler GUI-Versionen 14.1 und 13.1 finden Sie unter Kompatible Browser.

## Unterstützte Prozessoren für NetScaler VPX™

| PLATTFORMEN | INTEL-PROZESSOR | AMD-PROZESSOR |
|---|---|---|
| Citrix Hypervisor | Ja | Ja |
| ESXi-Hypervisor | Ja | Ja |
| Hyper-V | Ja | Nein |
| KVM | Ja | Nein |

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

| PLATTFORMEN | INTEL-PROZESSOR | AMD-PROZESSOR |
|---|---|---|
| Nutanix AHV | Ja | Nein |
| AWS | Ja | Ja |
| Azure | Ja | Ja |
| GCP | Ja | Ja |

## Unterstützte NICs für NetScaler® VPX

**HINWEIS:**

NetScaler VPX unterstützt paravirtualisierte vNICs wie VirtIO, NetVSC und XenNetFront, die vom Hypervisor auf unterstützten physischen Netzwerkadaptern bereitgestellt werden. Zusätzlich sind die in der folgenden Tabelle aufgeführten NIC-Treiber für SR-IOV- und PCI-Passthrough (PCI-PT)-Modi qualifiziert.

Die folgende Tabelle listet die auf einer VPX-Plattform oder in der Cloud unterstützten NICs auf.

| NICS → PLATTFORMEN ↓ | MELLANOX CX-3 | MELLANOX CX-4 | MELLANOX CX-5 | INTEL 82599 SRIOV VF | INTEL X710/ X722/ XL710 SRIOV VF | INTEL X710/ XL710/ XXV710 PCI-PASSTHROUGH MODE |
|---|---|---|---|---|---|---|
| Citrix Hypervisor | NA | NA | NA | Ja | Ja | Nein |
| ESXi Hypervisor | Nein | Ja | Nein | Ja | Nein | Ja |
| Hyper-V | NA | NA | NA | Nein | Nein | Nein |

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

| NICS → PLATTFORMEN ↓ | MELLANOX CX-3 | MELLANOX CX-4 | MELLANOX CX-5 | INTEL 82599 SRIOV VF | INTEL X710/ X722/ XL710 SRIOV VF | INTEL X710/ XL710/ XXV710 PCI-PASSTHROUGH MODE |
|---|---|---|---|---|---|---|
| KVM | Nein | Ja | Ja | Ja | Ja | Nein |
| Nutanix AHV | Nein | Nein | Nein | Nein | Nein | Nein |
| AWS | NA | NA | NA | Ja | NA | NA |
| Azure | Ja | Ja | Ja | NA | NA | NA |
| GCP | NA | NA | NA | NA | NA | NA |

## Weitere Referenzen

- Besuchen Sie für Citrix Ready-Produkte den Citrix Ready Marketplace.
- Informationen zum Citrix Ready-Produktsupport finden Sie auf der Citrix Ready-Partnerseite.
- Informationen zu VMware ESX-Hardwareversionen finden Sie unter Upgrading VMware Tools.

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

# Optimieren der NetScaler VPX-Leistung auf VMware ESX, Linux KVM und Citrix Hypervisoren

Die NetScaler VPX-Leistung variiert stark je nach Hypervisor, zugewiesenen Systemressourcen und Host-Konfigurationen. Um die gewünschte Leistung zu erzielen, befolgen Sie zunächst die Empfehlungen im VPX-Datenblatt und optimieren Sie sie dann weiter mithilfe der in diesem Dokument bereitgestellten Best Practices.

## NetScaler VPX-Instanz auf VMware ESX-Hypervisoren

Dieser Abschnitt enthält Details zu konfigurierbaren Optionen und Einstellungen sowie weitere Vorschläge, die Ihnen helfen, die optimale Leistung der NetScaler VPX-Instanz auf VMware ESX-Hypervisoren zu erzielen.

- Empfohlene Konfiguration auf ESX-Hosts
- NetScaler VPX mit E1000-Netzwerkschnittstellen
- NetScaler VPX mit VMXNET3-Netzwerkschnittstellen
- NetScaler VPX mit SR-IOV- und PCI-Passthrough-Netzwerkschnittstellen

### Empfohlene Konfiguration auf ESX-Hosts

Um eine hohe Leistung für VPX mit E1000-, VMXNET3-, SR-IOV- und PCI-Passthrough-Netzwerkschnittstellen zu erzielen, befolgen Sie diese Empfehlungen:

- Die Gesamtzahl der auf dem ESX-Host bereitgestellten virtuellen CPUs (vCPUs) muss kleiner oder gleich der Gesamtzahl der physischen CPUs (pCPUs) auf dem ESX-Host sein.
- Non-uniform Memory Access (NUMA)-Affinität und CPU-Affinität müssen für den ESX-Host festgelegt werden, um gute Ergebnisse zu erzielen.

  – Um die NUMA-Affinität eines Vmnic zu ermitteln, melden Sie sich lokal oder remote am Host an und geben Sie Folgendes ein:

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

```
#vsish -e get /net/pNics/vmnic7/properties | grep NUMA

Device NUMA Node: 0
```

- Informationen zum Festlegen der NUMA- und vCPU-Affinität für eine VM finden Sie in der VMware-Dokumentation.

## NetScaler VPX mit E1000-Netzwerkschnittstellen

Führen Sie die folgenden Einstellungen auf dem VMware ESX-Host durch:

- Erstellen Sie auf dem VMware ESX-Host zwei vNICs aus einem pNIC-vSwitch. Mehrere vNICs erstellen mehrere Empfangs- (Rx) Threads im ESX-Host. Dies erhöht den Rx-Durchsatz der pNIC-Schnittstelle.
- Aktivieren Sie VLANs auf der vSwitch-Portgruppenebene für jede vNIC, die Sie erstellt haben.
- Um den vNIC-Sende- (Tx) Durchsatz zu erhöhen, verwenden Sie einen separaten Tx-Thread im ESX-Host pro vNIC. Verwenden Sie den folgenden ESX-Befehl:
  - Für ESX-Version 5.5:

    ```
    esxcli system settings advanced set –o /Net/NetTxWorldlet –i
    ```

  - Für ESX-Version 6.0 und höher:

    ```
    esxcli system settings advanced set -o /Net/NetVMTxType –i 1
    ```

- Um den vNIC-Tx-Durchsatz weiter zu erhöhen, verwenden Sie einen separaten Tx-Abschluss-Thread und Rx-Threads pro Geräte- (NIC) Warteschlange. Verwenden Sie den folgenden ESX-Befehl:

  ```
  esxcli system settings advanced set -o /Net/
  NetNetqRxQueueFeatPairEnable -i 0
  ```

**HINWEIS:**

Stellen Sie sicher, dass Sie den VMware ESX-Host neu starten, um die aktualisierten Einstellungen zu übernehmen.

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

## Zwei vNICs pro pNIC-Bereitstellung

Im Folgenden finden Sie eine Beispieltopologie und Konfigurationsbefehle für das Bereitstellungsmodell **Zwei vNICs pro pNIC**, das eine bessere Netzwerkleistung bietet.

**NetScaler VPX-Beispielkonfiguration:**

Um die in der vorhergehenden Beispieltopologie gezeigte Bereitstellung zu erreichen, führen Sie die folgende Konfiguration auf der NetScaler VPX-Instanz durch:

- Binden Sie auf der Clientseite die SNIP (1.1.1.2) an die Netzwerkschnittstelle 1/1 und aktivieren Sie den VLAN-Tag-Modus.

```
bind vlan 2 -ifnum 1/1 –tagged

bind vlan 2 -IPAddress 1.1.1.2 255.255.255.0
```

- Binden Sie serverseitig den SNIP (2.2.2.2) an die Netzwerkschnittstelle 1/1 und aktivieren Sie den VLAN-Tag-Modus.

```
bind vlan 3 -ifnum 1/2 –tagged

bind vlan 3 -IPAddress 2.2.2.2 255.255.255.0
```

- Fügen Sie einen virtuellen HTTP-Server (1.1.1.100) hinzu und binden Sie ihn an einen Dienst (2.2.2.100).

```
add lb vserver v1 HTTP 1.1.1.100 80 -persistenceType NONE -Listenpolicy
None -cltTimeout 180

add service s1 2.2.2.100 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0 -cip
DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -svrTimeout
360 -CKA NO -TCPB NO -CMP NO

bind lb vserver v1 s1
```

**HINWEIS:**

Stellen Sie sicher, dass Sie die folgenden zwei Einträge in die Routing-Tabelle aufnehmen:

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

- 1.1.1.0/24 Subnetz mit Gateway, das auf SNIP 1.1.1.2 zeigt
- 2.2.2.0/24 Subnetz mit Gateway, das auf SNIP 2.2.2.2 zeigt

## NetScaler VPX mit VMXNET3-Netzwerkschnittstellen

Um eine hohe Leistung für VPX mit VMXNET3-Netzwerkschnittstellen zu erzielen, nehmen Sie die folgenden Einstellungen auf dem VMware ESX-Host vor:

- Erstellen Sie zwei vNICs aus einem pNIC vSwitch. Mehrere vNICs erstellen mehrere Rx-Threads im ESX-Host. Dies erhöht den Rx-Durchsatz der pNIC-Schnittstelle.
- Aktivieren Sie VLANs auf der vSwitch-Portgruppenebene für jede von Ihnen erstellte vNIC.
- Um den vNIC-Übertragungs-(Tx)-Durchsatz zu erhöhen, verwenden Sie einen separaten Tx-Thread im ESX-Host pro vNIC. Verwenden Sie die folgenden ESX-Befehle:
  - Für ESX Version 5.5:

```
esxcli system settings advanced set –o /Net/NetTxWorldlet –i
```

  - Für ESX Version 6.0 und höher:

```
esxcli system settings advanced set -o /Net/NetVMTxType –i 1
```

Führen Sie auf dem VMware ESX-Host die folgende Konfiguration durch:

- Erstellen Sie auf dem VMware ESX-Host zwei vNICs aus einem pNIC vSwitch. Mehrere vNICs erstellen mehrere Tx- und Rx-Threads im ESX-Host. Dies erhöht den Tx- und Rx-Durchsatz der pNIC-Schnittstelle.
- Aktivieren Sie VLANs auf der vSwitch-Portgruppenebene für jede vNIC, die Sie erstellt haben.
- Um den Tx-Durchsatz einer vNIC zu erhöhen, verwenden Sie einen separaten Tx-Completion-Thread und Rx-Threads pro Geräte- (NIC-)Warteschlange. Verwenden Sie den folgenden Befehl:

```
esxcli system settings advanced set -o /Net/
NetNetqRxQueueFeatPairEnable -i 0
```

- Konfigurieren Sie eine VM so, dass sie einen Übertragungs-Thread pro vNIC verwendet, indem Sie die folgende Einstellung zur Konfiguration der VM hinzufügen:

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

```
ethernetX.ctxPerDev = "1"
```

- Konfigurieren Sie eine VM so, dass sie bis zu 8 Übertragungs-Threads pro vNIC verwendet, indem Sie die folgende Einstellung zur Konfiguration der VM hinzufügen:

```
ethernetX.ctxPerDev = "3"
```

**HINWEIS:**

Das Erhöhen der Übertragungs-Threads pro vNIC erfordert mehr CPU-Ressourcen (bis zu 8) auf dem ESX-Host. Stellen Sie sicher, dass genügend CPU-Ressourcen verfügbar sind, bevor Sie die oben genannten Einstellungen vornehmen.

**HINWEIS:**

Stellen Sie sicher, dass Sie den VMware ESX-Host neu starten, um die aktualisierten Einstellungen zu übernehmen.

Sie können VMXNET3 als **Two vNICs per pNIC**-Bereitstellung konfigurieren. Weitere Informationen finden Sie unter Two vNICs per pNIC deployment.

### Konfigurieren Sie Multi-Queue- und RSS-Unterstützung auf VMware ESX für VMXNET3-Geräte

Standardmäßig unterstützt das VMXNET3-Gerät nur 8 Rx- und Tx-Warteschlangen. Wenn die Anzahl der vCPUs auf dem VPX 8 überschreitet, wechselt die Anzahl der für eine VMXNET3-Schnittstelle konfigurierten Rx- und Tx-Warteschlangen standardmäßig auf 1. Sie können bis zu 19 Rx- und Tx-Warteschlangen für VMXNET3-Geräte konfigurieren, indem Sie bestimmte Konfigurationen auf ESX ändern. Diese Option erhöht die Leistung und die gleichmäßige Verteilung der Pakete über die vCPUs der VPX-Instanz.

**HINWEIS:**

Ab NetScaler Release 13.1 Build 48.x unterstützt der NetScaler VPX bis zu 19 Rx- und Tx-Warteschlangen auf ESX für VMXNET3-Geräte.

**Voraussetzungen:**

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

Um bis zu 19 Rx- und Tx-Warteschlangen auf ESX für VMXNET3-Geräte zu konfigurieren, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Die NetScaler VPX-Version ist 13.1 Build 48.X und höher.
- NetScaler VPX ist mit einer virtuellen Maschine der Hardwareversion 17 und höher konfiguriert, die von VMware ESX 7.0 und höher unterstützt wird.

**VMXNET3-Schnittstellen zur Unterstützung von mehr als 8 Rx- und Tx-Warteschlangen konfigurieren:**

1. Öffnen Sie die Konfigurationsdatei der virtuellen Maschine (.vmx-Datei).
2. Geben Sie die Anzahl der Rx- und Tx-Warteschlangen an, indem Sie die Werte `ethernetX.maxTxQueues` und `ethernetX.maxRxQueues` konfigurieren (wobei X die Anzahl der zu konfigurierenden virtuellen NICs ist). Die maximal konfigurierte Anzahl von Warteschlangen darf nicht größer sein als die Anzahl der vCPUs in der virtuellen Maschine.

   **HINWEIS:**

   Das Erhöhen der Anzahl der Warteschlangen erhöht auch den Prozessor-Overhead auf dem ESX-Host. Stellen Sie daher sicher, dass auf dem ESX-Host genügend CPU-Ressourcen verfügbar sind, bevor Sie die Warteschlangen erhöhen. Sie können die maximal unterstützte Anzahl von Warteschlangen in Szenarien erhöhen, in denen die Anzahl der Warteschlangen als Leistungsengpass identifiziert wird. In diesen Situationen empfehlen wir, die Anzahl der Warteschlangen schrittweise zu erhöhen. Zum Beispiel von 8 auf 12, dann auf 16, dann auf 20 und so weiter. Bewerten Sie die Leistung bei jeder Einstellung, anstatt direkt auf das maximale Limit zu erhöhen.

### NetScaler VPX mit SR-IOV- und PCI-Passthrough-Netzwerkschnittstellen

Um eine hohe Leistung für NetScaler VPX mit SR-IOV- und PCI-Passthrough-Netzwerkschnittstellen zu erzielen, siehe Empfohlene Konfiguration auf ESX-Hosts.

## Nutzungsrichtlinien für VMware ESXi Hypervisor

- Wir empfehlen, eine NetScaler VPX-Instanz auf lokalen Festplatten des Servers oder auf SAN-basierten Speichervolumes bereitzustellen.

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

Siehe den Abschnitt **VMware ESXi CPU Considerations** im Dokument Performance Best Practices for VMware vSphere 6.5. Hier ist ein Auszug:

- Es wird nicht empfohlen, virtuelle Maschinen mit hohem CPU- oder Speicherbedarf auf einem überbelegten Host oder Cluster bereitzustellen.
- In den meisten Umgebungen ermöglicht ESXi ein erhebliches Maß an CPU-Überbelegung, ohne die Leistung der virtuellen Maschine zu beeinträchtigen. Auf einem Host können Sie mehr vCPUs ausführen, als die Gesamtzahl der physischen Prozessorkerne auf diesem Host beträgt.
- Wenn ein ESXi-Host CPU-gesättigt ist, d. h. die virtuellen Maschinen und andere Lasten auf dem Host alle verfügbaren CPU-Ressourcen beanspruchen, funktionieren latenzempfindliche Workloads möglicherweise nicht gut. Reduzieren Sie in diesem Fall die CPU-Last, indem Sie beispielsweise einige virtuelle Maschinen ausschalten oder auf einen anderen Host migrieren (oder DRS erlauben, sie automatisch zu migrieren).
- NetScaler empfiehlt die Verwendung der neuesten Hardware-Kompatibilitätsversion, um die neuesten Funktionssätze des ESXi-Hypervisors für die virtuelle Maschine zu nutzen. Weitere Informationen zur Hardware- und ESXi-Versionskompatibilität finden Sie in der VMware-Dokumentation.
- Die NetScaler VPX ist eine latenzempfindliche, hochleistungsfähige virtuelle Appliance. Um die erwartete Leistung zu erbringen, benötigt die Appliance vCPU-Reservierung, Speicherreservierung und vCPU-Pinning auf dem Host. Außerdem muss Hyper-Threading auf dem Host deaktiviert sein. Wenn der Host diese Anforderungen nicht erfüllt, können folgende Probleme auftreten:
  - Hochverfügbarkeits-Failover
  - CPU-Spitze innerhalb der VPX-Instanz
  - Trägheit beim Zugriff auf die VPX-CLI
  - Absturz des Pit-Boss-Daemons
  - Paketverluste
  - Geringer Durchsatz
- Ein Hypervisor gilt als überprovisioniert, wenn eine der folgenden zwei Bedingungen erfüllt ist:
  - Die Gesamtzahl der auf dem Host bereitgestellten virtuellen Kerne (vCPUs) ist größer als die Gesamtzahl der physischen Kerne (pCPUs).
  - Die Gesamtzahl der bereitgestellten VMs verbraucht mehr vCPUs als die Gesamtzahl der pCPUs.

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

Wenn eine Instanz überprovisioniert ist, kann der Hypervisor die für die Instanz reservierten Ressourcen (wie CPU, Speicher und andere) möglicherweise nicht garantieren, aufgrund von Hypervisor-Scheduling-Overheads, Fehlern oder Einschränkungen des Hypervisors. Dieses Verhalten kann zu einem Mangel an CPU-Ressourcen für NetScaler führen und zu den im ersten Punkt unter **Nutzungsrichtlinien** genannten Problemen. Wir empfehlen den Administratoren, die Belegung des Hosts zu reduzieren, sodass die Gesamtzahl der auf dem Host bereitgestellten vCPUs kleiner oder gleich der Gesamtzahl der pCPUs ist.

**Beispiel:**

Für den ESX-Hypervisor, wenn der `%RDY%`-Parameter einer VPX-vCPU in der `esxtop`-Befehlsausgabe größer als 0 ist, wird dem ESX-Host nachgesagt, Scheduling-Overheads zu haben, was zu latenzbezogenen Problemen für die VPX-Instanz führen kann.

In einer solchen Situation reduzieren Sie die Belegung auf dem Host, sodass `%RDY%` immer 0 zurückgibt. Alternativ wenden Sie sich an den Hypervisor-Anbieter, um den Grund für die Nichteinhaltung der Ressourcenreservierung zu klären.

# Befehle zur Steuerung der CPU-Auslastung der Paket-Engine

Sie können zwei Befehle (`set ns vpxparam` und `show ns vpxparam`) verwenden, um das CPU-Nutzungsverhalten der Paket-Engine (Nicht-Management) von VPX-Instanzen in Hypervisor- und Cloud-Umgebungen zu steuern:

- `set ns vpxparam [-cpuyield (YES | NO | DEFAULT)] [-masterclockcpu1 (YES | NO)]`

  Ermöglicht jeder VM, die CPU-Ressourcen zu nutzen, die einer anderen VM zugewiesen, aber nicht verwendet werden.

  `Set ns vpxparam` Parameter:

  **-cpuyield**: Freigabe oder Nicht-Freigabe von zugewiesenen, aber ungenutzten CPU-Ressourcen.

  - **YES**: Ermöglicht die Nutzung zugewiesener, aber ungenutzter CPU-Ressourcen durch eine andere VM.

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

- **NO**: Reserviert alle CPU-Ressourcen für die VM, der sie zugewiesen wurden. Diese Option zeigt einen höheren Prozentsatz in Hypervisor- und Cloud-Umgebungen für die VPX-CPU-Auslastung.
- **DEFAULT**: Nein.

**HINWEIS:**

Auf allen NetScaler VPX-Plattformen beträgt die vCPU-Auslastung auf dem Hostsystem 100 Prozent. Verwenden Sie den Befehl `set ns vpxparam –cpuyield YES`, um diese Auslastung zu überschreiben.

Wenn Sie die Cluster-Knoten auf „yield“ setzen möchten, müssen Sie die folgenden zusätzlichen Konfigurationen auf CCO durchführen:

- Wenn ein Cluster gebildet wird, werden alle Knoten auf „yield=DEFAULT“ gesetzt.
- Wenn ein Cluster mit Knoten gebildet wird, die bereits auf „yield=YES“ gesetzt sind, werden die Knoten dem Cluster mit dem „DEFAULT“-Yield hinzugefügt.

**HINWEIS:**

Wenn Sie die Clusterknoten auf „yield=YES“ setzen möchten, können Sie dies erst nach der Bildung des Clusters konfigurieren, aber nicht bevor der Cluster gebildet wurde.

**-masterclockcpu1**: Sie können die Haupttaktquelle von CPU0 (Management-CPU) auf CPU1 verschieben. Dieser Parameter hat die folgenden Optionen:

- **YES**: Ermöglicht der VM, die Haupttaktquelle von CPU0 auf CPU1 zu verschieben.
- **NO**: Die VM verwendet CPU0 als Haupttaktquelle. Standardmäßig ist CPU0 die Haupttaktquelle.

- `show ns vpxparam`

  Dieser Befehl zeigt die aktuellen `vpxparam`-Einstellungen an.

## NetScaler VPX-Instanz auf der Linux-KVM-Plattform

Dieser Abschnitt enthält Details zu konfigurierbaren Optionen und Einstellungen sowie weitere Vorschläge, die Ihnen helfen, die optimale Leistung der NetScaler VPX-Instanz auf der Linux-KVM-Plattform zu erzielen.

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

- Leistungseinstellungen für KVM
- NetScaler VPX mit PV-Netzwerkschnittstellen
- NetScaler VPX mit SR-IOV- und Fortville PCIe-Passthrough-Netzwerkschnittstellen

## Leistungseinstellungen für KVM

Führen Sie die folgenden Einstellungen auf dem KVM-Host durch:

**Ermitteln Sie die NUMA-Domäne der NIC mit dem Befehl `lstopo`:**

Stellen Sie sicher, dass der Speicher für die VPX und die CPU am selben Ort fixiert ist. In der folgenden Ausgabe ist die 10G-NIC „ens2“ an die NUMA-Domäne #1 gebunden.

**Weisen Sie den VPX-Speicher der NUMA-Domäne zu.**

Der Befehl `numactl` gibt die NUMA-Domäne an, aus der der Speicher zugewiesen wird. In der folgenden Ausgabe werden etwa 10 GB RAM vom NUMA-Knoten Nr. 0 zugewiesen.

Um die NUMA-Knotenzuordnung zu ändern, führen Sie die folgenden Schritte aus.

1. Bearbeiten Sie die .xml-Datei des VPX auf dem Host.

   ```
   /etc/libvirt/qemu/<VPX_name>.xml
   ```

2. Fügen Sie das folgende Tag hinzu:

   ```
   <numatune>

   <memory mode="strict" nodeset="1"/>   ▫ This is the NUMA domain name

   </numatune>
   ```

3. Fahren Sie den VPX herunter.
4. Führen Sie den folgenden Befehl aus:

   ```
   virsh define /etc/libvirt/qemu/<VPX_name>.xml
   ```

   Dieser Befehl aktualisiert die Konfigurationsinformationen für die VM mit den NUMA-Knotenzuordnungen.

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

5. Schalten Sie den VPX ein. Überprüfen Sie dann die Ausgabe des Befehls `numactl –hardware` auf dem Host, um die aktualisierten Speicherzuweisungen für den VPX anzuzeigen.

**Binden Sie vCPUs des VPX an physische Kerne.**

- Um die vCPU-zu-pCPU-Zuordnungen eines VPX anzuzeigen, geben Sie den folgenden Befehl ein:

```
virsh vcpupin <VPX name>
```

  Die vCPUs 0–4 sind den physischen Kernen 8–11 zugeordnet.

- Um die aktuelle pCPU-Auslastung anzuzeigen, geben Sie den folgenden Befehl ein:

```
mpstat -P ALL 5
```

  In dieser Ausgabe ist 8 die Management-CPU und 9–11 sind Paket-Engines.

- Um die vCPU-zu-pCPU-Anheftung zu ändern, gibt es zwei Optionen.
  - Ändern Sie dies zur Laufzeit, nachdem die VPX hochgefahren ist, mit dem folgenden Befehl:

```
virsh vcpupin <VPX name> <vCPU id>  <pCPU number>

virsh vcpupin NetScaler-VPX-XML 0 8

virsh vcpupin NetScaler-VPX-XML 1 9

virsh vcpupin NetScaler-VPX-XML 2 10

virsh vcpupin NetScaler-VPX-XML 3 11
```

  - Um statische Änderungen an der VPX vorzunehmen, bearbeiten Sie die Datei `.xml` wie zuvor mit den folgenden Tags:

    a. Bearbeiten Sie die .xml-Datei der VPX auf dem Host

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

```
/etc/libvirt/qemu/<VPX_name>.xml
```

b. Fügen Sie das folgende Tag hinzu:

```
<vcpu placement='static' cpuset='8-11'>4</vcpu>

    <cputune>

        <vcpupin vcpu='0' cpuset='8'/>

        <vcpupin vcpu='1' cpuset='9'/>

        <vcpupin vcpu='2' cpuset='10'/>

        <vcpupin vcpu='3' cpuset='11'/>

    </cputune>
```

c. Fahren Sie die VPX herunter.

d. Aktualisieren Sie die Konfigurationsinformationen für die VM mit den NUMA-Knotenzuordnungen mithilfe des folgenden Befehls:

```
virsh define /etc/libvirt/qemu/ <VPX_name>.xml
```

e. Schalten Sie die VPX ein. Überprüfen Sie dann die Befehlsausgabe `virsh vcpupin <VPX name>` auf dem Host, um die aktualisierte CPU-Anheftung zu sehen.

**Host-Interrupt-Overhead eliminieren.**

- Erkennen Sie VM_EXITS mit dem Befehl `kvm_stat`.

  Auf Hypervisor-Ebene werden Host-Interrupts denselben pCPUs zugeordnet, an die die vCPUs der VPX angeheftet sind. Dies kann dazu führen, dass vCPUs auf der VPX periodisch entfernt werden.

  Um die VM-Exits zu finden, die von VMs ausgeführt werden, die den Host betreiben, verwenden Sie den Befehl `kvm_stat`.

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

```
[root@localhost ~]# kvm_stat -1  | grep EXTERNAL

kvm_exit(EXTERNAL_INTERRUPT)  1728349 27738

[root@localhost ~]#
```

Ein höherer Wert in der Größenordnung von 1+M deutet auf ein Problem hin.

Wenn eine einzelne VM vorhanden ist, liegt der erwartete Wert bei 30–100 K. Alles, was darüber liegt, kann darauf hindeuten, dass ein oder mehrere Host-Interrupt-Vektoren derselben pCPU zugeordnet sind.

- Host-Interrupts erkennen und Host-Interrupts migrieren.

  Wenn Sie den Befehl `concatenate` für die Datei „/proc/interrupts“ ausführen, werden alle Host-Interrupt-Zuordnungen angezeigt. Wenn ein oder mehrere aktive IRQs derselben pCPU zugeordnet sind, erhöht sich der entsprechende Zähler.

  Verschieben Sie alle Interrupts, die sich mit den pCPUs Ihres NetScaler VPX überschneiden, auf ungenutzte pCPUs:

  ```
  echo 0000000f > /proc/irq/55/smp_affinity

  0000000f - - > it is a bitmap, LSBs indicates that IRQ 55 can only be
  scheduled on pCPUs 0 – 3
  ```

- IRQ-Balance deaktivieren.

  Deaktivieren Sie den IRQ-Balance-Daemon, damit keine Neuplanung spontan erfolgt.

  ```
  service irqbalance stop

  service irqbalance show - To check the status

  service irqbalance start - Enable if needed
  ```

  Stellen Sie sicher, dass Sie den Befehl `kvm_stat` ausführen, um zu gewährleisten, dass es nicht viele Zähler gibt.

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

## NetScaler VPX mit PV-Netzwerkschnittstellen

Sie können para-virtualisierte (PV), SR-IOV- und PCIe-Passthrough-Netzwerkschnittstellen als **Zwei vNICs pro pNIC**-Bereitstellung konfigurieren. Weitere Informationen finden Sie unter Zwei vNICs pro pNIC-Bereitstellung.

Für eine optimale Leistung von PV (virtio)-Schnittstellen führen Sie die folgenden Schritte aus:

- Identifizieren Sie die NUMA-Domäne, zu der der PCIe-Steckplatz/NIC gehört.
- Der Speicher und die vCPU für den VPX müssen an dieselbe NUMA-Domäne gebunden sein.
- Der Vhost-Thread muss an die CPUs in derselben NUMA-Domäne gebunden sein.

**Binden Sie die virtuellen Host-Threads an die entsprechenden CPUs:**

1. Sobald der Datenverkehr gestartet ist, führen Sie den Befehl `top` auf dem Host aus.

   ☐

2. Identifizieren Sie die Affinität des virtuellen Host-Prozesses (benannt als `vhost-<pid-of-qemu>`).
3. Binden Sie die vHost-Prozesse mit dem folgenden Befehl an die physischen Kerne in der zuvor identifizierten NUMA-Domäne:

   ```
   taskset –pc <core-id> <process-id>
   ```

   **Beispiel:**

   ```
   taskset –pc 12 29838
   ```

4. Die Prozessorkerne, die der NUMA-Domäne entsprechen, können mit dem folgenden Befehl identifiziert werden:

   ```
   [root@localhost ~]# virsh capabilities | grep cpu

   <cpu>

       </cpu>

           <cpus num='8'>

               <cpu id='0' socket_id='0' core_id='0' siblings='0'/>
   ```

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

```
            <cpu id='1' socket_id='0' core_id='1' siblings='1'/>
            <cpu id='2' socket_id='0' core_id='2' siblings='2'/>
            <cpu id='3' socket_id='0' core_id='3' siblings='3'/>
            <cpu id='4' socket_id='0' core_id='4' siblings='4'/>
            <cpu id='5' socket_id='0' core_id='5' siblings='5'/>
            <cpu id='6' socket_id='0' core_id='6' siblings='6'/>
            <cpu id='7' socket_id='0' core_id='7' siblings='7'/>
        </cpus>


        <cpus num='8'>
        <cpu id='8' socket_id='1' core_id='0' siblings='8'/>
        <cpu id='9' socket_id='1' core_id='1' siblings='9'/>
        <cpu id='10' socket_id='1' core_id='2' siblings='10'/>
        <cpu id='11' socket_id='1' core_id='3' siblings='11'/>
        <cpu id='12' socket_id='1' core_id='4' siblings='12'/>
        <cpu id='13' socket_id='1' core_id='5' siblings='13'/>
        <cpu id='14' socket_id='1' core_id='6' siblings='14'/>
        <cpu id='15' socket_id='1' core_id='7' siblings='15'/>
        </cpus>


    <cpuselection/>
    <cpuselection/>
```

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

```
```

**Binden Sie den QEMU-Prozess an den entsprechenden physischen Kern:**

1. Identifizieren Sie die physischen Kerne, auf denen der QEMU-Prozess ausgeführt wird. Weitere Informationen finden Sie in der vorhergehenden Ausgabe.
2. Binden Sie den QEMU-Prozess mit dem folgenden Befehl an dieselben physischen Kerne, an die Sie die vCPUs binden:

```
taskset –pc 8-11 29824
```

## NetScaler VPX mit SR-IOV- und Fortville-PCIe-Passthrough-Netzwerkschnittstellen

Für eine optimale Leistung der SR-IOV- und Fortville-PCIe-Passthrough-Netzwerkschnittstellen führen Sie die folgenden Schritte aus:

- Identifizieren Sie die NUMA-Domäne, zu der der PCIe-Steckplatz/NIC gehört.
- Der Speicher und die vCPU für NetScaler VPX müssen an dieselbe NUMA-Domäne gebunden sein.

**Beispiel-VPX-XML-Datei für vCPU- und Speicher-Pinning für Linux KVM:**

```
<domain type='kvm'>

    <name>NetScaler-VPX</name>

    <uuid>138f7782-1cd3-484b-8b6d-7604f35b14f4</uuid>

    <memory unit='KiB'>8097152</memory>

    <currentMemory unit='KiB'>8097152</currentMemory>

    <vcpu placement='static'>4</vcpu>



<cputune>

    <vcpupin vcpu='0' cpuset='8'/>
```

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

```
        <vcpupin vcpu='1' cpuset='9'/>
        <vcpupin vcpu='2' cpuset='10'/>
        <vcpupin vcpu='3' cpuset='11'/>
    </cputune>

    <numatune>
    <memory mode='strict' nodeset='1'/>
    </numatune>

    </domain>
```

# NetScaler VPX-Instanz auf Citrix Hypervisors

Dieser Abschnitt enthält Details zu konfigurierbaren Optionen und Einstellungen sowie weitere Vorschläge, die Ihnen helfen, die optimale Leistung der NetScaler VPX-Instanz auf Citrix Hypervisors zu erzielen.

- Leistungseinstellungen für Citrix Hypervisors
- NetScaler VPX mit SR-IOV-Netzwerkschnittstellen
- NetScaler VPX mit paravirtualisierten Schnittstellen

## Leistungseinstellungen für Citrix Hypervisors

**Ermitteln Sie die NUMA-Domäne der NIC mithilfe des Befehls „xl“:**

```
xl info -n
```

**Fixieren Sie vCPUs der VPX an physische Kerne.**

```
xl vcpu-pin <Netsclaer VM Name>  <vCPU id>  <physical CPU id>
```

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

**Überprüfen Sie die Bindung von vCPUs.**

```
xl vcpu-list
```

**Weisen Sie NetScaler VMs mehr als 8 vCPUs zu.**

Um mehr als 8 vCPUs zu konfigurieren, führen Sie die folgenden Befehle von der Citrix Hypervisor™-Konsole aus:

```
xe vm-param-set uuid=your_vms_uuid VCPUs-max=16

xe vm-param-set uuid=your_vms_uuid VCPUs-at-startup=16
```

## NetScaler VPX mit SR-IOV-Netzwerkschnittstellen

Für eine optimale Leistung der SR-IOV-Netzwerkschnittstellen gehen Sie wie folgt vor:

- Identifizieren Sie die NUMA-Domäne, an die der PCIe-Steckplatz oder die NIC gebunden ist.
- Fixieren Sie den Speicher und die vCPU für die VPX an dieselbe NUMA-Domäne.
- Binden Sie die Domain-0-vCPU an die verbleibende CPU.

## NetScaler VPX mit paravirtualisierten Schnittstellen

Für optimale Leistung werden, wie in anderen PV-Umgebungen, Konfigurationen mit zwei vNICs pro pNIC und einer vNIC pro pNIC empfohlen.

Um eine optimale Leistung von paravirtualisierten (Netfront-)Schnittstellen zu erzielen, führen Sie die folgenden Schritte aus:

- Identifizieren Sie die NUMA-Domäne, zu der der PCIe-Steckplatz oder die NIC gehört.
- Fixieren Sie den Speicher und die vCPU für den VPX an dieselbe NUMA-Domäne.
- Binden Sie die Domain-0-vCPU an die verbleibende CPU derselben NUMA-Domäne.
- Fixieren Sie Host-Rx/Tx-Threads der vNIC an Domain-0-vCPUs.

**Host-Threads an Domain-0-vCPUs fixieren:**

1. Suchen Sie die Xen-ID von NetScaler VPX, indem Sie den Befehl `xl list` in der Citrix Hypervisor Host-Shell verwenden.
2. Identifizieren Sie Host-Threads mit dem folgenden Befehl:

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

```
ps -ax | grep vif <Xen-ID>
```

Im folgenden Beispiel bedeuten diese Werte:

- **vif5.0** – Die Threads für die erste Schnittstelle, die dem VPX in XenCenter zugewiesen wurde (Managementschnittstelle).
- **vif5.1** – Die Threads für die zweite Schnittstelle, die dem VPX zugewiesen wurde, und so weiter.

3. Fixieren Sie die Threads mit dem folgenden Befehl an die Domain-0 vCPUs:

```
taskset –pc <core-id> <process-id>
```

**Beispiel:**

```
taskset -pc 1 29189
```

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

# Unterstützung für die Erhöhung des NetScaler VPX-Festplattenspeichers

NetScaler VPX™ unterstützt einen standardmäßigen Festplattenspeicher von 20 GB. Wenn Sie aus verschiedenen Gründen auf Festplattengrößenbeschränkungen stoßen, stehen Ihnen die folgenden Optionen zur Verfügung, um den VPX-Festplattenspeicher zu erhöhen:

- Primäre Festplattengröße dynamisch erhöhen
- Sekundäre Festplatte hinzufügen
- Primäre Festplattengröße manuell erhöhen

**HINWEIS:**

Die Möglichkeit, den NetScaler VPX-Festplattenspeicher zu erhöhen, ist sowohl für VPX On-Premises- als auch für VPX Cloud-Bereitstellungen verfügbar. Die Größenänderung der primären NetScaler VPX-Festplatte wird über den SDX Management Service nicht unterstützt.

## Primäre Festplattengröße auf NetScaler VPX dynamisch erhöhen

Administratoren können die primäre Festplattengröße auf NetScaler VPX dynamisch von 20 GB auf bis zu 1 TB gleichzeitig erhöhen. Bei jeder weiteren Erhöhung können Sie erneut auf bis zu 1 TB erweitern. Stellen Sie sicher, dass Sie die VM jedes Mal herunterfahren, wenn Sie die Größe der primären Festplatte erhöhen. Dadurch kann das System die neue Festplattengröße ordnungsgemäß erkennen, die Partitionstabelle aktualisieren und die Systemstabilität aufrechterhalten. Um den Festplattenspeicher zu erhöhen, erweitern Sie die primäre Festplattengröße in der jeweiligen Cloud- oder Hypervisor-Benutzeroberfläche um mindestens 1 GB.

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

**HINWEIS:**

Sie können die Größe der Festplatten nur erhöhen. Sobald die neue Größe zugewiesen ist, können Sie sie später nicht mehr verringern. Erhöhen Sie daher die Festplattengröße nur, wenn dies unbedingt erforderlich ist.

## Sekundäre Festplatte hinzufügen

Sie können den Festplattenspeicher auf der NetScaler VPX-Instanz durch Hinzufügen einer sekundären Festplatte erhöhen. Wenn Sie die sekundäre Festplatte anschließen, wird das `/var/crash` Verzeichnis automatisch auf dieser Festplatte gemountet. Die sekundäre Festplatte wird zum Speichern von Core-Dateien und Protokollen verwendet. Bestehende Verzeichnisse für Core-Dateien und Protokolldateien funktionieren weiterhin wie zuvor.

**HINWEIS:**

Erstellen Sie ein externes Backup, bevor Sie die NetScaler Appliance herabstufen, um Datenverlust zu vermeiden.

Informationen zum Anschließen eines neuen Festplattenlaufwerks (HDD) an eine NetScaler VPX-Instanz in einer Cloud finden Sie unter den folgenden Links:

- Azure-Dokumentation

  **HINWEIS:**

  Um eine sekundäre Festplatte an auf Azure bereitgestellten VPX-Instanzen anzuschließen, stellen Sie sicher, dass die Azure VM-Größen über eine lokale temporäre Festplatte verfügen. Weitere Informationen finden Sie unter Azure VM-Größen ohne lokale temporäre Festplatte.

- AWS-Dokumentation
- GCP-Dokumentation

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

**WARNUNG:**

Nach dem Hinzufügen einer HDD zu VPX können einige Skripte, die mit Dateien arbeiten, die auf die neue HDD verschoben wurden, unter der folgenden Bedingung fehlschlagen:

- Wenn Sie den Shell-Befehl `link` verwenden, um Hardlinks zu den Dateien zu erstellen, die auf die neue HDD verschoben wurden.

Ersetzen Sie alle derartigen Befehle durch `ln -s`, um einen symbolischen Link zu verwenden. Aktualisieren Sie auch die fehlerhaften Skripte entsprechend.

## Manuelles Erhöhen der primären Festplattengröße auf NetScaler VPX

Führen Sie die folgenden Schritte aus, um die primäre VPX-Festplattengröße manuell mithilfe eines Hypervisors oder einer Cloud-Plattform zu erhöhen:

1. Fahren Sie die VM herunter.
2. Erweitern Sie die Standardfestplattengröße von 20 GB auf einen höheren Wert, z. B. 30 GB oder 40 GB. Für Azure erweitern Sie die Standardfestplattengröße von 32 GB auf 64 GB.
3. Schalten Sie die VM ein und rufen Sie die Boot-Eingabeaufforderung auf.
4. Melden Sie sich im Einzelbenutzermodus mit dem Befehl `boot -s` an.
5. Überprüfen Sie den Speicherplatz. Sie können den neu zugewiesenen Speicherplatz mit dem Befehl `gpart show` überprüfen.
6. Notieren Sie den Partitionsnamen. Im folgenden Beispiel ist die VM-Partition da0.
7. Ändern Sie die Größe der Festplattenpartition mit dem Befehl `gpart resize`.

   **Beispiel:** Wir ändern die Größe der da0 MBR-Partition, um 10 GB freien Speicherplatz einzuschließen, indem wir den folgenden Befehl ausführen.

   ```
   gpart resize -i 1 da0
   ```
8. Führen Sie den freien Speicherplatz mit der letzten Partition zusammen.

   **Beispiel:**

   ```
   gpart resize -i 5 da0s1
   ```
9. Erweitern Sie das Dateisystem, um den neu zugewiesenen freien Speicherplatz einzuschließen, indem Sie den Befehl `growfs` verwenden.

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

**Beispiel:**

```
growfs /dev/da0s1e
```

10. Starten Sie die VM neu und überprüfen Sie den erhöhten Speicherplatz mit dem Befehl `df -h` an der Shell-Eingabeaufforderung.

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

# Zusätzlichen Management-CPU-Kern auf NetScaler VPX konfigurieren

NetScaler VPX-Appliances verwenden typischerweise einen einzigen CPU-Kern für Verwaltungsaufgaben wie Konfiguration, Überwachung und Steuerungsoperationen. In Umgebungen mit erheblichen Managementanforderungen führt diese Standardkonfiguration zu Leistungsengpässen, was zu langsameren Reaktionszeiten und potenziellen Verzögerungen bei Managementoperationen führt.

Diese Funktion ermöglicht es Administratoren, einen zusätzlichen CPU-Kern speziell für Managementfunktionen zuzuweisen. Diese Verbesserung ermöglicht eine effizientere Ressourcenzuweisung, was zu verbesserten Managementoperationen führt, ohne die Verarbeitungsfähigkeit des Datenverkehrs zu beeinträchtigen. Benutzer profitieren von erhöhter Reaktionsfähigkeit und besserer Managementleistung, insbesondere in Umgebungen mit hohen Anforderungen an die Management-Arbeitslast.

**Wichtige Überlegungen:**

- Diese Funktion wird nur auf NetScaler VPX-Instanzen mit mindestens 4 vCPUs und mehr als zwei Paket-Engines unterstützt.
- Die Aktivierung dieser Funktion reduziert die für die Datenverkehrsverarbeitung zugewiesenen CPU-Kerne.
- Planen Sie diese Konfigurationsänderung während eines Wartungsfensters ein, da das Gerät neu gestartet werden muss, damit die Änderungen wirksam werden.

## Zusätzlichen Management-CPU-Kern über die CLI konfigurieren

Um den zusätzlichen Management-CPU-Kern zu aktivieren, verwenden Sie den folgenden Befehl:

```
enable extramgmtcpu
```

Um den zusätzlichen Management-CPU-Kern zu deaktivieren, verwenden Sie den folgenden Befehl:

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

```
disable extramgmtcpu
```

**HINWEIS:**

Ein Neustart ist erforderlich, damit die Konfigurationsänderungen wirksam werden.

Um zu überprüfen, ob die Funktion des zusätzlichen Management-CPU-Kerns aktiviert oder deaktiviert ist, verwenden Sie den folgenden Befehl:

```
show extramgmtcpu



ConfiguredState: DISABLED

EffectiveState: DISABLED
```

Dieser Befehl gibt die konfigurierten und effektiven Zustände des zusätzlichen Management-CPU-Kerns zurück. Dieser Befehl hilft Administratoren, den Betriebsstatus schnell zu beurteilen und festzustellen, ob weitere Maßnahmen zur Aktivierung oder Deaktivierung erforderlich sind.

## Zusätzlichen Management-CPU-Kern über die GUI konfigurieren

1. Navigieren Sie zu **Configuration > System > Settings**.
2. Klicken Sie auf **Configure Extra Management CPU**.

3. Wählen Sie im Dropdown-Menü **Configured State** die Option **ENABLED** aus, und klicken Sie dann auf **OK**.

4. Um die Änderungen zu übernehmen, kehren Sie zu **Configuration > System** zurück und klicken Sie auf **Reboot**. Bestätigen Sie die Aktion, indem Sie auf **OK** klicken.

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

**HINWEIS:**

- Um die Funktion zu deaktivieren, wählen Sie im Dropdown-Menü **Configured State** die Option **DISABLED** aus.
- In einer Hochverfügbarkeitsbereitstellung muss die zusätzliche Management-CPU auf jedem Knoten unabhängig aktiviert werden.

## Statistiken und Überwachung

Die folgenden Beispiele zeigen die Änderungen in der `stat cpu` Befehlsausgabe vor und nach der Zuweisung einer zusätzlichen Management-CPU auf einem 4-vCPU-System.

**Vor der Aktivierung der zusätzlichen Management-CPU:**

**Nach der Aktivierung der zusätzlichen Management-CPU:**

Nach zusätzlicher CPU(/en-us/vpx/media/extra-mgmt-stat-cpu-after.png)

Die Nutzung der zusätzlichen Management-CPU kann anhand der Zähler in der `stat system`-Ausgabe überwacht werden.

Statistik-Systemausgabe(/en-us/vpx/media/extra-mgmt-stat-cpu-output.png)

## Fehlerbehebung bei zusätzlicher Management-CPU

Wenn die Voraussetzungen von mindestens 4 vCPUs und mindestens zwei Paket-Engines nicht erfüllt sind, wird beim Ausführen von CLI-Befehlen eine Fehlermeldung angezeigt. Wenn beispielsweise nur eine Paket-Engine betriebsbereit ist, zeigt das System an:

"**Warnung:** Vorgang nicht zulässig. Der PE-Pool ist nicht ausreichend, um eine zusätzliche Management-CPU zu aktivieren.".

Standardmäßig weist NetScaler VPX CPU-Kern 0 für Managementfunktionen zu. Sie können dies mit den folgenden Shell-Befehlen überprüfen:

- `sysctl netscaler.additional_mgmt_cpu`

  `netscaler.additional_mgmt_cpu = 0` zeigt an, dass keine zusätzliche Management-CPU konfiguriert ist.

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

- `sysctl netscaler.cpus_in_mgmt_pool`

  `netscaler.cpus_in_mgmt_pool : CPU(s) 0` bestätigt, dass Kern 0 als Standard-Management-CPU festgelegt ist.

Wenn eine zusätzliche Management-CPU, z. B. CPU-Kern 3, konfiguriert ist, kann die Ausgabe dieser Befehle wie folgt abweichen:

- `sysctl netscaler.additional_mgmt_cpu` zeigt `1` an, was bedeutet, dass eine zusätzliche Management-CPU aktiv ist.
- `sysctl netscaler.cpus_in_mgmt_pool` zeigt `CPU(s) 0,3` an, was darauf hinweist, dass sowohl CPU-Kern 0 als auch Kern 3 zugewiesen sind.

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

# Anwenden von NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance in der Cloud

Sie können die NetScaler VPX-Konfigurationen während des ersten Starts der NetScaler Appliance in einer Cloud-Umgebung anwenden. Diese Phase wird in diesem Dokument als **Preboot**-Phase bezeichnet. Daher wird in bestimmten Fällen, wie z. B. bei der ADC-Pool-Lizenzierung, eine spezifische VPX-Instanz in wesentlich kürzerer Zeit hochgefahren. Diese Funktion ist in Microsoft Azure, Google Cloud Platform und AWS Clouds verfügbar.

## Was sind Benutzerdaten

Wenn Sie eine VPX-Instanz in einer Cloud-Umgebung bereitstellen, haben Sie die Möglichkeit, Benutzerdaten an die Instanz zu übergeben. Die Benutzerdaten ermöglichen es Ihnen, gängige automatisierte Konfigurationsaufgaben durchzuführen, das Startverhalten von Instanzen anzupassen und Skripte nach dem Start der Instanz auszuführen. Beim ersten Start führt die NetScaler VPX-Instanz die folgenden Aufgaben aus:

- Liest die Benutzerdaten.
- Interpretiert die in den Benutzerdaten bereitgestellte Konfiguration.
- Wendet die neu hinzugefügte Konfiguration während des Startvorgangs an.

## So stellen Sie Preboot-Benutzerdaten in der Cloud-Instanz bereit

Sie können Preboot-Benutzerdaten für die Cloud-Instanz im XML-Format bereitstellen. Verschiedene Clouds verfügen über unterschiedliche Schnittstellen zur Bereitstellung von Benutzerdaten.

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

# Bereitstellen von Preboot-Benutzerdaten über die AWS-Konsole

Wenn Sie eine NetScaler VPX-Instanz über die AWS-Konsole bereitstellen, navigieren Sie zu **Instanzdetails konfigurieren > Erweiterte Details** und geben Sie die Preboot-Benutzerdatenkonfiguration in das Feld **Benutzerdaten** ein.

Detaillierte Anweisungen zu den einzelnen Schritten finden Sie unter Bereitstellen einer NetScaler VPX-Instanz auf AWS mithilfe der AWS-Webkonsole. Weitere Informationen finden Sie in der AWS-Dokumentation unter Starten einer Instanz.

**HINWEIS:**

Der AWS IMDSv2-Only-Modus für die Preboot-Benutzerdatenfunktion wird ab NetScaler VPX Release 13.1.48.x und späteren Releases unterstützt.

## Preboot-Benutzerdaten mithilfe der AWS CLI bereitstellen

Geben Sie den folgenden Befehl in der AWS CLI ein:

```
aws ec2 run-instances \

    --image-id ami-0abcdef1234567890 \

    --instance-type t2.micro \

    --count 1 \

    --subnet-id subnet-08fc749671b2d077c \

    --key-name MyKeyPair \

    --security-group-ids sg-0b0384b66d7d692f9 \

    --user-data file://my_script.txt
```

Weitere Informationen finden Sie in der AWS-Dokumentation zu Ausführen von Instanzen.

Weitere Informationen finden Sie in der AWS-Dokumentation zu Verwenden von Instanz-Benutzerdaten

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

# Preboot-Benutzerdaten mithilfe der Azure-Konsole bereitstellen

Wenn Sie eine NetScaler VPX-Instanz über die Azure-Konsole bereitstellen, navigieren Sie zur Registerkarte **Virtuellen Computer erstellen > Erweitert**. Geben Sie im Feld **Benutzerdefinierte Daten** die Preboot-Benutzerdatenkonfiguration an.

## Preboot-Benutzerdaten mithilfe der Azure CLI bereitstellen

Geben Sie den folgenden Befehl in der Azure CLI ein:

```
az vm create \

  --resource-group myResourceGroup \

  --name MyVm \

  --image debian \

  --custom-data MyCloudInitScript.txt \
```

**Beispiel:**

```
az vm create --resource-group MyResourceGroup -name MyVm --image debian --
custom-data MyCloudInitScript.txt
```

Sie können Ihre benutzerdefinierten Daten oder die Preboot-Konfiguration als Datei an den Parameter „--custom-data“ übergeben. In diesem Beispiel lautet der Dateiname **MyCloudInitScript.txt**.

Weitere Informationen finden Sie in der Azure CLI-Dokumentation.

# Preboot-Benutzerdaten mithilfe der GCP-Konsole bereitstellen

Wenn Sie eine NetScaler VPX-Instanz über die GCP-Konsole bereitstellen, füllen Sie die Instanzeigenschaften aus. erweitern **Verwaltung, Sicherheit, Datenträger, Netzwerk,**

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

**Einzelmandantenfähigkeit**. Navigieren Sie zur Registerkarte **Verwaltung**. Geben Sie im Abschnitt **Automatisierung** die Preboot-Benutzerdatenkonfiguration im Feld **Startskript** an.

Ausführliche Informationen zum Erstellen der VPX-Instanz mithilfe von GCP finden Sie unter Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform.

### Preboot-Benutzerdaten mithilfe der gcloud CLI bereitstellen

Geben Sie den folgenden Befehl in der GCP CLI ein:

```
gcloud compute instances create INSTANCE_NAMES --metadata-from-
file=startup-script=LOCAL_FILE_PATH
```

**metadata-from-file** – Liest den Wert oder die Benutzerdaten aus einer Datei, die unter <LOCAL_FILE_PATH> gespeichert ist.

Weitere Informationen finden Sie unter gcloud CLI-Dokumentation

## Format der Preboot-Benutzerdaten

Die Preboot-Benutzerdaten müssen der Cloud-Instanz im XML-Format bereitgestellt werden. Die NetScaler-Preboot-Benutzerdaten, die Sie während des Starts über die Cloud-Infrastruktur bereitstellen, können die folgenden vier Abschnitte umfassen:

- NetScaler-Konfiguration, dargestellt mit dem `<NS-CONFIG>` Tag.
- Benutzerdefiniertes Bootstrapping des NetScaler, dargestellt mit dem `<NS-BOOTSTRAP>` Tag.
- Speichern von Benutzerskripten in NetScaler, dargestellt mit dem `<NS-SCRIPTS>` Tag.
- Gepoolte Lizenzierungskonfiguration, dargestellt mit dem `<NS-LICENSE-CONFIG>` Tag.

Sie können die vorangegangenen vier Abschnitte in beliebiger Reihenfolge innerhalb der ADC-Preboot-Konfiguration bereitstellen. Stellen Sie sicher, dass Sie beim Bereitstellen der Preboot-Benutzerdaten die in den folgenden Abschnitten gezeigte Formatierung strikt einhalten.

**HINWEIS:**

Die gesamte Preboot-Benutzerdatenkonfiguration muss in den `<NS-PRE-BOOT-CONFIG>` Tag eingeschlossen werden, wie in den folgenden Beispielen gezeigt.

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

**Beispiel 1:**

```
<NS-PRE-BOOT-CONFIG>

     <NS-CONFIG>          </NS-CONFIG>

     <NS-BOOTSTRAP>       </NS-BOOTSTRAP>

     <NS-SCRIPTS>         </NS-SCRIPTS>

     <NS-LICENSE-CONFIG>  </NS-LICENSE-CONFIG>

</NS-PRE-BOOT-CONFIG>
```

**Beispiel 2:**

```
<NS-PRE-BOOT-CONFIG>

    <NS-LICENSE-CONFIG> </NS-LICENSE-CONFIG>

    <NS-SCRIPTS>        </NS-SCRIPTS>

    <NS-BOOTSTRAP>      </NS-BOOTSTRAP>

    <NS-CONFIG>         </NS-CONFIG>

</NS-PRE-BOOT-CONFIG>
```

Verwenden Sie das `<NS-CONFIG>` Tag, um die spezifischen NetScaler VPX-Konfigurationen bereitzustellen, die in der Preboot-Phase auf die VPX-Instanz angewendet werden müssen.

**HINWEIS:**

Der `<NS-CONFIG>` Abschnitt muss gültige ADC CLI-Befehle enthalten. Die CLIs werden nicht auf syntaktische Fehler oder Formatierung überprüft.

## NetScaler-Konfigurationen

Verwenden Sie das `<NS-CONFIG>` Tag, um die spezifischen NetScaler VPX-Konfigurationen bereitzustellen, die in der Preboot-Phase auf die VPX-Instanz angewendet werden müssen.

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

**HINWEIS:**

Der `<NS-CONFIG>` Abschnitt muss gültige ADC CLI-Befehle enthalten. Die CLIs werden nicht auf syntaktische Fehler oder Formatierung überprüft.

**Beispiel:**

Im folgenden Beispiel enthält der `<NS-CONFIG>` Abschnitt die Details der Konfigurationen. Ein VLAN mit der ID '5' wird konfiguriert und an die SNIP (5.0.0.1) gebunden. Ein virtueller Lastausgleichsserver (4.0.0.101) wird ebenfalls konfiguriert.

Sie können die im vorhergehenden Screenshot gezeigte Konfiguration von hier kopieren:

```
<NS-PRE-BOOT-CONFIG>

     <NS-CONFIG>

          add vlan 5

          add ns ip 5.0.0.1 255.255.255.0

          bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0

          enable ns feature WL SP LB RESPONDER

          add server 5.0.0.201 5.0.0.201

          add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE
-maxClient 0 -maxReq 0 -cip DISABLED -usip

 NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO
-TCPB NO -CMP NO

          add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -persistenceType
NONE -cltTimeout 180

     </NS-CONFIG>

</NS-PRE-BOOT-CONFIG>
```

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

Die NetScaler VPX-Instanz wird mit der Konfiguration gestartet, die im `<NS-CONFIG>` Abschnitt angewendet wurde, wie in den folgenden Abbildungen gezeigt.

## Benutzerskripte

Verwenden Sie das `<NS-SCRIPTS>`-Tag, um Skripte bereitzustellen, die in der NetScaler VPX-Instanz gespeichert und ausgeführt werden müssen.

Sie können viele Skripte innerhalb des `<NS-SCRIPTS>`-Tags einfügen. Jedes Skript muss innerhalb des `<SCRIPT>`-Tags enthalten sein. Jeder `<SCRIPT>`-Abschnitt entspricht einem Skript und enthält alle Details des Skripts unter Verwendung der folgenden Unter-Tags.

- **`<SCRIPT-NAME>:`** Gibt den Namen der Skriptdatei an, die gespeichert werden muss.
- **`<SCRIPT-CONTENT>:`** Gibt den Inhalt der Datei an, die gespeichert werden muss.
- **`<SCRIPT-TARGET-LOCATION>:`** Gibt den vorgesehenen Zielspeicherort an, an dem diese Datei gespeichert werden muss. Wenn der Zielspeicherort nicht angegeben wird, wird die Datei oder das Skript standardmäßig im Verzeichnis „/nsconfig“ gespeichert.
- **`<SCRIPT-NS-BOOTUP>:`** Geben Sie die Befehle an, die Sie zum Ausführen des Skripts verwenden.
  - Wenn Sie den `<SCRIPT-NS-BOOTUP>`-Abschnitt verwenden, werden die in diesem Abschnitt angegebenen Befehle in „/nsconfig/nsafter.sh“ gespeichert und nach dem Start der Paket-Engine als Teil der Ausführung von „nsafter.sh“ ausgeführt.
  - Wenn Sie den `<SCRIPT-NS-BOOTUP>`-Abschnitt nicht verwenden, wird die Skriptdatei am von Ihnen angegebenen Zielspeicherort gespeichert.

**Beispiel 1:**

In diesem Beispiel enthält das `<NS-SCRIPTS>`-Tag Details zu nur einem Skript: script-1.sh. Das Skript „script-1.sh“ wird im Verzeichnis „/var“ gespeichert. Das Skript wird mit den angegebenen Inhalten gefüllt und nach dem Start der Paket-Engine mit dem Befehl „sh /var/script-1.sh“ ausgeführt.

Sie können die im vorhergehenden Screenshot gezeigte Konfiguration von hier kopieren:

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

```
<NS-PRE-BOOT-CONFIG>

    <NS-SCRIPTS>

    <SCRIPT>

            <SCRIPT-CONTENT>

                #Shell script

                echo "Running script 1" > /var/script-1.output

                date >> /var/script-1.output

            </SCRIPT-CONTENT>



                <SCRIPT-NAME> script-1.sh </SCRIPT-NAME>

                <SCRIPT-TARGET-LOCATION> /var/ </SCRIPT-TARGET-LOCATION>

                <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP>

        </SCRIPT>

    </NS-SCRIPTS>

</NS-PRE-BOOT-CONFIG>
```

Im folgenden Snapshot können Sie überprüfen, ob das Skript „script-1.sh“ im Verzeichnis „/var/“ gespeichert ist. Das Skript „Script-1.sh“ wird ausgeführt und die Ausgabedatei wird entsprechend erstellt.

**Beispiel 2:**

Im folgenden Beispiel enthält der `<NS-SCRIPTS>` Tag Details zu zwei Skripten.

- Das erste Skript wird als „script-1.sh“ im Verzeichnis „/var“ gespeichert. Das Skript wird mit den angegebenen Inhalten gefüllt und nach dem Start der Paket-Engine mit dem Befehl „sh /var/script-1.sh“ ausgeführt.

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

- Das zweite Skript wird als „file-2.txt“ im Verzeichnis „/var“ gespeichert. Diese Datei wird mit den angegebenen Inhalten gefüllt. Sie wird jedoch nicht ausgeführt, da der Startausführungsbefehl `<SCRIPT-NS-BOOTUP>` nicht angegeben ist.

Sie können die in der vorhergehenden Abbildung gezeigte Konfiguration hier kopieren:

```
<NS-PRE-BOOT-CONFIG>

    <NS-SCRIPTS>

        <SCRIPT>

            <SCRIPT-CONTENT>

               #Shell script

               echo "Running script 1" > /var/script-1.output

               date >> /var/script-1.output

            </SCRIPT-CONTENT>



            <SCRIPT-NAME>  script-1.sh  </SCRIPT-NAME>

            <SCRIPT-TARGET-LOCATION> /var/  </SCRIPT-TARGET-LOCATION>

            <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP>

            </SCRIPT>



        <SCRIPT>

            <SCRIPT-CONTENT>

                This script has no execution point.

                It will just be saved at the target location
```

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

```
                NS Consumer module should consume this script/file

            </SCRIPT-CONTENT>

            <SCRIPT-NAME>file-2.txt</SCRIPT-NAME>

            <SCRIPT-TARGET-LOCATION>/var/</SCRIPT-TARGET-LOCATION>

        </SCRIPT>

    </NS-SCRIPTS>

</NS-PRE-BOOT-CONFIG>
```

Im folgenden Snapshot können Sie überprüfen, ob script-1.sh und file-2.txt im Verzeichnis „/var/“ erstellt wurden. Das Skript-1.sh wird ausgeführt, und die Ausgabedatei wird entsprechend erstellt.

## Lizenzierung

Verwenden Sie den `<NS-LICENSE-CONFIG>` Tag, um die NetScaler-Pool-Lizenzierung beim Starten der VPX-Instanz anzuwenden. Verwenden Sie den `<LICENSE-COMMANDS>` Tag innerhalb des `<NS-LICENSE-CONFIG>` Abschnitts, um die Befehle für die Pool-Lizenzierung bereitzustellen. Diese Befehle müssen syntaktisch gültig sein.

Sie können die Details der Pool-Lizenzierung, wie Lizenztyp, Kapazität und Lizenzserver, im `<LICENSE-COMMANDS>` Abschnitt mithilfe der Standardbefehle für die Pool-Lizenzierung angeben. Weitere Informationen finden Sie unter NetScaler-Pool-Kapazitätslizenzierung konfigurieren.

Nach dem Anwenden von `<NS-LICENSE-CONFIG>` startet die VPX mit der angeforderten Edition, und die VPX versucht, die konfigurierten Lizenzen vom Lizenzserver auszuchecken.

- Wenn das Auschecken der Lizenz erfolgreich ist, wird die konfigurierte Bandbreite auf die VPX angewendet.
- Wenn das Auschecken der Lizenz fehlschlägt, wird die Lizenz innerhalb von etwa 10–12 Minuten nicht vom Lizenzserver abgerufen. Infolgedessen wird das System neu gestartet und wechselt in einen nicht lizenzierten Zustand.

**Beispiel:**

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

Im folgenden Beispiel startet der VPX nach dem Anwenden von `<NS-LICENSE-CONFIG>` beim Booten mit der Premium Edition, und der VPX versucht, die konfigurierten Lizenzen vom Lizenzserver (10.102.38.214) auszuchecken.

Sie können die im vorhergehenden Screenshot gezeigte Konfiguration von hier kopieren:

```
<NS-PRE-BOOT-CONFIG>

   <NS-LICENSE-CONFIG>

        <LICENSE-COMMANDS>

            add ns licenseserver 10.102.38.214 -port 2800

            set ns capacity -unit gbps -bandwidth 3  edition platinum

        </LICENSE-COMMANDS>

    </NS-LICENSE-CONFIG>

</NS-PRE-BOOT-CONFIG>
```

Wie in der folgenden Abbildung gezeigt, können Sie den Befehl „show license server“ ausführen und überprüfen, ob der Lizenzserver (10.102.38.214) zum VPX hinzugefügt wurde.

# Bootstrapping

Verwenden Sie das Tag `<NS-BOOTSTRAP>`, um die benutzerdefinierten Bootstrapping-Informationen bereitzustellen. Sie können die Tags `<SKIP-DEFAULT-BOOTSTRAP>` und `<NEW-BOOTSTRAP-SEQUENCE>` innerhalb des Abschnitts `<NS-BOOTSTRAP>` verwenden. Dieser Abschnitt informiert die NetScaler Appliance darüber, ob das Standard-Bootstrapping vermieden werden soll oder nicht. Wenn das Standard-Bootstrapping vermieden wird, bietet Ihnen dieser Abschnitt die Möglichkeit, eine neue Bootstrapping-Sequenz bereitzustellen.

## Standard-Bootstrap-Konfiguration

Die Standard-Bootstrap-Konfiguration in der NetScaler Appliance folgt diesen Schnittstellenzuweisungen:

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

- **Eth0** – Managementschnittstelle mit einer bestimmten NSIP-Adresse.
- **Eth1** – Client-seitige Schnittstelle mit einer bestimmten VIP-Adresse.
- **Eth2** – Server-seitige Schnittstelle mit einer bestimmten SNIP-Adresse.

## Bootstrap-Konfiguration anpassen

Sie können die Standard-Bootstrap-Sequenz überspringen und eine neue Bootstrap-Sequenz für die NetScaler VPX-Instanz bereitstellen. Verwenden Sie das Tag `<NS-BOOTSTRAP>`, um die benutzerdefinierten Bootstrapping-Informationen bereitzustellen. Sie können beispielsweise das Standard-Bootstrapping ändern, bei dem die Managementschnittstelle (NSIP), die Client-seitige Schnittstelle (VIP) und die Server-seitige Schnittstelle (SNIP) immer in einer bestimmten Reihenfolge bereitgestellt werden.

Die folgende Tabelle zeigt das Bootstrapping-Verhalten mit den verschiedenen zulässigen Werten für die Tags `<SKIP-DEFAULT-BOOTSTRAP>` und `<NEW-BOOTSTRAP-SEQUENCE>`.

| SKIP-DEFAULT-BOOTSTRAP | NEW-BOOTSTRAP-SEQUENCE | BOOTSTRAP-VERHALTEN |
|---|---|---|
| JA | JA | Das standardmäßige Bootstrapping-Verhalten wird übersprungen, und eine neue benutzerdefinierte Bootstrap-Sequenz, die im Abschnitt `<NS-BOOTSTRAP>` bereitgestellt wird, wird ausgeführt. |
| JA | NEIN | Das standardmäßige Bootstrapping-Verhalten wird übersprungen. Die im Abschnitt `<NS-CONFIG>` bereitgestellten Bootstrap-Befehle werden ausgeführt. |

Sie können die Bootstrap-Konfiguration mit den folgenden drei Methoden anpassen:

- Nur die Schnittstellendetails angeben
- Die Schnittstellendetails zusammen mit IP-Adressen und Subnetzmaske angeben
- Bootstrap-bezogene Befehle im Abschnitt `<NS-CONFIG>` angeben

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

# Methode 1: Benutzerdefiniertes Bootstrap durch Angabe nur der Schnittstellendetails

Sie geben die Management-, Client-seitigen und Server-seitigen Schnittstellen an, aber nicht deren IP-Adressen und Subnetzmasken. Die IP-Adressen und Subnetzmasken werden durch Abfragen der Cloud-Infrastruktur gefüllt.

## Benutzerdefiniertes Bootstrap-Beispiel für AWS

Sie stellen die benutzerdefinierte Bootstrap-Sequenz wie im folgenden Beispiel gezeigt bereit. Weitere Informationen finden Sie unter Bereitstellen von Preboot-Benutzerdaten in einer Cloud-Instanz. Die Eth1-Schnittstelle wird als Verwaltungsschnittstelle (NSIP), die Eth0-Schnittstelle als Clientschnittstelle (VIP) und die Eth2-Schnittstelle als Serverschnittstelle (SNIP) zugewiesen. Der Abschnitt `<NS-BOOTSTRAP>` enthält nur die Schnittstellendetails und nicht die Details der IP-Adressen und Subnetzmasken.

Nachdem die VM-Instanz erstellt wurde, können Sie im AWS-Portal die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

1. Navigieren Sie zu **AWS Portal > EC2-Instanzen**, und wählen Sie die Instanz aus, die Sie durch Bereitstellung der benutzerdefinierten Bootstrap-Informationen erstellt haben.
2. Auf der Registerkarte **Beschreibung** können Sie die Eigenschaften jeder Netzwerkschnittstelle überprüfen, wie in den folgenden Abbildungen gezeigt.

Sie können den Befehl `show nsip` in der **ADC CLI** ausführen und die Netzwerkschnittstellen überprüfen, die während des ersten Starts der ADC-Appliance auf die NetScaler VPX-Instanz angewendet wurden.

## Benutzerdefiniertes Bootstrap-Beispiel für Azure

Sie stellen die benutzerdefinierte Bootstrap-Sequenz wie im folgenden Beispiel gezeigt bereit. Weitere Informationen finden Sie unter Bereitstellen von Preboot-Benutzerdaten in einer Cloud-Instanz. Die Eth2-Schnittstelle wird als Verwaltungsschnittstelle (NSIP), die Eth1-Schnittstelle als Clientschnittstelle (VIP) und die Eth0-Schnittstelle als Serverschnittstelle (SNIP) zugewiesen. Der

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

Abschnitt `<NS-BOOTSTRAP>` enthält nur die Schnittstellendetails und nicht die Details der IP-Adressen und Subnetzmasken.

Sie können sehen, dass die NetScaler VPX-Instanz mit drei Netzwerkschnittstellen erstellt wird. Navigieren Sie zu **Azure-Portal > VM-Instanz > Netzwerk**, und überprüfen Sie die Netzwerkeigenschaften der drei NICs, wie in den folgenden Abbildungen gezeigt.

Sie können den Befehl "show nsip" in der ADC-CLI ausführen und überprüfen, ob die neue Bootstrap-Sequenz, die im Abschnitt `<NS-BOOTSTRAP>` angegeben ist, angewendet wurde. Sie können den Befehl "show route" ausführen, um die Subnetzmaske zu überprüfen.

## Benutzerdefinierte Bootstrap-Beispiele für GCP

Sie stellen die benutzerdefinierte Bootstrap-Sequenz wie im folgenden Beispiel gezeigt bereit. Weitere Informationen finden Sie unter Bereitstellen von Preboot-Benutzerdaten in der Cloud-Instanz. Die Eth1-Schnittstelle wird als Verwaltungsschnittstelle (NSIP), die Eth0-Schnittstelle als Client-Schnittstelle (VIP) und die Eth2-Schnittstelle als Server-Schnittstelle (SNIP) zugewiesen. Der Abschnitt `<NS-BOOTSTRAP>` enthält nur die Schnittstellendetails und nicht die Details der IP-Adressen und Subnetzmasken.

Nachdem die VM-Instanz im GCP-Portal erstellt wurde, können Sie die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

1. Wählen Sie die Instanz aus, die Sie durch Angabe der benutzerdefinierten Bootstrap-Informationen erstellt haben.
2. Navigieren Sie zu den Eigenschaften der Netzwerkschnittstelle und überprüfen Sie die NIC-Details wie folgt:

Sie können den Befehl `show nsip` in der **ADC-CLI** ausführen und die Netzwerkschnittstellen überprüfen, die während des ersten Starts der ADC-Appliance auf die NetScaler VPX-Instanz angewendet wurden.

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

# Methode 2: Benutzerdefinierter Bootstrap durch Angabe der Schnittstellen, IP-Adressen und Subnetzmasken

Sie geben die Management-, Client-seitige und Server-seitige Schnittstellen zusammen mit ihren IP-Adressen und der Subnetzmaske an.

## Benutzerdefinierte Bootstrap-Beispiele für AWS

Im folgenden Beispiel überspringen Sie den Standard-Bootstrap und führen eine neue Bootstrap-Sequenz für die NetScaler Appliance aus. Für die neue Bootstrap-Sequenz geben Sie die folgenden Details an:

- **Managementschnittstelle:** Schnittstelle - Eth1, NSIP - 172.31.52.88 und Subnetzmaske - 255.255.240.0
- **Client-seitige Schnittstelle:** Schnittstelle - Eth0, VIP - 172.31.5.155 und Subnetzmaske - 255.255.240.0.
- **Server-seitige Schnittstelle:** Schnittstelle - Eth2, SNIP - 172.31.76.177 und Subnetzmaske - 255.255.240.0.

Sie können den Befehl `show nsip` in der ADC-CLI ausführen und überprüfen, ob die neue Bootstrap-Sequenz, die im Abschnitt `<NS-BOOTSTRAP>` angegeben ist, angewendet wird. Sie können den Befehl „show route“ ausführen, um die Subnetzmaske zu überprüfen.

## Benutzerdefiniertes Bootstrap-Beispiel für Azure

Im folgenden Beispiel wird eine neue Bootstrap-Sequenz für ADC erwähnt und der Standard-Bootstrap wird übersprungen. Sie geben die Schnittstellendetails zusammen mit den IP-Adressen und Subnetzmasken wie folgt an:

- Managementschnittstelle (eth2), NSIP (172.27.2.53) und Subnetzmaske (255.255.255.0)
- Client-seitige Schnittstelle (eth1), VIP (172.27.1.53) und Subnetzmaske (255.255.255.0)
- Server-seitige Schnittstelle (eth0), SNIP (172.27.0.53) und Subnetzmaske (255.255.255.0)

Sie können sehen, dass die NetScaler VPX-Instanz mit drei Netzwerkschnittstellen erstellt wird. Navigieren Sie zu **Azure-Portal > VM-Instanz > Netzwerk**, und überprüfen Sie die Netzwerkeigenschaften der drei NICs, wie in den folgenden Abbildungen gezeigt.

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

Sie können den Befehl `show nsip` in der ADC-CLI ausführen und überprüfen, ob die neue Bootstrap-Sequenz, die im Abschnitt `<NS-BOOTSTRAP>` angegeben ist, angewendet wurde. Sie können den Befehl „show route“ ausführen, um die Subnetzmaske zu überprüfen.

### Beispiel für benutzerdefinierten Bootstrap für GCP

Im folgenden Beispiel wird eine neue Bootstrap-Sequenz für ADC erwähnt und der Standard-Bootstrap wird übersprungen. Sie geben die Schnittstellendetails zusammen mit den IP-Adressen und Subnetzmasken wie folgt an:

- Verwaltungsschnittstelle (eth2), NSIP (10.128.4.31) und Subnetzmaske (255.255.255.0)
- Client-seitige Schnittstelle (eth1), VIP (10.128.0.43) und Subnetzmaske (255.255.255.0)
- Server-seitige Schnittstelle (eth0), SNIP (10.160.0.75) und Subnetzmaske (255.255.255.0)

Nachdem die VM-Instanz im GCP-Portal mit dem benutzerdefinierten Bootstrap erstellt wurde, können Sie die Netzwerkschnittstelleneigenschaften wie folgt überprüfen:

1. Wählen Sie die Instanz aus, die Sie durch Angabe der benutzerdefinierten Bootstrap-Informationen erstellt haben.
2. Navigieren Sie zu den Eigenschaften der Netzwerkschnittstelle und überprüfen Sie die NIC-Details wie folgt.

Sie können den Befehl `show nsip` in der ADC-CLI ausführen und überprüfen, ob die neue Bootstrap-Sequenz, die im Abschnitt `<NS-BOOTSTRAP>` angegeben ist, angewendet wird. Sie können den Befehl „show route“ ausführen, um die Subnetzmaske zu überprüfen.

## Methode 3: Benutzerdefinierter Bootstrap durch Bereitstellung von Bootstrap-bezogenen Befehlen im Abschnitt `<NS-CONFIG>`

Sie können die Bootstrap-bezogenen Befehle im Abschnitt `<NS-CONFIG>` angeben. Im Abschnitt `<NS-BOOTSTRAP>` müssen Sie `<NEW-BOOTSTRAP-SEQUENCE>` als „No“ angeben, um die Bootstrapping-Befehle im Abschnitt `<NS-CONFIG>` auszuführen. Sie müssen auch die Befehle zur

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

Zuweisung von NSIP, Standardroute und NSVLAN angeben. Geben Sie außerdem die für die von Ihnen verwendete Cloud relevanten Befehle an.

Bevor Sie einen benutzerdefinierten Bootstrap bereitstellen, stellen Sie sicher, dass Ihre Cloud-Infrastruktur eine bestimmte Schnittstellenkonfiguration unterstützt.

## Beispiel für benutzerdefinierten Bootstrap für AWS

In diesem Beispiel werden Bootstrap-bezogene Befehle im Abschnitt `<NS-CONFIG>` bereitgestellt. Der Abschnitt `<NS-BOOTSTRAP>` zeigt an, dass das Standard-Bootstrapping übersprungen wird und die im Abschnitt `<NS-CONFIG>` bereitgestellten benutzerdefinierten Bootstrap-Informationen ausgeführt werden. Sie müssen auch die Befehle zum Erstellen von NSIP, Hinzufügen einer Standardroute und Hinzufügen von NSVLAN angeben.

Sie können die in der vorhergehenden Abbildung gezeigte Konfiguration hier kopieren:

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>



        set ns config -IPAddress 172.31.52.88 -netmask 255.255.240.0

        add route 0.0.0.0 0.0.0.0 172.31.48.1

        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO

        add route 172.31.0.2 255.255.255.255 172.31.48.1



        enable ns feature WL SP LB RESPONDER

        add server 5.0.0.201 5.0.0.201

        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -maxClient
0 -maxReq 0 -cip DISABLED -usip NO - useproxyport YES -sp OFF -cltTimeout
180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -persistenceType
NONE -cltTimeout 180
```

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

```
    </NS-CONFIG>


    <NS-BOOTSTRAP>
     <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
     <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
    </NS-BOOTSTRAP>



</NS-PRE-BOOT-CONFIG>
```

Nachdem die VM-Instanz erstellt wurde, können Sie im AWS-Portal die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

1. Navigieren Sie zu **AWS Portal > EC2-Instanzen**, und wählen Sie die Instanz aus, die Sie durch Bereitstellung der benutzerdefinierten Bootstrap-Informationen erstellt haben.
2. Auf der Registerkarte **Beschreibung** können Sie die Eigenschaften jeder Netzwerkschnittstelle überprüfen, wie in den folgenden Abbildungen gezeigt.

Sie können den Befehl `show nsip` in der **ADC CLI** ausführen und die auf die NetScaler VPX-Instanz angewendeten Netzwerkschnittstellen während des ersten Starts der ADC-Appliance überprüfen.

## Benutzerdefiniertes Bootstrap-Beispiel für Azure

In diesem Beispiel werden Bootstrap-bezogene Befehle im Abschnitt `<NS-CONFIG>` bereitgestellt. Der Abschnitt `<NS-BOOTSTRAP>` zeigt an, dass das Standard-Bootstrapping übersprungen wird

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

und die im Abschnitt `<NS-CONFIG>` bereitgestellten benutzerdefinierten Bootstrap-Informationen ausgeführt werden.

**HINWEIS:**

Für die Azure-Cloud sind der Instance Metadata Server (IMDS) und DNS-Server nur über die primäre Schnittstelle (Eth0) zugänglich. Wenn die Eth0-Schnittstelle daher nicht als Verwaltungsschnittstelle (NSIP) verwendet wird, muss die Eth0-Schnittstelle zumindest als SNIP konfiguriert werden, damit der IMDS- oder DNS-Zugriff funktioniert. Die Route zum IMDS-Endpunkt (169.254.169.254) und DNS-Endpunkt (168.63.129.16) über das Gateway von Eth0 muss ebenfalls hinzugefügt werden.

```
<NS-PRE-BOOT-CONFIG>


   <NS-CONFIG>


        set ns config -IPAddress 172.27.2.61 -netmask 255.255.255.0

        add route 0.0.0.0   0.0.0.0   172.27.2.1

        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO

        add ns ip 172.27.0.61   255.255.255.0   -type SNIP

        add route 169.254.169.254 255.255.255.255 172.27.0.1

        add route 168.63.129.16 255.255.255.255 172.27.0.1


        add vlan 5

        bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0

        enable ns feature WL SP LB RESPONDER
```

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

```
        add server 5.0.0.201 5.0.0.201

        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -maxClient
0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout
180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -persistenceType
NONE -cltTimeout 180



    </NS-CONFIG>



    <NS-BOOTSTRAP>



    <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>

    <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>



    </NS-BOOTSTRAP>



</NS-PRE-BOOT-CONFIG>
```

Sie können sehen, dass die NetScaler VPX-Instanz mit drei Netzwerkschnittstellen erstellt wird. Navigieren Sie zum **Azure-Portal > VM-Instanz > Netzwerk**, und überprüfen Sie die Netzwerkeigenschaften der drei NICs, wie in den folgenden Abbildungen gezeigt.

Sie können den Befehl `show nsip` in der ADC CLI ausführen und überprüfen, ob die neue Bootstrap-Sequenz, die im Abschnitt `<NS-BOOTSTRAP>` angegeben ist, angewendet wird. Sie können den Befehl „show route“ ausführen, um die Subnetzmaske zu überprüfen.

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

## Benutzerdefiniertes Bootstrap-Beispiel für GCP

In diesem Beispiel werden Bootstrap-bezogene Befehle im Abschnitt `<NS-CONFIG>` bereitgestellt. Der Abschnitt `<NS-BOOTSTRAP>` zeigt an, dass das Standard-Bootstrapping übersprungen und die benutzerdefinierten Bootstrap-Informationen, die im Abschnitt `<NS-CONFIG>` bereitgestellt werden, angewendet werden.

Sie können die in dem vorhergehenden Screenshot gezeigte Konfiguration von hier kopieren:

```
<NS-PRE-BOOT-CONFIG>



    <NS-CONFIG>



        set ns config -IPAddress 10.128.0.2 -netmask 255.255.255.0

        add route 0.0.0.0 0.0.0.0 10.128.0.1

        set ns config -nsvlan 10 -ifnum 1/1  -tagged NO



        enable ns feature WL SP LB RESPONDER

        add server 5.0.0.201 5.0.0.201

        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -maxClient
0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout
180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -persistenceType
NONE -cltTimeout 180



    </NS-CONFIG>
```

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

```
    <NS-BOOTSTRAP>

        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>

        <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>

    </NS-BOOTSTRAP>



</NS-PRE-BOOT-CONFIG>
```

Nachdem die VM-Instanz im GCP-Portal mit dem benutzerdefinierten Bootstrap erstellt wurde, können Sie die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

1. Wählen Sie die Instanz aus, die Sie durch Bereitstellung der benutzerdefinierten Bootstrap-Informationen erstellt haben.
2. Navigieren Sie zu den Eigenschaften der Netzwerkschnittstelle und überprüfen Sie die NIC-Details, wie in der Abbildung gezeigt.

Sie können den Befehl `show nsip` in der **ADC CLI** ausführen und überprüfen, ob die Konfigurationen, die im vorhergehenden Abschnitt `<NS-CONFIG>` bereitgestellt wurden, beim ersten Start der ADC-Appliance angewendet werden.

## Auswirkungen des Anhängens und Entfernens von NICs in AWS und Azure

AWS und Azure bieten die Möglichkeit, eine Netzwerkschnittstelle an eine Instanz anzuhängen und eine Netzwerkschnittstelle von einer Instanz zu trennen. Das Anhängen oder Trennen von Schnittstellen kann die Schnittstellenpositionen ändern. Daher empfiehlt Citrix, Schnittstellen nicht von der NetScaler VPX-Instanz zu trennen. Wenn Sie eine Schnittstelle trennen oder anhängen, während benutzerdefiniertes Bootstrapping konfiguriert ist, weist die NetScaler VPX-Instanz die primäre IP der neu verfügbaren Schnittstelle an der Position der Verwaltungsschnittstelle als NSIP neu zu. Wenn nach der von Ihnen getrennten Schnittstelle keine weiteren Schnittstellen verfügbar sind, wird die erste Schnittstelle zur Verwaltungsschnittstelle für die NetScaler VPX-Instanz gemacht.

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

Zum Beispiel wird eine NetScaler VPX-Instanz mit 3 Schnittstellen gestartet: Eth0 (SNIP), Eth1 (NSIP) und Eth2 (VIP). Wenn Sie die Eth1-Schnittstelle von der Instanz trennen, die eine Verwaltungsschnittstelle ist, konfiguriert ADC die nächste verfügbare Schnittstelle (Eth2) als Verwaltungsschnittstelle. Dadurch ist die NetScaler VPX-Instanz weiterhin über die primäre IP der Eth2-Schnittstelle zugänglich. Wenn Eth2 ebenfalls nicht verfügbar ist, wird die verbleibende Schnittstelle (Eth0) zur Verwaltungsschnittstelle gemacht. Daher bleibt der Zugriff auf die NetScaler VPX-Instanz bestehen.

Betrachten wir eine andere Zuweisung von Schnittstellen wie folgt: Eth0 (SNIP), Eth1 (VIP) und Eth2 (NSIP). Wenn Sie Eth2 (NSIP) trennen, da nach Eth2 keine neue Schnittstelle verfügbar ist, wird die erste Schnittstelle (Eth0) zur Verwaltungsschnittstelle gemacht.

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

# Verbessern der SSL-TPS-Leistung auf öffentlichen Cloud-Plattformen

Sie können eine bessere SSL-TPS-Leistung in AWS- und GCP-Clouds erzielen, indem Sie die Paket-Engine (PE)-Gewichtungen gleichmäßig verteilen. Die Aktivierung dieser Funktion kann zu einem leichten Rückgang des HTTP-Durchsatzes um etwa 10–12 % führen.

In AWS- und GCP-Clouds zeigen die NetScaler VPX-Instanzen mit 10–16 vCPUs keine Leistungsverbesserung, da die PE-Gewichtungen standardmäßig gleichmäßig verteilt sind.

**HINWEIS:**

In der Azure-Cloud sind die PE-Gewichtungen standardmäßig gleichmäßig verteilt. Diese Funktion verbessert die Leistung der Azure-Instanzen nicht.

## Konfigurieren des PE-Modus über die NetScaler CLI

Nach dem Festlegen des PE-Modus müssen Sie das System neu starten, damit die Konfigurationsänderungen wirksam werden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cpuparam pemode [CPUBOUND | Default]
```

Wenn der PE-Modus auf CPUBOUND eingestellt ist, werden die PE-Gewichtungen gleichmäßig verteilt. Wenn der PE-Modus auf DEFAULT eingestellt ist, werden die PE-Gewichtungen auf Standardwerte gesetzt.

**HINWEIS:**

Dieser Befehl ist knotenspezifisch. In einer Hochverfügbarkeits- oder Cluster-Einrichtung müssen Sie den Befehl auf jedem Knoten ausführen. Wenn Sie den Befehl auf CLIP ausführen, tritt der folgende Fehler auf: `Operation not permitted on CLIP`

Um den Status des konfigurierten PE-Modus anzuzeigen, führen Sie den folgenden Befehl aus:

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

```
show cpuparam
```

**Beispiel:**

```
> show cpuparam

    Pemode:  CPUBOUND

 Done
```

## Anwenden der PE-Modus-Konfiguration beim ersten Start der NetScaler Appliance in der Cloud

Um die PE-Modus-Konfiguration beim ersten Start der NetScaler Appliance in der Cloud anzuwenden, müssen Sie eine `/nsconfig/.cpubound.conf`-Datei mit dem benutzerdefinierten Skript erstellen. Weitere Informationen finden Sie unter Anwenden von NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance in der Cloud.

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

# Gleichzeitiges Multithreading für NetScaler VPX in öffentlichen Clouds konfigurieren

NetScaler® verwendet verschiedene dedizierte Kerne für seine Verwaltungs- und Datenebenenfunktionen. Ein Kern wird typischerweise den Verwaltungsfunktionen zugewiesen. Die restlichen verfügbaren Kerne werden den Datenebenenfunktionen zugewiesen.

Die folgende Abbildung zeigt eine vereinfachte Darstellung eines 4-Kern-NetScaler VPX.

Abbildung 1. NetScaler Verwaltungs- und Datenebenen-Workload auf einem 4-Kern-System

Während die vorhergehende Abbildung die Verteilung der NetScaler-Funktionen auf die verfügbaren Kerne zeigt, ist sie nicht unbedingt eine genaue Darstellung der zugrunde liegenden Hardware. Die meisten modernen x86-CPUs bieten zwei logische Kerne pro physischem Kern, durch Funktionen, die kommerziell als Intel Hyperthreading (HT) oder AMD Simultaneous Multithreading (SMT) bekannt sind.

Die folgende Abbildung zeigt NetScaler VPX, der auf einer modernen CPU mit deaktiviertem SMT läuft. Jeder CPU-Kern ist in zwei oder mehr logische CPUs aufgeteilt, die gemeinhin als Threads bezeichnet werden. Jeder Thread verfügt über eigene replizierte Ressourcen, einen Teil der partitionierten Ressourcen und konkurriert mit seinen Geschwister-Threads um gemeinsam genutzte Ressourcen.

Abbildung 2. NetScaler Verwaltungs- und Datenebenen-Workload auf einem 4-Kern/8-Thread-System mit deaktiviertem SMT

Die folgende Abbildung zeigt NetScaler VPX, der auf einer modernen CPU mit aktiviertem SMT läuft.

Abbildung 3. NetScaler Verwaltungs- und Datenebenen-Workload auf einem 4-Kern-System mit aktiviertem SMT

Das Aktivieren von SMT verbessert die NetScaler-Leistung durch:

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

- Ausführen von Datenebenenfunktionen auf allen physischen Kernen.
- Verschieben der Verwaltungsfunktionen auf den Geschwister-Thread.
- Einführung eines flexiblen Ressourcenbegrenzungsmechanismus, um zu verhindern, dass Funktionen der Management-Ebene die Leistung der Funktionen der Datenebene beeinträchtigen.

## SMT-Unterstützungsmatrix

Die VPX-Plattformen, Cloud-Instanztypen und NetScaler-Versionen, die SMT unterstützen, sind in der folgenden Tabelle aufgeführt.

| VPX-PLATTFORM | INSTANZTYPEN | NETSCALER VPX-VERSION |
|---|---|---|
| AWS | M5, m5n, c5, c5n | 14.1-12.x und höher |
| Azure | Jede Instanzfamilie mit Hyperthreading, zum Beispiel Ds_v4 | 14.1-12.x und höher |
| GCP | e2-Instanzen | 14.1-12.x und höher |

**HINWEIS:**

Durch die Aktivierung der SMT-Funktion wird die Leistung von NetScaler VPX auf den unterstützten Typen gesteigert.

## Einschränkungen

Die SMT-Funktion verdoppelt effektiv die für eine NetScaler Appliance verfügbaren vCPUs. Die Lizenzbeschränkungen müssen berücksichtigt werden, damit die NetScaler Appliance diese nutzen kann.

Betrachten Sie beispielsweise NetScaler VPX, wie in Abbildung 3 dargestellt. Wenn eine durchsatzbasierte Lizenzierung verwendet wird, ist eine Lizenz von 10 Gbit/s oder mehr mit der SMT-Funktion erforderlich, um 8 vCPUs zu aktivieren. Zuvor war eine 1-Gbit/s-Lizenz ausreichend, um 4 vCPUs zu aktivieren. Wenn eine vCPU-Lizenzierung verwendet wird, muss NetScaler VPX so konfiguriert werden, dass Lizenzen für die doppelte Anzahl von vCPUs für den ordnungsgemäßen Betrieb ausgecheckt werden. Wenden Sie sich an den technischen Support von NetScaler, um weitere Anleitungen zu diesem Thema zu erhalten.

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

# SMT konfigurieren

Bevor Sie die SMT-Funktion aktivieren, stellen Sie sicher, dass Ihre Plattform diese Funktion unterstützt. Siehe die Support-Matrix-Tabelle im vorherigen Abschnitt.

Gehen Sie wie folgt vor, um die SMT-Funktion zu aktivieren:

1. Erstellen Sie eine leere Datei mit dem Namen `.smt_handling` im Verzeichnis „/nsconfig“.
2. Speichern Sie die aktuelle Konfiguration.
3. Starten Sie die NetScaler VPX-Instanz neu.

```
nscli> shell touch /nsconfig/.smt_handling

  Done

nscli> reboot

Are you sure you want to restart NetScaler (Y/N)? [N]:Y

Done
```

4. Nach dem Neustart zeigt NetScaler an, dass die Funktion sowohl verfügbar als auch aktiviert ist.

```
smt_handling and smt_handling_active are set to “1”



> shell sysctl -a | grep smt_handling

netscaler.smt_handling_platform: 1

netscaler.smt_handling: 1

netscaler.smt_handling_active: 1
```

Gehen Sie wie folgt vor, um die SMT-Funktion zu deaktivieren:

1. Entfernen Sie die Datei `.smt_handling`.
2. Starten Sie die NetScaler VPX-Instanz neu.

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

```
shell rm -f /nsconfig/.smt_handling

  Done



reboot



Are you sure you want to restart NetScaler (Y/N)? [N]:Y

Done
```

3. Nach dem Neustart zeigt NetScaler an, dass die Funktion verfügbar, aber deaktiviert ist.

```
> shell sysctl -a | grep smt_handling

netscaler.smt_handling_platform: 1

netscaler.smt_handling: 0

netscaler.smt_handling_active: 0
```

## Fehlerbehebung

Führen Sie den Shell-Befehl `sysctl` aus, um den Status der SMT-Funktion zu überprüfen.

```
```

> shell sysctl -a | grep smt_handling

>

```
```

Der Befehl kann eine der folgenden Ausgaben zurückgeben.

- Die SMT-Funktion fehlt.

  Der Befehl `sysctl` gibt keine Ausgabe zurück.

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

- Die SMT-Funktion wird nicht unterstützt.

  Die SMT-Funktion wird aus einem der folgenden Gründe nicht unterstützt:

  - Ihr NetScaler VPX ist älter als 13.1-48.x oder 14.1-12.x.
  - Ihre Cloud unterstützt SMT nicht.
  - Ihr VM-Instanztyp unterstützt SMT nicht, z. B. ist die vCPU-Anzahl größer als 8.

    ```
    > shell sysctl -a | grep smt_handling

    netscaler.smt_handling_platform: 0(indicates not supported)

    netscaler.smt_handling: 0 (indicates not enabled)

    netscaler.smt_handling_active: 0 (indicates not active)
    ```

- Die SMT-Funktion wird unterstützt, ist aber nicht aktiviert.

  ```
  > shell sysctl -a | grep smt_handling

  netscaler.smt_handling_platform: 1 (available)

  netscaler.smt_handling: 0         (not enabled)

  netscaler.smt_handling_active: 0  (not active)
  ```

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

# NetScaler Sanity Checker Tool

Das Sanity Checker Tool bewertet den Zustand und die Leistung von NetScalerund identifiziert auch die häufigsten Konfigurationsprobleme.

**HINWEIS:**

Derzeit wird das NetScaler Sanity Checker Tool nur für die AWS Cloud unterstützt.

Das NetScaler Sanity Checker Tool führt auch die folgenden Aktivitäten aus:

- Validiert HA-Topologie, Netzwerk, Lizenzierung und Berechtigungen.
- Optimiert den Fehlerbehebungsprozess.
- Ermöglicht eine schnelle Behebung von Problemen, die in öffentlichen Clouds auftreten.
- Generiert Ergebnisse in mehreren Formaten wie z. B. Klartextprotokollen, JSON und HTML.

## NetScaler Sanity Checker Tool für AWS

Das NetScaler Sanity Checker Tool umfasst die folgenden Validierungen basierend auf dem Bereitstellungstyp.

| EIGENSTÄNDIGE UND HA-BEREITSTELLUNGEN IN DERSELBEN ZONE | MULTIZONEN-HA-BEREITSTELLUNG MIT ELASTISCHEN IP-ADRESSEN | MULTIZONEN-HA-BEREITSTELLUNG MIT PRIVATEN IP-ADRESSEN |
|---|---|---|
| • IAM-Berechtigungsvalidierung<br>• Lizenzprüfung<br>• Speicherprüfung<br>• Metadatenroutenprüfung | • IAM-Berechtigungsvalidierung<br>• Schnittstellenprüfung<br>• EIPs-Prüfung | • IAM-Berechtigungsvalidierung<br>• Schnittstellenprüfung<br>• Routenprüfung |

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

| EIGENSTÄNDIGE UND HA-BEREITSTELLUNGEN IN DERSELBEN ZONE | MULTIZONEN-HA-BEREITSTELLUNG MIT ELASTISCHEN IP-ADRESSEN | MULTIZONEN-HA-BEREITSTELLUNG MIT PRIVATEN IP-ADRESSEN | |
|---|---|---|---|
| • DNS-Auflösungsprüfung<br>• EC2-Endpunktprüfung<br>• Standard-Gateway-Prüfung<br>• VLAN-Konfigurationsprüfung<br>• ARP-Prüfung<br>• SysID-Prüfung<br>• Cloudhadaemon-Prüfung | • INC-Modus-Prüfung<br>• IPSet-Prüfung | • Geräteindexprüfung<br>• Src/Dst-Prüfung | |

## Ausführen des Sanity Checker Tools mithilfe der NetScaler CLI

Geben Sie an der Eingabeaufforderung ein:

```
> Shell

> root@ns# sanitychecker -c [standalone | multizone]
```

Nach Ausführung des Sanity Checker Tools werden die folgenden Dateien im JSON- und HTML-Format generiert.

- /var/cloudsanitychecker/results.json
- /var/cloudsanitychecker/standalone.html

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

Diese Dateien enthalten die detaillierten Ergebnisse der durchgeführten Prüfungen, die verwendet werden können, um potenzielle Probleme zu identifizieren und zu analysieren.

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

# Installieren einer NetScaler VPX-Instanz auf einem Bare-Metal-Server

Ein Bare Metal ist ein vollständig dedizierter physischer Server, der physische Isolation bietet und vollständig in die Cloud-Umgebung integriert ist. Er wird auch als Single-Tenant-Server bezeichnet. Single Tenancy ermöglicht es Ihnen, den Noisy-Neighbor-Effekt zu vermeiden. Mit Bare Metal erleben Sie den Noisy-Neighbor-Effekt nicht, da Sie der einzige Benutzer sind.

Ein Bare-Metal-Server, auf dem ein Hypervisor installiert ist, bietet Ihnen eine Verwaltungssuite zum Erstellen virtueller Maschinen auf dem Server. Der Hypervisor führt Anwendungen nicht nativ aus. Sein Zweck ist es, Ihre Workloads in separate virtuelle Maschinen zu virtualisieren, um die Flexibilität und Zuverlässigkeit der Virtualisierung zu nutzen.

## Voraussetzungen für die Installation einer NetScaler VPX-Instanz auf Bare-Metal-Servern

Ein Bare-Metal-Server muss von einem Cloud-Anbieter bezogen werden, der alle Systemanforderungen für den jeweiligen Hypervisor erfüllt.

## Installieren der NetScaler VPX-Instanz auf Bare-Metal-Servern

Um NetScaler VPX-Instanzen auf einem Bare-Metal-Server zu installieren, müssen Sie zunächst einen Bare-Metal-Server mit ausreichenden Systemressourcen von einem Cloud-Anbieter beziehen. Auf diesem Bare-Metal-Server muss einer der unterstützten Hypervisoren wie Linux KVM, VMware ESX, Citrix Hypervisor oder Microsoft Hyper-V installiert und konfiguriert werden, bevor die NetScaler VPX-Instanz bereitgestellt wird.

Weitere Informationen zur Liste der verschiedenen Hypervisoren und der auf einer NetScaler VPX-Instanz unterstützten Funktionen finden Sie unter Supportmatrix und Nutzungsrichtlinien.

Weitere Informationen zur Installation von NetScaler VPX-Instanzen auf verschiedenen Hypervisoren finden Sie in der jeweiligen Dokumentation.

- **Citrix Hypervisor:** Siehe Installieren einer NetScaler VPX-Instanz auf Citrix Hypervisor.
- **VMware ESX:** Siehe Installieren einer NetScaler VPX-Instanz auf VMware ESX.

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

- **Microsoft Hyper-V:** Siehe Installieren einer NetScaler VPX-Instanz auf einem Microsoft Hyper-V-Server.
- **Linux KVM-Plattform:** Siehe Installieren einer NetScaler VPX-Instanz auf einer Linux-KVM-Plattform.

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

# Installieren einer NetScaler VPX-Instanz auf Citrix Hypervisor/XenServer

Um VPX-Instanzen auf dem Citrix Hypervisor/XenServer zu installieren, müssen Sie zuerst den Hypervisor auf einem Computer mit ausreichenden Systemressourcen installieren. Um die NetScaler VPX-Instanz zu installieren, verwenden Sie Citrix XenCenter, das auf einem Remote-Computer mit Netzwerkzugriff auf den Hypervisor-Host installiert sein muss.

Weitere Informationen zum Hypervisor finden Sie in der Citrix Hypervisor-Dokumentation.

Die folgende Abbildung zeigt die Bare-Metal-Lösungsarchitektur der NetScaler VPX-Instanz auf dem Hypervisor.

**Abbildung.** Eine NetScaler VPX-Instanz auf Citrix Hypervisor/XenServer

## Voraussetzungen für die Installation einer NetScaler VPX-Instanz auf dem Hypervisor

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, führen Sie die folgenden Schritte aus:

- Installieren Sie Hypervisor Version 6.0 oder höher auf Hardware, die die Mindestanforderungen erfüllt.
- Installieren Sie XenCenter® auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.
- Besorgen Sie sich Lizenzdateien für virtuelle Appliances. Weitere Informationen zu Lizenzen für virtuelle Appliances finden Sie im NetScaler Licensing Guide.

### Hardwareanforderungen für den Hypervisor

Die folgende Tabelle beschreibt die Mindesthardwareanforderungen für eine Hypervisor-Plattform, auf der eine NetScaler VPX-Instanz ausgeführt wird.

**Tabelle 1**. Mindestsystemanforderungen für Hypervisor, auf dem eine nCore VPX-Instanz ausgeführt wird

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

| KOMPONENTE | ANFORDERUNG |
|---|---|
| CPU | 2 oder mehr 64-Bit-x86-CPUs mit aktivierter Virtualisierungsunterstützung (Intel-VT oder AMD-V). Um die NetScaler VPX-Instanz auszuführen, muss die Hardwareunterstützung für die Virtualisierung auf dem Hypervisor-Host aktiviert sein. Stellen Sie sicher, dass die BIOS-Option für die Virtualisierungsunterstützung nicht deaktiviert ist. Weitere Informationen finden Sie in der BIOS-Dokumentation. |
| RAM | 3 GB |
| Festplattenspeicher | Lokal angeschlossener Speicher (PATA, SATA, SCSI) mit 40 GB Festplattenspeicher. |
| | **Hinweis:** Die Hypervisor-Installation erstellt eine 4-GB-Partition für die Steuerdomäne des Hypervisor-Hosts. Der verbleibende Speicherplatz steht für NetScaler VPX-Instanzen und andere virtuelle Maschinen zur Verfügung. |
| NIC | Eine 1-Gbit/s-NIC; empfohlen: zwei 1-Gbit/s-NICs |

Weitere Informationen finden Sie in der XenServer-Dokumentation.

Die folgende Tabelle listet die virtuellen Computerressourcen auf, die der Hypervisor für jede nCore VPX Virtual Appliance bereitstellen muss.

**Tabelle 2**. Mindestressourcen für virtuelle Computer, die für den Betrieb einer nCore VPX-Instanz erforderlich sind

| KOMPONENTE | ANFORDERUNG |
|---|---|
| Arbeitsspeicher | 2 GB |
| Virtuelle CPU (vCPU) | 2 |

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

| KOMPONENTE | ANFORDERUNG |
| --- | --- |
| Virtuelle Netzwerkschnittstellen | 2 |

**HINWEIS:**

Für den Produktionseinsatz der NetScaler VPX-Instanz empfiehlt Citrix, dass die CPU-Priorität (in den Eigenschaften der virtuellen Maschine) auf die höchste Stufe eingestellt werden muss, um das Planungsverhalten und die Netzwerklatenz zu verbessern.

### XenCenter-Systemanforderungen

XenCenter ist eine Windows-Clientanwendung. Sie kann nicht auf demselben Computer wie der Hypervisor-Host ausgeführt werden. Weitere Informationen zu den Mindestsystemanforderungen und zur Installation von XenCenter finden Sie in den folgenden Hypervisor-Dokumenten:

- Systemanforderungen
- Installation

## NetScaler VPX-Instanzen auf Hypervisor mit XenCenter installieren

Nachdem Sie Hypervisor und XenCenter installiert und konfiguriert haben, können Sie XenCenter verwenden, um virtuelle Appliances auf Hypervisor zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge des verfügbaren Arbeitsspeichers auf der Hardware ab, auf der Hypervisor ausgeführt wird.

Gehen Sie wie folgt vor, um NetScaler VPX-Instanzen auf Hypervisor mit XenCenter zu installieren:

1. Starten Sie **XenCenter** auf Ihrer Arbeitsstation.
2. Klicken Sie im Menü **Server** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Neuen Server hinzufügen** im Textfeld für den Hostnamen die IP-Adresse oder den DNS-Namen des Hypervisors ein, mit dem Sie eine Verbindung herstellen möchten.
4. Geben Sie in die Textfelder **Benutzername** und **Passwort** die Administratoranmeldeinformationen ein und klicken Sie dann auf **Verbinden**. Der Hypervisor-

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

Name wird im Navigationsbereich mit einem grünen Kreis angezeigt, der anzeigt, dass der Hypervisor verbunden ist.

5. Klicken Sie im Navigationsbereich auf den Namen des Hypervisors, auf dem Sie die NetScaler VPX-Instanz installieren möchten.
6. Klicken Sie im Menü **VM** auf **Importieren**.
7. Navigieren Sie im Dialogfeld **Importieren** im Feld für den Importdateinamen zu dem Speicherort, an dem Sie die NetScaler VPX-Instanz `.xva`-Imagedatei gespeichert haben. Stellen Sie sicher, dass die Option Exportierte VM ausgewählt ist, und klicken Sie dann auf **Weiter**.
8. Wählen Sie den Hypervisor aus, auf dem Sie die virtuelle Appliance installieren möchten, und klicken Sie dann auf **Weiter**.
9. Wählen Sie das lokale Speicher-Repository aus, in dem die virtuelle Appliance gespeichert werden soll, und klicken Sie dann auf **Importieren**, um den Importvorgang zu starten.
10. Sie können die virtuellen Netzwerkschnittstellen nach Bedarf hinzufügen, ändern oder löschen. Klicken Sie anschließend auf **Weiter**.
11. Klicken Sie auf **Fertig stellen**, um den Importvorgang abzuschließen.

    **HINWEIS:**

    Um den Status des Importvorgangs anzuzeigen, klicken Sie auf die Registerkarte **Protokoll**.

12. Wenn Sie eine weitere virtuelle Appliance installieren möchten, wiederholen Sie die Schritte 5 bis 11.

**HINWEIS:**

Nach der Erstkonfiguration der VPX-Instanz, wenn Sie die Appliance auf die neueste Softwareversion aktualisieren möchten, siehe Aktualisieren oder Herabstufen der Systemsoftware.

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

# Konfigurieren von VPX-Instanzen zur Verwendung von Single Root I/O Virtualization (SR-IOV)-Netzwerkschnittstellen

Nachdem Sie eine NetScaler VPX-Instanz auf Citrix Hypervisor installiert und konfiguriert haben, können Sie die virtuelle Appliance so konfigurieren, dass sie SR-IOV-Netzwerkschnittstellen verwendet.

Die folgenden NICs werden unterstützt:

- Intel 82599 10G
- Intel X710 10G
- Intel XL710 40G

## Einschränkungen

Citrix Hypervisor™ unterstützt einige Funktionen auf SR-IOV-Schnittstellen nicht. Die Einschränkungen bei Intel 82599-, Intel X710- und Intel XL710-NICs sind in den folgenden Abschnitten aufgeführt.

### Einschränkungen für Intel 82599 NIC

Die Intel 82599 NIC unterstützt die folgenden Funktionen nicht:

- L2-Modusumschaltung
- Clustering
- Admin-Partitionierung \[Gemeinsamer VLAN-Modus\]
- Hochverfügbarkeit
- Jumbo-Frames
- IPv6-Protokoll in Cluster-Umgebung

### Einschränkungen für Intel X710 10G und Intel XL710 40G NICs

Die Intel X710 10G und Intel XL710 40G NICs weisen die folgenden Einschränkungen auf:

- L2-Modusumschaltung wird nicht unterstützt.
- Administrator-Partitionierung (gemeinsamer VLAN-Modus) wird nicht unterstützt.
- In einem Cluster werden Jumbo-Frames nicht unterstützt, wenn die XL710 NIC als Datenschnittstelle verwendet wird.

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

- Die Reihenfolge der Schnittstellenliste ändert sich, wenn Schnittstellen getrennt und wieder verbunden werden.
- Schnittstellenparameterkonfigurationen wie Geschwindigkeit, Duplex und Auto-Negotiation werden nicht unterstützt.
- Sowohl für Intel X710 10G als auch für Intel XL710 40G NICs wird die Schnittstelle als 40/x-Schnittstelle angezeigt.
- Auf einer VPX-Instanz können nur bis zu 16 Intel X710/XL710 SR-IOV-Schnittstellen unterstützt werden.

**HINWEIS:**

Damit Intel X710 10G und Intel XL710 40G NICs IPv6 unterstützen, aktivieren Sie den Vertrauensmodus für die virtuellen Funktionen (VFs), indem Sie den folgenden Befehl auf dem Citrix Hypervisor-Host eingeben:

```
# ip link set <PNIC> <VF> trust on
```

**Beispiel:**

```
# ip link set ens785f1 vf 0 trust on
```

## Voraussetzungen für Intel 82599 NIC

Stellen Sie auf dem Citrix Hypervisor-Host sicher, dass Sie:

- Fügen Sie die Intel 82599 NIC (NIC) zum Host hinzu.
- Sperren Sie den `ixgbevf` Treiber, indem Sie den folgenden Eintrag zur Datei **/etc/modprobe.d/blacklist.conf** hinzufügen:

  **Blacklist ixgbevf**
- Aktivieren Sie SR-IOV Virtual Functions (VFs), indem Sie den folgenden Eintrag zur Datei **/etc/modprobe.d/ixgbe** hinzufügen:

  **Optionen ixgbe max_vfs=**\<*Anzahl_der_VFs*\>

  wobei \<*number_VFs*\> die Anzahl der SR-IOV VFs ist, die Sie erstellen möchten.
- Stellen Sie sicher, dass SR-IOV im BIOS aktiviert ist.

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

**HINWEIS:**

Es wird die IXGBE-Treiberversion 3.22.3 empfohlen.

## Zuweisen von Intel 82599 SR-IOV VFs zur NetScaler VPX-Instanz über den Citrix Hypervisor-Host

Um Intel 82599 SR-IOV VFs einer NetScaler VPX-Instanz zuzuweisen, führen Sie die folgenden Schritte aus:

1. Verwenden Sie auf dem Citrix Hypervisor-Host den folgenden Befehl, um die SR-IOV VFs der NetScaler VPX-Instanz zuzuweisen:

   **xe host-call-plugin plugin=iovirt host-uuid**=*<Xen-Host-UUID*\> **fn=assign_free_vf args:uuid**=*<NetScaler-VM-UUID*\> **args:ethdev**=*<Schnittstellenname*\> **args:mac=***<Mac-Adresse*\>

   Wo:

   - *<Xen-Host-UUID*\> ist die UUID des Citrix Hypervisor-Hosts.
   - *<NetScaler VM-UUID*\> ist die UUID der NetScaler VPX-Instanz.
   - *<Schnittstellenname*\> ist die Schnittstelle für die SR-IOV VFs.
   - *<MAC-Adresse*\> ist die MAC-Adresse des SR-IOV VF.

   **HINWEIS:**

   Geben Sie die MAC-Adresse an, die Sie im Parameter args:Mac= verwenden möchten. Wenn nicht angegeben, generiert und weist das `iovirt` Skript zufällig eine MAC-Adresse zu. Wenn Sie die SR-IOV VFs im Link-Aggregation-Modus verwenden möchten, stellen Sie außerdem sicher, dass Sie die MAC-Adresse als 00:00:00:00:00:00 angeben.

2. Starten Sie die NetScaler VPX-Instanz.

## Zuweisung von Intel 82599 SR-IOV VFs zur NetScaler VPX-Instanz über den Citrix Hypervisor-Host aufheben

Wenn Sie falsche SR-IOV VFs zugewiesen haben oder zugewiesene SR-IOV VFs ändern möchten, müssen Sie die SR-IOV VFs der NetScaler VPX-Instanz aufheben und neu zuweisen.

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

Um die Zuweisung einer SR-IOV-Netzwerkschnittstelle zu einer NetScaler VPX-Instanz aufzuheben, führen Sie die folgenden Schritte aus:

1. Verwenden Sie auf dem Citrix Hypervisor-Host den folgenden Befehl, um die SR-IOV VFs der NetScaler VPX-Instanz zuzuweisen und die NetScaler VPX-Instanz neu zu starten:

   **xe host-call-plugin plugin**=iovirt **host-uuid**=\<Xen_host_UUID\> **fn**=unassign_all **args:uuid**=\<Netscaler_VM_UUID\>

   Wo:

   - \<Xen_host_UUID\> – Die UUID des Citrix Hypervisor-Hosts.
   - \<Netscaler_VM_UUID\> – Die UUID der NetScaler VPX-Instanz

2. Starten Sie die NetScaler VPX-Instanz.

## Zuweisen von Intel X710/XL710 SR-IOV VFs zur NetScaler VPX-Instanz mithilfe des Citrix Hypervisor-Hosts

Um eine Intel X710/XL710 SR-IOV VF der NetScaler VPX-Instanz zuzuweisen, führen Sie die folgenden Schritte aus:

1. Führen Sie den folgenden Befehl auf dem Citrix Hypervisor-Host aus, um ein Netzwerk zu erstellen.

   ```
   xe network-create name-label=<network-name>
   ```

   **Beispiel:**

   ```
   xe network-create name-label=SR-IOV-NIC-18 8ee59b73-7319-6998-cd69-b9fa3e8d7503
   ```

2. Bestimmen Sie die PIF Universal Unique Identifier (UUID) der NIC, auf der das SR-IOV-Netzwerk konfiguriert werden soll.

   ```
   xe pif-list



              uuid ( RO)  : e2874343-f1de-1fa7-8fef-98547c348783
   ```

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

```
            device ( RO): eth18

currently-attached ( RO): true

              VLAN ( RO): -1

      network-uuid ( RO): f865bd85-44dd-b865-ab65-dcd6ae28c16e
```

3. Konfigurieren Sie das Netzwerk als SR-IOV-Netzwerk. Der folgende Befehl gibt auch die UUID des neu erstellten SR-IOV-Netzwerks zurück:

   ```
   xe network-sriov-create network-uuid=<network-uuid> pif-uuid=<physical-pif-uuid>
   ```

   **Beispiel:**

   ```
   xe network-sriov-create network-uuid=8ee59b73-7319-6998-cd69-b9fa3e8d7503 pif-uuid=e2874343-f1de-1fa7-8fef-98547c3487831629b44f-832a-084e-d67d-5d6d314d5e0f
   ```

   Um weitere Informationen zu den SR-IOV-Netzwerkparametern zu erhalten, führen Sie den folgenden Befehl aus:

   ```
   [root@citrix-XS82-TOPO ~]# xe network-sriov-param-list uuid=1629b44f-832a-084e-d67d-5d6d314d5e0f



              uuid ( RO): 1629b44f-832a-084e-d67d-5d6d314d5e0f

      physical-PIF ( RO): e2874343-f1de-1fa7-8fef-98547c348783

       logical-PIF ( RO): 85d52771-5814-c62d-45fa-f37b536144ff

   requires-reboot ( RO): false

remaining-capacity ( RO): 32
   ```

4. Erstellen Sie eine virtuelle Schnittstelle (VIF) und hängen Sie sie an die Ziel-VM an.

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

```
xe vif-create device=0 mac=b2:61:fc:ae:00:1d network-
uuid=8ee59b73-7319-6998-cd69-b9fa3e8d7503 vm-uuid=b507e8a6-
f5ca-18eb-561d-308218a9dd68

3e1e2e58-b2ad-6dc0-61d4-1d149c9c6466
```

**HINWEIS:**

Die NIC-Indexnummer der VM muss mit 0 beginnen.

Verwenden Sie den folgenden Befehl, um die VM-UUID zu finden:

```
[root@citrix-XS82-TOPO ~]# xe vm-list

uuid ( RO): b507e8a6-f5ca-18eb-561d-308218a9dd68

 name-label ( RW): sai-vpx-1

power-state ( RO): halted
```

## Entfernen von Intel X710/XL710 SR-IOV VFs aus der NetScaler-Instanz mithilfe des Citrix Hypervisor-Hosts

Gehen Sie wie folgt vor, um eine Intel X710/XL710 SR-IOV VF aus einer NetScaler VPX-Instanz zu entfernen:

1. Kopieren Sie die UUID für die VIF, die Sie zerstören möchten.
2. Führen Sie den folgenden Befehl auf dem Citrix Hypervisor-Host aus, um die VIF zu zerstören.

```
xe vif-destroy uuid=<vif-uuid>
```

**Beispiel:**

```
[root@citrix-XS82-TOPO ~]# xe vif-destroy uuid=3e1e2e58-
b2ad-6dc0-61d4-1d149c9c6466
```

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

## Link-Aggregation auf der SR-IOV-Schnittstelle konfigurieren

Um die virtuellen SR-IOV-Funktionen (VFs) im Link-Aggregation-Modus zu verwenden, müssen Sie die Spoof-Prüfung für die von Ihnen erstellten virtuellen Funktionen deaktivieren.

Verwenden Sie auf dem Citrix Hypervisor-Host den folgenden Befehl, um die Spoof-Prüfung zu deaktivieren:

**ip link set** \<*interface*_*name*\> **vf** \<*VF*_*id*\> **spoofchk** off

Dabei gilt:

- \<interface_name\> ist der Schnittstellenname.
- \<VF_id\> ist die ID der virtuellen Funktion.

Nachdem Sie die Spoof-Prüfung für alle von Ihnen erstellten virtuellen Funktionen deaktiviert haben, starten Sie die NetScaler VPX-Instanz neu und konfigurieren Sie die Link-Aggregation. Anweisungen finden Sie unter Link-Aggregation konfigurieren.

**WICHTIG:**

Stellen Sie beim Zuweisen der SR-IOV-VFs zur NetScaler VPX-Instanz sicher, dass Sie die MAC-Adresse 00:00:00:00:00:00 für die VFs angeben.

## VLAN auf der SR-IOV-Schnittstelle konfigurieren

Sie können VLAN auf den virtuellen SR-IOV-Funktionen konfigurieren. Anweisungen finden Sie unter Konfigurieren eines VLANs.

**WICHTIG:**

Stellen Sie sicher, dass der Citrix Hypervisor-Host keine VLAN-Einstellungen für die VF-Schnittstelle enthält.

## Weitere Verweise

SR-IOV-fähige NICs

Ein SR-IOV-Netzwerk hinzufügen

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

# Installieren einer NetScaler VPX-Instanz auf VMware ESX

Bevor Sie NetScaler VPX-Instanzen auf VMware ESX installieren, stellen Sie sicher, dass der VMware ESX Server auf einem Computer mit ausreichenden Systemressourcen installiert ist. Um eine NetScaler VPX-Instanz auf VMware ESXi zu installieren, verwenden Sie den VMware vSphere Client. Der Client oder das Tool muss auf einem Remote-Computer installiert sein, der über das Netzwerk eine Verbindung zu VMware ESX herstellen kann.

Dieser Abschnitt enthält die folgenden Themen:

- Voraussetzungen
- Installieren einer NetScaler VPX-Instanz auf VMware ESX

**WICHTIG:**

Sie können keine standardmäßigen VMware Tools installieren oder die auf einer NetScaler VPX-Instanz verfügbare VMware Tools-Version aktualisieren. VMware Tools für eine NetScaler VPX-Instanz werden als Teil der NetScaler-Softwareversion bereitgestellt.

## Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, führen Sie die folgenden Schritte aus:

- Installieren Sie VMware ESX auf Hardware, die die Mindestanforderungen erfüllt.
- Installieren Sie VMware Client auf einer Verwaltungsarbeitsstation, die die Mindestsystemanforderungen erfüllt.
- Laden Sie die Setup-Dateien der NetScaler VPX-Appliance herunter.
- Erstellen Sie einen virtuellen Switch und verbinden Sie die physische NIC mit dem virtuellen Switch.
- Fügen Sie eine Portgruppe hinzu und verbinden Sie sie mit dem virtuellen Switch.
- Verbinden Sie die Portgruppe mit der VM.

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

- VPX-Lizenzdateien beschaffen. Weitere Informationen zu NetScaler VPX-Instanzlizenzen finden Sie unter Lizenzübersicht.

## Hardwareanforderungen für VMware ESX

Die folgende Tabelle beschreibt die Mindestsystemanforderungen für VMware ESX-Server, auf denen die virtuelle NetScaler VPX nCore-Appliance ausgeführt wird.

Tabelle 1. Mindestsystemanforderungen für einen VMware ESX-Server, auf dem eine NetScaler VPX-Instanz ausgeführt wird

| KOMPONENTE | ANFORDERUNG |
|---|---|
| CPU | 2 oder mehr 64-Bit x86-CPUs mit aktivierter Virtualisierungsunterstützung (Intel-VT). Um eine NetScaler VPX-Instanz auszuführen, muss die Hardwareunterstützung für die Virtualisierung auf dem VMware ESX-Host aktiviert sein. Stellen Sie sicher, dass die BIOS-Option für die Virtualisierungsunterstützung nicht deaktiviert ist. Weitere Informationen finden Sie in Ihrer BIOS-Dokumentation. Ab NetScaler Version 13.1 unterstützt die NetScaler VPX-Instanz auf dem VMware ESXi-Hypervisor AMD-Prozessoren. |
| RAM | 2 GB VPX. Für kritische Bereitstellungen empfehlen wir 2 GB RAM für VPX nicht, da das System in einer speicherbeschränkten Umgebung arbeitet. Dies kann zu Problemen bei Skalierung, Leistung oder Stabilität führen. Empfohlen werden 4 GB RAM oder 8 GB RAM. |
| Festplattenspeicher | 20 GB mehr als die Mindestserveranforderungen von VMware für die Einrichtung von ESXi. Die Mindestserveranforderungen finden Sie in der VMware-Dokumentation. |
| Netzwerk | Eine 1-Gbit/s-NIC (NIC); Zwei 1-Gbit/s-NICs empfohlen |

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

Informationen zur Installation von VMware ESX finden Sie unter `<http://www.vmware.com/>`.

Für die SR-IOV-Netzwerkschnittstelle oder die PCI-Passthrough-Unterstützung stellen Sie sicher, dass die folgenden Prozessoren und Einstellungen aktiviert sind:

- Intel-Prozessoren, die Intel-VT unterstützen
- AMD-Prozessoren, die AMD-V unterstützen
- I/O Memory Management Unit (IOMMU) oder SR-IOV ist im BIOS aktiviert

Die folgenden NICs werden im SR-IOV-Modus unterstützt:

- Mellanox ConnectX-4 NIC, ab NetScaler-Version 13.1-42.x
- Intel 82599 NIC

Die folgende Tabelle listet die virtuellen Computerressourcen auf, die der VMware ESX-Server für jede virtuelle VPX nCore-Appliance bereitstellen muss.

Tabelle 2. Mindestressourcen für virtuelle Computer, die für den Betrieb einer NetScaler VPX-Instanz erforderlich sind

| KOMPONENTE | ANFORDERUNG |
|---|---|
| Arbeitsspeicher | 4 GB |
| Virtuelle CPU (vCPU) | 2 |
| Virtuelle Netzwerkschnittstellen | In ESX können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird. |
| Festplattenspeicher | 20 GB |

**HINWEIS:**

Dies gilt zusätzlich zu allen Festplattenanforderungen für den Hypervisor.

Für den Produktionseinsatz der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden. CPU-Zyklen (in MHz), die mindestens der Geschwindigkeit eines CPU-Kerns des ESX entsprechen, müssen reserviert werden.

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

## Systemanforderungen für den VMware vSphere Client

VMware vSphere ist eine Client-Anwendung, die auf Windows- und Linux-Betriebssystemen ausgeführt werden kann. Sie kann nicht auf derselben Maschine wie der VMware ESX-Server ausgeführt werden. Die folgende Tabelle beschreibt die Mindestsystemanforderungen.

Tabelle 3. Mindestsystemanforderungen für die Installation des VMware vSphere Clients

| KOMPONENTE | ANFORDERUNG |
|---|---|
| Betriebssystem | Detaillierte Anforderungen von VMware finden Sie in der PDF-Datei „vSphere Compatibility Matrixes“ unter `<http://kb.vmware.com/>`. |
| CPU | 750 MHz; 1 Gigahertz (GHz) oder schneller empfohlen |
| RAM | 1 GB. 2 GB empfohlen |
| NIC (NIC) | 100 Mbit/s oder schnellere NIC |

## Systemanforderungen für OVF Tool 1.0

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. Es kann nicht auf derselben Maschine wie der VMware ESX-Server ausgeführt werden. Die folgende Tabelle beschreibt die Mindestsystemanforderungen.

Tabelle 4. Mindestsystemanforderungen für die OVF Tool-Installation

| KOMPONENTE | ANFORDERUNG |
|---|---|
| Betriebssystem | Für detaillierte Anforderungen von VMware suchen Sie nach der PDF-Datei „OVF Tool User Guide“ unter `<http://kb.vmware.com/>`. |
| CPU | Mindestens 750 MHz, 1 GHz oder schneller empfohlen |
| RAM | 1 GB Minimum, 2 GB empfohlen |
| NIC (NIC) | 100 MBit/s oder schnellere Netzwerkkarte |

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

Informationen zur Installation von OVF finden Sie in der PDF-Datei „OVF Tool User Guide“ unter `<http://kb.vmware.com/>`.

### Herunterladen der NetScaler VPX-Setup-Dateien

Das NetScaler VPX-Instanz-Setup-Paket für VMware ESX folgt dem Standard des Open Virtual Machine (OVF)-Formats. Sie können die Dateien von der Citrix-Website herunterladen. Sie benötigen ein Citrix-Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.com auf, klicken Sie auf den Link **Neue Benutzer** und folgen Sie den Anweisungen, um ein Citrix-Konto zu erstellen.

Nach der Anmeldung navigieren Sie auf der Citrix®-Startseite zum folgenden Pfad:

Citrix.com > **Downloads > NetScaler > Virtuelle Appliances**.

Kopieren Sie die folgenden Dateien auf eine Workstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX-\<release number\>-\<build number\>-disk1.vmdk (zum Beispiel, NSVPX-ESX-13.0-71.44_nc_64-disk1.vmdk)
- NSVPX-ESX-\<release number\>-\<build number\>.ovf (zum Beispiel, NSVPX-ESX-13.0-71.44_nc_64.ovf)
- NSVPX-ESX-\<release number\>-\<build number\>.mf (zum Beispiel, NSVPX-ESX-13.0-71.44_nc_64.mf)

## Installieren einer NetScaler VPX-Instanz auf VMware ESX

Nachdem Sie VMware ESX installiert und konfiguriert haben, können Sie den VMware vSphere Client verwenden, um virtuelle Appliances auf dem VMware ESX-Server zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge des verfügbaren Speichers auf der Hardware ab, auf der VMware ESX ausgeführt wird.

Um NetScaler VPX-Instanzen auf VMware ESX mit dem VMware vSphere Client zu installieren, führen Sie die folgenden Schritte aus:

1. Starten Sie den VMware vSphere Client auf Ihrer Arbeitsstation.
2. Geben Sie im Textfeld **IP-Adresse / Name** die IP-Adresse des VMware ESX-Servers ein, mit dem Sie eine Verbindung herstellen möchten.
3. Geben Sie in die Textfelder **Benutzername** und **Passwort** die Administratoranmeldeinformationen ein und klicken Sie dann auf Anmelden.

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

4. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
5. Navigieren Sie im Dialogfeld **OVF-Vorlage bereitstellen** unter **Bereitstellen aus Datei** zu dem Speicherort, an dem Sie die NetScaler VPX-Instanz-Setup-Dateien gespeichert haben, wählen Sie die .ovf-Datei aus und klicken Sie auf **Weiter**.
6. Ordnen Sie die in der OVF-Vorlage der virtuellen Appliance angezeigten Netzwerke den Netzwerken zu, die Sie auf dem ESX-Host konfiguriert haben. Klicken Sie auf **Weiter**, um die Installation einer virtuellen Appliance auf VMware ESX zu starten. Wenn die Installation abgeschlossen ist, informiert Sie ein Pop-up-Fenster über die erfolgreiche Installation.
7. Sie können die NetScaler VPX-Instanz nun starten. Wählen Sie im Navigationsbereich die installierte NetScaler VPX-Instanz aus und wählen Sie im Kontextmenü **Einschalten**.
8. Nachdem die VM gestartet wurde, konfigurieren Sie über die Konsole die NetScaler IP-, Netzmasken- und Gateway-Adressen. Wenn Sie die Konfiguration abgeschlossen haben, wählen Sie die Option **Speichern und Beenden** in der Konsole.
9. Um eine weitere virtuelle Appliance zu installieren, wiederholen Sie die Schritte 6 bis 8.

**HINWEIS:**

Standardmäßig verwendet die NetScaler VPX-Instanz E1000-Netzwerkschnittstellen.

Nach der Installation können Sie den vSphere Client oder vSphere Web Client verwenden, um virtuelle Appliances auf VMware ESX zu verwalten.
Um VLAN-Tagging auf VMware ESX zu aktivieren, konfigurieren Sie die VLAN-ID der Portgruppe auf dem vSwitch auf Alle (4095). Detaillierte Anweisungen zum Festlegen einer VLAN-ID auf dem vSwitch finden Sie in der VMware-Dokumentation.

## Migrieren einer NetScaler VPX-Instanz mit VMware vMotion

Sie können eine NetScaler VPX-Instanz mit VMware vSphere vMotion migrieren.

Beachten Sie die folgenden Nutzungsrichtlinien:

- VMware unterstützt die vMotion-Funktion auf virtuellen Maschinen, die mit PCI-Passthrough- und SR-IOV-Schnittstellen konfiguriert sind, nicht.
- Unterstützte Schnittstellen sind E1000 und VMXNET3. Um vMotion auf Ihrer VPX-Instanz zu verwenden, stellen Sie sicher, dass die Instanz mit einer unterstützten Schnittstelle konfiguriert ist.

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

- Weitere Informationen zur Migration einer Instanz mithilfe von VMware vMotion finden Sie in der VMware-Dokumentation.

## Konfigurieren einer NetScaler VPX-Instanz zur Verwendung der VMXNET3-Netzwerkschnittstelle

Nachdem Sie die NetScaler VPX-Instanz auf dem VMware ESX installiert und konfiguriert haben, können Sie den VMware vSphere Web Client verwenden, um die virtuelle Appliance für die Verwendung von VMXNET3-Netzwerkschnittstellen zu konfigurieren.

So konfigurieren Sie NetScaler VPX-Instanzen für die Verwendung von VMXNET3-Netzwerkschnittstellen mit dem VMware vSphere Web Client:

1. Wählen Sie im vSphere Web Client die Option Hosts und Cluster aus.
2. Aktualisieren Sie die Kompatibilitätseinstellung der NetScaler VPX-Instanz auf ESX, wie folgt:

   a. Schalten Sie die NetScaler VPX-Instanz aus.

   b. Klicken Sie mit der rechten Maustaste auf die NetScaler VPX-Instanz und wählen Sie **Kompatibilität > VM-Kompatibilität aktualisieren**.

   c. Wählen Sie im Dialogfeld **VM-Kompatibilität konfigurieren** aus der Dropdown-Liste „Kompatibel mit“ die Option **ESXi 7.0 und höher** aus und klicken Sie auf **OK**.
3. Klicken Sie mit der rechten Maustaste auf die NetScaler VPX-Instanz und klicken Sie auf **Einstellungen bearbeiten**.

4. Klicken Sie im Dialogfeld \<virtual_appliance\> - Einstellungen bearbeiten auf den Abschnitt **CPU**.

5. Aktualisieren Sie im Abschnitt **CPU** Folgendes:

   - Anzahl der CPUs
   - Anzahl der Sockets
   - Reservierungen
   - Limit
   - Anteile

   Legen Sie die Werte wie folgt fest:

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

a. Wählen Sie im Dropdown-Menü **CPU** die Anzahl der CPUs aus, die der virtuellen Appliance zugewiesen werden sollen.

b. Wählen Sie in der Dropdown-Liste **Kerne pro Socket** die Anzahl der Sockets aus.

c. (Optional) Aktivieren oder deaktivieren Sie im Feld **CPU Hot Plug** das Kontrollkästchen **CPU Hot Add aktivieren**.

**HINWEIS:**

Citrix® empfiehlt, die Standardeinstellung (deaktiviert) zu übernehmen.

d. Wählen Sie in der Dropdown-Liste **Reservierung** die Zahl aus, die als Maximalwert angezeigt wird.

e. Wählen Sie in der Dropdown-Liste Limit die Zahl aus, die als Maximalwert angezeigt wird.

f. Wählen Sie in den Dropdown-Listen Anteile die Option Benutzerdefiniert und die Zahl aus, die als Maximalwert angezeigt wird.

6. Im Abschnitt Arbeitsspeicher aktualisieren Sie Folgendes:

   - Größe des Arbeitsspeichers
   - Reservierungen
   - Grenzwert
   - Anteile

   Legen Sie die Werte wie folgt fest:

   a. Wählen Sie in der Dropdown-Liste RAM die Größe des Arbeitsspeichers aus. Sie muss der Anzahl der vCPUs x 2 GB entsprechen. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, muss der Arbeitsspeicher 4 x 2 GB = 8 GB betragen.

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

**HINWEIS:**

Stellen Sie für eine Advanced- oder Premium-Edition der NetScaler VPX Appliance sicher, dass Sie jedem vCPU 4 GB RAM zuweisen. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, beträgt der RAM 4 x 4 GB = 16 GB.

b. Geben Sie in der Dropdown-Liste Reservierung den Wert für die Speicherreservierung ein und aktivieren Sie das Kontrollkästchen Alle Gastspeicher reservieren (Alle gesperrt). Die Speicherreservierung muss der Anzahl der vCPUs x 2 GB entsprechen. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, muss die Speicherreservierung 4 x 2 GB = 8 GB betragen.

**HINWEIS:**

Stellen Sie für eine Advanced- oder Premium-Edition der NetScaler VPX Appliance sicher, dass Sie jedem vCPU 4 GB RAM zuweisen. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, beträgt der RAM 4 x 4 GB = 16 GB.

c. Wählen Sie in der Dropdown-Liste **Grenzwert** die Zahl aus, die als Maximalwert angezeigt wird.

d. Wählen Sie in der Dropdown-Liste **Shares** die Option **Benutzerdefiniert** und die Zahl, die als Maximalwert angezeigt wird.

7. Fügen Sie eine VMXNET3-Netzwerkschnittstelle hinzu. Wählen Sie in der Dropdown-Liste „Neues Gerät“ „Netzwerk“ aus und klicken Sie auf „Hinzufügen“.

8. Wählen Sie im Abschnitt **Neuer Netzwerkadapter** die Netzwerkschnittstelle aus der Dropdown-Liste aus und führen Sie die folgenden Schritte aus:

   a. Wählen Sie in der Dropdown-Liste **Adaptertyp** die Option **VMXNET3** aus.

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

**WICHTIG:**

Die standardmäßige E1000-Netzwerkschnittstelle und VMXNET3 können nicht koexistieren. Stellen Sie sicher, dass Sie die E1000-Netzwerkschnittstelle entfernen und VMXNET3 (0/1) als Verwaltungsschnittstelle verwenden.

9. Klicken Sie auf **OK**.
10. Starten Sie die NetScaler VPX-Instanz.
11. Sobald die NetScaler VPX-Instanz gestartet ist, können Sie den folgenden Befehl verwenden, um die Konfiguration zu überprüfen:

    Schnittstellenzusammenfassung anzeigen

Die Ausgabe muss alle Schnittstellen anzeigen, die Sie konfiguriert haben:

```
> show interface summary

------------------------------------------------------------------------
------

      Interface  MTU        MAC                Suffix

------------------------------------------------------------------------
------

1     0/1        1500       00:0c:29:89:1d:0e    NetScaler Vir...rface,
VMXNET3

2     1/1        9000       00:0c:29:89:1d:18    NetScaler Vir...rface,
VMXNET3

3     1/2        9000       00:0c:29:89:1d:22    NetScaler Vir...rface,
VMXNET3

4     LO/1       9000       00:0c:29:89:1d:0e    Netscaler Loopback
interface
```

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

**HINWEIS:**

Nachdem Sie mehr als vier VMXNET3-Schnittstellen hinzugefügt und die NetScaler VPX Appliance neu gestartet haben, kann der VMware ESX Hypervisor die Reihenfolge ändern, in der die NIC der VPX Appliance präsentiert wird. Daher bleibt Netzwerkadapter 1 möglicherweise nicht immer 0/1, was zu einem Verlust der Management-Konnektivität zur VPX Appliance führt.

Dies ist eine Einschränkung des VMware ESX Hypervisors.

### Empfangsringgröße für die VMXNET3-Netzwerkschnittstelle festlegen

Sie können die Empfangsringgröße für VMXNET3-Netzwerkschnittstellen auf VMware ESX erhöhen. Eine höhere Ringgröße reduziert Paketverluste, wenn ein plötzlicher Datenverkehrsstoß auftritt.

**HINWEIS:**

Diese Funktion ist in Release 14.1 Build 14.x und höher verfügbar.

#### So legen Sie die Ringgröße auf einer VMXNET3-Netzwerkschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set interface *id* [-ringsize *positive_integer*]
```

Die maximale Ringgröße, die Sie auf einer VMXNET3-Schnittstelle festlegen können, beträgt 2048. Nur der feste Ringtyp wird unterstützt. Sie müssen die Konfiguration speichern und die NetScaler VPX™ Instanz neu starten, damit die Einstellungen wirksam werden.

## Konfigurieren einer NetScaler VPX-Instanz zur Verwendung der SR-IOV-Netzwerkschnittstelle

Nachdem Sie die NetScaler VPX-Instanz auf VMware ESX installiert und konfiguriert haben, können Sie den VMware vSphere Web Client verwenden, um die virtuelle Appliance für die Verwendung von Single Root I/O Virtualization (SR-IOV)-Netzwerkschnittstellen zu konfigurieren.

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

## Einschränkungen

Eine NetScaler VPX, die mit einer SR-IOV-Netzwerkschnittstelle konfiguriert ist, weist die folgenden Einschränkungen auf:

- Die folgenden Funktionen werden auf SR-IOV-Schnittstellen mit der Intel 82599 10G NIC auf ESX VPX nicht unterstützt:
  - L2-Modus-Umschaltung
  - Statische Link-Aggregation und LACP
  - Clustering
  - Administratorpartitionierung \[Shared VLAN mode\]
  - Hochverfügbarkeit
  - Jumbo-Frames
  - IPv6
- Die folgenden Funktionen werden auf der SR-IOV-Schnittstelle mit einer Intel 82599 10G NIC auf KVM VPX nicht unterstützt:
  - Statische Link-Aggregation und LACP
  - L2-Modus-Umschaltung
  - Clustering
  - Admin-Partitionierung \[Shared-VLAN-Modus\]
  - Hochverfügbarkeit
  - Jumbo-Frames
  - IPv6
  - VLAN-Konfiguration auf dem Hypervisor für die SR-IOV VF-Schnittstelle über den `ip link` Befehl wird nicht unterstützt

### Voraussetzung

- Stellen Sie sicher, dass Sie eine der folgenden NICs zum ESX-Host hinzufügen:
  - Intel 82599 NIC, IXGBE Treiberversion 3.7.13.7.14iov oder höher wird empfohlen.
  - Mellanox ConnectX-4 NIC
- Aktivieren Sie SR-IOV auf dem physischen Host-Adapter.

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

Führen Sie die folgenden Schritte aus, um SR-IOV auf dem physischen Host-Adapter zu aktivieren:

a. Navigieren Sie im vSphere Web Client zum Host.

b. Wählen Sie auf der Registerkarte **Verwalten > Netzwerk** die Option **Physische Adapter**. Das Feld SR-IOV-Status zeigt an, ob ein physischer Adapter SR-IOV unterstützt.

c. Wählen Sie den physischen Adapter aus und klicken Sie dann auf das Bleistiftsymbol, um das Dialogfeld **Einstellungen bearbeiten** zu öffnen.

d. Wählen Sie unter SR-IOV aus der Dropdown-Liste **Status** die Option **Aktiviert** aus.

e. Geben Sie im Feld **Anzahl der virtuellen Funktionen** die Anzahl der virtuellen Funktionen ein, die Sie für den Adapter konfigurieren möchten.

f. Klicken Sie auf **OK**.

g. Starten Sie den Host neu.

- Erstellen Sie einen Distributed Virtual Switch (DVS) und `Portgroups`. Anweisungen finden Sie in der VMware-Dokumentation.

  **HINWEIS:**

  Citrix hat die SR-IOV-Konfiguration nur auf DVS und `Portgroups` qualifiziert.

**So konfigurieren Sie NetScaler VPX-Instanzen zur Verwendung der SR-IOV-Netzwerkschnittstelle mithilfe des VMware vSphere Web Client:**

1. Wählen Sie im vSphere Web Client **Hosts und Cluster** aus.
2. Aktualisieren Sie die Kompatibilitätseinstellung der NetScaler VPX-Instanz auf ESX 5.5 oder höher, wie folgt:

   a. Schalten Sie die NetScaler VPX-Instanz aus.

   b. Klicken Sie mit der rechten Maustaste auf die NetScaler VPX-Instanz und wählen Sie **Kompatibilität > VM-Kompatibilität aktualisieren**.

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

c. Wählen Sie im Dialogfeld **VM-Kompatibilität konfigurieren** aus der Dropdown-Liste **Kompatibel mit** die Option **ESXi 5.5 und höher** aus und klicken Sie auf **OK**.

3. Klicken Sie mit der rechten Maustaste auf die NetScaler VPX-Instanz und klicken Sie auf **Einstellungen bearbeiten**.

4. Klicken Sie im Dialogfeld **\<virtuelle_Appliance\> - Einstellungen bearbeiten** auf den Abschnitt **CPU**.

5. Aktualisieren Sie im Abschnitt **CPU** die folgenden Einstellungen:

   - Anzahl der CPUs
   - Anzahl der Sockets
   - Reservierungen
   - Limit
   - Anteile

   Legen Sie die Werte wie folgt fest:

   a. Wählen Sie in der Dropdown-Liste **CPU** die Anzahl der CPUs aus, die der virtuellen Appliance zugewiesen werden sollen.

   b. Wählen Sie in der Dropdown-Liste **Kerne pro Socket** die Anzahl der Sockets aus.

   c. (Optional) Aktivieren oder deaktivieren Sie im Feld **CPU Hot Plug** das Kontrollkästchen **CPU Hot Add aktivieren**.

   **HINWEIS:**

   Citrix® empfiehlt, die Standardeinstellung (deaktiviert) zu übernehmen.

   d. Wählen Sie in der Dropdown-Liste **Reservierung** die Zahl aus, die als Maximalwert angezeigt wird.

   e. Wählen Sie in der Dropdown-Liste **Limit** die Zahl aus, die als Maximalwert angezeigt wird.

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

f. Wählen Sie in den Dropdown-Listen **Shares** die Option **Benutzerdefiniert** und die Zahl aus, die als Maximalwert angezeigt wird.

6. Aktualisieren Sie im Abschnitt **Arbeitsspeicher** die folgenden Einstellungen:

   - Größe des RAM
   - Reservierungen
   - Limit
   - Shares

   Legen Sie die Werte wie folgt fest:

   a. Wählen Sie in der Dropdown-Liste **RAM** die Größe des RAM aus. Sie muss der Anzahl der vCPUs x 2 GB entsprechen. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, dann ist RAM = 4 x 2 GB = 8 GB.

   **HINWEIS:**

   Stellen Sie für die Advanced- oder Premium-Edition der NetScaler VPX Appliance sicher, dass Sie jedem vCPU 4 GB RAM zuweisen. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, dann ist RAM = 4 x 4 GB = 16 GB.

   b. Geben Sie in der Dropdown-Liste **Reservierung** den Wert für die Speicherreservierung ein und aktivieren Sie das Kontrollkästchen **Gesamten Gastspeicher reservieren (Alle gesperrt)**. Die Speicherreservierung muss der Anzahl der vCPUs x 2 GB entsprechen. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, muss die Speicherreservierung 4 x 2 GB = 8 GB betragen.

   **HINWEIS:**

   Stellen Sie für die Advanced- oder Premium-Edition der NetScaler VPX Appliance sicher, dass Sie jedem vCPU 4 GB RAM zuweisen. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, dann ist RAM = 4 x 4 GB = 16 GB.

   c. Wählen Sie in der Dropdown-Liste **Limit** die Zahl aus, die als Maximalwert angezeigt wird.

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

d. Wählen Sie in den Dropdown-Listen **Shares Benutzerdefiniert** aus und wählen Sie die Zahl aus, die als Maximalwert angezeigt wird.

7. Fügen Sie eine SR-IOV-Netzwerkschnittstelle hinzu. Wählen Sie in der Dropdown-Liste **Neues Gerät Netzwerk** aus und klicken Sie auf **Hinzufügen**.

8. Im Abschnitt **Neues Netzwerk**. Wählen Sie aus der Dropdown-Liste die von Ihnen erstellte `Portgroup` aus und führen Sie die folgenden Schritte aus:

   a. Wählen Sie in der Dropdown-Liste **Adaptertyp** die Option **SR-IOV-Passthrough** aus.

   b. Wählen Sie in der Dropdown-Liste **Physische Funktion** den physischen Adapter aus, der der `Portgroup` zugeordnet ist.

   c. Wählen Sie in der Dropdown-Liste **Gast-OS-MTU-Änderung** die Option **Nicht zulassen** aus.

9. Klicken Sie im Dialogfeld **\<virtual_appliance\> - Einstellungen bearbeiten** auf die Registerkarte **VM-Optionen**.

10. Wählen Sie auf der Registerkarte **VM-Optionen** den Abschnitt **Erweitert** aus. Wählen Sie aus der Dropdown-Liste **Latenzempfindlichkeit** die Option **Hoch** aus.

11. Klicken Sie auf **OK**.

12. Schalten Sie die NetScaler VPX-Instanz ein.

13. Nachdem die NetScaler VPX-Instanz eingeschaltet wurde, können Sie den folgenden Befehl verwenden, um die Konfiguration zu überprüfen:

    Schnittstellenübersicht anzeigen

Die Ausgabe muss alle von Ihnen konfigurierten Schnittstellen anzeigen:

```
> show interface summary

---------------------------------------------------------------------------
------

      Interface  MTU        MAC                Suffix
```

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

```
-------------------------------------------------------------------------
------

1     0/1        1500       00:0c:29:1b:81:0b    NetScaler Virtual
Interface

2     10/1       1500       00:50:56:9f:0c:6f    Intel 82599 10G VF
Interface

3     10/2       1500       00:50:56:9f:5c:1e    Intel 82599 10G VF
Interface

4     10/3       1500       00:50:56:9f:02:1b    Intel 82599 10G VF
Interface

5     10/4       1500       00:50:56:9f:5a:1d    Intel 82599 10G VF
Interface

6     10/5       1500       00:50:56:9f:4e:0b    Intel 82599 10G VF
Interface

7     LO/1       1500       00:0c:29:1b:81:0b    Netscaler Loopback
interface

 Done

> show inter 10/1

1)      Interface 10/1 (Intel 82599 10G VF Interface) #1

        flags=0xe460 &lt;ENABLED, UP, UP, HAMON, 802.1q>

        MTU=1500, native vlan=55, MAC=00:50:56:9f:0c:6f, uptime 0h21m53s

        Actual: media FIBER, speed 10000, duplex FULL, fctl NONE,
throughput 10000

        LLDP Mode: NONE,                LR Priority: 1024



        RX: Pkts(838020742) Bytes(860888485431) Errs(0) Drops(2527)
Stalls(0)
```

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

```
        TX: Pkts(838149954) Bytes(860895860507) Errs(0) Drops(0) Stalls(0)

        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)

        Bandwidth thresholds are not set.

Done
```

# Konfigurieren einer NetScaler VPX auf dem ESX-Hypervisor zur Verwendung von Intel QAT für die SSL-Beschleunigung im SR-IOV-Modus

Die NetScaler VPX-Instanz auf dem VMware ESX-Hypervisor kann die Intel QuickAssist Technology (QAT) verwenden, um die NetScaler SSL-Leistung zu beschleunigen. Mithilfe von Intel QAT kann die gesamte kryptografische Verarbeitung mit hoher Latenz auf den Chip ausgelagert werden, wodurch eine oder mehrere Host-CPUs für andere Aufgaben freigegeben werden.

Zuvor wurde die gesamte kryptografische Verarbeitung des NetScaler-Datenpfads in der Software unter Verwendung von Host-vCPUs durchgeführt.

**HINWEIS:**

Derzeit unterstützt NetScaler VPX nur das C62x-Chipmodell der Intel QAT-Familie. Diese Funktion wird ab NetScaler Release 14.1 Build 8.50 unterstützt.

## Voraussetzungen

- Der ESX-Host ist mit einem oder mehreren Intel C62x (QAT)-Chips ausgestattet.
- NetScaler VPX erfüllt die Hardwareanforderungen von VMware ESX. Weitere Informationen finden Sie unter Installieren einer NetScaler VPX-Instanz auf VMware ESX.

## Einschränkungen

Es gibt keine Möglichkeit, Krypto-Einheiten oder Bandbreite für einzelne VMs zu reservieren. Alle verfügbaren Krypto-Einheiten jeder Intel QAT-Hardware werden von allen VMs, die die QAT-Hardware verwenden, gemeinsam genutzt.

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

## Einrichten der Hostumgebung für die Verwendung von Intel QAT

1. Laden Sie den von Intel bereitgestellten VMware-Treiber für das C62x-Serien (QAT)-Chipmodell auf dem VMware-Host herunter und installieren Sie ihn. Weitere Informationen zu den Intel-Paket-Downloads und Installationsanweisungen finden Sie unter Intel QuickAssist Technology Driver for VMware.
2. Aktivieren Sie SR-IOV auf dem ESX-Host.
3. Erstellen Sie virtuelle Maschinen. Weisen Sie beim Erstellen einer VM die entsprechende Anzahl von PCI-Geräten zu, um die Leistungsanforderungen zu erfüllen.

**HINWEIS:**

Jeder C62x (QAT)-Chip kann bis zu drei separate PCI-Endpunkte haben. Jeder Endpunkt ist eine logische Sammlung von VFs und teilt die Bandbreite gleichmäßig mit anderen PCI-Endpunkten des Chips. Jeder Endpunkt kann bis zu 16 VFs haben, die als 16 PCI-Geräte erscheinen. Sie können diese Geräte der VM hinzufügen, um die Krypto-Beschleunigung mit dem QAT-Chip durchzuführen.

## Hinweise

- Wenn die Krypto-Anforderung der VM die Verwendung von mehr als einem QAT-PCI-Endpunkt/Chip vorsieht, wird empfohlen, die entsprechenden PCI-Geräte/VFs im Round-Robin-Verfahren auszuwählen, um eine symmetrische Verteilung zu gewährleisten.
- Es wird empfohlen, dass die Anzahl der ausgewählten PCI-Geräte der Anzahl der lizenzierten vCPUs entspricht (ohne die Anzahl der Management-vCPUs). Das Hinzufügen von mehr PCI-Geräten als die verfügbare Anzahl von vCPUs verbessert die Leistung nicht unbedingt.

  **Beispiel:**

  Betrachten Sie einen ESX-Host mit einem Intel C62x-Chip, der 3 Endpunkte hat. Wenn Sie eine VM mit 6 vCPUs bereitstellen, wählen Sie 2 VFs von jedem Endpunkt aus und weisen Sie diese der VM zu. Diese Art der Zuweisung gewährleistet eine effektive und gleichmäßige Verteilung der Krypto-Einheiten für die VM. Von den insgesamt verfügbaren vCPUs ist standardmäßig eine vCPU für die Management-Ebene reserviert, und die restlichen vCPUs stehen für die Data-Plane-PEs zur Verfügung.

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

### QAT-VFs mit dem vSphere Web Client VPX zuweisen

1. Navigieren Sie im vSphere Web Client zum ESX-Host, auf dem sich die virtuelle Maschine befindet, und klicken Sie auf **Ausschalten**.

2. Navigieren Sie zu **Aktionen > Einstellungen bearbeiten > Anderes Gerät hinzufügen**, und wählen Sie PCI-Gerät aus.

3. Weisen Sie für das neu hinzugefügte PCI-Gerät den c6xx QAT VF zu und speichern Sie die Konfiguration.

4. Schalten Sie die VM erneut ein.
5. Führen Sie den Befehl `stat ssl` in der NetScaler CLI aus, um die SSL-Zusammenfassung anzuzeigen und die SSL-Karten nach der Zuweisung von QAT VFs zu VPX zu überprüfen.

### Informationen zur Bereitstellung

Diese Bereitstellung wurde mit den folgenden Komponentenspezifikationen getestet:

- **NetScaler VPX Version und Build:** 14.1–8.50
- **VMware ESXi Version:** 7.0.3 (Build 20036589)
- **Intel C62x QAT Treiberversion für VMware:** 1.5.1.54

## Migration der NetScaler VPX von E1000 auf SR-IOV- oder VMXNET3-Netzwerkschnittstellen

May 24, 2018

Sie können Ihre bestehenden NetScaler VPX-Instanzen, die E1000-Netzwerkschnittstellen verwenden, so konfigurieren, dass sie SR-IOV- oder VMXNET3-Netzwerkschnittstellen verwenden.

Informationen zum Konfigurieren einer bestehenden NetScaler VPX-Instanz zur Verwendung von SR-IOV-Netzwerkschnittstellen finden Sie unter Konfigurieren einer NetScaler VPX-Instanz zur Verwendung von SR-IOV-Netzwerkschnittstellen.

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

Informationen zum Konfigurieren einer bestehenden NetScaler VPX-Instanz zur Verwendung von VMXNET3-Netzwerkschnittstellen finden Sie unter Konfigurieren einer NetScaler VPX-Instanz zur Verwendung von VMXNET3-Netzwerkschnittstellen.

# Eine NetScaler VPX-Instanz zur Verwendung von PCI-Passthrough-Netzwerkschnittstellen konfigurieren

## Übersicht

Nachdem Sie eine NetScaler VPX-Instanz auf VMware ESX Server installiert und konfiguriert haben, können Sie den vSphere Web Client verwenden, um die virtuelle Appliance für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen zu konfigurieren.

Die PCI-Passthrough-Funktion ermöglicht einer Gast-VM den direkten Zugriff auf physische PCI- und PCIe-Geräte, die mit einem Host verbunden sind.

## Voraussetzungen

- Die Firmware-Version der Intel XL710 NIC auf dem Host ist 5.04.
- Ein PCI-Passthrough-Gerät, das mit dem Host verbunden und auf diesem konfiguriert ist
- Unterstützte NICs:
  - Intel X710 10G NIC
  - Intel XL710 Dual-Port 40G NIC
  - Intel XL710 Single-Port 40G NIC
  - Intel XXV710 Dual-Port 25G NIC

## Passthrough-Geräte auf einem Host konfigurieren

Bevor Sie ein Passthrough-PCI-Gerät auf einer virtuellen Maschine konfigurieren, müssen Sie es auf der Hostmaschine konfigurieren. Führen Sie die folgenden Schritte aus, um Passthrough-Geräte auf einem Host zu konfigurieren.

1. Wählen Sie den Host im Navigator-Panel des vSphere Web Client aus.
2. Klicken Sie auf **Verwalten** > **Einstellungen** > **PCI-Geräte**. Alle verfügbaren Passthrough-Geräte werden angezeigt.
3. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.

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

4. Das Fenster **PCI-Geräteverfügbarkeit bearbeiten** wird angezeigt.
5. Wählen Sie die Geräte aus, die für Passthrough verwendet werden sollen, und klicken Sie auf **OK**.

6. Starten Sie die Hostmaschine neu.

## Konfigurieren von Passthrough-Geräten auf einer NetScaler VPX-Instanz

Führen Sie die folgenden Schritte aus, um ein Passthrough-PCI-Gerät auf einer NetScaler VPX-Instanz zu konfigurieren.

1. Schalten Sie die virtuelle Maschine aus.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** im Dropdown-Menü **Neues Gerät** die Option **PCI-Gerät** aus und klicken Sie auf **Hinzufügen**.

4. erweitern **Neues PCI-Gerät**, wählen Sie das Passthrough-Gerät aus, das mit der virtuellen Maschine verbunden werden soll, aus der Dropdown-Liste und klicken Sie auf **OK**.

**HINWEIS:**

VMXNET3-Netzwerkschnittstelle und PCI-Passthrough-Netzwerkschnittstelle können nicht koexistieren.

5. Starten Sie die Gast-VM.

Sie haben die Schritte zur Konfiguration von NetScaler VPX zur Verwendung von PCI-Passthrough-Netzwerkschnittstellen abgeschlossen.

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

# NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance auf dem VMware ESX-Hypervisor anwenden

Sie können die NetScaler VPX-Konfigurationen während des ersten Starts der NetScaler-Appliance auf dem VMware ESX-Hypervisor anwenden. Daher wird in bestimmten Fällen ein bestimmtes Setup oder eine VPX-Instanz in wesentlich kürzerer Zeit hochgefahren.

Weitere Informationen zu Preboot-Benutzerdaten und deren Format finden Sie unter NetScaler VPX-Konfigurationen beim ersten Start der NetScaler-Appliance in der Cloud anwenden.

**HINWEIS:**

Um mit Preboot-Benutzerdaten in ESX zu booten, muss die Standard-Gateway-Konfiguration im Abschnitt `<NS-CONFIG>` übergeben werden. Weitere Informationen zum Inhalt des Tags `<NS-CONFIG>` finden Sie unter Beispiel- `<NS-CONFIG>` -Abschnitt.

**Beispiel- `<NS-CONFIG>` -Abschnitt:**

```
<NS-PRE-BOOT-CONFIG>


    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0  10.102.38.1
    </NS-CONFIG>


    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>


        <MGMT-INTERFACE-CONFIG>
```

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

```
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>

                <IP> 10.102.38.216 </IP>

                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>

        </MGMT-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>



</NS-PRE-BOOT-CONFIG>
```

## Bereitstellen von Preboot-Benutzerdaten auf dem ESX-Hypervisor

Sie können Preboot-Benutzerdaten auf dem ESX-Hypervisor über den Webclient oder vSphere Client auf die folgenden zwei Arten bereitstellen:

- Verwenden von CD/DVD-ISO
- Verwenden der OVF-Eigenschaft

## Benutzerdaten mithilfe von CD/DVD-ISO bereitstellen

Sie können den VMware vSphere Client verwenden, um Benutzerdaten als ISO-Image über das CD/DVD-Laufwerk in die VM zu einschleusen.

Führen Sie die folgenden Schritte aus, um Benutzerdaten mithilfe des CD/DVD-ISO bereitzustellen:

1. Erstellen Sie eine Datei mit dem Dateinamen `userdata`, die den Inhalt der Preboot-Benutzerdaten enthält. Weitere Informationen zum Inhalt des Tags `<NS-CONFIG>` finden Sie unter Beispiel-`<NS-CONFIG>`-Abschnitt.

   **HINWEIS:**

   Der Dateiname muss strengstens als `userdata` verwendet werden.

2. Speichern Sie die `userdata`-Datei in einem Ordner und erstellen Sie ein ISO-Image mit diesem Ordner.

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

Sie können ein ISO-Image mit der `userdata`-Datei auf die folgenden zwei Arten erstellen:

- Verwenden eines Bildverarbeitungstools wie PowerISO.
- Verwenden des `mkisofs`-Befehls unter Linux.

Die folgende Beispielkonfiguration zeigt, wie ein ISO-Image mit dem `mkisofs`-Befehl unter Linux generiert wird.

```
root@ubuntu:~/sai/14jul2021# ls -l total 4

drwxr-xr-x 2 root root 4096 Jul 14 12:32 esx_preboot_userdata

root@ubuntu:~/sai/14jul2021#

root@ubuntu:~/sai/14jul2021# ls -l esx_preboot_userdata/total 4

-rw-r--r-- 1 root root 3016 Jul 14 12:32 userdata

root@ubuntu:~/sai/14jul2021# mkisofs -o esx_preboot_userdata.iso ./
esx_preboot_userdata

I: -input-charset not specified, using utf-8 (detected in locale
settings)

Total translation table size: 0

Total rockridge attributes bytes: 0

Total directory bytes: 112

Path table size(bytes): 10

Max brk space used 0

176 extents written (0 MB)

root@ubuntu:~/sai/14jul2021# ls -lh

total 356K

drwxr-xr-x 2 root root 4.0K Jul 14 12:32 esx_preboot_userdata

-rw-r--r-- 1 root root 352K Jul 14 12:34 esx_preboot_userdata.iso
```

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

```
root@ubuntu:~/sai# ls preboot_userdata_155_193 userdata

root@ubuntu:~/sai# mkisofs -o preboot_userdata_155_193.iso ./
preboot_userdata_155_193

I: -input-charset not specified, using utf-8 (detected in locale
settings)

Total translation table size: 0

Total rockridge attributes bytes: 0

Total directory bytes: 112

Path table size(bytes): 10

Max brk space used 0

176 extents written (0 MB)
```

3. Stellen Sie die NetScaler VPX-Instanz mithilfe des Standardbereitstellungsprozesses bereit, um die VM zu erstellen. Schalten Sie die VM jedoch nicht automatisch ein.

4. Nachdem die VM erfolgreich erstellt wurde, hängen Sie die ISO-Datei als CD/DVD-Laufwerk an die VM an.

5. Navigieren Sie zu **Neues CD/DVD-Laufwerk** und wählen Sie **Datastore-ISO-Datei** aus dem Dropdown-Menü.

6. Wählen Sie einen Datastore im vSphere Client aus.

7. Schalten Sie die VM ein.

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

## Benutzerdaten mithilfe der OVF-Eigenschaft über den ESX-Webclient bereitstellen

Führen Sie die folgenden Schritte aus, um Benutzerdaten mithilfe der OVF-Eigenschaft bereitzustellen.

1. Erstellen Sie eine Datei mit Benutzerdateninhalt.

2. Kodieren Sie den Benutzerdateninhalt mit Base64-Kodierung. Sie können die Base64-Kodierung mithilfe der folgenden zwei Methoden durchführen:

   - Unter Linux verwenden Sie den folgenden Befehl:

     ```
     base64 <userdata-filename>  >   <outuput-file>
     ```

     **Beispiel:**

     ```
     base64 esx_userdata.xml  > esx_userdata_b64
     ```

   - Verwenden Sie Online-Tools, um Benutzerdateninhalt zu kodieren, zum Beispiel Base64 Encode and Decode.

3. Fügen Sie einen **Product**-Abschnitt in die OVF-Vorlage einer NetScaler VPX-Instanz auf dem ESX-Hypervisor ein.

   **Beispiel für den Product-Abschnitt:**

```
<ProductSection>



  <Info>Information about the installed software</Info>

  <Product>NSVPX-VSK Template</Product>

  <Vendor>Citrix</Vendor>

  <VendorUrl>www.citrix.com</VendorUrl>

  <Category> Preboot Userdata </Category>
```

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

```
  <Property ovf:key="guestinfo.userdata" ovf:type="string"
ovf:userConfigurable="true" ovf:value="">


    <Label>Userdata</Label>

    <Description> Userdata for ESX VPX </Description>

  </Property>


</ProductSection>
```

4. Geben Sie die Base64-kodierten Benutzerdaten als `ovf:value` für die `guestinfo.userdata`-Eigenschaft im Product-Abschnitt an.

```
<ProductSection>


  <Info>Information about the installed software</Info>

  <Product>NSVPX-VSK Template</Product>

  <Vendor>Citrix</Vendor>

  <VendorUrl>www.citrix.com</VendorUrl>

  <Category> Preboot Userdata </Category>

  <Property ovf:key="guestinfo.userdata" ovf:type="string"
ovf:userConfigurable="true"


ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+CglhZGQgcm91
dGUgMC4wLjAuMCAw


```

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

```
LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkF
QPgog


ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1
CT09U


U1RSQVA+CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJ
PT1RT


VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICA
gICAg


ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAgICA
gICAg


ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5
FVC1N


QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgICAgPC9NR01ULUlOVEV
SRkFD


RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg==
">



    <Label>Userdata</Label>

    <Description> Userdata for ESX VPX </Description>

  </Property>



</ProductSection>
```

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

5. Verwenden Sie die geänderte OVF-Vorlage mit Product-Abschnitt für die VM-Bereitstellung.

## Benutzerdaten mithilfe der OVF-Eigenschaft über den ESX vSphere Client bereitstellen

Führen Sie die folgenden Schritte aus, um Benutzerdaten mithilfe der OVF-Eigenschaft vom ESX vSphere Client bereitzustellen.

1. Erstellen Sie eine Datei mit Benutzerdateninhalt.

2. Codieren Sie den Benutzerdateninhalt mit Base64-Codierung. Sie können die Base64-Codierung mit den folgenden zwei Methoden durchführen:

   - Verwenden Sie unter Linux den folgenden Befehl:

     ```
     base64 <userdata-filename>  >   <outuput-file>
     ```

     **Beispiel:**

     ```
     base64 esx_userdata.xml  > esx_userdata_b64
     ```

   - Verwenden Sie Online-Tools, um Benutzerdateninhalte zu codieren, zum Beispiel Base64 Encode and Decode.

3. Fügen Sie einen **Produkt**-Abschnitt in die OVF-Vorlage einer NetScaler VPX-Instanz auf dem ESX-Hypervisor ein.

   **Beispiel Produktabschnitt:**

```
<ProductSection>



  <Info>Information about the installed software</Info>

  <Product>NSVPX-VSK Template</Product>

  <Vendor>Citrix</Vendor>
```

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

```
  <VendorUrl>www.citrix.com</VendorUrl>

  <Category> Preboot Userdata </Category>



  <Property ovf:key="guestinfo.userdata" ovf:type="string"
ovf:userConfigurable="true" ovf:value="">



    <Label>Userdata</Label>

    <Description> Userdata for ESX VPX </Description>

  </Property>



</ProductSection>
```

4. Geben Sie die Base64-codierten Benutzerdaten als `ovf:value` für die Eigenschaft `guestinfo.userdata` im Produktabschnitt an.

```
<ProductSection>



  <Info>Information about the installed software</Info>

  <Product>NSVPX-VSK Template</Product>

  <Vendor>Citrix</Vendor>

  <VendorUrl>www.Citrix.com</VendorUrl>

  <Category> Preboot Userdata </Category>

  <Property ovf:key="guestinfo.userdata" ovf:type="string"
ovf:userConfigurable="true"
```

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

```
ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+CglhZGQgcm91
dGUgMC4wLjAuMCAw

LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkF
QPgog

ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1
CT09U

U1RSQVA+CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJ
PT1RT

VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICA
gICAg

ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICA
gICAg

ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgPFNVQk5
FVC1N

QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULUlOVEV
SRkFD

RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg=
=">



    <Label>Userdata</Label>

    <Description> Userdata for ESX VPX </Description>

  </Property>
```

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

```
</ProductSection>
```

5. Fügen Sie die Eigenschaft `ovf:transport="com.vmware.guestInfo"` wie folgt zu VirtualHardwareSection hinzu:

```
<VirtualHardwareSection  ovf:transport="com.vmware.guestInfo">
```

6. Verwenden Sie die geänderte OVF-Vorlage mit dem Produktabschnitt für die VM-Bereitstellung.

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

# Installieren einer NetScaler VPX-Instanz in der VMware Cloud auf AWS

Die VMware Cloud (VMC) auf AWS ermöglicht es Ihnen, Cloud-Software-definierte Rechenzentren (SDDC) auf AWS mit der gewünschten Anzahl von ESX-Hosts zu erstellen. Die VMC auf AWS unterstützt NetScaler VPX-Bereitstellungen. VMC bietet eine Benutzeroberfläche, die der von lokalen vCenter-Instanzen gleicht. Sie funktioniert identisch mit den ESX-basierten NetScaler VPX-Bereitstellungen.

## Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, führen Sie die folgenden Schritte aus:

- Ein VMware SDDC muss mit mindestens einem Host vorhanden sein.
- Laden Sie die Setup-Dateien der NetScaler VPX-Appliance herunter.
- Erstellen Sie auf dem VMware SDDC geeignete Netzwerksegmente, mit denen sich die virtuellen Maschinen verbinden.
- Besorgen Sie VPX-Lizenzdateien. Weitere Informationen zu NetScaler VPX-Instanzlizenzen finden Sie im *NetScaler VPX Licensing Guide* unter </de-de/licensing/licensing-guide-for-netscaler.html>.

## Hardwareanforderungen für VMware Cloud

Die folgende Tabelle listet die virtuellen Computerressourcen auf, die das VMware SDDC für jede virtuelle VPX nCore-Appliance bereitstellen muss.

Tabelle 1. Mindestanforderungen an virtuelle Computerressourcen für den Betrieb einer NetScaler VPX-Instanz

| KOMPONENTE | ANFORDERUNG |
|---|---|
| Arbeitsspeicher | 2 GB |
| Virtuelle CPU (vCPU) | 2 |

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

| KOMPONENTE | ANFORDERUNG |
| --- | --- |
| Virtuelle Netzwerkschnittstellen | In VMware SDDC können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird. |
| Festplattenspeicher | 20 GB |

**HINWEIS:**

Dies gilt zusätzlich zu allen Festplattenanforderungen für den Hypervisor.

Für den Produktionseinsatz der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden.

## OVF Tool 1.0 Systemanforderungen

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. Die folgende Tabelle beschreibt die Mindestsystemanforderungen.

Tabelle 2. Mindestsystemanforderungen für die OVF-Tool-Installation

| KOMPONENTE | ANFORDERUNG |
| --- | --- |
| Betriebssystem | Detaillierte Anforderungen von VMware finden Sie in der PDF-Datei „OVF Tool User Guide“ unter `<http://kb.vmware.com/>`. |
| CPU | 750 MHz Minimum, 1 GHz oder schneller empfohlen |
| RAM | 1 GB Minimum, 2 GB empfohlen |
| NIC | 100 Mbit/s oder schnellere NIC |

Informationen zur Installation von OVF finden Sie in der PDF-Datei „OVF Tool User Guide“ unter `<http://kb.vmware.com/>`.

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

# Herunterladen der NetScaler VPX-Setup-Dateien

Das NetScaler VPX-Instanz-Setup-Paket für VMware ESX folgt dem Open Virtual Machine (OVF)-Formatstandard. Sie können die Dateien von der Citrix-Website herunterladen. Sie benötigen ein Citrix-Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.com auf. Klicken Sie auf den Link **New Users** und folgen Sie den Anweisungen, um ein neues Citrix-Konto zu erstellen.

Nach der Anmeldung navigieren Sie auf der Citrix®-Startseite über den folgenden Pfad:

Citrix.com > **Downloads > NetScaler > Virtual Appliances**.

Kopieren Sie die folgenden Dateien auf eine Workstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX-\<release number\>-\<build number\>-disk1.vmdk (zum Beispiel NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX-\<release number\>-\<build number\>.ovf (zum Beispiel NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX-\<release number\>-\<build number\>.mf (zum Beispiel NSVPX-ESX-13.0-79.64.mf)

# Installieren einer NetScaler VPX-Instanz in der VMware Cloud

Nachdem Sie VMware SDDC installiert und konfiguriert haben, können Sie das SDDC verwenden, um virtuelle Appliances in der VMware Cloud zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der im SDDC verfügbaren Speichermenge ab.

Um NetScaler VPX-Instanzen in der VMware Cloud zu installieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie VMware SDDC auf Ihrer Workstation.
2. Geben Sie in den Textfeldern **Benutzername** und **Passwort** die Administratoranmeldeinformationen ein und klicken Sie dann auf Anmelden.
3. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
4. Suchen Sie im Dialogfeld **OVF-Vorlage bereitstellen** unter **Aus Datei bereitstellen** den Speicherort, an dem Sie die Setup-Dateien der NetScaler VPX-Instanz gespeichert haben, wählen Sie die .ovf-Datei aus und klicken Sie auf **Weiter**.

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

**HINWEIS:**

Standardmäßig verwendet die NetScaler VPX-Instanz E1000-Netzwerkschnittstellen. Um ADC mit der VMXNET3-Schnittstelle bereitzustellen, ändern Sie die OVF so, dass die VMXNET3-Schnittstelle anstelle von E1000 verwendet wird.

5. Ordnen Sie die in der OVF-Vorlage der virtuellen Appliance angezeigten Netzwerke den Netzwerken zu, die Sie im VMware SDDC konfiguriert haben. Klicken Sie auf **Weiter**, um die Installation einer virtuellen Appliance im VMware SDDC zu starten.
6. Sie können die NetScaler VPX-Instanz nun starten. Wählen Sie im Navigationsbereich die installierte NetScaler VPX-Instanz aus und wählen Sie im Kontextmenü **Einschalten** aus. Klicken Sie auf die Registerkarte **Konsole**, um einen Konsolenport zu emulieren.
7. Wenn Sie eine weitere virtuelle Appliance installieren möchten, wiederholen Sie den Vorgang ab Schritt 6.
8. Geben Sie die Management-IP-Adresse aus demselben Segment an, das als Management-Netzwerk ausgewählt ist. Dasselbe Subnetz wird für das Gateway verwendet.
9. Das VMware SDDC erfordert, dass NAT- und Firewall-Regeln explizit für alle privaten IP-Adressen erstellt werden, die zu Netzwerksegmenten gehören.

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

# Installieren einer NetScaler VPX-Instanz auf einem Microsoft Hyper-V-Server

Um NetScaler VPX-Instanzen auf Microsoft Windows Server zu installieren, müssen Sie zunächst Windows Server mit aktivierter Hyper-V-Rolle auf einem Computer mit ausreichenden Systemressourcen installieren. Achten Sie bei der Installation der Hyper-V-Rolle darauf, die NICs auf dem Server anzugeben, die Hyper-V zum Erstellen der virtuellen Netzwerke verwendet. Sie können einige NICs für den Host reservieren. Verwenden Sie den Hyper-V-Manager, um die Installation der NetScaler VPX-Instanz durchzuführen.

Die NetScaler VPX-Instanz für Hyper-V wird im Format einer virtuellen Festplatte (VHD) bereitgestellt. Sie enthält die Standardkonfiguration für Elemente wie CPU, Netzwerkschnittstellen sowie Festplattengröße und -format. Nach der Installation der NetScaler VPX-Instanz können Sie die Netzwerkadapter auf einer virtuellen Appliance konfigurieren, virtuelle NICs hinzufügen und dann die NetScaler IP-Adresse, Subnetzmaske und das Gateway zuweisen und die grundlegende Konfiguration der virtuellen Appliance abschließen.

Wenn Sie die Appliance nach der Erstkonfiguration der VPX-Instanz auf die neueste Softwareversion aktualisieren möchten, lesen Sie Aktualisieren einer eigenständigen NetScaler VPX-Appliance

**HINWEIS:**

Das Intermediate System-to-Intermediate System (ISIS)-Protokoll wird auf der NetScaler VPX Virtual Appliance, die auf der HyperV-2012-Plattform gehostet wird, nicht unterstützt.

## Voraussetzungen für die Installation der NetScaler VPX-Instanz auf Microsoft-Servern

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, führen Sie die folgenden Schritte aus:

- Aktivieren Sie die Hyper-V-Rolle auf Windows-Servern. Weitere Informationen finden Sie unter `<http://technet.microsoft.com/de-de/library/ee344837(WS.10).aspx>`.
- Laden Sie die Setup-Dateien der virtuellen Appliance herunter.

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

- Besorgen Sie sich NetScaler VPX-Instanz-Lizenzdateien. Weitere Informationen zu NetScaler VPX-Instanz-Lizenzen finden Sie im *NetScaler VPX Licensing Guide* unter `<https://support.citrix.com/s/article/CTX255959-how-to-allocate-and-install-citrix-netscaler-vpx-licenses?language=en_US>`.

## Hardwareanforderungen für Microsoft-Server

Die folgende Tabelle beschreibt die Mindestsystemanforderungen für Microsoft-Server.

Tabelle 1. Mindestsystemanforderungen für Microsoft-Server

| KOMPONENTE | ANFORDERUNG |
|---|---|
| CPU | 1,4 GHz 64-Bit-Prozessor |
| RAM | 8 GB |
| Festplattenspeicher | 32 GB oder mehr |

Die folgende Tabelle listet die virtuellen Computerressourcen für jede NetScaler VPX-Instanz auf.

Tabelle 2. Mindestanforderungen an virtuelle Computerressourcen für den Betrieb einer NetScaler VPX-Instanz

| KOMPONENTE | ANFORDERUNG |
|---|---|
| RAM | 4 GB |
| Virtuelle CPU | 2 |
| Festplattenspeicher | 20 GB |
| Virtuelle Netzwerkschnittstellen | 1 |

## Herunterladen der NetScaler VPX-Setup-Dateien

Die NetScaler VPX-Instanz für Hyper-V wird im VHD-Format (Virtual Hard Disk) bereitgestellt. Sie können die Dateien von der Citrix-Website herunterladen. Sie benötigen ein Citrix-Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Homepage unter http://www.citrix.com auf, klicken Sie auf **Anmelden > Mein Konto > Citrix-Konto erstellen**, und befolgen Sie die Anweisungen zum Erstellen eines Citrix-Kontos.

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

Gehen Sie wie folgt vor, um die Setup-Dateien der NetScaler VPX-Instanz herunterzuladen:

1. Gehen Sie in einem Webbrowser zu `<http://www.citrix.com/>`.
2. Melden Sie sich mit Ihrem Benutzernamen und Kennwort an.
3. Klicken Sie auf **Downloads**.
4. Wählen Sie im Dropdown-Menü **Produkt auswählen** die Option **NetScaler (NetScaler ADC)** aus.
5. Klicken Sie unter **NetScaler Release X.X > Virtuelle Appliances** auf **NetScaler VPX Release X.X**
6. Laden Sie die komprimierte Datei auf Ihren Server herunter.

# Installieren der NetScaler VPX-Instanz auf Microsoft-Servern

Nachdem Sie die Hyper-V-Rolle auf dem Microsoft Server aktiviert und die Dateien der virtuellen Appliance extrahiert haben, können Sie den Hyper-V-Manager verwenden, um die NetScaler VPX-Instanz zu installieren. Nach dem Import der virtuellen Maschine müssen Sie die virtuellen NICs konfigurieren, indem Sie sie den von Hyper-V erstellten virtuellen Netzwerken zuordnen.

Sie können maximal acht virtuelle NICs konfigurieren. Auch wenn die physische NIC AUS ist, geht die virtuelle Appliance davon aus, dass die virtuelle NIC AN ist, da sie weiterhin mit den anderen virtuellen Appliances auf demselben Host (Server) kommunizieren kann.

**HINWEIS:**

Sie können keine Einstellungen ändern, während die virtuelle Appliance läuft. Fahren Sie die virtuelle Appliance herunter und nehmen Sie dann die Änderungen vor.

**So installieren Sie eine NetScaler VPX-Instanz auf einem Microsoft Server mithilfe des Hyper-V-Managers:**

1. Um den Hyper-V-Manager zu starten, klicken Sie auf **Start**, zeigen Sie auf **Verwaltung** und klicken Sie dann auf **Hyper-V-Manager**.
2. Wählen Sie im Navigationsbereich unter **Hyper-V-Manager** den Server aus, auf dem Sie die NetScaler VPX-Instanz installieren möchten.
3. Klicken Sie im Menü **Aktion** auf **Virtuelle Maschine importieren**.

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

4. Geben Sie im Dialogfeld **Virtuelle Maschine importieren** unter **Speicherort** den Pfad des Ordners an, der die Softwaredateien der NetScaler VPX-Instanz enthält, und wählen Sie dann **Virtuelle Maschine kopieren (neue eindeutige ID erstellen)**. Dieser Ordner ist der übergeordnete Ordner, der die Ordner Snapshots, Virtuelle Festplatten und Virtuelle Maschinen enthält.

**HINWEIS:**

Wenn Sie eine komprimierte Datei erhalten haben, stellen Sie sicher, dass Sie die Dateien in einen Ordner extrahieren, bevor Sie den Pfad zum Ordner angeben.

1. Klicken Sie auf **Importieren**.
2. Vergewissern Sie sich, dass die von Ihnen importierte virtuelle Appliance unter **Virtuelle Maschinen** aufgeführt ist.
3. Um eine weitere virtuelle Appliance zu installieren, wiederholen Sie die Schritte **2** bis **6**.

**WICHTIG:**

Stellen Sie sicher, dass Sie die Dateien in Schritt **4** in einen anderen Ordner extrahieren.

## Automatische Bereitstellung einer NetScaler VPX-Instanz auf Hyper-V

Die automatische Bereitstellung der NetScaler VPX-Instanz ist optional. Wenn die automatische Bereitstellung nicht erfolgt ist, bietet die virtuelle Appliance eine Option zur Konfiguration der IP-Adresse usw.

Um eine NetScaler VPX-Instanz auf Hyper-V automatisch bereitzustellen, führen Sie die folgenden Schritte aus.

1. Erstellen Sie ein ISO9660-kompatibles ISO-Image unter Verwendung der XML-Datei, wie im Beispiel dargestellt. Stellen Sie sicher, dass der Name der XML-Datei **userdata** lautet.

   Sie können eine ISO-Datei aus einer XML-Datei erstellen, indem Sie Folgendes verwenden:

   • Jedes Bildverarbeitungstool wie PowerISO.

   • `mkisofs`-Befehl in Linux.

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

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<Environment xmlns:oe=`"http://schemas.dmtf.org/ovf/environment/1`"

xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"

oe:id=""

xmlns=`"http://schemas.dmtf.org/ovf/environment/1`">

<PlatformSection>

<Kind>HYPER-V</Kind>

<Version>2013.1</Version>

<Vendor>CITRIX</Vendor>

<Locale>en</Locale>

</PlatformSection>
```

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

```
<PropertySection>


<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>


<Property oe:key="com.citrix.netscaler.platform" oe:value="NS1000V"/>


<Property oe:key="com.citrix.netscaler.orch\_env" oe:value="cisco-orch-
env"/>


<Property oe:key="com.citrix.netscaler.mgmt.ip"
oe:value="10.102.100.122"/>


<Property oe:key="com.citrix.netscaler.mgmt.netmask"
oe:value="255.255.255.128"/>


<Property oe:key="com.citrix.netscaler.mgmt.gateway"
oe:value="10.102.100.67"/></PropertySection>


</Environment>
```

2. Kopieren Sie das ISO-Image auf den Hyper-V-Server.
3. Wählen Sie die importierte virtuelle Appliance aus, und wählen Sie dann im Menü **Aktion** die Option **Einstellungen**. Sie können die virtuelle Appliance auch auswählen, dann mit der rechten Maustaste klicken und **Einstellungen** auswählen. Das Fenster **Einstellungen** für die ausgewählte virtuelle Appliance wird angezeigt.
4. Klicken Sie im Fenster **Einstellungen** unter dem Abschnitt Hardware auf **IDE-Controller**.

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

5. Wählen Sie im rechten Fensterbereich **DVD-Laufwerk** aus und klicken Sie auf **Hinzufügen**. Das DVD-Laufwerk wird im linken Fensterbereich unter dem Abschnitt **IDE-Controller** hinzugefügt.
6. Wählen Sie das in Schritt 5 hinzugefügte **DVD-Laufwerk** aus. Wählen Sie im rechten Fensterbereich die Optionsschaltfläche **Image-Datei** aus, klicken Sie auf **Durchsuchen** und wählen Sie das ISO-Image aus, das Sie in Schritt 2 auf den Hyper-V-Server kopiert haben.
7. Klicken Sie auf **Übernehmen**.

**HINWEIS:**

Die Instanz der virtuellen Appliance wird mit der Standard-IP-Adresse gestartet, wenn:

- Das DVD-Laufwerk ist angeschlossen und die ISO-Datei wird nicht bereitgestellt.
- Die ISO-Datei enthält die Benutzerdatendatei nicht.
- Der Name oder das Format der Benutzerdatendatei ist nicht korrekt.

Führen Sie die folgenden Schritte aus, um virtuelle NICs auf der NetScaler VPX-Instanz zu konfigurieren:

1. Wählen Sie die virtuelle Appliance aus, die Sie importiert haben, und wählen Sie dann im Menü **Aktion** die Option **Einstellungen**.
2. Klicken Sie im Dialogfeld **Einstellungen für \<Name der virtuellen Appliance\>** im linken Bereich auf **Hardware hinzufügen**.
3. Wählen Sie im rechten Bereich aus der Geräteliste **Netzwerkadapter** aus.
4. Klicken Sie auf **Hinzufügen**.
5. Stellen Sie sicher, dass **Netzwerkadapter (nicht verbunden)** im linken Bereich angezeigt wird.
6. Wählen Sie den Netzwerkadapter im linken Bereich aus.
7. Wählen Sie im rechten Bereich im Menü **Netzwerk** das virtuelle Netzwerk aus, mit dem der Adapter verbunden werden soll.
8. Um das virtuelle Netzwerk für andere Netzwerkadapter auszuwählen, die Sie verwenden möchten, wiederholen Sie die Schritte **6** und **7**.
9. Klicken Sie auf **Übernehmen** und dann auf **OK**.

**So konfigurieren Sie die NetScaler VPX-Instanz:**

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

1. Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance, die Sie zuvor installiert haben, und wählen Sie dann **Starten**.
2. Greifen Sie auf die Konsole zu, indem Sie auf die virtuelle Appliance doppelklicken.
3. Geben Sie die NetScaler IP-Adresse, Subnetzmaske und das Gateway für Ihre virtuelle Appliance ein.

Sie haben die grundlegende Konfiguration Ihrer virtuellen Appliance abgeschlossen. Geben Sie die IP-Adresse in einem Webbrowser ein, um auf die virtuelle Appliance zuzugreifen.

**HINWEIS:**

Sie können auch eine Vorlage für virtuelle Maschinen (VM) zur Bereitstellung einer NetScaler VPX-Instanz mithilfe von SCVMM verwenden.

Wenn Sie die Microsoft Hyper-V NIC-Teaming-Lösung mit NetScaler VPX-Instanzen verwenden, finden Sie weitere Informationen im Artikel CTX224494.

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

# Installieren einer NetScaler VPX-Instanz auf der Linux-KVM-Plattform

Um eine NetScaler VPX für die Linux-KVM-Plattform einzurichten, können Sie die grafische Anwendung Virtual Machine Manager (Virtual Manager) verwenden. Wenn Sie die Linux-KVM-Befehlszeile bevorzugen, können Sie das Programm `virsh` verwenden.

Das Host-Linux-Betriebssystem muss auf geeigneter Hardware unter Verwendung von Virtualisierungstools wie KVM-Modul und QEMU installiert werden. Die Anzahl der virtuellen Maschinen (VMs), die auf dem Hypervisor bereitgestellt werden können, hängt von den Anwendungsanforderungen und der gewählten Hardware ab.

Nachdem Sie eine NetScaler VPX-Instanz bereitgestellt haben, können Sie weitere Schnittstellen hinzufügen.

## Einschränkungen und Nutzungsrichtlinien

### Allgemeine Empfehlungen

Um unvorhersehbares Verhalten zu vermeiden, beachten Sie die folgenden Empfehlungen:

- Ändern Sie nicht die MTU der VNet-Schnittstelle, die der VPX-VM zugeordnet ist. Fahren Sie die VPX-VM herunter, bevor Sie Konfigurationsparameter wie Schnittstellenmodi oder CPU ändern.
- Erzwingen Sie kein Herunterfahren der VPX-VM. Das heißt, verwenden Sie nicht den Befehl **Force off**.
- Alle Konfigurationen, die auf dem Host-Linux vorgenommen werden, können persistent sein oder auch nicht, abhängig von den Einstellungen Ihrer Linux-Distribution. Sie können diese Konfigurationen persistent machen, um ein konsistentes Verhalten bei Neustarts des Host-Linux-Betriebssystems zu gewährleisten.
- Das NetScaler-Paket muss für jede bereitgestellte NetScaler VPX-Instanz eindeutig sein.

### Einschränkungen

- Live-Migration einer VPX-Instanz, die auf KVM läuft, wird nicht unterstützt.

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

# Voraussetzungen für die Installation einer NetScaler VPX-Instanz auf der Linux-KVM-Plattform

Überprüfen Sie die Mindestsystemanforderungen für einen Linux-KVM-Server, auf dem eine NetScaler VPX-Instanz ausgeführt wird.

**CPU-Anforderung**:

- 64-Bit-x86-Prozessoren mit der Hardware-Virtualisierungsfunktion, die in Intel VT-X-Prozessoren enthalten ist.

Um zu testen, ob Ihre CPU den Linux-Host unterstützt, geben Sie den folgenden Befehl an der Linux-Shell-Eingabeaufforderung des Hosts ein:

```
*.egrep '^flags.*(vmx|svm)' /proc/cpuinfo*
```

Wenn die **BIOS**-Einstellungen für die vorhergehende Erweiterung deaktiviert sind, müssen Sie diese im BIOS aktivieren.

- Stellen Sie dem Host-Linux mindestens 2 CPU-Kerne zur Verfügung.
- Es gibt keine spezifische Empfehlung für die Prozessorgeschwindigkeit, aber je höher die Geschwindigkeit, desto besser die Leistung der VM-Anwendung.

**Arbeitsspeicher (RAM)-Anforderung**:

Mindestens 4 GB für den Host-Linux-Kernel. Fügen Sie bei Bedarf mehr Arbeitsspeicher für die VMs hinzu.

**Festplattenanforderung**:

Berechnen Sie den Speicherplatz für den Host-Linux-Kernel und die VM-Anforderungen. Eine einzelne NetScaler VPX VM benötigt 20 GB Festplattenspeicher.

## Softwareanforderungen

Der verwendete Host-Kernel muss ein 64-Bit-Linux-Kernel, Version 2.6.20 oder höher, mit allen Virtualisierungstools sein. Citrix empfiehlt neuere Kernel, wie 3.6.11-4 und höher.

Viele Linux-Distributionen wie Red Hat, CentOS und Fedora verfügen über getestete Kernel-Versionen und zugehörige Virtualisierungstools.

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

## Hardwareanforderungen für Gast-VM

NetScaler VPX unterstützt IDE- und virtIO-Festplattentypen. Der Festplattentyp wurde in der XML-Datei konfiguriert, die Teil des NetScaler-Pakets ist.

## Netzwerkanforderungen

NetScaler VPX unterstützt virtIO-paravirtualisierte, SR-IOV- und PCI-Passthrough-Netzwerkschnittstellen.

Weitere Informationen zu den unterstützten Netzwerkschnittstellen finden Sie unter:

- Bereitstellen der NetScaler VPX-Instanz mithilfe des Virtual Machine Managers
- Konfigurieren einer NetScaler VPX-Instanz zur Verwendung von SR-IOV-Netzwerkschnittstellen
- Konfigurieren einer NetScaler VPX-Instanz zur Verwendung von PCI-Passthrough-Netzwerkschnittstellen

### Quellschnittstelle und Modi

Der Quellgerätetyp kann entweder Bridge oder MacVTap sein. In MacVTap sind vier Modi möglich: VEPA, Bridge, Private und Pass-through. Überprüfen Sie die Arten von Schnittstellen, die Sie verwenden können, und die unterstützten Verkehrstypen gemäß den folgenden Angaben:

**Bridge**:

- Linux-Bridge.
- `Ebtables`- und `iptables`-Einstellungen auf dem Host-Linux könnten den Datenverkehr auf der Bridge filtern, wenn Sie nicht die richtige Einstellung wählen oder `IPtable`-Dienste deaktivieren.

**MacVTap (VEPA-Modus)**:

- Bessere Leistung als eine Bridge.
- Schnittstellen desselben untergeordneten Geräts können zwischen den VMs geteilt werden.
- Inter-VM-Kommunikation unter Verwendung desselben
- untergeordneten Geräts ist nur möglich, wenn der Upstream- oder Downstream-Switch den VEPA-Modus unterstützt.

**MacVTap (privater Modus)**:

- Bessere Leistung als eine Bridge.

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

- Schnittstellen desselben untergeordneten Geräts können zwischen den VMs geteilt werden.
- Inter-VM-Kommunikation unter Verwendung desselben untergeordneten Geräts ist nicht möglich.

**MacVTap (Bridge-Modus)**:

- Besser im Vergleich zu einer Bridge.
- Schnittstellen desselben untergeordneten Geräts können zwischen den VMs geteilt werden.
- Inter-VM-Kommunikation unter Verwendung desselben untergeordneten Geräts ist möglich, wenn die Verbindung des untergeordneten Geräts aktiv ist.

**MacVTap (Pass-Through-Modus)**:

- Besser im Vergleich zu einer Bridge.
- Schnittstellen desselben untergeordneten Geräts können nicht zwischen den VMs geteilt werden.
- Nur eine VM kann das untergeordnete Gerät nutzen.

**HINWEIS:**

Um die beste Leistung der VPX-Instanz zu erzielen, stellen Sie sicher, dass die `gro`- und `lro`-Funktionen auf den Quellschnittstellen deaktiviert sind.

## Eigenschaften der Quellschnittstellen

Stellen Sie sicher, dass Sie die Generic-Receive-Offload- (`gro`) und Large-Receive-Offload- (`lro`) Funktionen der Quellschnittstellen deaktivieren. Um die `gro`- und `lro`-Funktionen zu deaktivieren, führen Sie die folgenden Befehle an der Linux-Host-Shell-Eingabeaufforderung aus.

`ethtool -K eth6 gro off` `ethool -K eth6 lro off`

**Beispiel**:

```
    [root@localhost ~]# ethtool -K eth6



                  Offload parameters for eth6:
```

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

```
                                rx-checksumming: on

                                tx-checksumming: on

                    scatter-gather: on

                    tcp-segmentation-offload: on

                    udp-fragmentation-offload: off

                    generic-segmentation-offload: on

                    generic-receive-offload: off

                    large-receive-offload: off

                    rx-vlan-offload: on

                    tx-vlan-offload: on

                    ntuple-filters: off
```

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

```
                    receive-hashing: on



    [root@localhost ~]#
```

**Beispiel**:

Wenn die Host-Linux-Bridge als Quellgerät verwendet wird, wie im folgenden Beispiel, müssen die `lro`-Funktionen auf den VNet-Schnittstellen deaktiviert werden, die die virtuellen Schnittstellen sind, die den Host mit den Gast-VMs verbinden.

```
    [root@localhost ~]# brctl show eth6_br



    bridge name     bridge  id              STP enabled interfaces



    eth6_br         8000.00e0ed1861ae          no         eth6

                                                          vnet0

                                                          vnet2



    [root@localhost ~]#
```

Im vorhergehenden Beispiel werden die beiden virtuellen Schnittstellen von eth6_br abgeleitet und als vnet0 und vnet2 dargestellt. Führen Sie die folgenden Befehle aus, um die `gro`- und `lro`-Funktionen auf diesen Schnittstellen zu deaktivieren.

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

```
ethtool -K vnet0 gro off

        ethtool -K vnet2 gro off

        ethtool -K vnet0 lro off

                ethtool -K vnet2 lro off
```

### Promiskuitiver Modus

Der promiskuitiver Modus muss für die folgenden Funktionen aktiviert sein:

- L2-Modus
- Multicast-Verkehrsverarbeitung
- Broadcast
- IPV6-Verkehr
- virtuelle MAC
- Dynamisches Routing

Verwenden Sie den folgenden Befehl, um den Promiscuous-Modus zu aktivieren.

```
[root@localhost ~]# ifconfig eth6 promisc

[root@localhost ~]# ifconfig eth6

eth6       Link encap:Ethernet  HWaddr 78:2b:cb:51:54:a3

           inet6 addr: fe80::7a2b:cbff:fe51:54a3/64 Scope:Link

           UP BROADCAST RUNNING PROMISC MULTICAST  MTU:9000  Metric:1

           RX packets:142961 errors:0 dropped:0 overruns:0 frame:0

           TX packets:2895843 errors:0 dropped:0 overruns:0 carrier:0

           collisions:0 txqueuelen:1000

           RX bytes:14330008 (14.3 MB)  TX bytes:1019416071 (1.0 GB)
```

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

```
[root@localhost ~]#
```

### Erforderliches Modul

Für eine bessere Netzwerkleistung stellen Sie sicher, dass das Modul vhost_net auf dem Linux-Host vorhanden ist. Um die Existenz des vhost_net-Moduls zu überprüfen, führen Sie den folgenden Befehl auf dem Linux-Host aus:

```
lsmod | grep "vhost\_net"
```

Wenn vhost_net noch nicht ausgeführt wird, geben Sie den folgenden Befehl ein, um es auszuführen:

```
modprobe vhost\_net
```

## Bereitstellen der NetScaler VPX-Instanz mit dem Virtual Machine Manager

Der Virtual Machine Manager ist ein Desktop-Tool zur Verwaltung von VM-Gästen. Er ermöglicht Ihnen das Erstellen neuer VM-Gäste und verschiedener Speichertypen sowie die Verwaltung virtueller Netzwerke. Sie können mit dem integrierten VNC-Viewer auf die grafische Konsole von VM-Gästen zugreifen und Leistungsstatistiken lokal oder remote anzeigen.

Nach der Installation Ihrer bevorzugten Linux-Distribution mit aktivierter KVM-Virtualisierung können Sie mit der Bereitstellung virtueller Maschinen fortfahren.

Bei der Bereitstellung einer NetScaler VPX-Instanz mit dem Virtual Machine Manager haben Sie zwei Optionen:

- IP-Adresse, Gateway und Netzmaske manuell eingeben
- IP-Adresse, Gateway und Netzmaske automatisch zuweisen (automatische Bereitstellung)

Sie können zwei Arten von Images verwenden, um eine NetScaler VPX-Instanz bereitzustellen:

- RAW
- QCOW2

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

Sie können ein NetScaler VPX RAW-Image in ein QCOW2-Image konvertieren und die NetScaler VPX-Instanz bereitstellen. Um das RAW-Image in ein QCOW2-Image zu konvertieren, geben Sie den folgenden Befehl ein:

```
qemu-img convert -O qcow2 original-image.raw image-converted.qcow2
```

**Beispiel:**

```
qemu-img convert -O qcow2 NSVPX-KVM-11.1-12.5_nc.raw NSVPX-KVM-11.1-12.5_nc.qcow2
```

Eine typische NetScaler VPX-Bereitstellung auf KVM umfasst die folgenden Schritte:

- Prüfen der Voraussetzungen für die automatische Bereitstellung einer NetScaler VPX-Instanz
- Bereitstellen der NetScaler VPX-Instanz mithilfe eines RAW-Images
- Bereitstellen der NetScaler VPX-Instanz mithilfe eines QCOW2-Images
- Hinzufügen weiterer Schnittstellen zu einer VPX-Instanz mithilfe des Virtual Machine Managers

## Voraussetzungen für die automatische Bereitstellung einer NetScaler VPX-Instanz prüfen

Die automatische Bereitstellung ist eine optionale Funktion, bei der Daten vom CD-ROM-Laufwerk verwendet werden. Wenn diese Funktion aktiviert ist, müssen Sie die Verwaltungs-IP-Adresse, die Netzmaske und das Standard-Gateway der NetScaler VPX-Instanz während der Ersteinrichtung nicht eingeben.

Sie müssen die folgenden Aufgaben ausführen, bevor Sie eine VPX-Instanz automatisch bereitstellen können:

1. Erstellen Sie eine angepasste OVF-XML-Datei (Open Virtualization Format) oder eine Benutzerdatendatei.
2. Konvertieren Sie die OVF-Datei mithilfe einer Online-Anwendung (z. B. PowerISO) in ein ISO-Image.
3. Mounten Sie das ISO-Image auf dem KVM-Host mithilfe beliebiger SCP-basierter (Secure Copy) Tools.

**Beispiel einer OVF-XML-Datei**:

Hier ist ein Beispiel für den Inhalt einer OVF-XML-Datei, die Sie als Vorlage zum Erstellen Ihrer Datei verwenden können.

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

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<Environment xmlns:oe="`http://schemas.dmtf.org/ovf/environment/1"`

xmlns:xsi="`http://www.w3.org/2001/XMLSchema-instance"`

oe:id=""

xmlns="`http://schemas.dmtf.org/ovf/environment/1"`

xmlns:cs="`http://schemas.citrix.com/openstack">`

<PlatformSection>

<Kind></Kind>

<Version>2016.1</Version>

<Vendor>VPX</Vendor>

<Locale>en</Locale>
```

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

```
</PlatformSection>

<PropertySection>

<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"/>

<Property oe:key="com.citrix.netscaler.platform" oe:value="NSVPX"/>

<Property oe:key="com.citrix.netscaler.orch\_env" oe:value="KVM"/>

<Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.1.2.22"/>

<Property oe:key="com.citrix.netscaler.mgmt.netmask"
oe:value="255.255.255.0"/>

<Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="10.1.2.1"/>

</PropertySection>

</Environment>
```

In der vorangehenden OVF-XML-Datei wird „PropertySection“ für die NetScaler®-Netzwerkkonfiguration verwendet. Wenn Sie die Datei erstellen, geben Sie Werte für die Parameter an, die am Ende des Beispiels hervorgehoben sind:

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

- Verwaltungs-IP-Adresse
- Netzmaske
- Gateway

**WICHTIG**

Wenn die OVF-Datei nicht ordnungsgemäß im XML-Format vorliegt, wird der VPX-Instanz die Standard-Netzwerkkonfiguration zugewiesen, nicht die in der Datei angegebenen Werte.

## Bereitstellen der NetScaler VPX-Instanz mithilfe eines RAW-Images

Der Virtual Machine Manager ermöglicht Ihnen die Bereitstellung einer NetScaler VPX-Instanz mithilfe eines RAW-Images.

Um eine NetScaler VPX-Instanz mithilfe des Virtual Machine Managers bereitzustellen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie den Virtual Machine Manager (**Anwendung** > **Systemwerkzeuge** > **Virtual Machine Manager**) und geben Sie die Anmeldeinformationen im Fenster **Authentifizieren** ein.
2. Klicken Sie auf das Symbol

   oder klicken Sie mit der rechten Maustaste auf **localhost (QEMU)**, um eine neue NetScaler VPX-Instanz zu erstellen.

3. Geben Sie im Textfeld **Name** einen Namen für die neue VM ein (zum Beispiel NetScaler-VPX).
4. Wählen Sie im Fenster **Neue VM** unter „Wie möchten Sie das Betriebssystem installieren?“ die Option **Vorhandenes Festplatten-Image importieren** aus und klicken Sie dann auf **Weiter**.

5. Navigieren Sie im Feld **Vorhandenen Speicherpfad angeben** zum Pfad des Images. Wählen Sie den OS-Typ als UNIX und die Version als FreeBSD 6.x. Klicken Sie dann auf **Weiter**.

6. Wählen Sie unter **Speicher- und CPU-Einstellungen auswählen** die folgenden Einstellungen aus und klicken Sie dann auf **Weiter**:

   - Arbeitsspeicher (RAM) – 2048 MB
   - CPUs – 2

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

7. Wählen Sie das Kontrollkästchen **Konfiguration vor der Installation anpassen** aus. Optional können Sie unter **Erweiterte Optionen** die MAC-Adresse anpassen. Stellen Sie sicher, dass der ausgewählte **Virt-Typ** KVM und die ausgewählte Architektur x86_64 ist. Klicken Sie auf **Fertig stellen**.

8. Wählen Sie eine NIC aus und geben Sie die folgende Konfiguration an:

   - Quellgerät – `ethX macvtap` oder Bridge
   - Gerätemodell – `virtio`
   - Quellmodus – Bridge

9. Klicken Sie auf **Übernehmen**.
10. Wenn Sie die VPX-Instanz automatisch bereitstellen möchten, lesen Sie den Abschnitt **Automatisches Provisioning durch Anschließen eines CD-ROM-Laufwerks aktivieren** in diesem Dokument. Andernfalls klicken Sie auf **Installation starten**. Nachdem Sie die NetScaler VPX auf KVM bereitgestellt haben, können Sie weitere Schnittstellen hinzufügen.

## Bereitstellen der NetScaler VPX-Instanz mithilfe eines QCOW2-Images

Mit dem Virtual Machine Manager können Sie die NetScaler VPX-Instanz mithilfe eines QCOW2-Images bereitstellen.

Um eine NetScaler VPX-Instanz mithilfe eines QCOW2-Images bereitzustellen, führen Sie die folgenden Schritte aus:

1. Führen Sie **Schritt 1** bis **Schritt 8** in Bereitstellen der NetScaler VPX-Instanz mithilfe eines RAW-Images aus.

   **HINWEIS:**

   Stellen Sie sicher, dass Sie das **qcow2**-Image in **Schritt 5** auswählen.

2. Wählen Sie **Disk 1** aus und klicken Sie auf **Erweiterte Optionen**.
3. Wählen Sie **qcow2** aus der Dropdown-Liste „Speicherformat“ aus.

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

4. Klicken Sie auf **Anwenden** und dann auf **Installation starten**. Nachdem Sie die NetScaler VPX auf KVM bereitgestellt haben, können Sie weitere Schnittstellen hinzufügen.

## Automatische Bereitstellung durch Anschließen eines CD-ROM-Laufwerks aktivieren

1. Klicken Sie auf **Hardware hinzufügen > Speicher > Gerätetyp > CD-ROM-Gerät**.
2. Klicken Sie auf **Verwalten**, wählen Sie die korrekte ISO-Datei aus, die Sie im Abschnitt „Voraussetzungen für die automatische Bereitstellung einer NetScaler VPX-Instanz“ gemountet haben, und klicken Sie auf **Fertig stellen**. Eine neue CD-ROM unter „Ressourcen“ auf Ihrer NetScaler VPX-Instanz wird erstellt.

3. Schalten Sie die VPX-Instanz ein, und sie wird automatisch mit der in der OVF-Datei bereitgestellten Netzwerkkonfiguration bereitgestellt, wie im Beispiel-Screenshot gezeigt.

4. Wenn die automatische Bereitstellung fehlschlägt, wird die Instanz mit der Standard-IP-Adresse (192.168.100.1) gestartet. In diesem Fall müssen Sie die Erstkonfiguration manuell abschließen. Weitere Informationen finden Sie unter ADC zum ersten Mal konfigurieren.

## Weitere Schnittstellen zur NetScaler VPX-Instanz mithilfe des Virtual Machine Managers hinzufügen

Nachdem Sie die NetScaler VPX™-Instanz auf KVM bereitgestellt haben, können Sie zusätzliche Schnittstellen hinzufügen.

Um weitere Schnittstellen hinzuzufügen, gehen Sie wie folgt vor.

1. Fahren Sie die auf dem KVM ausgeführte NetScaler VPX-Instanz herunter.
2. Klicken Sie mit der rechten Maustaste auf die VPX-Instanz und wählen Sie **Öffnen** aus dem Kontextmenü.
3. Klicken Sie auf das

   Symbol in der Kopfzeile, um die Details der virtuellen Hardware anzuzeigen.
4. Klicken Sie auf **Hardware hinzufügen**. Wählen Sie im Fenster **Neue virtuelle Hardware hinzufügen** die Option **Netzwerk** aus dem Navigationsmenü.

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

5. Wählen Sie im Feld **Hostgerät** den Typ der physischen Schnittstelle aus. Der Hostgerätetyp kann entweder Bridge oder MacVTap sein. Im Falle von MacVTap sind vier Modi möglich: VEPA, Bridge, Private und Pass-through.

   a. Für Bridge

      i. Hostgerät — Wählen Sie die Option „Freigegebenen Gerätenamen angeben“.

      ii. Geben Sie den Bridge-Namen an, der im KVM-Host konfiguriert ist.

      > **HINWEIS:**
      >
      > Stellen Sie sicher, dass Sie eine Linux-Bridge im KVM-Host konfiguriert, die physische Schnittstelle an die Bridge gebunden und die Bridge in den UP-Zustand versetzt haben.

      iii. Gerätemodell— `virtio`.

      iv. Klicken Sie auf **Fertig stellen**.

   b. Für MacVTap

      i. Hostgerät – Wählen Sie die physische Schnittstelle aus dem Menü aus.

      ii. Gerätemodell – `virtio`.

      iii. Klicken Sie auf **Fertig stellen**. Sie können die neu hinzugefügte NIC im Navigationsbereich anzeigen.

      iv. Wählen Sie die neu hinzugefügte NIC aus und wählen Sie den Quellmodus für diese NIC. Die verfügbaren Modi sind VEPA, Bridge, Private und Passthrough. Weitere Informationen zur Schnittstelle und den Modi finden Sie unter Quellschnittstelle und Modi.

      v. Klicken Sie auf **Übernehmen**.

6. Wenn Sie die VPX-Instanz automatisch bereitstellen möchten, lesen Sie den Abschnitt „Hinzufügen eines Konfigurationslaufwerks zur Aktivierung der automatischen Bereitstellung“ in diesem Dokument. Andernfalls schalten Sie die VPX-Instanz ein, um die Erstkonfiguration manuell abzuschließen.

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

**WICHTIG:**

Schnittstellenparameterkonfigurationen wie Geschwindigkeit, Duplex und Auto-Negotiation werden nicht unterstützt.

# Konfigurieren einer NetScaler VPX-Instanz zur Verwendung von SR-IOV-Netzwerkschnittstellen

Sie können eine NetScaler VPX-Instanz, die auf der Linux-KVM-Plattform ausgeführt wird, mithilfe von Single Root I/O Virtualization (SR-IOV) mit den folgenden NICs konfigurieren:

- Intel 82599 10G
- Intel X710 10G
- Intel XL710 40G
- Intel X722 10G

Weitere Informationen finden Sie unter Unterstützte NICs für NetScaler VPX.

Dieser Abschnitt beschreibt, wie Sie vorgehen können:

- Konfigurieren einer NetScaler VPX-Instanz zur Verwendung der SR-IOV-Netzwerkschnittstelle
- Konfigurieren von statischem LA/LACP auf der SR-IOV-Schnittstelle
- Konfigurieren von VLAN auf der SR-IOV-Schnittstelle

## Einschränkungen

Beachten Sie die Einschränkungen bei der Verwendung von Intel 82599-, X710-, XL710- und X722-NICs. Die folgenden Funktionen werden nicht unterstützt.

**Einschränkungen für Intel 82599 NIC**:

- L2-Modus-Umschaltung.
- Admin-Partitionierung (gemeinsamer VLAN-Modus).
- Hochverfügbarkeit (Aktiv-Aktiv-Modus).
- Jumbo-Frames.
- IPv6: Sie können nur bis zu 30 eindeutige IPv6-Adressen in einer VPX-Instanz konfigurieren, wenn Sie mindestens eine SR-IOV-Schnittstelle haben.

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

- VLAN-Konfiguration auf dem Hypervisor für die SRIOV VF-Schnittstelle über den `ip link` Befehl wird nicht unterstützt.
- Schnittstellenparameterkonfigurationen wie Geschwindigkeit, Duplex und Autonegotiation werden nicht unterstützt.

**Einschränkungen für Intel X710 10G, Intel XL710 40G und Intel X722 10G NICs**:

- L2-Modus-Umschaltung.
- Admin-Partitionierung (gemeinsamer VLAN-Modus).
- In einem Cluster werden Jumbo-Frames nicht unterstützt, wenn die XL710 NIC als Datenschnittstelle verwendet wird.
- Die Schnittstellenliste wird neu geordnet, wenn Schnittstellen getrennt und wieder verbunden werden.
- Schnittstellenparameterkonfigurationen wie Geschwindigkeit, Duplex und Autonegotiation werden nicht unterstützt.
- Der Schnittstellenname ist 40/X für Intel X710 10G, Intel XL710 40G und Intel X722 10G NICs
- Bis zu 16 Intel XL710/X710/X722 SRIOV- oder PCI-Passthrough-Schnittstellen können auf einer VPX-Instanz unterstützt werden.

**HINWEIS:**

Damit Intel X710 10G-, Intel XL710 40G- und Intel X722 10G-NICs IPv6 unterstützen, müssen Sie den Vertrauensmodus für die Virtuellen Funktionen (VFs) aktivieren, indem Sie den folgenden Befehl auf dem KVM-Host eingeben:

```
# ip link set <PNIC> <VF> trust on
```

Beispiel:

```
# ip link set ens785f1 vf 0 trust on
```

## Voraussetzungen

Bevor Sie eine NetScaler VPX-Instanz für die Verwendung von SR-IOV-Netzwerkschnittstellen konfigurieren, führen Sie die folgenden Voraussetzungen aus. Details zum Abschluss der entsprechenden Aufgaben finden Sie in der Spalte NIC.

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

| AUFGABE | INTEL 82599 NIC | INTEL X710, XL710 UND X722 NICS |
|---|---|---|
| 1. Fügen Sie die NIC zum KVM-Host hinzu. | - | - |
| 1. Laden Sie den neuesten Intel-Treiber herunter und installieren Sie ihn. | IXGBE-Treiber | I40E-Treiber |
| 1. Setzen Sie den Treiber auf dem KVM-Host auf die Blacklist. | Fügen Sie den folgenden Eintrag in die Datei /etc/modprobe.d/blacklist.conf ein: `blacklist ixgbevf`. Verwenden Sie IXGBE-Treiberversion 4.3.15 (empfohlen). | Fügen Sie den folgenden Eintrag in die Datei /etc/modprobe.d/blacklist.conf ein: `blacklist i40evf`. Verwenden Sie i40e-Treiberversion 2.0.26 (empfohlen). |
| 1. Aktivieren Sie SR-IOV Virtual Functions (VFs) auf dem KVM-Host. In beiden Befehlen in den nächsten beiden Spalten: `number_of_VFs` = die Anzahl der virtuellen VFs, die Sie erstellen möchten. `device_name` = der Schnittstellenname. | Wenn Sie eine frühere Version von Kernel 3.8 verwenden, fügen Sie den folgenden Eintrag in die Datei /etc/modprobe.d/ixgbe ein und starten Sie den KVM-Host neu: `options ixgbe max_vfs=<number_of_VFs>`. Wenn Sie Kernel Version 3.8 oder höher verwenden, erstellen Sie VFs mit dem folgenden Befehl: `echo <number_of_VFs> > /sys/class/net/<device_name>/device/sriov_numvfs`. Siehe Beispiel in Abbildung 1. | Wenn Sie eine frühere Version von Kernel 3.8 verwenden, fügen Sie den folgenden Eintrag in die Datei /etc/modprobe.d/i40e.conf ein und starten Sie den KVM-Host neu: `options i40e max_vfs=<number_of_VFs>`. Wenn Sie Kernel Version 3.8 oder höher verwenden, erstellen Sie VFs mit dem folgenden Befehl: `echo<number_of_VFs> > /sys/class/net/<device_name>/device/sriov_numvfs`. Siehe Beispiel in Abbildung 2. |

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

| AUFGABE | INTEL 82599 NIC | INTEL X710, XL710 UND X722 NICS |
|---|---|---|
| 1. Machen Sie die VFs persistent, indem Sie die Befehle, die Sie zum Erstellen der VFs verwendet haben, zur Datei rc.local hinzufügen. | Siehe Beispiel in Abbildung 3. | Siehe Beispiel in Abbildung 3. |

**WICHTIG:**

Stellen Sie beim Erstellen der SR-IOV VFs sicher, dass Sie den VFs keine MAC-Adressen zuweisen.

**Abbildung 1**: SR-IOV VFs auf dem KVM-Host für Intel 82599 10G NIC aktivieren.

**Abbildung 2:** SR-IOV VFs auf dem KVM-Host für Intel X710 10G und XL710 40G NICs aktivieren.

**Abbildung 3:** SR-IOV VFs auf dem KVM-Host für Intel X722 10G NIC aktivieren.

**Abbildung 4**: VFs persistent machen.

## Konfigurieren einer NetScaler VPX-Instanz zur Verwendung der SR-IOV-Netzwerkschnittstelle

Um die NetScaler VPX-Instanz zur Verwendung der SR-IOV-Netzwerkschnittstelle mit dem Virtual Machine Manager zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Schalten Sie die NetScaler VPX-Instanz aus.
2. Wählen Sie die NetScaler VPX-Instanz aus und wählen Sie dann Öffnen.
3. Wählen Sie im Fenster \<virtuelle Maschine auf KVM\> das Symbol **i** aus.

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

4. Wählen Sie **Hardware hinzufügen**.

5. Führen Sie im Dialogfeld **Neue virtuelle Hardware hinzufügen** die folgenden Schritte aus:

   a. Wählen Sie PCI-Hostgerät aus.

   b. Wählen Sie im Abschnitt Host-Gerät die von Ihnen erstellte VF aus und klicken Sie auf Fertig stellen.

   **Abbildung 4**: VF für Intel 82599 10G NIC

   **Abbildung 5**: VF für Intel XL710 40G NIC

   **Abbildung 6**: VF für Intel X722 10G NIC

6. Wiederholen Sie Schritt 4 und 5, um die von Ihnen erstellten VFs hinzuzufügen.
7. Schalten Sie die NetScaler VPX-Instanz ein.
8. Nachdem die NetScaler VPX-Instanz eingeschaltet wurde, verwenden Sie den folgenden Befehl, um die Konfiguration zu überprüfen:

   ```
   show interface summary
   ```

   Die Ausgabe zeigt alle Schnittstellen, die Sie konfiguriert haben.

   **Abbildung 6**: Ausgabezusammenfassung für Intel 82599 NIC.

   **Abbildung 7**. Ausgabezusammenfassung für Intel X710 und XL710 NICs.

## Statische LA/LACP auf der SR-IOV-Schnittstelle konfigurieren

**WICHTIG:**

Stellen Sie beim Erstellen der SR-IOV-VFs sicher, dass Sie den VFs keine MAC-Adressen zuweisen.

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

Um die SR-IOV-VFs im Link-Aggregation-Modus zu verwenden, deaktivieren Sie die Spoof-Prüfung für die von Ihnen erstellten VFs. Verwenden Sie auf dem KVM-Host den folgenden Befehl, um die Spoof-Prüfung zu deaktivieren:

```
*ip link set \<interface\_name\> vf \<VF\_id\> spoofchk off*
```

Dabei gilt:

- Interface_name – ist der Schnittstellenname.
- VF_id – ist die ID der virtuellen Funktion.

**Beispiel:**

Nachdem Sie die Spoof-Prüfung für alle von Ihnen erstellten VFs deaktiviert haben, starten Sie die NetScaler VPX-Instanz neu und konfigurieren Sie die Link-Aggregation. Detaillierte Anweisungen finden Sie unter Link-Aggregation konfigurieren.

### VLAN auf der SR-IOV-Schnittstelle konfigurieren

Sie können VLAN auf SR-IOV-VFs konfigurieren. Detaillierte Anweisungen finden Sie unter VLAN konfigurieren.

**WICHTIG:**

Stellen Sie sicher, dass der KVM-Host keine VLAN-Einstellungen für die VF-Schnittstelle enthält.

## Konfigurieren Sie eine NetScaler VPX auf dem KVM-Hypervisor zur Verwendung von Intel QAT für die SSL-Beschleunigung im SR-IOV-Modus

Die NetScaler VPX-Instanz auf dem Linux KVM-Hypervisor kann die Intel QuickAssist Technology (QAT) verwenden, um die NetScaler SSL-Leistung zu beschleunigen. Mithilfe von Intel QAT können alle kryptografischen Verarbeitungen mit hoher Latenz auf den Chip ausgelagert werden, wodurch eine oder mehrere Host-CPUs für andere Aufgaben freigegeben werden.

Bisher erfolgte die gesamte kryptografische Verarbeitung des NetScaler®-Datenpfads in der Software unter Verwendung von Host-vCPUs.

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

**HINWEIS:**

Derzeit unterstützt NetScaler VPX nur das C62x-Chipmodell aus der Intel QAT-Familie. Diese Funktion wird ab NetScaler Release 14.1 Build 8.50 unterstützt.

## Voraussetzungen

- Der Linux-Host ist mit einem Intel QAT C62x-Chip ausgestattet, entweder direkt in das Motherboard integriert oder auf einer externen PCI-Karte hinzugefügt.

  **Intel QAT C62x Serienmodelle:** C625, C626, C627, C628. Nur diese C62x-Modelle verfügen über die Public Key Encryption (PKE)-Funktion. Andere C62x-Varianten unterstützen PKE nicht.

- Die NetScaler VPX erfüllt die Hardwareanforderungen von VMware ESX. Weitere Informationen finden Sie unter Installieren einer NetScaler VPX-Instanz auf der Linux KVM-Plattform.

## Einschränkungen

Es gibt keine Möglichkeit, Krypto-Einheiten oder Bandbreite für einzelne VMs zu reservieren. Alle verfügbaren Krypto-Einheiten jeder Intel QAT-Hardware werden von allen VMs, die die QAT-Hardware verwenden, gemeinsam genutzt.

## Richten Sie die Host-Umgebung für die Verwendung von Intel QAT ein

1. Laden Sie den von Intel bereitgestellten Treiber für das C62x-Serien (QAT)-Chipmodell auf dem Linux-Host herunter und installieren Sie ihn. Weitere Informationen zu den Intel-Paket-Downloads und Installationsanweisungen finden Sie unter Intel QuickAssist Technology Driver for Linux. Eine Readme-Datei ist Teil des Download-Pakets. Diese Datei enthält Anweisungen zum Kompilieren und Installieren des Pakets auf dem Host.

   Nachdem Sie den Treiber heruntergeladen und installiert haben, führen Sie die folgenden Überprüfungen durch:

   - Beachten Sie die Anzahl der C62x-Chips. Jeder C62x-Chip verfügt über bis zu 3 PCIe-Endpunkte.
   - Stellen Sie sicher, dass alle Endpunkte UP sind. Führen Sie den Befehl `adf_ctl status` aus, um den Status aller PF-Endpunkte (bis zu 3) anzuzeigen.

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

```
root@Super-Server:~# adf_ctl status



Checking status of all devices.

There is 51 QAT acceleration device(s) in the system

qat_dev0 - type: c6xx,  inst_id: 0,  node_id: 0,  bsf: 0000:1a:00.0,
 #accel: 5 #engines: 10 state: up

qat_dev1 - type: c6xx,  inst_id: 1,  node_id: 0,  bsf: 0000:1b:00.0,
 #accel: 5 #engines: 10 state: up

qat_dev2 - type: c6xx,  inst_id: 2,  node_id: 0,  bsf: 0000:1c:00.0,
 #accel: 5 #engines: 10 state: up
```

- Aktivieren Sie SRIOV (VF-Unterstützung) für alle QAT-Endpunkte.

```
root@Super-Server:~# echo 1 > /sys/bus/pci/devices/0000\:1a\:00.0/
sriov_numvfs

root@Super-Server:~# echo 1 > /sys/bus/pci/devices/0000\:1b\:00.0/
sriov_numvfs

root@Super-Server:~# echo 1 > /sys/bus/pci/devices/0000\:1c\:00.0/
sriov_numvfs
```

- Stellen Sie sicher, dass alle VFs angezeigt werden (16 VFs pro Endpunkt, insgesamt 48 VFs).
- Führen Sie den Befehl adf_ctl status aus, um zu überprüfen, ob alle PF-Endpunkte (bis zu 3) und die VFs jedes Intel QAT-Chips UP sind. In diesem Beispiel verfügt das System nur über einen C62x-Chip. Es hat also insgesamt 51 Endpunkte (3 + 48 VFs).

2. Aktivieren Sie SR-IOV auf dem Linux-Host.
3. Erstellen Sie virtuelle Maschinen. Weisen Sie beim Erstellen einer VM die entsprechende Anzahl von PCI-Geräten zu, um die Leistungsanforderungen zu erfüllen.

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

**HINWEIS:**

Jeder C62x (QAT)-Chip kann bis zu drei separate PCI-Endpunkte haben. Jeder Endpunkt ist eine logische Sammlung von VFs und teilt die Bandbreite gleichmäßig mit anderen PCI-Endpunkten des Chips. Jeder Endpunkt kann bis zu 16 VFs haben, die als 16 PCI-Geräte angezeigt werden. Fügen Sie diese Geräte der VM hinzu, um die Krypto-Beschleunigung mit dem QAT-Chip durchzuführen.

## Wichtige Hinweise

- Wenn die Krypto-Anforderung der VM die Verwendung von mehr als einem QAT-PCI-Endpunkt/Chip vorsieht, empfehlen wir, die entsprechenden PCI-Geräte/VFs im Round-Robin-Verfahren auszuwählen, um eine symmetrische Verteilung zu gewährleisten.
- Wir empfehlen, dass die Anzahl der ausgewählten PCI-Geräte der Anzahl der lizenzierten vCPUs entspricht (ohne die Anzahl der Management-vCPUs). Das Hinzufügen von mehr PCI-Geräten als die verfügbare Anzahl von vCPUs verbessert die Leistung nicht unbedingt.

  **Beispiel:**

  Betrachten Sie einen Linux-Host mit einem Intel C62x-Chip, der 3 Endpunkte hat. Wenn Sie eine VM mit 6 vCPUs bereitstellen, wählen Sie 2 VFs von jedem Endpunkt aus und weisen Sie diese der VM zu. Diese Zuweisung gewährleistet eine effektive und gleichmäßige Verteilung der Krypto-Einheiten für die VM. Von den insgesamt verfügbaren vCPUs ist standardmäßig eine vCPU für die Management-Ebene reserviert, und die restlichen vCPUs stehen für die PEs der Datenebene zur Verfügung.

## Zuweisen von QAT-VFs zu NetScaler VPX, das auf dem Linux KVM-Hypervisor bereitgestellt wird

1. Stellen Sie im Linux KVM Virtual Machine Manager sicher, dass die VM (NetScaler VPX) ausgeschaltet ist.
2. Navigieren Sie zu **Hardware hinzufügen > PCI-Hostgerät**.
3. Weisen Sie dem PCI-Gerät Intel QAT VF zu.

   Intel QAT VF zuweisen(/en-us/vpx/media/linux-add-hardware.png)
4. Klicken Sie auf **Fertig stellen**.

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

5. Wiederholen Sie die vorhergehenden Schritte, um der NetScaler VPX-Instanz eine oder mehrere Intel QAT VFs zuzuweisen, bis zu einer Grenze von einem weniger als die Gesamtzahl der vCPUs. Da eine vCPU für den Verwaltungsprozess reserviert ist.

   Anzahl der QAT VFs pro VM = Anzahl der vCPUs - 1
6. Schalten Sie die VM ein.
7. Führen Sie den Befehl `stat ssl` in der NetScaler CLI aus, um die SSL-Zusammenfassung anzuzeigen und die SSL-Karten nach der Zuweisung von QAT VFs zu NetScaler VPX zu überprüfen.

   In diesem Beispiel haben wir 5 vCPUs verwendet, was 4 Paket-Engines (PEs) bedeutet.

   stat SSL-Befehl(/en-us/vpx/media/kvm-ssl-summary.png)

### Informationen zur Bereitstellung

Diese Bereitstellung wurde mit den folgenden Komponentenspezifikationen getestet:

- **NetScaler VPX Version und Build:** 14.1–8.50
- **Ubuntu Version:** 18.04, Kernel 5.4.0-146
- **Intel C62x QAT-Treiberversion für Linux:** L.4.21.0-00001

## Konfigurieren Sie eine NetScaler VPX-Instanz zur Verwendung von PCI-Passthrough-Netzwerkschnittstellen

Nachdem Sie eine NetScaler VPX-Instanz auf der Linux-KVM-Plattform installiert und konfiguriert haben, können Sie den Virtual Machine Manager verwenden, um die virtuelle Appliance zur Verwendung von PCI-Passthrough-Netzwerkschnittstellen zu konfigurieren.

### Voraussetzungen

- Die Firmware-Version der Intel XL710 NIC (NIC) auf dem KVM-Host ist 5.04.
- Der KVM-Host unterstützt Input-Output Memory Management Unit (IOMMU) und Intel VT-d, und diese sind im BIOS des KVM-Hosts aktiviert. Um IOMMU auf dem KVM-Host zu aktivieren, fügen Sie den folgenden Eintrag zur Datei **/boot/grub2/grub.cfg** hinzu: **intel_iommu=1**
- Führen Sie den folgenden Befehl aus und starten Sie den KVM-Host neu: **Grub2-mkconfig –o /boot/grub2/grub.cfg**

**So konfigurieren Sie NetScaler VPX-Instanzen zur Verwendung von PCI-Passthrough-Netzwerkschnittstellen mithilfe des Virtual Machine Managers:**

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

1. Schalten Sie die NetScaler VPX-Instanz aus.
2. Wählen Sie die NetScaler VPX-Instanz aus und klicken Sie auf **Öffnen**.

3. Klicken Sie im Fenster **virtual_machine on KVM>** auf das **i**-Symbol.

4. Klicken Sie auf **Hardware hinzufügen**.
5. Gehen Sie im Dialogfeld **Neue virtuelle Hardware hinzufügen** wie folgt vor:

   a. Wählen Sie **PCI-Hostgerät** aus.

   b. Wählen Sie im Abschnitt **Host-Gerät** die physische Funktion Intel XL710 aus.

   c. Klicken Sie auf **Fertig stellen**.

6. Wiederholen Sie die Schritte **4** und **5**, um weitere physische Funktionen von Intel XL710 hinzuzufügen.
7. Schalten Sie die NetScaler VPX-Instanz ein.
8. Sobald die NetScaler VPX-Instanz eingeschaltet ist, können Sie den folgenden Befehl verwenden, um die Konfiguration zu überprüfen:

   Die Ausgabe muss alle Schnittstellen anzeigen, die Sie konfiguriert haben:

## NetScaler VPX-Instanz mithilfe des `virsh`-Programms bereitstellen

Das `virsh`-Programm ist ein Befehlszeilentool zur Verwaltung von VM-Gästen. Seine Funktionalität ähnelt der des Virtual Machine Managers. Es ermöglicht Ihnen, den Status eines VM-Gastes zu ändern (Starten, Stoppen, Anhalten usw.), neue Gäste und Geräte einzurichten und bestehende Konfigurationen zu bearbeiten. Das `virsh`-Programm ist auch nützlich für die Skripterstellung von VM-Gast-Verwaltungsvorgängen.

Um NetScaler VPX mithilfe des `virsh`-Programms bereitzustellen, gehen Sie wie folgt vor:

1. Verwenden Sie den tar-Befehl, um das NetScaler VPX-Paket zu entpacken. Das NSVPX-KVM-*_nc.tgz-Paket enthält die folgenden Komponenten:

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

- Die Domain-XML-Datei, die VPX-Attribute angibt \[NSVPX-KVM-*_nc.xml\]
- Prüfsumme des NS-VM-Festplatten-Images \[Checksum.txt\]
- NS-VM-Festplatten-Image \[NSVPX-KVM-*_nc.raw\]

Beispiel:

```
tar -xvzf NSVPX-KVM-10.1-117_nc.tgz

NSVPX-KVM-10.1-117_nc.xml

NSVPX-KVM-10.1-117_nc.raw

checksum.txt
```

2. Kopieren Sie die Datei `NSVPX-KVM-*\_nc.xml XML` in eine Datei namens `\<DomainName\>-NSVPX-KVM-*\_nc.xml`. Der \<DomainName\> ist auch der Name der virtuellen Maschine. Beispiel:

```
cp NSVPX-KVM-10.1-117_nc.xml NetScaler-VPX-NSVPX-KVM-10.1-117_nc.xml
```

3. Bearbeiten Sie die Datei `\<DomainName\>-NSVPX-KVM-*\_nc.xml`, um die folgenden Parameter anzugeben:

   - Name – Geben Sie den Namen an.
   - MAC – Geben Sie die MAC-Adresse an.

     **HINWEIS:**

     Der Domänenname und die MAC-Adresse müssen eindeutig sein.

   - Quelldatei – Geben Sie den absoluten Quellpfad des Festplatten-Images an. Der Dateipfad muss absolut sein. Sie können den Pfad der RAW-Image-Datei oder einer QCOW2-Image-Datei angeben.

     Wenn Sie eine RAW-Imagedatei angeben möchten, geben Sie den Quellpfad des Datenträger-Images wie im folgenden Beispiel gezeigt an:

     Beispiel:

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

```
<name>NetScaler-VPX</name>

<mac address='52:54:00:29:74:b3'/>

<source file='/root/NSVPX-KVM-10.1-117_nc.raw'/>
```

Geben Sie den absoluten QCOW2-Datenträger-Image-Quellpfad an und definieren Sie den Treibertyp als **qcow2**, wie im folgenden Beispiel gezeigt:

Beispiel:

```
<name>NetScaler-VPX</name>

<mac address='52:54:00:29:74:b3'/>

<driver name ='qemu' type='qcow2'/>

<source file='/root/NSVPX-KVM-10.1-117_nc.qcow'/>*
```

4. Bearbeiten Sie die Datei `\<DomainName\>-NSVPX-KVM-*\_nc.xml`, um die Netzwerkdetails zu konfigurieren:

   - source dev – geben Sie die Schnittstelle an.
   - mode – geben Sie den Modus an. Die Standardschnittstelle ist **Macvtap Bridge**.

   Beispiel: Modus: MacVTap Bridge Zielschnittstelle als `ethx` und Modus als Bridge Modelltyp als `virtio` festlegen

   ```
   <interface type='direct'>

       <mac address='52:54:00:29:74:b3'/>

       <source dev='eth0' mode='bridge'/>

       <target dev='macvtap0'/>

       <model type='virtio'/>

       <alias name='net0'/>

       <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
   ```

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

```
function='0x0'/>

  </interface>
```

Hier ist eth0 die physische Schnittstelle, die an die VM angeschlossen ist.

5. Definieren Sie die VM-Attribute in der Datei `\<DomainName\>-NSVPX-KVM-*\_nc.xml` mit dem folgenden Befehl:

```
virsh define \<DomainName\>-NSVPX-KVM-\*\_nc.xml
```

Beispiel:

```


virsh define NS-VPX-NSVPX-KVM-10.1-117_nc.xml
```

6. Starten Sie die VM, indem Sie den folgenden Befehl eingeben:

```
virsh start \[\<DomainName\> | \<DomainUUID\>\]
```

Beispiel:

```
virsh start NetScaler-VPX
```

7. Verbinden Sie die Gast-VM über die Konsole:

```
virsh console \[\<DomainName\> | \<DomainUUID\> |\<DomainID\> \]
```

Beispiel:

```
virsh console NetScaler-VPX
```

## Weitere Schnittstellen zur NetScaler VPX-Instanz mit dem `virsh`-Programm hinzufügen

Nachdem Sie die NetScaler VPX auf KVM bereitgestellt haben, können Sie zusätzliche Schnittstellen hinzufügen.

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

Um weitere Schnittstellen hinzuzufügen, gehen Sie wie folgt vor:

1. Fahren Sie die NetScaler VPX-Instanz herunter, die auf dem KVM ausgeführt wird.
2. Bearbeiten Sie die `\<DomainName\>-NSVPX-KVM-*\_nc.xml`-Datei mit dem Befehl:

   ```
   virsh edit \[\<DomainName\> | \<DomainUUID\>\]
   ```

3. Fügen Sie in der `\<DomainName\>-NSVPX-KVM-*\_nc.xml`-Datei die folgenden Parameter an:

   a. **Für MacVTap**

   - Schnittstellentyp— Geben Sie den Schnittstellentyp als „direct“ an.
   - MAC-Adresse— Geben Sie die MAC-Adresse an und stellen Sie sicher, dass die MAC-Adresse über alle Schnittstellen hinweg eindeutig ist.
   - Quell-Dev— Geben Sie den Schnittstellennamen an.
   - Modus— Geben Sie den Modus an. Die unterstützten Modi sind – Bridge, VEPA, Private und Pass-through.
   - Modelltyp— Geben Sie den Modelltyp als `virtio` an.

   Beispiel:

   Modus: MacVTap Pass-through

   Zielschnittstelle festlegen als `ethx`, Modus als Bridge und Modelltyp als `virtio`

   ```
   <interface type='direct'>

         <mac address='52:54:00:29:74:b3'/>

         <source dev='eth1' mode='passthrough'/>

         <model type='virtio'/>

    </interface>
   ```

   Hier ist eth1 die physische Schnittstelle, die an die VM angeschlossen ist.

   b. **Für den Bridge-Modus**

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

**HINWEIS:**

Stellen Sie sicher, dass Sie eine Linux-Bridge im KVM-Host konfiguriert, die physische Schnittstelle an die Bridge gebunden und die Bridge in den UP-Zustand versetzt haben.

- Schnittstellentyp – Geben Sie den Schnittstellentyp als 'bridge' an.
- MAC-Adresse – Geben Sie die MAC-Adresse an und stellen Sie sicher, dass die MAC-Adresse über alle Schnittstellen hinweg eindeutig ist.
- Quell-Bridge – Geben Sie den Bridge-Namen an.
- Modelltyp – Geben Sie den Modelltyp als `virtio` an.

Beispiel: Bridge-Modus

```
<interface type='bridge'>

      <mac address='52:54:00:2d:43:a4'/>

      <source bridge='br0'/>

      <model type='virtio'/>

 </interface>
```

# Verwalten der NetScaler VPX Gast-VMs

Sie können den Virtual Machine Manager und das `virsh` Programm verwenden, um Verwaltungsaufgaben durchzuführen, wie z.B. das Starten oder Stoppen einer VM-Gastinstanz, das Einrichten neuer Gastinstanzen und Geräte, das Bearbeiten bestehender Konfigurationen und das Herstellen einer Verbindung zur grafischen Konsole über Virtual Network Computing (VNC).

## Verwalten der VPX Gast-VMs mithilfe des Virtual Machine Managers

- Auflisten der VM-Gastinstanzen

  Das Hauptfenster des Virtual Machine Managers zeigt eine Liste aller VM-Gastinstanzen für jeden VM-Hostserver an, mit dem es verbunden ist. Jeder VM-Gasteintrag enthält den Namen der virtuellen Maschine zusammen mit ihrem Status (Wird ausgeführt, Angehalten oder Heruntergefahren), der wie im Symbol angezeigt wird.

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

- Eine grafische Konsole öffnen

  Das Öffnen einer grafischen Konsole für eine VM-Gastinstanz ermöglicht Ihnen die Interaktion mit der Maschine, wie Sie es mit einem physischen Host über eine VNC-Verbindung tun würden. Um die grafische Konsole im Virtual Machine Manager zu öffnen, klicken Sie mit der rechten Maustaste auf den VM-Gasteintrag und wählen Sie die Option „Öffnen“ aus dem Kontextmenü.

- Starten und Herunterfahren einer Gastinstanz

  Sie können eine VM-Gastinstanz über den Virtual Machine Manager starten oder stoppen. Um den Status der VM zu ändern, klicken Sie mit der rechten Maustaste auf den VM-Gasteintrag und wählen Sie „Ausführen“ oder eine der Optionen zum Herunterfahren aus dem Kontextmenü.

- Neustarten einer Gastinstanz

  Sie können eine VM-Gastinstanz über den Virtual Machine Manager neu starten. Um die VM neu zu starten, klicken Sie mit der rechten Maustaste auf den VM-Gasteintrag und wählen Sie dann „Herunterfahren > Neustart“ aus dem Kontextmenü.

- Löschen einer Gastinstanz

  Das Löschen einer VM-Gastinstanz entfernt standardmäßig deren XML-Konfiguration. Sie können auch die Speicherdateien einer Gastinstanz löschen. Dadurch wird die Gastinstanz vollständig gelöscht.

  a. Klicken Sie im Virtual Machine Manager mit der rechten Maustaste auf den VM-Gasteintrag.
  b. Wählen Sie im Kontextmenü die Option Löschen. Ein Bestätigungsfenster wird geöffnet.

     **HINWEIS:**

     Die Option Löschen ist nur aktiviert, wenn der VM-Gast heruntergefahren ist.

  c. Klicken Sie auf **Löschen**.
  d. Um den Gast vollständig zu löschen, löschen Sie die zugehörige .raw-Datei, indem Sie das Kontrollkästchen 'Zugehörige Speicherdateien löschen' aktivieren.

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

## Verwalten der NetScaler VPX Gast-VMs mithilfe des `virsh` Programms

- Listen Sie die VM-Gäste und deren aktuellen Status auf.

  Um `virsh` zu verwenden, um Informationen über die Gäste anzuzeigen

  `virsh list --all`

  Die Befehlsausgabe zeigt alle Domänen mit ihrem Status an. Beispielausgabe:

  ```
  Id Name                 State

  ----------------------------------

    0 Domain-0           running

    1 Domain-1           paused

    2 Domain-2           inactive

    3 Domain-3           crashed
  ```

- Öffnen Sie eine `virsh` Konsole.

  Verbinden Sie die Gast-VM über die Konsole

  `virsh console [<DomainID> | <DomainName> | <DomainUUID>]`

  Beispiel:

  `virsh console NetScaler-VPX`

- Einen Gast starten und herunterfahren.

  Gäste können mit dem DomainNamen oder der Domain-UUID gestartet werden.

  `virsh start [<DomainName> | <DomainUUID>]`

  Beispiel:

  `virsh start NetScaler-VPX`

  **So fahren Sie einen Gast herunter**:

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

`virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]`

Beispiel:

`virsh shutdown NetScaler-VPX`

- Einen Gast neu starten

`virsh reboot [<DomainID> | <DomainName> | <DomainUUID>]`

Beispiel:

`virsh reboot NetScaler-VPX`

Einen Gast löschen

Um eine Gast-VM zu löschen, müssen Sie den Gast herunterfahren und die \<DomainName\>-NSVPX-KVM-*_nc.xml undefinieren, bevor Sie den Löschbefehl ausführen.

```
virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]

virsh undefine [<DomainName> | <DomainUUID>]
```

Beispiel:

```
virsh shutdown NetScaler-VPX

virsh undefine NetScaler-VPX
```

**HINWEIS:**

Der Löschbefehl entfernt die Disk-Image-Datei nicht, diese muss manuell entfernt werden.

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

# Konfigurieren einer NetScaler VPX-Instanz auf KVM zur Verwendung von OVS DPDK-basierten Host-Schnittstellen

Sie können eine NetScaler VPX-Instanz, die auf KVM (Fedora und RHOS) ausgeführt wird, so konfigurieren, dass sie Open vSwitch (OVS) mit Data Plane Development Kit (DPDK) für eine bessere Netzwerkleistung verwendet. Dieses Dokument beschreibt, wie die NetScaler VPX-Instanz konfiguriert wird, um auf den von OVS-DPDK auf dem KVM-Host bereitgestellten `vhost-user` Ports zu arbeiten.

OVS ist ein mehrschichtiger virtueller Switch, der unter der Open-Source-Lizenz Apache 2.0 lizenziert ist. DPDK ist eine Reihe von Bibliotheken und Treibern für die schnelle Paketverarbeitung.

Die folgenden Fedora-, RHOS-, OVS- und DPDK-Versionen sind für die Konfiguration einer NetScaler VPX-Instanz qualifiziert:

| FEDORA | RHOS |
|---|---|
| Fedora 25 | RHOS 7.4 |
| OVS 2.7.0 | OVS 2.6.1 |
| DPDK 16.11.12 | DPDK 16.11.12 |

## Voraussetzungen

Bevor Sie DPDK installieren, stellen Sie sicher, dass der Host über 1 GB Huge Pages verfügt.

Weitere Informationen finden Sie in dieser DPDK-Systemanforderungen-Dokumentation. Hier ist eine Zusammenfassung der Schritte, die erforderlich sind, um eine NetScaler VPX-Instanz auf KVM für die Verwendung von OVS DPDK-basierten Host-Schnittstellen zu konfigurieren:

- DPDK installieren.
- OVS erstellen und installieren.
- Eine OVS-Bridge erstellen.
- Eine physische Schnittstelle an die OVS-Bridge anhängen.
- `vhost-user` Ports an den OVS-Datenpfad anhängen.
- Eine KVM-VPX mit OVS-DPDK-basierten `vhost-user` Ports bereitstellen.

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

## DPDK installieren

Um DPDK zu installieren, folgen Sie den Anweisungen in diesem Dokument Open vSwitch with DPDK.

## OVS erstellen und installieren

Laden Sie OVS von der OVS-Download-Seite herunter. Erstellen und installieren Sie anschließend OVS mithilfe eines DPDK-Datenpfads. Befolgen Sie die Anweisungen im Dokument Installing Open vSwitch.

Weitere detaillierte Informationen finden Sie im DPDK Getting Started Guide for Linux.

## Eine OVS-Bridge erstellen

Geben Sie je nach Bedarf den Fedora- oder RHOS-Befehl ein, um eine OVS-Bridge zu erstellen:

**Fedora-Befehl**:

```
> $OVS_DIR/utilities/ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
datapath_type=netdev
```

**RHOS-Befehl**:

```
ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0 datapath_type=netdev
```

## Physische Schnittstelle an die OVS-Bridge anbinden

Binden Sie die Ports an DPDK und verbinden Sie sie dann mit der OVS-Bridge, indem Sie die folgenden Fedora- oder RHOS-Befehle eingeben:

**Fedora-Befehl**:

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface
dpdk0 type=dpdk  options:dpdk-devargs=0000:03:00.0
```

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

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface
dpdk1 type=dpdk  options:dpdk-devargs=0000:03:00.1
```

**RHOS-Befehl**:

```
ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
 options:dpdk-devargs=0000:03:00.0




ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface dpdk1 type=dpdk
 options:dpdk-devargs=0000:03:00.1
```

Das `dpdk-devargs`, das als Teil der Optionen angezeigt wird, gibt den PCI-BDF der jeweiligen physischen NIC an.

## `vhost-user`-Ports an den OVS-Datenpfad anbinden

Geben Sie die folgenden Fedora- oder RHOS-Befehle ein, um `vhost-user`-Ports an den OVS-Datenpfad anzubinden:

**Fedora-Befehl**:

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user1 -- set
Interface vhost-user1 type=dpdkvhostuser -- set Interface vhost-user1
 mtu_request=9000



> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user2 -- set
Interface vhost-user2 type=dpdkvhostuser -- set Interface vhost-user2
 mtu_request=9000



chmod g+w  /usr/local/var/run/openvswitch/vhost*
```

**RHOS-Befehl**:

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

```
ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1
type=dpdkvhostuser -- set Interface vhost-user1  mtu_request=9000



ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2
type=dpdkvhostuser -- set Interface vhost-user2  mtu_request=9000



chmod g+w /var/run/openvswitch/vhost*
```

## Eine KVM-VPX mit OVS-DPDK-basierten `vhost-user`-Ports bereitstellen

Sie können eine VPX-Instanz auf Fedora KVM mit OVS-DPDK-basierten `vhost-user`-Ports nur über die CLI bereitstellen, indem Sie die folgenden QEMU-Befehle verwenden: **Fedora-Befehl**:

```
qemu-system-x86_64 -name KVM-VPX -cpu host -enable-kvm -m 4096M \



-object memory-backend-file,id=mem,size=4096M,mem-path=/dev/
hugepages,share=on -numa node,memdev=mem \



-mem-prealloc -smp sockets=1,cores=2 -drive file=<absolute-path-to-disc-
image-file>,if=none,id=drive-ide0-0-0,format=<disc-image-format> \



-device ide-drive,bus=ide.0,unit=0,drive=drive-
ide0-0-0,id=ide0-0-0,bootindex=1 \



-netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \



-device virtio-net-
```

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

```
pci,netdev=hostnet0,id=net0,mac=52:54:00:3c:d1:ae,bus=pci.0,addr=0x3 \



-chardev socket,id=char0,path=</usr/local/var/run/openvswitch/vhost-user1>
\



-netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device virtio-
net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \



-chardev socket,id=char1,path=</usr/local/var/run/openvswitch/vhost-user2>
\



-netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device virtio-
net



pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \



--nographic
```

Verwenden Sie für RHOS die folgende Beispiel-XML-Datei, um die NetScaler VPX-Instanz mithilfe von `virsh` bereitzustellen.

```
<domain type='kvm'>



  <name>dpdk-vpx1</name>



  <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
```

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

```
<memory unit='KiB'>16777216</memory>

<currentMemory unit='KiB'>16777216</currentMemory>

<memoryBacking>

  <hugepages>

    <page size='1048576' unit='KiB'/>

  </hugepages>

</memoryBacking>

<vcpu placement='static'>6</vcpu>

<cputune>

  <shares>4096</shares>

  <vcpupin vcpu='0' cpuset='0'/>
```

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

```
    <vcpupin vcpu='1' cpuset='2'/>

    <vcpupin vcpu='2' cpuset='4'/>

    <vcpupin vcpu='3' cpuset='6'/>

    <emulatorpin cpuset='0,2,4,6'/>

  </cputune>

  <numatune>

    <memory mode='strict' nodeset='0'/>

  </numatune>

  <resource>

    <partition>/machine</partition>

  </resource>
```

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

```
<os>

  <type arch='x86\_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>

  <boot dev='hd'/>

</os>

<features>

  <acpi/>

  <apic/>

</features>

<cpu mode='custom' match='minimum' check='full'>

  <model fallback='allow'>Haswell-noTSX</model>

  <vendor>Intel</vendor>
```

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

```
    <topology sockets='1' cores='6' threads='1'/>

    <feature policy='require' name='ss'/>

    <feature policy='require' name='pcid'/>

    <feature policy='require' name='hypervisor'/>

    <feature policy='require' name='arat'/>

<domain type='kvm'>

  <name>dpdk-vpx1</name>

  <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>

  <memory unit='KiB'>16777216</memory>

  <currentMemory unit='KiB'>16777216</currentMemory>

  <memoryBacking>
```

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

```
    <hugepages>

      <page size='1048576' unit='KiB'/>

    </hugepages>

  </memoryBacking>

  <vcpu placement='static'>6</vcpu>

  <cputune>

    <shares>4096</shares>

    <vcpupin vcpu='0' cpuset='0'/>

    <vcpupin vcpu='1' cpuset='2'/>

    <vcpupin vcpu='2' cpuset='4'/>

    <vcpupin vcpu='3' cpuset='6'/>
```

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

```
  <emulatorpin cpuset='0,2,4,6'/>

</cputune>

<numatune>

  <memory mode='strict' nodeset='0'/>

</numatune>

<resource>

  <partition>/machine</partition>

</resource>

<os>

  <type arch='x86\_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>

  <boot dev='hd'/>
```

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

```
</os>

<features>

  <acpi/>

  <apic/>

</features>

<cpu mode='custom' match='minimum' check='full'>

  <model fallback='allow'>Haswell-noTSX</model>

  <vendor>Intel</vendor>

  <topology sockets='1' cores='6' threads='1'/>

  <feature policy='require' name='ss'/>

  <feature policy='require' name='pcid'/>
```

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

```
    <feature policy='require' name='hypervisor'/>

    <feature policy='require' name='arat'/>

    <feature policy='require' name='tsc\_adjust'/>

    <feature policy='require' name='xsaveopt'/>

    <feature policy='require' name='pdpe1gb'/>

    <numa>

      <cell id='0' cpus='0-5' memory='16777216' unit='KiB'
memAccess='shared'/>

    </numa>

  </cpu>

  <clock offset='utc'/>

  <on\_poweroff>destroy</on\_poweroff>
```

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

```
  <on\_reboot>restart</on\_reboot>

  <on\_crash>destroy</on\_crash>

  <devices>

    <emulator>/usr/libexec/qemu-kvm</emulator>

    <disk type='file' device='disk'>

      <driver name='qemu' type='qcow2' cache='none'/>

      <source file='/home/NSVPX-KVM-12.0-52.18\_nc.qcow2'/>

      <target dev='vda' bus='virtio'/>

      <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
function='0x0'/>

    </disk>
```

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

```
    <controller type='ide' index='0'>


      <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
function='0x1'/>


    </controller>


    <controller type='usb' index='0' model='piix3-uhci'>


      <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
function='0x2'/>


    </controller>


    <controller type='pci' index='0' model='pci-root'/>


    <interface type='direct'>


      <mac address='52:54:00:bb:ac:05'/>


      <source dev='enp129s0f0' mode='bridge'/>


      <model type='virtio'/>
```

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

```
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
function='0x0'/>


    </interface>


    <interface type='vhostuser'>


      <mac address='52:54:00:55:55:56'/>


      <source type='unix' path='/var/run/openvswitch/vhost-user1'
mode='client'/>


      <model type='virtio'/>


      <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
function='0x0'/>


    </interface>


    <interface type='vhostuser'>


      <mac address='52:54:00:2a:32:64'/>
```

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

```
      <source type='unix' path='/var/run/openvswitch/vhost-user2'
mode='client'/>


      <model type='virtio'/>


      <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
function='0x0'/>


    </interface>


    <interface type='vhostuser'>


      <mac address='52:54:00:2a:32:74'/>


      <source type='unix' path='/var/run/openvswitch/vhost-user3'
mode='client'/>


      <model type='virtio'/>


      <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
function='0x0'/>


    </interface>
```

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

```
    <interface type='vhostuser'>

      <mac address='52:54:00:2a:32:84'/>

      <source type='unix' path='/var/run/openvswitch/vhost-user4'
mode='client'/>

     <model type='virtio'/>

      <address type='pci' domain='0x0000' bus='0x00' slot='0x09'
function='0x0'/>

    </interface>

    <serial type='pty'>

      <target port='0'/>

    </serial>

    <console type='pty'>
```

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

```
      <target type='serial' port='0'/>


    </console>


    <input type='mouse' bus='ps2'/>


    <input type='keyboard' bus='ps2'/>


    <graphics type='vnc' port='-1' autoport='yes'>


      <listen type='address'/>


    </graphics>


    <video>


      <model type='cirrus' vram='16384' heads='1' primary='yes'/>


      <address type='pci' domain='0x0000' bus='0x00' slot='0x02'
function='0x0'/>


    </video>
```

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

```
    <memballoon model='virtio'>


      <address type='pci' domain='0x0000' bus='0x00' slot='0x08'
function='0x0'/>


    </memballoon>


  </devices>


</domain
```

## Hinweise

In der XML-Datei muss die `hugepage`-Größe 1 GB betragen, wie in der Beispieldatei gezeigt.

```
<memoryBacking>


    <hugepages>


      <page size='1048576' unit='KiB'/>


    </hugepages>
```

Außerdem ist in der Beispieldatei vhost-user1 der `vhost`-Benutzerport, der an ovs-br0 gebunden ist.

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

```
<interface type='vhostuser'>


      <mac address='52:54:00:55:55:56'/>


      <source type='unix' path='/var/run/openvswitch/vhost-user1'
mode='client'/>


      <model type='virtio'/>


      <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
function='0x0'/>


    </interface>
```

Um die NetScaler VPX-Instanz zu starten, verwenden Sie den Befehl `virsh`.

## NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance auf dem KVM-Hypervisor anwenden

Sie können die NetScaler VPX-Konfigurationen auf dem KVM-Hypervisor während des ersten Starts der NetScaler Appliance anwenden. Daher kann ein Kunden-Setup auf einer VPX-Instanz in wesentlich kürzerer Zeit konfiguriert werden.

Weitere Informationen zu Preboot-Benutzerdaten und deren Format finden Sie unter Anwenden von NetScaler VPX-Konfigurationen beim ersten Start der NetScaler Appliance in der Cloud.

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

**HINWEIS:**

Um mit Preboot-Benutzerdaten im KVM-Hypervisor zu booten, muss die Standard-Gateway-Konfiguration im Abschnitt `<NS-CONFIG>` übergeben werden. Weitere Informationen zum Inhalt des Tags `<NS-CONFIG>` finden Sie im folgenden Beispielabschnitt `<NS-CONFIG>`.

**Beispielabschnitt `<NS-CONFIG>`:**

```
<NS-PRE-BOOT-CONFIG>



    <NS-CONFIG>

        add route 0.0.0.0 0.0.0.0  10.102.38.1

    </NS-CONFIG>



    <NS-BOOTSTRAP>

            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>

            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>



        <MGMT-INTERFACE-CONFIG>

                <INTERFACE-NUM> eth0 </INTERFACE-NUM>

                <IP> 10.102.38.216 </IP>

                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>

        </MGMT-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>
```

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

```
</NS-PRE-BOOT-CONFIG>
```

## So stellen Sie Preboot-Benutzerdaten auf dem KVM-Hypervisor bereit

Sie können Preboot-Benutzerdaten auf dem KVM-Hypervisor über eine ISO-Datei bereitstellen, die über ein CD-ROM-Gerät angehängt wird.

## Benutzerdaten mithilfe einer CD-ROM-ISO-Datei bereitstellen

Sie können den Virtual Machine Manager (VMM) verwenden, um Benutzerdaten als ISO-Image über das CD-ROM-Gerät in die virtuelle Maschine (VM) zu einschleusen. KVM unterstützt CD-ROMs in VM-Gästen, entweder durch direkten Zugriff auf ein physisches Laufwerk auf dem VM-Hostserver oder durch Zugriff auf ISO-Images.

Die folgenden Schritte ermöglichen Ihnen die Bereitstellung von Benutzerdaten mithilfe der CD-ROM-ISO-Datei:

1. Erstellen Sie eine Datei mit dem Dateinamen `userdata`, die den Inhalt der Preboot-Benutzerdaten enthält.

   **HINWEIS:**

   Der Dateiname muss strikt als `userdata` verwendet werden.

2. Speichern Sie die Datei `userdata` in einem Ordner und erstellen Sie ein ISO-Image aus diesem Ordner.

   Sie können ein ISO-Image mit der `userdata`-Datei auf die folgenden zwei Arten erstellen:

   - Verwenden eines beliebigen Bildverarbeitungstools wie PowerISO.
   - Verwenden des `mkisofs`-Befehls in Linux.

   Die folgende Beispielkonfiguration zeigt, wie ein ISO-Image mithilfe des `mkisofs`-Befehls in Linux generiert wird.

   ```
   root@ubuntu:~/sai/19oct# ls -lh

   total 4.0K
   ```

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

```
-rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata

root@ubuntu:~/sai/19oct#

root@ubuntu:~/sai/19oct# mkisofs -o kvm-userdata.iso userdata

I: -input-charset not specified, using utf-8 (detected in locale
settings)

Total translation table size: 0

Total rockridge attributes bytes: 0

Total directory bytes: 0

Path table size(bytes): 10

Max brk space used 0

175 extents written (0 MB)

root@ubuntu:~/sai/19oct#

root@ubuntu:~/sai/19oct# ls -lh

total 356K

-rw-r--r-- 1 root root 350K Oct 19 16:25 kvm-userdata.iso

-rw-r--r-- 1 root root 1.1K Oct 19 16:25 userdata
```

3. Stellen Sie die NetScaler VPX-Instanz mithilfe des Standardbereitstellungsprozesses bereit, um die VM zu erstellen. Schalten Sie die VM jedoch nicht automatisch ein.
4. Fügen Sie ein CD-ROM-Gerät mit dem Virtual Machine Manager mithilfe der folgenden Schritte hinzu:

   a. Doppelklicken Sie auf einen VM-Gast-Eintrag im Virtual Machine Manager, um dessen Konsole zu öffnen, und wechseln Sie zur Detailansicht mit **View > Details**.

   b. Klicken Sie auf **Hardware hinzufügen > Speicher > Gerätetyp > CDROM-Gerät**.

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

c. Klicken Sie auf **Verwalten**, wählen Sie die richtige ISO-Datei aus und klicken Sie auf **Fertig stellen**. Ein neues CD-ROM-Laufwerk unter **Ressourcen** auf Ihrer NetScaler VPX-Instanz wird erstellt.

5. Schalten Sie die VM ein.

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

# NetScaler VPX auf Red Hat OpenShift Virtualization installieren

NetScaler® bietet ein dediziertes VPX-Image für Red Hat® OpenShift® Virtualization (RHOCPV), das die Bereitstellungs- und Verwaltungserfahrung erheblich verbessert. Sie können Instanzen jetzt über die RHOCPV-Konsole bereitstellen. Kunden erhalten offiziellen Support und Zugriff auf alle notwendigen Ressourcen. Dies stellt sicher, dass Sie nahtlos auf der RHOCPV-Infrastruktur bereitstellen können.

**WICHTIG:**

RHOCPV-Unterstützung ist in NetScaler Release 14.1 Build 66.64 und höher verfügbar. Nach der allgemeinen Verfügbarkeit (GA) können Sie das RHOCPV-Image verwenden, um virtuelle NetScaler VPX™-Maschinen auf RHOCPV bereitzustellen.

## Systemanforderungen

Die CPU- und Speicheranforderungen für die Bereitstellung von NetScaler VPX auf RHOCPV hängen vom VPX-Modell und der erwarteten Arbeitslast ab.

- **CPU**: Mindestens 2 vCPUs
- **Arbeitsspeicher**: Mindestens 4 GB RAM
- **Speicher**: Mindestens 20 GB Festplattenspeicher

**HINWEIS:**

Ab NetScaler Release 14.1-72.x kann NetScaler VPX auf RHOCPV mit 2 GB RAM bereitgestellt werden.

## NetScaler VPX-Instanzen auf OpenShift Virtualization installieren

Befolgen Sie dieses Schritt-für-Schritt-Verfahren, um NetScaler VPX auf der RHOCPV-Konsole zu installieren.

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

**Schritt 1. Umgebung vorbereiten.**

- Stellen Sie sicher, dass Ihr RHOCPV-Cluster betriebsbereit ist.
- Stellen Sie sicher, dass Sie Administratorzugriff zum Erstellen der VMs haben.
- Stellen Sie sicher, dass der Virtualisierungsoperator aktiviert ist, um VMs zu erstellen und zu verwalten.

**Schritt 2. NetScaler VPX-Image abrufen.**

1. Navigieren Sie zu **Citrix.com > Downloads > NetScaler > Virtual Appliances**, und laden Sie das mit RHOCPV kompatible NetScaler VPX-Image von der Seite Citrix Downloads herunter.
2. Extrahieren Sie die heruntergeladene Datei „NSVPX-RHOV-`<version-build>`_lx_64.tgz“, um die qcow2-Imagedatei zu erhalten.

   **HINWEIS:**

   Laden Sie für eine FIPS-Bereitstellung stattdessen das FreeBSD-basierte NetScaler VPX FIPS-Image herunter, das das Namensformat `NSVPX-RHOCPV-<release-build>.fips_nc_64.tgz` verwendet (zum Beispiel `NSVPX-RHOCPV-14.1-72.61.fips_nc_64.tgz`). VPX FIPS auf RHOCPV wird ab NetScaler Release 14.1-72.x unterstützt. Weitere Informationen finden Sie unter VPX FIPS-Appliances.

**Schritt 3. Image auf das bootfähige RHOCPV-Volume hochladen.**

1. Melden Sie sich bei Ihrer Red Hat OpenShift-Konsole an.
2. Navigieren Sie im Dashboard zu **Virtualization > Bootable Volumes**.
3. Klicken Sie oben rechts auf **Add volume** und wählen Sie **With Form**.
4. Laden Sie die NetScaler VPX-Imagedatei hoch.

5. Geben Sie einen Namen für das Volume ein.
6. Klicken Sie auf **Save**.

**Schritt 4. Erstellen Sie die NetScaler VPX VM.**

Sie können die VM entweder über den Instanztyp oder die YAML-Konfiguration erstellen.

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

**Option 1. VM aus Instanztyp erstellen:**

1. Gehen Sie zu **Virtualization > VirtualMachine** und klicken Sie auf **Create**.
2. Wählen Sie **From InstanceType**.
3. Wählen Sie das bootfähige Volume aus, das Sie in Schritt 3 erstellt haben.

4. Wählen Sie einen Instanztyp, der den Hardware-Spezifikationen der VM für Ihr VPX-Modell entspricht. Weitere Informationen finden Sie unter Systemanforderungen.

5. Geben Sie einen Namen für die VM ein.
6. Klicken Sie auf **Create VirtualMachine**.

**Option 2. VM mit YAML erstellen:**

1. Gehen Sie zu **Virtualization > VirtualMachine** und klicken Sie auf **Create**.
2. Wählen Sie **With YAML**.
3. Bearbeiten Sie die erforderlichen Felder mit Ihren Werten.
4. Aktualisieren Sie die Startdiskette so, dass sie auf das NetScaler-Image verweist, das Sie in **Schritt 3** importiert haben.

   **Beispiel-YAML-Datei:**

```
apiVersion: kubevirt.io/v1

kind: VirtualMachine

metadata:

name: <vm-name>

annotations:

description: <VM description>

labels:

app: default
```

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

```
os.template.kubevirt.io/rhel10: 'true'

spec:

runStrategy: Once

template:

metadata:

annotations:

  vm.kubevirt.io/flavor: small

  vm.kubevirt.io/os: rhel10

  vm.kubevirt.io/workload: server

labels:

  kubevirt.io/domain: default

  kubevirt.io/size: small

spec:

 domain:

  cpu:

    cores: <2>

    sockets: 1

    threads: 1

  devices:

    disks:

      - disk:

          bus: virtio
```

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

```
        name: <disk-name>
    interfaces:
      - masquerade: {}
        model: virtio
        name: default
    networkInterfaceMultiqueue: true
    rng: {}
  memory:
    guest: <4Gi>
hostname: <vm-name>
networks:
  - name: default
    pod: {}
terminationGracePeriodSeconds: 180
volumes:
  - name: <diskname>
    persistentVolumeClaim:
      claimName: <14.1-66.4-lx-amd64>
```

5. Klicken Sie auf **Erstellen**.

**Schritt 5. Konfigurieren Sie die NetScaler VPX VM.**

1. Gehen Sie zu **Virtualisierung > Virtuelle Maschine** und wählen Sie die neu erstellte NetScaler VM aus.

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

2. Vergewissern Sie sich, dass sich die VM im Zustand **Ausgeschaltet** befindet.
3. Klicken Sie auf **Konfiguration**. Überprüfen Sie die Konfigurationsoptionen im Abschnitt **Netzwerk** und konfigurieren Sie die VM-Schnittstellen: Management und Daten.

   **HINWEIS:**

   Die RHOCPV-GUI zeigt die Netzwerkschnittstellen manchmal in einer anderen Reihenfolge an, als Sie sie hinzugefügt haben. Überprüfen Sie jede Schnittstelle anhand ihrer MAC-Adresse und Konfiguration, anstatt sich auf die angezeigte Reihenfolge zu verlassen.

**Schritt 6. Konfigurieren Sie die Management-IP-Adresse.**

1. Beim ersten Start verwendet NetScaler eine Standard-IP-Adresse für das Management-Netzwerk. Führen Sie die folgenden Schritte aus, um die Management-IP-Adresse zu konfigurieren:
2. Legen Sie die Management-IP-Adresse und die Netzmaske mit dem folgenden Befehl fest:

   ```
   set ns config -IPAddress <ip> -netmask <mask>
   ```

3. Fügen Sie die Standardroute mit dem folgenden Befehl hinzu:

   ```
   add route <network> <netmask> <gateway>
   ```

4. Speichern Sie die Konfiguration mit dem folgenden Befehl:

   ```
   save config
   ```

5. Starten Sie die VM neu, damit die Änderungen wirksam werden.
6. Nachdem die VPX-Instanz gestartet ist, greifen Sie über die NetScaler-Konsole oder die NSIP-Adresse auf die Verwaltungsoberfläche zu.

**Schritt 7. Konfiguration abschließen.**

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

Nachdem Sie die Lizenzen angewendet und die Netzwerkeinstellungen konfiguriert haben, richten Sie NetScaler-Funktionen wie Lastausgleich, SSL-Offloading oder Anwendungs-Firewall nach Bedarf für Ihre Bereitstellung ein.

**HINWEIS:**

RHOCPV-Bereitstellungen werden mit Bare-Metal-SNO-Clustern und Allzweck-U-Serien-Instanzen getestet und qualifiziert.

# Upgrade von NetScaler VPX auf OpenShift Virtualization

**Schritt 1: Laden Sie das RHOCPV-spezifische NetScaler-Upgrade-Bundle herunter.**

1. Navigieren Sie zu **Citrix.com > Downloads > NetScaler > Virtual Appliances**, und laden Sie das mit RHOCPV kompatible NetScaler VPX-Upgrade-Bundle von der Citrix Downloads Seite herunter.

   **HINWEIS:**

   Verwenden Sie beim Upgrade von NetScaler VPX auf RHOCPV nicht das Standard-NetScaler-Upgrade-Bundle, da das Upgrade fehlschlägt. Stellen Sie stattdessen sicher, dass Sie das RHOCPV-spezifische Upgrade-Bundle mit dem Namen „build-\<version-build>_lx_64.tgz“ verwenden, um Kompatibilitätsprobleme zu vermeiden.

2. Kopieren und entpacken Sie die heruntergeladene Datei „build-\<version-build>_lx_64.tgz“ in das `/var/nsinstall/` Verzeichnis in der NetScaler VPX Shell.
3. Führen Sie `./installns` aus und starten Sie neu, um NetScaler VPX zu aktualisieren.

# Nicht unterstützte Funktionen und Einschränkungen

Eine Liste der NetScaler-Funktionen, -Protokolle und -Systemfunktionen, die in der NetScaler VPX-Bereitstellung auf RHOCPV nicht unterstützt werden, finden Sie unter Einschränkungen für NetScaler VPX-Bereitstellungen auf Red Hat OpenShift Virtualization und Nutanix AHV.

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

**HINWEIS:**

Für NetScaler VPX-Bereitstellungen auf RHOCPV setzen Sie nach dem Ausführen des Befehls `clear config` auf der Instanz den MSS-Wert des TCP-Profils auf `1360`. Wenn Sie einen höheren MSS-Wert konfigurieren, werden TCP-Pakete auf Netzwerkebene verworfen, was zu Fehlern im Secure Copy Protocol (SCP)- und Secure Shell (SSH)-Datenverkehr führt.

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

# Installieren von NetScaler VPX auf dem Nutanix Acropolis Hypervisor

NetScaler bietet ein dediziertes VPX-Image für Nutanix Acropolis Hypervisor (AHV), das die Bereitstellungs- und Verwaltungserfahrung erheblich verbessert. Zuvor verließen sich Kunden auf ein generisches KVM-Hypervisor-Image im Rahmen des Citrix Ready partnership-Programms. Das neue Image vereinfacht die Bereitstellung von NetScaler VPX. Sie können Instanzen jetzt über den standardmäßigen AHV Prism Central bereitstellen. Kunden erhalten offiziellen Support und können auf alle notwendigen Ressourcen zugreifen, was eine nahtlose Bereitstellung auf der Nutanix-Infrastruktur ermöglicht.

**WICHTIG:**

Die Nutanix AHV-Unterstützung ist ab NetScaler Release 14.1 Build 51.x verfügbar. Nach der allgemeinen Verfügbarkeit (GA) dieses dedizierten Nutanix VPX-Images werden Bereitstellungen mit dem Citrix Ready KVM VPX-Image auf Nutanix AHV nicht mehr unterstützt. Kunden wird empfohlen, ihre bestehenden virtuellen Citrix Ready KVM VPX-Maschinen auf das neue, offiziell unterstützte Nutanix VPX-Image zu migrieren.

## Systemanforderungen

Die CPU- und Speicheranforderungen für die Bereitstellung von NetScaler VPX auf Nutanix AHV hängen vom VPX-Modell und der erwarteten Arbeitslast ab.

- **CPU**: Mindestens 2 vCPUs.
- **Arbeitsspeicher**: Mindestens 4 GB RAM.
- **Speicher**: Mindestens 20 GB Festplattenspeicher.

**HINWEIS:**

Ab NetScaler Release 14.1-72.x kann NetScaler VPX auf Nutanix AHV mit 2 GB RAM bereitgestellt werden.

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

# Installieren von NetScaler VPX-Instanzen auf Nutanix AHV mit Prism

Befolgen Sie diese Schritt-für-Schritt-Anleitung, um einen NetScaler VPX auf Nutanix AHV zu installieren.

**Schritt 1. Umgebung vorbereiten.**

- Stellen Sie sicher, dass Ihr Nutanix AHV-Cluster betriebsbereit ist.
- Stellen Sie sicher, dass Sie Zugriff auf Prism Central, die Verwaltungsoberfläche von Nutanix, haben.
- Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen zum Erstellen und Verwalten von VMs in der Nutanix-Umgebung verfügen.

**Schritt 2. Das NetScaler VPX-Image abrufen.**

1. Navigieren Sie zu **Citrix.com > Downloads > NetScaler > Virtual Appliances**, und laden Sie das mit Nutanix AHV kompatible NetScaler VPX-Image von der Seite Citrix Downloads herunter.
2. Extrahieren Sie die heruntergeladene Datei „NSVPX-NUTANIX-`<version-build>`_lx_64.tgz“, um die qcow2-Imagedatei zu erhalten.

**Schritt 3: Das Image in Nutanix AHV hochladen.**

1. Melden Sie sich bei Ihrer Nutanix Prism-Webkonsole an.
2. Gehen Sie im Prism Central-Dashboard zum Abschnitt **Compute > Image** und klicken Sie auf **Add image**.
3. Laden Sie die NetScaler VPX-Imagedatei hoch und stellen Sie sicher, dass Sie den richtigen Imagetyp (DISK-Image) und das richtige Format (qcow2) auswählen.

4. Klicken Sie auf **Save**.

**Schritt 4. Die NetScaler VPX-VM erstellen.**

1. Gehen Sie in Prism Central zum Abschnitt **Compute > VM** und klicken Sie auf **Create VM**.
2. Konfigurieren Sie die Hardware-Spezifikationen der VM gemäß den Empfehlungen von NetScaler® für das VPX-Modell, das Sie bereitstellen. Weitere Informationen finden Sie unter Systemanforderungen.

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

3. Klicken Sie auf **Neue Festplatte hinzufügen** und geben Sie die folgenden Details ein:

   - **Typ** – Festplatte.
   - **Vorgang** – Klonen aus Image-Dienst.
   - **Image** – Weisen Sie das im vorherigen Schritt hochgeladene VPX-Image als Festplatte der VM zu.

4. Klicken Sie auf **Neue NIC hinzufügen** und geben Sie die erforderlichen Details ein.

5. Speichern Sie die Konfigurationen.

**Schritt 5. Starten Sie die NetScaler VPX VM.**

1. Schalten Sie die neu erstellte VPX VM ein.
2. Überwachen Sie den Startvorgang über die von Prism bereitgestellte Konsole, um sicherzustellen, dass die NetScaler VPX-Instanz korrekt startet.

**Schritt 6. Erstkonfiguration.**

1. Während des Startvorgangs zeigt NetScaler eine menügesteuerte Oberfläche an. Führen Sie die Erstkonfiguration durch, indem Sie IP-Adressen, Subnetzmasken und Gateway-Adressen einrichten, und wählen Sie dann die Option **Speichern und fortfahren**.
2. Sobald die VPX-Instanz aktiv ist, greifen Sie über die NetScaler-Konsole oder NSIP auf ihre Verwaltungsoberfläche zu.

**Schritt 7: Konfiguration abschließen.**

Nachdem Sie die Lizenzen angewendet und die Netzwerkeinstellungen konfiguriert haben, richten Sie NetScaler-Funktionen wie Lastenausgleich, SSL-Offloading oder die Anwendungs-Firewall nach Bedarf für Ihre Bereitstellung ein.

# NetScaler VPX™ auf Nutanix AHV aktualisieren

**Schritt 1: Laden Sie das Nutanix-spezifische NetScaler-Upgrade-Paket herunter.**

1. Navigieren Sie zu **Citrix.com > Downloads > NetScaler > Virtual Appliances**, und laden Sie das mit Nutanix AHV kompatible NetScaler VPX-Upgrade-Paket von der Citrix Downloads-Seite herunter.

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

**HINWEIS:**

Verwenden Sie beim Upgrade des NetScaler VPX auf Nutanix AHV nicht das Standard-NetScaler-Upgrade-Paket, da das Upgrade fehlschlägt. Stellen Sie stattdessen sicher, dass Sie das Nutanix-spezifische Upgrade-Paket verwenden, das für VPX auf AHV entwickelt wurde, um Kompatibilitätsprobleme zu vermeiden.

1. Kopieren und entpacken Sie die heruntergeladene Datei „build-`<version-build>`_lx_64.tgz“ in das Verzeichnis `/var/nsinstall/` auf der NetScaler VPX Shell.
2. Führen Sie `./installns` aus und starten Sie neu, um NetScaler VPX zu aktualisieren.

**HINWEIS:**

Ein Upgrade von „Citrix Ready®“ NetScaler VPX unter Verwendung des Nutanix-spezifischen NetScaler-Upgrade-Pakets wird nicht unterstützt.

## Nicht unterstützte Funktionen und Einschränkungen

Bestimmte Funktionen, Protokolle und Systemfähigkeiten werden für NetScaler VPX-Bereitstellungen auf Nutanix AHV nicht unterstützt. Eine vollständige Liste finden Sie unter Einschränkungen für NetScaler VPX-Bereitstellungen auf Red Hat OpenShift Virtualization und Nutanix AHV.

## Migration von Citrix Ready KVM VPX zu offiziell unterstütztem NetScaler VPX™ auf Nutanix AHV

Der Citrix Ready® KVM-basierte NetScaler VPX auf Nutanix AHV wurde von vielen Kunden verwendet, verfügt jedoch nicht über offiziellen Citrix®-Support und erweiterte Automatisierungsfunktionen. Daher empfehlen wir unseren Kunden, von Citrix Ready KVM VPX zu offiziell unterstütztem NetScaler VPX auf Nutanix AHV zu migrieren.

### Voraussetzung

Überprüfen Sie vor der Migration die Einschränkungen des Nutanix AHV-spezifischen VPX-Images, um sicherzustellen, dass Ihre Umgebung nicht von ausgeschlossenen Funktionen abhängt. Weitere Informationen finden Sie unter Nicht unterstützte Funktionen und Einschränkungen.

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

Sie können mit einer der folgenden Methoden von Citrix Ready KVM VPX zu offiziell unterstütztem NetScaler VPX auf Nutanix AHV migrieren:

- Direktes Upgrade von Citrix Ready KVM VPX auf offiziell unterstütztes NetScaler VPX auf Nutanix AHV
- Migration mithilfe des Node-by-Node-Hochverfügbarkeits-(HA)-Ersatzes

## Direktes Upgrade von Citrix Ready KVM VPX auf offiziell unterstütztes NetScaler VPX auf Nutanix AHV

Ab NetScaler Release 14.1 Build 66.x können Sie ein direktes Upgrade von Citrix Ready KVM-basierten VPX-Instanzen auf den offiziell unterstützten NetScaler VPX auf Nutanix AHV durchführen.

**WICHTIG:**

Citrix Ready VPX-Instanzen, die auf Version 14.1-66.x oder höher aktualisiert werden, müssen das offiziell unterstützte Nutanix-spezifische Upgrade-Bundle verwenden. Das Standard-Upgrade-Bundle wird für diese Migration nicht unterstützt.

### Voraussetzungen

- **Mindestversion von NetScaler:** Stellen Sie sicher, dass die aktuelle NetScaler-Version 14.1–56.74 oder höher ist. Wenn die aktuelle Version älter ist, aktualisieren Sie die Appliance vor dem Fortfahren mit dem Standard-Upgrade-Bundle.

- **Hardwareanforderungen:** Für jede vCPU sind mindestens 2 GB RAM erforderlich. Eine VM mit 4 vCPUs muss beispielsweise mindestens 8 GB RAM zugewiesen haben.
- **Einschränkungen überprüfen:** Überprüfen Sie die Nutanix AHV-spezifischen VPX-Einschränkungen, bevor Sie fortfahren.

### Wichtige Überlegungen vor dem Upgrade

- **VM-Snapshot (obligatorisch):** Sie müssen einen Snapshot der laufenden VM erstellen, bevor Sie mit dem Upgrade fortfahren. Dadurch können Sie die VM wiederherstellen, falls Konfigurationsdaten verloren gehen. Weitere Informationen finden Sie unter Manuelles Erstellen eines VM-Snapshots.
- **Externe Sicherung (empfohlen):** Wir empfehlen Ihnen, eine externe Sicherung kritischer Konfigurationen und benutzerdefinierter Daten zu erstellen, insbesondere für Dateien, die sich

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

außerhalb der geschützten Verzeichnisse befinden. Dieser Schritt ist optional, wenn bereits ein VM-Snapshot erstellt wurde.

- **Datensicherung und -erhaltung:** Lesen Sie den Abschnitt Datensicherung und -erhaltung während des Upgrades.

### Datensicherung und -erhaltung während des Upgrades

- Das Upgrade bewahrt benutzerdefinierte Dateien, Zertifikate und Signaturdateien in bestimmten Verzeichnissen automatisch auf. Daten, die sich außerhalb dieser Pfade befinden, werden nicht beibehalten und erfordern eine manuelle Sicherung und Wiederherstellung.

  **Geschützte Verzeichnisse:**

  - `/flash/nsconfig`
  - `/flash/boot`
  - `/flash/configdb`
  - `/var/tmp/*.csv`
  - `/var/AAA`
  - `/var/analytics_conf`
  - `/var/download`
  - `/var/krb`
  - `/var/learnt_data`
  - `/var/metrics_conf`
  - `/var/netscaler/gui`
  - `/var/netscaler/locdb`
  - `/var/netscaler/logon`
  - `/var/netscaler/ssl`
  - `/var/nstemplates`
  - `/var/vpn`
  - `/var/vpns`
  - `/var/clusterd/nsclusterd.conf`

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

- Wenn Sie angepasste Konfigurationsdateien im `/etc` Verzeichnis haben, lesen Sie Überlegungen zum Upgrade für angepasste Konfigurationsdateien im Verzeichnis /etc, bevor Sie mit der Migration fortfahren.
- Anpassungen, die an den folgenden Dateien vorgenommen wurden, bleiben während des Migrationsprozesses erhalten, funktionieren aber möglicherweise nicht mehr wie vor der Migration:
  - `rc.netscaler`
  - `nsbefore.sh`
  - `nsafter.sh`
  - `crontab`

  Sie müssen diese Anpassungsdateien überprüfen und aktualisieren, um die Kompatibilität mit dem aktualisierten NetScaler sicherzustellen.

### Upgrade-Verfahren

1. Laden Sie das mit Nutanix AHV kompatible NetScaler VPX-Upgrade-Bundle (Format: `build-<version-build>_lx_64.tgz`) von der Citrix Downloads-Seite herunter.
2. Navigieren Sie zu **Citrix.com > Downloads > NetScaler > Virtual Appliances**, und laden Sie das mit Nutanix AHV kompatible NetScaler VPX-Upgrade-Bundle von der Citrix Downloads-Seite herunter.
3. Kopieren Sie die heruntergeladene Datei `build-<version-build>_lx_64.tgz` in das Verzeichnis `/var/nsinstall/` auf der NetScaler VPX Shell und entpacken Sie sie.
4. Führen Sie `./installns` aus und starten Sie die Appliance neu, wenn Sie dazu aufgefordert werden. Schalten Sie die VM während der für den Vorgang erforderlichen mehreren Neustarts nicht aus.

### Validierung nach dem Upgrade

1. Melden Sie sich bei der NetScaler VPX GUI/CLI an und überprüfen Sie, ob die ausgeführte Version mit der Ziel-Upgrade-Bundle-Version übereinstimmt.
2. Validieren Sie alle virtuellen Dienste, SSL-Zertifikate und Richtlinien, um die korrekte Funktionalität sicherzustellen.

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

## Migration mithilfe der Node-by-Node-Hochverfügbarkeits- (HA) Ersatzmethode

Die HA-Node-by-Node-Ersatzmethode ermöglicht ein Upgrade ohne Ausfallzeiten und mit vollständiger Unterstützung vom Citrix Ready KVM VPX auf das offiziell unterstützte Nutanix AHV VPX-Image. Dieser Übergang erschließt erweiterte Automatisierungsfunktionen, vollständigen offiziellen Support und eine modernisierte Bereitstellungsplattform für NetScaler.

**Schritt 1:** Sperren Sie den HA-Status Ihres älteren primären Knotens.

1. Melden Sie sich bei Ihrem Citrix Ready KVM VPX-Primärknoten an und führen Sie den folgenden Befehl aus:

   ```
   set ha node -hastatus STAYPRIMARY
   ```

2. Entfernen Sie auf dem sekundären Legacy-Knoten dessen HA-Kopplung mit dem primären Knoten mithilfe des folgenden Befehls:

   ```
   rm ha node <primary-nsip>
   ```

3. Vergewissern Sie sich, dass der primäre Knoten den Datenverkehr ohne Unterbrechung weiterleitet, während Sie mit den Migrations- oder Ersetzungsaufgaben fortfahren.

**Schritt 2:** Stellen Sie einen neuen sekundären Knoten bereit.

1. Stellen Sie eine neue NetScaler VPX-Instanz mithilfe des offiziellen Nutanix AHV 14.1-51.x-Images bereit.
2. Weisen Sie die Verwaltungs-IP-Adresse zu, die zuvor von Ihrem sekundären Legacy-Knoten verwendet wurde.
3. Schließen Sie die Ersteinrichtung ab, wenden Sie die Lizenz an und überprüfen Sie, ob die Netzwerkkonfiguration korrekt ist.
4. Verbinden Sie HA-Knoten, indem Sie den folgenden Befehl ausführen:

   ```
   add ha node <primary-nsip>
   ```

5. Überprüfen Sie mithilfe des folgenden Befehls, ob der HA-Status **UP** ist und die Synchronisierung erfolgreich war:

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

```
show ha node status
```

**Schritt 3:** Befördern Sie den neuen sekundären Knoten zum primären Knoten.

1. Heben Sie auf dem alten primären Knoten (dem Legacy KVM VPX) den Status „stay primary“ mithilfe des folgenden Befehls auf:

   ```
   unset ha node -stayprimary
   ```

2. Erzwingen Sie ein Failover mithilfe des folgenden Befehls:

   ```
   force ha failover
   ```

3. Vergewissern Sie sich, dass der neu bereitgestellte sekundäre Knoten erfolgreich zum primären Knoten geworden und voll funktionsfähig ist.

   ```
   show ha node status
   ```

4. Stellen Sie den neuen primären Knoten mithilfe des folgenden Befehls auf „stay primary“ ein:

   ```
   set ha node -hastatus STAYPRIMARY
   ```

   **HINWEIS:**

   Wenn die HA-Synchronisierung fehlschlägt, synchronisieren Sie die RPC-Passwörter auf beiden Knoten manuell mithilfe des Befehls `set rpcNode <peer-ip> -password <password>`.

5. Sollten bei diesem Schritt Probleme auftreten, wechseln Sie zurück zum alten primären Knoten und stellen Sie den alten sekundären Knoten wieder her. Für Unterstützung wenden Sie sich an das Citrix Support-Team.

**Schritt 4:** Ersetzen Sie den alten sekundären Knoten durch eine neue VPX.

1. Entfernen Sie den alten sekundären Knoten mit dem folgenden Befehl aus der HA-Konfiguration:

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

```
rm ha node <legacy-secondary-nsip>
```

2. Stellen Sie eine weitere neue VPX-Instanz mit dem offiziellen Nutanix AHV 14.1-51.x Image bereit.
3. Weisen Sie der neuen VPX-Instanz die Management-IP-Adresse des alten sekundären Knotens zu.
4. Schließen Sie die Einrichtung und Lizenzaktivierung ab.
5. Fügen Sie diese neue VPX mit dem folgenden Befehl dem HA-Paar hinzu:

```
add ha node <new-primary-nsip>
```

6. Überprüfen Sie mit dem folgenden Befehl, ob der HA-Status stabil, „UP“ und synchronisiert ist.

```
show ha node status
```

**Schritt 5:** Validieren und abschließen.

1. Überprüfen Sie die HA-Rollen und den Synchronisierungsstatus auf beiden neuen Knoten.
2. Validieren Sie alle virtuellen Dienste, SSL-Zertifikate und Richtlinien, um die korrekte Funktionalität sicherzustellen.
3. Führen Sie Failover- und Failback-Tests durch, um die Redundanz zu überprüfen.
4. Sichern Sie alle Konfigurationen und erstellen Sie einen Snapshot der neuen Umgebung.
5. Löschen Sie nach erfolgreicher Validierung die alten VPX-Instanzen, um Ressourcen freizugeben.

## Wichtige Überlegungen

- **Sicherung:** Es ist unerlässlich, Sicherungen Ihrer älteren Knoten beizubehalten, bis die neue VPX-Umgebung vollständig validiert und stabil ist.
- **Nicht unterstützte Funktionen:** Eine Migration wird nicht empfohlen, wenn Ihre aktuelle Bereitstellung auf Funktionen basiert, die im neuen Nutanix AHV VPX-Image nicht unterstützt werden. Weitere Informationen finden Sie unter Nicht unterstützte Funktionen und Einschränkungen.

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

# NetScaler VPX™ auf Nutanix Acropolis Hypervisor – FAQs

- **Wie viel Arbeitsspeicher ist mindestens für NetScaler VPX auf Nutanix AHV erforderlich?**

  Für NetScaler VPX auf Nutanix AHV sind mindestens 4 GB Arbeitsspeicher erforderlich.

  **HINWEIS:**

  Ab NetScaler Release 14.1-72.x kann NetScaler VPX auf Nutanix AHV mit 2 GB RAM bereitgestellt werden.

- **Unterstützt VPX auf Nutanix AHV die Festplattenerweiterung über 20 GB hinaus?**

  Ja. Um den Festplattenspeicher auf NetScaler® VPX, der auf Nutanix AHV bereitgestellt wird, zu erhöhen, stellen Sie sicher, dass der erforderliche zusätzliche Festplattenspeicher während der anfänglichen Bereitstellungsphase zugewiesen wird. Nutanix AHV unterstützt die Erhöhung der Festplattengröße nach der Bereitstellung der VM nicht.

- **Wird eine sekundäre Festplatte auf Nutanix AHV unterstützt?**

  Ja, eine sekundäre Festplatte wird ab NetScaler Release 14.1-72.x unterstützt.

- **Wird sysctl für NetScaler-Variablen auf Nutanix AHV unterstützt?**

  Nein. Es wird empfohlen, spezifische NSCLI-Befehle zu verwenden, um dieselben Daten abzurufen. Anstatt `sysctl netscaler.version` zu verwenden, verwenden Sie den NetScaler CLI-Befehl `show version`.

- **Wie ändere ich den Hostnamen von NetScaler auf Nutanix AHV?**

  Der Hostname kann mit dem Befehl `set hostname <hostName>` festgelegt werden.

- **Welche Festplattenpartitionen bleiben bei Neustarts und Upgrades/Neuinstallationen in VPX Nutanix erhalten?**

  Nur Dateien in den folgenden Verzeichnissen bleiben bei Neustarts erhalten:

  - `/nsconfig`, der auf das `/flash/nsconfig` Verzeichnis verweist
  - `/var` Verzeichnis

  Alle anderen Dateien werden bei Neustarts gelöscht.

- **Wie stelle ich versehentlich gelöschte Systemdateien (z. B. Binärdateien in /usr/sbin) in VPX Nutanix wieder her?**

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

Starten Sie NetScaler neu und wählen Sie während des Starts „NetScaler-Firmware-Version 14.1 x.x neu installieren“ aus. Diese Aktion hat keine Auswirkungen auf gespeicherte Konfigurationen.

- **Wie konfiguriere ich eine benutzerdefinierte Protokollrotation in VPX auf Nutanix AHV?**

  Auf Nutanix AHV wird `newsyslog.conf` nicht unterstützt. Stattdessen wird die Protokollrotation mit dem Linux-Dienstprogramm `logrotate` gehandhabt, das einmal pro Stunde ausgeführt wird. Die Konfigurationsdatei befindet sich unter: `/etc/logrotate.d/blx-syslog`.

- **Wird cloud-init auf Nutanix AHV unterstützt?**

  Ja, aber derzeit werden nur benutzerdefinierte Skripte unterstützt. Geführte Skripte werden noch nicht unterstützt.

  **Beispiele für cloud-init-Skripte:**

  - **Beispiel 1:** Leeres `cloud-init` Skript. Dies löst DHCP aus, und wenn eine statische oder DHCP-IP-Adresse auf der ersten Schnittstelle konfiguriert ist, wird diese automatisch als NetScaler-IP-Adresse konfiguriert.

    ```
    #cloud-config
    ```

  - **Beispiel 2:** Legt den Hostnamen auf „vpx-nutanix“ fest

    ```
    #cloud-config

    fqdn: vpx-nutanix
    ```

- **Kann ich die NSIP automatisch von der primären statischen/DHCP-IP-Adresse zuweisen, die auf der ersten Schnittstelle in VPX Nutanix konfiguriert ist?**

  Ja, Sie müssen jedoch eine Dummy-`cloud-init` Konfiguration in der benutzerdefinierten Konfiguration angeben, während Sie die Instanz erstellen.

- **Wie konfiguriere ich das Domain Name System (DNS) für NetScaler auf Nutanix AHV?**

  Verwenden Sie den Befehl `add dns nameserver`, um DNS zu konfigurieren.

- **Wie behebe ich DNS-Probleme auf VPX Nutanix AHV?**

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

DNS-Dienstprogramme wie dig, nslookup und host werden ab NetScaler Release 14.1-72.x auf NetScaler VPX für Nutanix unterstützt. Für frühere Releases verwenden Sie den Befehl `systemd-resolve`, um die DNS-Auflösung zu überprüfen.

**Beispiel:**

```
root@ns# systemd-resolve www.google.com

www.google.com: 142.251.10.105                -- link: ns2

                142.251.10.147                -- link: ns2

                142.251.10.104                -- link: ns2

                142.251.10.103                -- link: ns2

                142.251.10.99                 -- link: ns2

                142.251.10.106                -- link: ns2

                2404:6800:4003:c0f::63        -- link: ns2
```

- **Welcher Texteditor ist in VPX auf Nutanix AHV verfügbar?**

  Vim ist als Texteditor verfügbar. Der Befehl „vi“ ist ein symbolischer Link zum Vim-Binary.

- **Wie kopiere ich Zeilen aus einer in Vim über eine SSH-Sitzung geöffneten Datei in die Zwischenablage?**

  Halten Sie die Umschalttaste gedrückt, klicken Sie mit der linken Maustaste und ziehen Sie, um den Text auszuwählen, den Sie kopieren möchten.

- **Wie füge ich Inhalte in den Vim-Editor ein?**

  Wechseln Sie mit „i“ in den Einfügemodus und fügen Sie mit der Tastenkombination „Umschalt + Einfügen“ ein.

- **Was ist die empfohlene Methode zum Konfigurieren von IP-Adressen auf Nutanix AHV-Schnittstellen in einem Overlay-Subnetz bei Verwendung von Hochverfügbarkeit (HA) mit NetScaler?**

  Bei Verwendung eines Nutanix-Overlay-Subnetzes können Sie einer Netzwerkschnittstelle sowohl primäre als auch sekundäre IP-Adressen zuweisen. Diese IPs sind jedoch an die

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

Schnittstelle des spezifischen Knotens gebunden und unterstützen kein HA-Failover, wenn sie als virtuelle IP-Adressen (VIPs) oder Subnetz-IP-Adressen (SNIPs) verwendet werden.

Um ein ordnungsgemäßes HA-Verhalten mit NetScaler zu gewährleisten, befolgen Sie diese Best Practices:

- Weisen Sie jeder Schnittstelle im Nutanix-Overlay-Subnetz nur eine (obligatorische) IP-Adresse zu.
- Verwenden Sie diese IP-Adresse nicht für Konfigurationen, die über HA-Knoten hinweg gemeinsam genutzt werden (z. B. VIP oder SNIP).
- Sie können diese IP-Adresse als NetScaler IP (NSIP) verwenden, da NSIP knotenspezifisch ist und kein Failover erfordert.
- Konfigurieren Sie VIPs und SNIPs manuell auf der NetScaler-Appliance, nicht auf der Nutanix-Schnittstelle.
- Stellen Sie sicher, dass die entsprechenden VLAN-Einstellungen auf NetScaler für die korrekte Weiterleitung und Kommunikation konfiguriert sind.

Dieser Ansatz vermeidet HA-Probleme und gewährleistet eine saubere Trennung zwischen knotenspezifischen und gemeinsam genutzten IP-Konfigurationen.

- **Wird getaggtes VLAN mit NetScaler VPX auf Nutanix AHV unterstützt?**

  Ja, NetScaler VPX unterstützt getaggtes VLAN, vorausgesetzt, der AHV-Hypervisor verfügt über die unter VLAN für Gast-VMs genannten Konfigurationen.

- **Wird der Befehl `nsapimgr` auf Nutanix AHV unterstützt?**

  Der Befehl `nsapimgr` wird auf Nutanix AHV unterstützt. Die Aufrufoptionen sind jedoch auf die folgenden beschränkt.

| BEFEHL 1 | BEFEHL 2 |
|---|---|
| `nsapimgr_wr.sh -ys call=ns_weak_sso_type_enable` | `nsapimgr_wr.sh -ys call=ns_weak_sso_type_disable` |
| `nsapimgr_wr.sh -ys call=ns_sso_ntlm_use_ntdomain` | `nsapimgr_wr.sh -ys call=ns_sso_ntlm_dont_use_ntdomain` |
| `nsapimgr_wr.sh -ys call=ns_sso_kcd_use_spn_host` | `nsapimgr_wr.sh -ys call=ns_sso_kcd_dont_use_spn_host` |

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

| BEFEHL 1 | BEFEHL 2 |
| --- | --- |
| `nsapimgr_wr.sh -ys call=ns_saml_redirect_for_artifact` | `nsapimgr_wr.sh -ys call=ns_saml_post_for_artifact` |
| `nsapimgr_wr.sh -ys call=ns_saml_enable_single_logout` | `nsapimgr_wr.sh -ys call=ns_saml_disable_single_logout` |
| `nsapimgr_wr.sh -ys call=ns_saml_enable_replay_protection` | `nsapimgr_wr.sh -ys call=ns_saml_disable_replay_protectio n` |
| `nsapimgr_wr.sh -ys call=ns_saml_enable_incl_ns_fix` | `nsapimgr_wr.sh -ys call=ns_saml_disable_incl_ns_fix` |
| `nsapimgr_wr.sh -ys call=ns_saml_enable_comma_sep_attr_re s_no_encode` | `nsapimgr_wr.sh -ys call=ns_saml_disable_comma_sep_attr_r es_no_encode` |
| `nsapimgr_wr.sh -ys call=ns_saml_enable_comma_sep_attr_re s` | `nsapimgr_wr.sh -ys call=ns_saml_disable_comma_sep_attr_r es` |
| `nsapimgr_wr.sh -ys call=ns_saml_dont_send_subject` | `nsapimgr_wr.sh -ys call=ns_saml_send_subject` |
| `nsapimgr_wr.sh -ys call=ns_saml_dont_send_session_index` | `nsapimgr_wr.sh -ys call=ns_saml_send_session_index` |
| `nsapimgr_wr.sh -ys call=ns_saml_dont_send_in_response` | `nsapimgr_wr.sh -ys call=ns_saml_send_in_response` |
| `nsapimgr_wr.sh -ys call=ns_saml_dont_send_full_metadata` | `nsapimgr_wr.sh -ys call=ns_saml_send_full_metadata` |
| `nsapimgr_wr.sh -ys call=ns_rba_login_enable_debug` | `nsapimgr_wr.sh -ys call=ns_rba_login_disable_debug` |
| `nsapimgr_wr.sh -ys call=ns_enable_schema_checks` | `nsapimgr_wr.sh -ys call=ns_disable_schema_checks` |

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

| BEFEHL 1 | BEFEHL 2 |
| --- | --- |
| `nsapimgr_wr.sh -ys call=ns_aaatm_drop_options_request` | `nsapimgr_wr.sh -ys call=ns_aaatm_dont_drop_options_request` |
| `nsapimgr_wr.sh -ys call=ns_aaatm_302_for_bearer` | `nsapimgr_wr.sh -ys call=ns_aaatm_401_for_bearer` |
| `nsapimgr_wr.sh -ys call=ns_aaa_enable_api_access` | `nsapimgr_wr.sh -ys call=ns_aaa_disable_api_access` |
| `nsapimgr_wr.sh -ys call=enable_webview_support` | `nsapimgr_wr.sh -ys call=disable_webview_support` |
| `nsapimgr_wr.sh -ys call=enable_rfweb_webview_support` | `nsapimgr_wr.sh -ys call=disable_rfweb_webview_support` |
| `nsapimgr_wr.sh -ys call=aaatm_disable_domain_cookie` | `nsapimgr_wr.sh -ys call=aaatm_enable_domain_cookie` |
| `nsapimgr_wr.sh -ys call=aaa_strip_domain` | `nsapimgr_wr.sh -ys call=aaa_dont_strip_domain` |
| `nsapimgr_wr.sh -ys arg1=<VAL> -ys call="ns_saml_set_deflate_size"` | `nsapimgr_wr.sh -ys call=ns_saml_unset_deflate_size` |
| `nsapimgr_wr.sh -ys arg1=<VAL> -ys call="ns_saml_send_binding"` | `nsapimgr_wr.sh -ys call=ns_saml_dont_send_binding` |
| `nsapimgr_wr.sh -ys arg1=<VAL> -ys call="ns_push_set_timeout"` | `nsapimgr_wr.sh -ys arg1=<VAL> -ys call="ns_aaatm_cgitm_duration"` |

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

# Einschränkungen für NetScaler VPX-Bereitstellungen auf Red Hat OpenShift Virtualization und Nutanix AHV

Dieses Dokument beschreibt die Funktionen und Fähigkeiten, die bei der Bereitstellung von NetScaler VPX™ auf Red Hat® OpenShift® Virtualization (RHOCPV) und Nutanix AHV-Plattformen derzeit nicht unterstützt werden.

**Nicht unterstützte NetScaler-Funktionen:**

- Admin-Partition(/de-de/citrix-adc/current-release/admin-partition)
- NextGen-API
- Front-End-Optimierung (FEO)(/de-de/citrix-adc/current-release/optimization/front-end-optimization.html)
- Jumbo-Frames(/de-de/citrix-adc/current-release/networking/interfaces/jumbo-frames/configuring-jumbo-frames-support-on-citrix-adc-appliance.html)
- Automatisches Speichern der laufenden Konfiguration
- Layer-3-(L3)-Cluster
- E-Mail-Einmalpasswort (OTP)
- Änderung des Sammlungspfads für Techsupport-Bundles(/de-de/citrix-adc/current-release/system/basic-operations#change-in-the-default-support-bundle-collection-directory-for-netscaler.html)
- IPsec-Protokoll

**Nicht unterstützte Konsolenfunktionen:**

- Telemetriestatus auf der Lizenzverwaltungsseite
- Überwachung der Dateintegrität(/de-de/netscaler-console-service/instance-advisory/file-integrity-monitoring.html)

**Systembeschränkungen:**

- Preboot-Benutzerdaten
- Nutanix Guest Tools

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

- `what` Dienstprogramm
- `nsapimgr` Aufrufoptionen werden teilweise unterstützt. Für die `nsapimgr` Unterstützung und zulässige Aufrufoptionen auf Nutanix AHV, siehe die zugehörige FAQ.

**Veraltete Funktionen:**

- Routing Information Protocol (RIP)
- Routing Information Protocol Next Generation (RIPng)
- Intermediate System to Intermediate System (IS-IS) Protocol
- PTP-Protokoll
- File Transfer Protocol (FTP)
- Telnet

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

# NetScaler VPX auf AWS

Sie können eine NetScaler VPX-Instanz auf Amazon Web Services (AWS) starten. Die NetScaler VPX-Appliance ist als Amazon Machine Image (AMI) im AWS Marketplace verfügbar. Eine NetScaler VPX-Instanz auf AWS ermöglicht es Ihnen, die Cloud-Computing-Funktionen von AWS zu nutzen und die NetScaler-Funktionen für Lastenausgleich und Datenverkehrsmanagement für Ihre Geschäftsanforderungen einzusetzen. Die VPX-Instanz unterstützt alle Datenverkehrsmanagementfunktionen einer physischen NetScaler-Appliance und kann als eigenständige Instanz oder in HA-Paaren bereitgestellt werden. Weitere Informationen zu den VPX-Funktionen finden Sie im VPX-Datenblatt.

## Erste Schritte

Bevor Sie mit Ihrer VPX-Bereitstellung beginnen, müssen Sie mit den folgenden Informationen vertraut sein:

- AWS-Terminologie
- AWS-VPX-Supportmatrix
- Einschränkungen und Nutzungsrichtlinien
- Voraussetzungen
- Funktionsweise einer NetScaler VPX-Instanz auf AWS

## Bereitstellen einer NetScaler VPX-Instanz auf AWS

In AWS werden die folgenden Bereitstellungstypen für VPX-Instanzen unterstützt:

- Eigenständig
- Hochverfügbarkeit (Aktiv-Passiv)
    - Hochverfügbarkeit innerhalb derselben Zone
    - Hochverfügbarkeit über verschiedene Zonen hinweg mit Elastic IP
    - Hohe Verfügbarkeit über verschiedene Zonen hinweg unter Verwendung privater IPs
- Aktiv-Aktiv GSLB

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

## Hybride Bereitstellungen

- NetScaler in AWS Outpost bereitstellen
- NetScaler in VMC in AWS bereitstellen

## Lizenzierung

Eine NetScaler VPX-Instanz auf AWS erfordert eine Lizenz. Die für NetScaler VPX-Instanzen, die auf AWS ausgeführt werden, verfügbare Lizenzierungsoption ist Bring Your Own License (BYOL).

## Automatisierung

- NetScaler ADM: Intelligente Bereitstellung
- GitHub CFTs: NetScaler-Vorlagen und -Skripte für die AWS-Bereitstellung
- GitHub Ansible: NetScaler-Vorlagen und -Skripte für die AWS-Bereitstellung
- GitHub Terraform: NetScaler-Vorlagen und -Skripte für die AWS-Bereitstellung
- AWS Pattern Library (PL): NetScaler VPX

## Blogs

- Wie NetScaler auf AWS Kunden hilft, Anwendungen sicher bereitzustellen
- Anwendungsbereitstellung in der Hybrid Cloud mit NetScaler und AWS
- Citrix ist ein AWS Networking Competency Partner
- NetScaler: Immer bereit für Public Clouds
- Einfaches Scale-out oder Scale-in in Public Clouds über NetScaler
- Citrix erweitert die ADC-Bereitstellungsoptionen mit AWS Outposts
- Verwenden von NetScaler mit Amazon VPC Ingress Routing
- Citrix bietet Auswahl, Leistung und vereinfachte Bereitstellung in AWS
- Die Sicherheit der NetScaler Web App Firewall – jetzt auf dem AWS Marketplace
- Wie Aria Systems die NetScaler Web App Firewall auf AWS verwendet

## Videos

- Vereinfachung von NetScaler-Bereitstellungen in der Public Cloud durch ADM

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

- Bereitstellung und Konfiguration von NetScaler VPX in AWS mithilfe gebrauchsfertiger Terraform-Skripte
- Bereitstellen von NetScaler HA in AWS mithilfe einer CloudFormation-Vorlage
- Bereitstellen von NetScaler HA über Availability Zones hinweg mithilfe von AWS QuickStart
- NetScaler Autoscale mit ADM

## Kundenreferenzen

- Technologielösung – Xenit AB
- Entdecken Sie die Vorteile von NetScaler und AWS

## Lösungen

- Digitale Werbeplattform auf AWS mit NetScaler bereitstellen
- Clickstream-Analysen in AWS mit NetScaler verbessern

## Support

- Supportfall öffnen
- Informationen zum NetScaler-Abonnementangebot finden Sie unter Fehlerbehebung bei einer VPX-Instanz auf AWS. Um einen Supportfall zu melden, suchen Sie Ihre AWS-Kontonummer und Ihren Support-PIN-Code und rufen Sie den NetScaler-Support an.
- Für NetScaler Customer Licensed Offering oder BYOL stellen Sie sicher, dass Sie über einen gültigen Support- und Wartungsvertrag verfügen. Wenn Sie keinen Vertrag haben, wenden Sie sich an Ihren NetScaler-Vertreter.

## Weitere Referenzen

- AWS On-Demand Webinar – NetScaler auf AWS
- NetScaler VPX-Datenblatt
- NetScaler im AWS Marketplace
- NetScaler ist Teil der AWS-Netzwerkpartnerlösungen (Lastverteiler)
- AWS-FAQs

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

# AWS-Terminologie

Dieser Abschnitt beschreibt die Liste der häufig verwendeten AWS-Begriffe und -Phrasen. Weitere Informationen finden Sie unter AWS-Glossar.

| BEGRIFF | DEFINITION |
| --- | --- |
| Amazon Machine Image (AMI) | Ein Maschinen-Image, das die zum Starten einer Instanz erforderlichen Informationen bereitstellt, wobei es sich um einen virtuellen Server in der Cloud handelt. |
| Elastic Block Store | Bietet persistente Block-Speichervolumes zur Verwendung mit Amazon EC2-Instanzen in der AWS Cloud. |
| Simple Storage Service (S3) | Speicher für das Internet. Er wurde entwickelt, um Web-Scale-Computing für Entwickler zu vereinfachen. |
| Elastic Compute Cloud (EC2) | Ein Webdienst, der sichere, skalierbare Rechenkapazität in der Cloud bereitstellt. Er wurde entwickelt, um Web-Scale-Cloud-Computing für Entwickler zu vereinfachen. |
| Elastic Load Balancing (ELB) | Verteilt eingehenden Anwendungsverkehr auf mehrere EC2-Instanzen in mehreren Availability Zones. Dies erhöht die Fehlertoleranz Ihrer Anwendungen. |
| Elastische Netzwerkschnittstelle (ENI) | Eine virtuelle Netzwerkschnittstelle, die Sie an eine Instanz in einer Virtual Private Cloud (VPC) anfügen können. |
| Elastic IP (EIP)-Adresse | Eine statische, öffentliche IPv4-Adresse, die Sie in Amazon EC2 oder Amazon VPC zugewiesen und dann an eine Instanz angefügt haben. Elastic IP-Adressen sind Ihrem Konto zugeordnet, nicht einer bestimmten Instanz. Sie sind elastisch, weil Sie sie je nach Bedarf einfach zuweisen, anfügen, trennen und freigeben können. |

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

| BEGRIFF | DEFINITION |
| --- | --- |
| Instance-Typ | 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 zu wählen. |
| Identitäts- und Zugriffsmanagement (IAM) | 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. Eine IAM-Rolle ist für die Bereitstellung von VPX-Instanzen in einer Hochverfügbarkeitskonfiguration erforderlich. |
| Internet-Gateway | Verbindet ein Netzwerk mit dem Internet. Sie können Datenverkehr für IP-Adressen außerhalb Ihrer VPC an das Internet-Gateway weiterleiten. |
| Schlüsselpaar | Ein Satz von Sicherheitsanmeldeinformationen, die Sie verwenden, um Ihre Identität elektronisch nachzuweisen. Ein Schlüsselpaar besteht aus einem privaten Schlüssel und einem öffentlichen Schlüssel. |
| Routentabellen | Ein Satz von Routing-Regeln, der den Datenverkehr steuert, der ein Subnetz verlässt, das der Routentabelle zugeordnet ist. Sie können mehrere Subnetze einer einzelnen Routentabelle zuordnen, aber ein Subnetz kann immer nur einer Routentabelle zugeordnet sein. |

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

| BEGRIFF | DEFINITION |
| --- | --- |
| Sicherheitsgruppen | Ein benannter Satz von zulässigen eingehenden Netzwerkverbindungen für eine Instanz. |
| Subnetze | Ein Segment des IP-Adressbereichs einer VPC, an das EC2-Instanzen angehängt werden können. Sie können Subnetze erstellen, um Instanzen entsprechend den Sicherheits- und betrieblichen Anforderungen zu gruppieren. |
| Virtual Private Cloud (VPC) | Ein Webdienst zur Bereitstellung eines logisch isolierten Bereichs der AWS Cloud, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. |
| Auto Scaling | Ein Webdienst zum automatischen Starten oder Beenden von Amazon EC2-Instanzen basierend auf benutzerdefinierten Richtlinien, Zeitplänen und Zustandsprüfungen. |
| CloudFormation | Ein Dienst zum Schreiben oder Ändern von Vorlagen, die zusammengehörige AWS-Ressourcen als eine Einheit erstellen und löschen. |

# AWS-VPX Support-Matrix

Die folgenden Abschnitte listen die unterstützten NetScaler VPX-Angebote, AWS-Regionen, Instanztypen und Dienste auf.

## Unterstützte VPX-Angebote auf AWS

| UNTERSTÜTZTE VPX-ANGEBOTE |
| --- |
| NetScaler VPX – vom Kunden lizenziert |
| NetScaler VPX FIPS – vom Kunden lizenziert |
| NetScaler VPX FIPS ENA – vom Kunden lizenziert |

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

## Unterstützte AWS-Regionen

| REGION | REGIONSCODE |
|---|---|
| US West | us-west-1, us-west-2 |
| US Ost | us-east-1, us-east-2 |
| Asien-Pazifik | ap-south-1, ap-southeast-4, ap-northeast-2, ap-southeast-1, ap-southeast-2, ap-northeast-1, ap-east-1, ap-northeast-3, ap-southeast-3, ap-south-2 |
| Kanada | ca-central-1, ca-west-1 |
| EU | eu-central-1, eu-west-1, eu-west-2, eu-west-3, eu-south-1, eu-north-1 |
| Südamerika | sa-east-1 |
| Israel | il-central-1 |
| Naher Osten | me-south-1, me-central-1 |
| Afrika | af-south-1 |
| AWS GovCloud | us-gov-east-1, us-gov-west-1 |
| US-Geheimdienst | us-iso-east-1, us-isob-east-1 |
| China | cn-north-1, cn-northwest-1 |

## Unterstützte AWS-Instanztypen

NetScaler empfiehlt die folgenden AWS-Instanztypen:

- M6i- und C5n-Serien für Marketplace-Editionen oder Bandbreiten-basierte Pool-Lizenzierung.

| VPX MIT POOLED- ODER FLEXED-LIZENZIERUNG (BANDBREITENLIZENZEN) | EMPFOHLENE AWS-INSTANZ |
|---|---|
| Bis zu 200 MBit/s | m6i.xlarge |
| 1–5 GBit/s | m6i.2xlarge |

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

| VPX MIT POOLED- ODER FLEXED-LIZENZIERUNG (BANDBREITENLIZENZEN) | EMPFOHLENE AWS-INSTANZ |
|---|---|
| 5–8 GBit/s | c5n.4xlarge |
| 8–25 Gbit/s | c5n.9xlarge |

Um die richtige Instanz für Ihre spezifischen Anforderungen basierend auf Metriken wie Paketen pro Sekunde oder SSL-Transaktionsraten zu ermitteln, wenden Sie sich an Ihren NetScaler-Vertreter, um Unterstützung zu erhalten.

| KATEGORIE | INSTANZFAMILIEN |
|---|---|
| Allgemeiner Zweck | M3, M4, M5, M5a, M5n, M6i, M7i, M8i, T2, T3a |
| Rechenoptimiert | C4, C5, C5n, C6in |
| Speicheroptimiert | R7iz |
| Speicheroptimiert | D2 |

## Unterstützte AWS-Dienste

| UNTERSTÜTZTE AWS-DIENSTE |
|---|
| **EC2:** Startet ADC-Instanzen. |
| **Lambda:** Ruft NetScaler VPX NITRO APIs während der Bereitstellung von NetScaler VPX-Instanzen aus CFT auf. |
| **VPC und VPC-Ingress-Routing:** VPC erstellt isolierte Netzwerke, in denen ADC gestartet werden kann. VPC-Ingress-Routing wird in der Firewall-Lastverteilungslösung verwendet. |
| **Route53:** Verteilt den Datenverkehr auf alle NetScaler VPX-Knoten in der NetScaler Autoscale-Lösung. |
| **ELB:** Verteilt den Datenverkehr auf alle NetScaler VPX-Knoten in der NetScaler Autoscale-Lösung. |
| **Cloudwatch:** Überwacht Leistung und Systemparameter für NetScaler VPX-Instanzen. |
| **AWS Autoscaling:** Wird für das Back-End-Server-Autoscaling verwendet. |

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

| UNTERSTÜTZTE AWS-DIENSTE |
| --- |
| **Cloud Formation:** CloudFormation-Vorlagen werden zur Bereitstellung von NetScaler VPX-Instanzen verwendet. |
| **Simple Queue Service (SQS):** Überwacht Scale-up- und Scale-down-Ereignisse im Back-End-Autoscaling. |
| **Simple Notification Service (SNS):** Überwacht Scale-up- und Scale-down-Ereignisse im Back-End-Autoscaling. |
| **Identity and Access Management (IAM):** Bietet Zugriff auf AWS-Dienste und -Ressourcen. |
| **AWS Outposts:** Stellt NetScaler VPX-Instanzen in AWS Outposts bereit. |

## Einschränkungen und Nutzungsrichtlinien

Die folgenden Einschränkungen und Nutzungsrichtlinien gelten bei der Bereitstellung einer NetScaler VPX-Instanz auf AWS:

- Bevor Sie beginnen, lesen Sie den Abschnitt zur AWS-Terminologie unter Bereitstellen einer NetScaler VPX-Instanz auf AWS.
- Damit das Hochverfügbarkeits-Setup effektiv funktioniert, weisen Sie der Verwaltungsschnittstelle ein dediziertes NAT-Gerät zu oder weisen Sie EIP dem NSIP zu. Weitere Informationen zu NAT finden Sie in der AWS-Dokumentation unter NAT-Instanzen.
- Datenverkehr und Verwaltungsdatenverkehr müssen mit ENIs, die zu verschiedenen Subnetzen gehören, getrennt werden.
- Nur die NSIP-Adresse darf auf der Verwaltungs-ENI vorhanden sein.
- Wenn eine NAT-Instanz zur Sicherheit verwendet wird, anstatt dem NSIP eine EIP zuzuweisen, sind entsprechende Routing-Änderungen auf VPC-Ebene erforderlich. Anweisungen zum Vornehmen von Routing-Änderungen auf VPC-Ebene finden Sie in der AWS-Dokumentation unter Szenario 2: VPC mit öffentlichen und privaten Subnetzen.
- Eine VPX-Instanz kann von einem EC2-Instanztyp zu einem anderen verschoben werden (z. B. von m3.large zu m3.xlarge).
- Für Speicheroptionen für VPX auf AWS empfiehlt Citrix® EBS, da es dauerhaft ist und die Daten auch nach dem Trennen von der Instanz verfügbar sind.

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

- Das dynamische Hinzufügen von ENIs zu VPX wird nicht unterstützt. Starten Sie die VPX-Instanz neu, um das Update anzuwenden. Citrix empfiehlt, die Standalone- oder HA-Instanz zu stoppen, die neue ENI anzuhängen und die Instanz dann neu zu starten.
- Sie können einer ENI mehrere IP-Adressen zuweisen. Die maximale Anzahl von IP-Adressen pro ENI wird durch den EC2-Instanztyp bestimmt. Siehe den Abschnitt „IP-Adressen pro Netzwerkschnittstelle pro Instanztyp“ unter Elastic Network Interfaces. Sie müssen die IP-Adressen in AWS zuweisen, bevor Sie sie den ENIs zuweisen. Weitere Informationen finden Sie unter Elastic Network Interfaces.
- Wir empfehlen, die Befehle zum Aktivieren und Deaktivieren von Schnittstellen auf NetScaler VPX-Schnittstellen zu vermeiden.
- IPv6 wird für VPX nicht unterstützt.
- Aufgrund von AWS-Einschränkungen werden diese Funktionen nicht unterstützt:
  - Gratuitous ARP (GARP)
  - L2 Modus
  - Getaggtes VLAN
  - Dynamisches Routing
  - virtuelle MAC
- Damit RNAT funktioniert, stellen Sie sicher, dass die **Quell-/Zielprüfung** deaktiviert ist. Weitere Informationen finden Sie unter „Ändern der Quell-/Zielprüfung“ in Elastic Network Interfaces.
- Bei einer NetScaler VPX-Bereitstellung auf AWS kann es in einigen AWS-Regionen vorkommen, dass die AWS-Infrastruktur AWS-API-Aufrufe nicht auflösen kann. Dies geschieht, wenn die API-Aufrufe über eine Nicht-Verwaltungsschnittstelle auf der NetScaler VPX-Instanz ausgegeben werden. Als Problemumgehung beschränken Sie die API-Aufrufe nur auf die Verwaltungsschnittstelle. Erstellen Sie dazu ein NSVLAN auf der VPX-Instanz und binden Sie die Verwaltungsschnittstelle mit dem entsprechenden Befehl an das NSVLAN. Zum Beispiel: `set ns config -nsvlan <vlan id> -ifnum 1/1 -tagged NO` `save config` Starten Sie die VPX-Instanz an der Eingabeaufforderung neu. Weitere Informationen zum Konfigurieren von `nsvlan` finden Sie unter Konfigurieren von NSVLAN.
- In der AWS-Konsole kann die für eine VPX-Instanz unter der Registerkarte **Überwachung** angezeigte vCPU-Auslastung hoch sein (bis zu 100 Prozent), selbst wenn die tatsächliche Auslastung niedriger ist. Um die tatsächliche vCPU-Auslastung anzuzeigen, navigieren Sie zu **Alle CloudWatch-Metriken anzeigen**. Weitere Informationen finden Sie unter Überwachen Ihrer Instanzen mit Amazon CloudWatch.

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

- Hot-Adding wird nur für PV- und SRIOV-Schnittstellen mit NetScaler auf AWS unterstützt. VPX-Instanzen mit ENA-Schnittstellen unterstützen kein Hot-Plug, und das Verhalten der Instanzen kann unvorhersehbar sein, wenn Hot-Plugging versucht wird.
- Das Hot-Entfernen über die AWS-Webkonsole oder die AWS-CLI-Schnittstelle wird mit den PV-, SRIOV- und ENA-Schnittstellen für NetScaler nicht unterstützt. Das Verhalten der Instanzen kann unvorhersehbar sein, wenn ein Hot-Entfernen versucht wird.

## Voraussetzungen

Bevor Sie versuchen, eine VPX-Instanz in AWS zu erstellen, stellen Sie sicher, dass Sie Folgendes haben:

- **Ein AWS-Konto**: um ein NetScaler VPX AMI in einer AWS Virtual Private Cloud (VPC) zu starten. Sie können ein kostenloses AWS-Konto unter www.aws.amazon.com erstellen.
- **Ein AWS Identity and Access Management (IAM)-Benutzerkonto**: um den Zugriff auf AWS-Dienste und -Ressourcen für Ihre Benutzer sicher zu steuern. Weitere Informationen zum Erstellen eines IAM-Benutzerkontos finden Sie unter Erstellen von IAM-Benutzern (Konsole). Eine IAM-Rolle ist sowohl für Standalone- als auch für Hochverfügbarkeitsbereitstellungen obligatorisch.

  Die mit Ihrem AWS-Konto verknüpfte IAM-Rolle muss die folgenden IAM-Berechtigungen für verschiedene Szenarien haben.

  **HA-Paar mit IPv4-Adressen in derselben AWS-Zone:**

  ```
  "ec2:DescribeInstances",

  "ec2:AssignPrivateIpAddresses",

  "iam:SimulatePrincipalPolicy",

  "iam:GetRole",

  "ec2:CreateTags"
  ```

  **HA-Paar mit IPv6-Adressen in derselben AWS-Zone:**

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

```
"ec2:DescribeInstances",

"ec2:AssignIpv6Addresses",

"ec2:UnassignIpv6Addresses",

"iam:SimulatePrincipalPolicy",

"iam:GetRole",

"ec2:CreateTags"
```

**HA-Paar mit sowohl IPv4- als auch IPv6-Adressen in derselben AWS-Zone:**

```
"ec2:DescribeInstances",

"ec2:AssignPrivateIpAddresses",

"ec2:AssignIpv6Addresses",

"ec2:UnassignIpv6Addresses",

"iam:SimulatePrincipalPolicy",

"iam:GetRole",

"ec2:CreateTags"
```

**HA-Paar mit elastischen IP-Adressen über verschiedene AWS-Zonen hinweg:**

```
"ec2:DescribeInstances",

"ec2:DescribeAddresses",

"ec2:AssociateAddress",

"ec2:DisassociateAddress",

"iam:SimulatePrincipalPolicy",

"iam:GetRole",
```

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

```
"ec2:CreateTags"
```

**HA-Paar mit privaten IP-Adressen über verschiedene AWS-Zonen hinweg:**

```
"ec2:DescribeInstances",

"ec2:DescribeRouteTables",

"ec2:DeleteRoute",

"ec2:CreateRoute",

"ec2:ModifyNetworkInterfaceAttribute",

"iam:SimulatePrincipalPolicy",

"iam:GetRole",

"ec2:CreateTags"
```

**HA-Paar mit sowohl privaten IP- als auch elastischen IP-Adressen über verschiedene AWS-Zonen hinweg:**

```
"ec2:DescribeInstances",

"ec2:DescribeAddresses",

"ec2:AssociateAddress",

"ec2:DisassociateAddress",

"ec2:DescribeRouteTables",

"ec2:DeleteRoute",

"ec2:CreateRoute",

"ec2:ModifyNetworkInterfaceAttribute",

"iam:SimulatePrincipalPolicy",
```

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

```
"iam:GetRole",

"ec2:CreateTags"
```

**AWS Backend-Autoscaling:**

```
"ec2:DescribeInstances",

"autoscaling:*",

"sns:CreateTopic",

"sns:DeleteTopic",

"sns:ListTopics",

"sns:Subscribe",

"sqs:CreateQueue",

"sqs:ListQueues",

"sqs:DeleteMessage",

"sqs:GetQueueAttributes",

"sqs:SetQueueAttributes",

"iam:SimulatePrincipalPolicy",

"iam:GetRole",

"ec2:CreateTags"
```

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

**HINWEIS:**

- Wenn Sie eine beliebige Kombination der vorstehenden Funktionen verwenden, nutzen Sie die Kombination der IAM-Berechtigungen für jede dieser Funktionen.
- Wenn Sie die Citrix CloudFormation-Vorlage verwenden, wird die IAM-Rolle automatisch erstellt. Die Vorlage erlaubt nicht die Auswahl einer bereits erstellten IAM-Rolle.
- Wenn Sie sich über die GUI bei der VPX-Instanz anmelden, wird eine Aufforderung zur Konfiguration der erforderlichen Berechtigungen für die IAM-Rolle angezeigt. Ignorieren Sie die Aufforderung, wenn Sie die Berechtigungen bereits konfiguriert haben.

- **AWS CLI**: Um alle Funktionen der AWS Management Console über Ihr Terminalprogramm zu nutzen. Weitere Informationen finden Sie im AWS CLI-Benutzerhandbuch. Sie benötigen die AWS CLI auch, um den Netzwerkschnittstellentyp in SR-IOV zu ändern.
- **Elastic Network Adapter (ENA)**: Für Instanztypen mit ENA-Treiber, zum Beispiel M5-, C5-Instanzen, muss die Firmware-Version 13.0 oder höher sein.
- Sie müssen den Instance Metadata Service (IMDS) auf der EC2-Instanz für NetScaler VPX konfigurieren. IMDSv1 und IMDSv2 sind zwei Modi, die für den Zugriff auf Instanzmetadaten von einer laufenden AWS EC2-Instanz verfügbar sind. IMDSv2 ist sicherer als IMDSv1. Sie können die Instanz so konfigurieren, dass sie entweder beide Methoden (die Standardoption) oder nur den IMDSv2-Modus (durch Deaktivieren von IMDSv1) verwendet. Citrix ADC VPX unterstützt den IMDSv2-only-Modus ab NetScaler VPX Release 13.1.48.x.

# AWS IAM-Rollen auf NetScaler VPX-Instanz konfigurieren

Anwendungen, die auf einer Amazon EC2-Instanz ausgeführt werden, müssen AWS-Anmeldeinformationen in den AWS-API-Anfragen enthalten. Sie können AWS-Anmeldeinformationen direkt in der Amazon EC2-Instanz speichern und Anwendungen in dieser Instanz die Verwendung dieser Anmeldeinformationen gestatten. Sie müssen dann jedoch die Anmeldeinformationen verwalten und sicherstellen, dass sie sicher an jede Instanz übergeben werden, und jede Amazon EC2-Instanz aktualisieren, wenn es Zeit ist, die Anmeldeinformationen zu rotieren. Das ist eine Menge zusätzlicher Arbeit.

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

Stattdessen können und müssen Sie eine Identity and Access Management (IAM)-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer Amazon EC2-Instanz ausgeführt werden. Wenn Sie eine Rolle verwenden, müssen Sie keine langfristigen Anmeldeinformationen (wie Benutzername und Passwort oder Zugriffsschlüssel) an eine Amazon EC2-Instanz verteilen. Stattdessen bietet die Rolle temporäre Berechtigungen, die Anwendungen verwenden können, wenn sie Aufrufe an andere AWS-Ressourcen tätigen. Wenn Sie eine Amazon EC2-Instanz starten, geben Sie eine IAM-Rolle an, die der Instanz zugeordnet werden soll. Anwendungen, die auf der Instanz ausgeführt werden, können dann die von der Rolle bereitgestellten temporären Anmeldeinformationen verwenden, um API-Anfragen zu signieren.

Die Ihrem AWS-Konto zugeordnete IAM-Rolle muss die folgenden IAM-Berechtigungen für verschiedene Szenarien besitzen.

**HA-Paar mit IPv4-Adressen in derselben AWS-Zone:**

```
"ec2:DescribeInstances",

"ec2:AssignPrivateIpAddresses",

"iam:SimulatePrincipalPolicy",

"iam:GetRole"
```

**HA-Paar mit IPv6-Adressen in derselben AWS-Zone:**

```
"ec2:DescribeInstances",

"ec2:AssignIpv6Addresses",

"ec2:UnassignIpv6Addresses",

"iam:SimulatePrincipalPolicy",

"iam:GetRole"
```

**HA-Paar mit sowohl IPv4- als auch IPv6-Adressen in derselben AWS-Zone:**

```
"ec2:DescribeInstances",

"ec2:AssignPrivateIpAddresses",
```

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

```
"ec2:AssignIpv6Addresses",

"ec2:UnassignIpv6Addresses",

"iam:SimulatePrincipalPolicy",

"iam:GetRole"
```

**HA-Paar mit elastischen IP-Adressen über verschiedene AWS-Zonen hinweg:**

```
"ec2:DescribeInstances",

"ec2:DescribeAddresses",

"ec2:AssociateAddress",

"ec2:DisassociateAddress",

"iam:SimulatePrincipalPolicy",

"iam:GetRole"
```

**HA-Paar mit privaten IP-Adressen über verschiedene AWS-Zonen hinweg:**

```
"ec2:DescribeInstances",

"ec2:DescribeRouteTables",

"ec2:DeleteRoute",

"ec2:CreateRoute",

"ec2:ModifyNetworkInterfaceAttribute",

"iam:SimulatePrincipalPolicy",

"iam:GetRole"
```

**HA-Paar mit sowohl privaten IP- als auch elastischen IP-Adressen über verschiedene AWS-Zonen hinweg:**

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

```
"ec2:DescribeInstances",

"ec2:DescribeAddresses",

"ec2:AssociateAddress",

"ec2:DisassociateAddress",

"ec2:DescribeRouteTables",

"ec2:DeleteRoute",

"ec2:CreateRoute",

"ec2:ModifyNetworkInterfaceAttribute",

"iam:SimulatePrincipalPolicy",

"iam:GetRole"
```

**AWS-Backend-Autoscaling:**

```
"ec2:DescribeInstances",

"autoscaling:*",

"sns:CreateTopic",

"sns:DeleteTopic",

"sns:ListTopics",

"sns:Subscribe",

"sqs:CreateQueue",

"sqs:ListQueues",

"sqs:DeleteMessage",

"sqs:GetQueueAttributes",
```

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

```
"sqs:SetQueueAttributes",

"iam:SimulatePrincipalPolicy",

"iam:GetRole"
```

**Hinweise:**

- Wenn Sie eine beliebige Kombination der vorstehenden Funktionen verwenden, verwenden Sie die Kombination der IAM-Berechtigungen für jede der Funktionen.
- Wenn Sie die Citrix CloudFormation-Vorlage verwenden, wird die IAM-Rolle automatisch erstellt. Die Vorlage erlaubt nicht die Auswahl einer bereits erstellten IAM-Rolle.
- Wenn Sie sich über die GUI bei der VPX-Instanz anmelden, wird eine Aufforderung zur Konfiguration der erforderlichen Berechtigungen für die IAM-Rolle angezeigt. Ignorieren Sie die Aufforderung, wenn Sie die Berechtigungen bereits konfiguriert haben.
- Eine IAM-Rolle ist sowohl für eigenständige als auch für Hochverfügbarkeitsbereitstellungen obligatorisch.

## Eine IAM-Rolle erstellen

Diese Prozedur beschreibt, wie eine IAM-Rolle für die AWS-Backend-Autoscaling-Funktion erstellt wird.

**HINWEIS:**

Sie können dieselbe Prozedur befolgen, um beliebige IAM-Rollen zu erstellen, die anderen Funktionen entsprechen.

1. Melden Sie sich bei der AWS Management Console für EC2 an.
2. Gehen Sie zur EC2-Instanzseite und wählen Sie Ihre ADC-Instanz aus.

3. Navigieren Sie zu **Aktionen > Sicherheit > IAM-Rolle ändern**.

4. Auf der Seite **IAM-Rolle ändern** können Sie entweder eine vorhandene IAM-Rolle auswählen oder eine IAM-Rolle erstellen.
5. Um eine IAM-Rolle zu erstellen, führen Sie die folgenden Schritte aus:

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

a. Auf der Seite **IAM-Rolle ändern** klicken Sie auf **Neue IAM-Rolle erstellen**.

b. Auf der Seite **Rollen** klicken Sie auf **Rolle erstellen**.

Rolle erstellen(/en-us/vpx/media/iam-create-role.png)

c. Wählen Sie **AWS service** unter **Trusted entity type** und **EC2** unter **Common use cases** aus und klicken Sie dann auf **Next**.

Vertrauenswürdige Entität(/en-us/vpx/media/iam-trusted-entity.png)

d. Auf der Seite **Add permissions** klicken Sie auf **Create policy**.

Richtlinie erstellen(/en-us/vpx/media/iam-create-policy.png)

e. Klicken Sie auf die Registerkarte **JSON**, um den JSON-Editor zu öffnen.

JSON(/en-us/vpx/media/iam-json.png)

f. Im JSON-Editor löschen Sie alles und fügen die IAM-Berechtigungen für die Funktion ein, die Sie verwenden möchten.

Fügen Sie beispielsweise die folgenden IAM-Berechtigungen für die AWS-Backend-Autoscaling-Funktion ein:

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Sid": "VisualEditor0",

            "Effect": "Allow",

            "Action": [

                "ec2:DescribeInstances",

                "autoscaling:*",

                "sns:CreateTopic",
```

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

```
                "sns:DeleteTopic",

                "sns:ListTopics",

                "sns:Subscribe",

                "sqs:CreateQueue",

                "sqs:ListQueues",

                "sqs:DeleteMessage",

                "sqs:GetQueueAttributes",

                "sqs:SetQueueAttributes",

                "iam:SimulatePrincipalPolicy",

                "iam:GetRole"

            ],

            "Resource": "*"

        }

    ]

}
```

Stellen Sie sicher, dass das von Ihnen angegebene Schlüssel-Wert-Paar „Version“ dasselbe ist wie das, das automatisch von AWS generiert wird.

g. Klicken Sie auf **Next: Review**.

IAM überprüfen(/en-us/vpx/media/iam-next-review.png)

h. Auf der Registerkarte **Review policy** geben Sie der Richtlinie einen gültigen Namen und klicken auf **Create Policy**.

Richtlinie überprüfen(/en-us/vpx/media/iam-review-policy.png)

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

i. Auf der Seite **Identity Access Management** klicken Sie auf den Richtliniennamen, den Sie erstellt haben. erweitern Sie die Richtlinie, um das gesamte JSON zu überprüfen, und klicken Sie auf **Next**.

j. Auf der Seite **Name, überprüfen und erstellen** geben Sie der Rolle einen gültigen Namen.

k. Klicken Sie auf **Rolle erstellen**.

6. Wiederholen Sie die Schritte 1, 2 und 3. Wählen Sie die Schaltfläche **Aktualisieren** und wählen Sie das Dropdown-Menü, um die von Ihnen erstellte Rolle anzuzeigen.

7. Klicken Sie auf **IAM-Rolle aktualisieren**.

## IAM-Richtlinien mit dem IAM-Richtliniensimulator testen

Der IAM-Richtliniensimulator ist ein Tool, mit dem Sie die Auswirkungen von IAM-Zugriffssteuerungsrichtlinien testen können, bevor Sie diese in die Produktion übernehmen. Es erleichtert die Überprüfung und Fehlerbehebung von Berechtigungen.

1. Auf der Seite **IAM** wählen Sie die IAM-Rolle aus, die Sie testen möchten, und klicken Sie auf **Simulieren**. Im folgenden Beispiel ist „ADC_IAMRole“ die IAM-Rolle.

2. In der Konsole des **IAM-Richtliniensimulators** wählen Sie **Vorhandene Richtlinien** als **Modus** aus.

3. Wählen Sie auf der Registerkarte **Benutzer, Gruppen und Rollen** im Dropdown-Menü **Rollen** aus und wählen Sie eine vorhandene Rolle.

4. Nachdem Sie die vorhandene Rolle ausgewählt haben, wählen Sie die darunterliegende vorhandene Richtlinie aus.

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

5. Nachdem Sie die Richtlinie ausgewählt haben, sehen Sie die genaue JSON-Struktur auf der linken Seite des Bildschirms. Wählen Sie die gewünschten Aktionen im Dropdown-Menü **Aktionen auswählen** aus.

6. Klicken Sie auf **Simulation ausführen**.

Weitere Informationen finden Sie in der AWS IAM-Dokumentation.

### Weitere Referenzen

Verwenden einer IAM-Rolle, um Anwendungen, die auf Amazon EC2-Instanzen ausgeführt werden, Berechtigungen zu erteilen

## Wie eine NetScaler VPX-Instanz auf AWS funktioniert

Die NetScaler VPX-Instanz ist als AMI im AWS Marketplace verfügbar und kann als EC2-Instanz innerhalb einer AWS VPC gestartet werden. Die NetScaler VPX AMI-Instanz erfordert mindestens 2 virtuelle CPUs und 2 GB Arbeitsspeicher. Eine innerhalb einer AWS VPC gestartete EC2-Instanz kann auch die mehreren Schnittstellen, mehrere IP-Adressen pro Schnittstelle sowie öffentliche und private IP-Adressen bereitstellen, die für die VPX-Konfiguration benötigt werden. Jede VPX-Instanz erfordert mindestens drei IP-Subnetze:

- Ein Management-Subnetz
- Ein clientseitiges Subnetz (VIP)
- Ein serverseitiges Subnetz (SNIP, MIP usw.)

Citrix® empfiehlt drei Netzwerkschnittstellen für die Installation einer Standard-VPX-Instanz auf AWS.

AWS stellt die Multi-IP-Funktionalität derzeit nur für Instanzen zur Verfügung, die innerhalb einer AWS VPC ausgeführt werden. Eine VPX-Instanz in einer VPC kann zum Lastenausgleich von Servern verwendet werden, die in EC2-Instanzen ausgeführt werden. Eine Amazon VPC ermöglicht es Ihnen, eine virtuelle Netzwerkumgebung zu erstellen und zu steuern, einschließlich Ihres eigenen IP-Adressbereichs, Subnetze, Routing-Tabellen und Netzwerk-Gateways.

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

**HINWEIS:**

Standardmäßig können Sie bis zu 5 VPC-Instanzen pro AWS-Region für jedes AWS-Konto erstellen. Sie können höhere VPC-Limits anfordern, indem Sie das Antragsformular von Amazon `<http://aws.amazon.com/contact-us/vpc-request>` einreichen.

**Abbildung 1.** Eine Beispielarchitektur für die Bereitstellung einer NetScaler VPX-Instanz auf AWS

Abbildung 1 zeigt eine einfache Topologie einer AWS VPC mit einer NetScaler VPX-Bereitstellung. Die AWS VPC verfügt über:

1. Ein einzelnes Internet-Gateway, um den Datenverkehr in und aus der VPC zu leiten.
2. Netzwerkkonnektivität zwischen dem Internet-Gateway und dem Internet.
3. Drei Subnetze, jeweils eines für Management, Client und Server.
4. Netzwerkkonnektivität zwischen dem Internet-Gateway und den beiden Subnetzen (Verwaltung und Client).
5. Eine eigenständige NetScaler VPX-Instanz, die innerhalb der VPC bereitgestellt wird. Die VPX-Instanz verfügt über drei ENIs, wobei eine an jedes Subnetz angehängt ist.

## Bereitstellen einer eigenständigen NetScaler VPX-Instanz in AWS

Sie können eine eigenständige NetScaler VPX-Instanz in AWS mit den folgenden Optionen bereitstellen:

- AWS-Webkonsole
- Von Citrix erstellte CloudFormation-Vorlage
- AWS CLI

Dieses Thema beschreibt das Verfahren zur Bereitstellung einer NetScaler VPX-Instanz in AWS.

Bevor Sie mit der Bereitstellung beginnen, lesen Sie die folgenden Themen:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien

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

## Bereitstellen einer NetScaler VPX-Instanz in AWS mithilfe der AWS-Webkonsole

Sie können eine NetScaler VPX-Instanz in AWS über die AWS-Webkonsole bereitstellen. Der Bereitstellungsprozess umfasst die folgenden Schritte:

1. Erstellen eines Schlüsselpaars
2. Erstellen einer Virtual Private Cloud (VPC)
3. Weitere Subnetze hinzufügen
4. Sicherheitsgruppen und Sicherheitsregeln erstellen
5. Routing-Tabellen hinzufügen
6. Ein Internet-Gateway erstellen
7. Eine NetScaler VPX-Instanz erstellen
8. Weitere Netzwerkschnittstellen erstellen und anhängen
9. Elastische IPs an die Management-NIC anhängen
10. Mit der VPX-Instanz verbinden

**Schritt 1: Ein Schlüsselpaar erstellen**.

Amazon EC2 verwendet ein Schlüsselpaar, um Anmeldeinformationen zu verschlüsseln und zu entschlüsseln. Um sich bei Ihrer Instanz anzumelden, müssen Sie ein Schlüsselpaar erstellen, den Namen des Schlüsselpaars beim Starten der Instanz angeben und den privaten Schlüssel bereitstellen, wenn Sie sich mit der Instanz verbinden.

Wenn Sie eine Instanz mithilfe des AWS Launch Instance-Assistenten überprüfen und starten, werden Sie aufgefordert, ein vorhandenes Schlüsselpaar zu verwenden oder ein neues Schlüsselpaar zu erstellen. Weitere Informationen zum Erstellen eines Schlüsselpaars finden Sie unter Amazon EC2 Key Pairs.

**Schritt 2: Eine VPC erstellen**.

Eine NetScaler VPC-Instanz wird innerhalb einer AWS VPC bereitgestellt. Eine VPC ermöglicht es Ihnen, das virtuelle Netzwerk zu definieren, das Ihrem AWS-Konto gewidmet ist. Weitere Informationen zu AWS VPC finden Sie unter Getting Started With Amazon VPC.

Beachten Sie beim Erstellen einer VPC für Ihre NetScaler VPX-Instanz die folgenden Punkte.

- Verwenden Sie die Option „VPC with a Single Public Subnet Only“, um eine AWS VPC in einer AWS-Verfügbarkeitszone zu erstellen.

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

- Citrix empfiehlt, mindestens **drei Subnetze** der folgenden Typen zu erstellen:
  - Ein Subnetz für den Management-Traffic. Sie platzieren die Management-IP (NSIP) in diesem Subnetz. Standardmäßig wird die elastische Netzwerkschnittstelle (ENI) eth0 für die Management-IP verwendet.
  - Ein oder mehrere Subnetze für den Client-Zugriffs-Traffic (Benutzer-zu-NetScaler VPX), über die Clients eine oder mehrere virtuelle IP-Adressen (VIP) erreichen, die NetScaler Load Balancing Virtual Servern zugewiesen sind.
  - Ein oder mehrere Subnetze für den Server-Zugriffs-Traffic (VPX-zu-Server), über die Ihre Server VPX-eigene Subnetz-IP-Adressen (SNIP) erreichen. Weitere Informationen zu NetScaler Load Balancing und Virtual Servern, virtuellen IP-Adressen (VIPs) und Subnetz-IP-Adressen (SNIPs) finden Sie unter:
  - Alle Subnetze müssen sich in derselben Availability Zone befinden.

**Schritt 3: Subnetze hinzufügen**.

Als Sie den VPC-Assistenten verwendet haben, wurde nur ein Subnetz erstellt. Je nach Anforderung möchten Sie möglicherweise weitere Subnetze erstellen. Weitere Informationen zum Erstellen weiterer Subnetze finden Sie unter Hinzufügen eines Subnetzes zu Ihrer VPC.

**Schritt 4: Sicherheitsgruppen und Sicherheitsregeln erstellen**.

Um den eingehenden und ausgehenden Datenverkehr zu steuern, erstellen Sie Sicherheitsgruppen und fügen Sie Regeln zu den Gruppen hinzu. Weitere Informationen zum Erstellen von Gruppen und Hinzufügen von Regeln finden Sie unter Sicherheitsgruppen für Ihre VPC.

Für NetScaler VPX-Instanzen bietet der EC2-Assistent Standardsicherheitsgruppen, die von AWS Marketplace generiert werden und auf den von Citrix empfohlenen Einstellungen basieren. Sie können jedoch weitere Sicherheitsgruppen basierend auf Ihren Anforderungen erstellen.

**HINWEIS:**

Die Ports 22, 80, 443 müssen in der Sicherheitsgruppe für SSH-, HTTP- bzw. HTTPS-Zugriff geöffnet sein.

**Schritt 5: Routing-Tabellen hinzufügen**.

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

Eine Routing-Tabelle enthält eine Reihe von Regeln, sogenannte Routen, die verwendet werden, um zu bestimmen, wohin der Netzwerkverkehr geleitet wird. Jedes Subnetz in Ihrer VPC muss einer Routing-Tabelle zugeordnet sein. Weitere Informationen zum Erstellen einer Routing-Tabelle finden Sie unter Routing-Tabellen.

**Schritt 6: Ein Internet-Gateway erstellen**.

Ein Internet-Gateway dient zwei Zwecken: Es stellt ein Ziel in Ihren VPC-Routing-Tabellen für internetfähigen Datenverkehr bereit und führt die Netzwerkadressübersetzung (NAT) für Instanzen durch, denen öffentliche IPv4-Adressen zugewiesen wurden.

Erstellen Sie ein Internet-Gateway für den Internetverkehr. Weitere Informationen zum Erstellen eines Internet-Gateways finden Sie im Abschnitt Anhängen eines Internet-Gateways.

**Schritt 7: Erstellen Sie eine NetScaler VPX-Instanz mithilfe des AWS EC2-Dienstes**.

Um eine NetScaler VPX-Instanz mithilfe des AWS EC2-Dienstes zu erstellen, führen Sie die folgenden Schritte aus.

1. Navigieren Sie vom AWS-Dashboard aus zu **Compute > EC2 > Launch Instance > AWS Marketplace**.

   Bevor Sie auf **Launch Instance** klicken, stellen Sie sicher, dass Ihre Region korrekt ist, indem Sie den Hinweis überprüfen, der unter **Launch Instance** angezeigt wird.

2. Suchen Sie in der Suchleiste des AWS Marketplace nach dem Schlüsselwort NetScaler VPX.
3. Wählen Sie die Version aus, die Sie bereitstellen möchten, und klicken Sie dann auf **Select**. Für die NetScaler VPX-Version stehen Ihnen die folgenden Optionen zur Verfügung:

   - Eine lizenzierte Version
   - NetScaler VPX Express Appliance (Dies ist eine kostenlose virtuelle Appliance, die ab NetScaler 12.0 56.20 verfügbar ist.)
   - Eigenes Gerät mitbringen

Der Assistent zum Starten einer Instanz wird gestartet. Folgen Sie dem Assistenten, um eine Instanz zu erstellen. Der Assistent fordert Sie auf:

- Instanztyp auswählen
- Instanz konfigurieren
- Speicher hinzufügen

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

- Tags hinzufügen
- Sicherheitsgruppe konfigurieren
- Überprüfen

**Schritt 8: Weitere Netzwerkschnittstellen erstellen und anfügen**.

Erstellen Sie zwei weitere Netzwerkschnittstellen für VIP und SNIP. Weitere Informationen zum Erstellen weiterer Netzwerkschnittstellen finden Sie im Abschnitt Erstellen einer Netzwerkschnittstelle.

Nachdem Sie die Netzwerkschnittstellen erstellt haben, müssen Sie diese an die VPX-Instanz anfügen. Bevor Sie die Schnittstelle anfügen, fahren Sie die VPX-Instanz herunter, fügen Sie die Schnittstelle an und schalten Sie die Instanz ein. Weitere Informationen zum Anfügen von Netzwerkschnittstellen finden Sie im Abschnitt Anfügen einer Netzwerkschnittstelle beim Starten einer Instanz.

**Schritt 9: Elastische IPs zuweisen und zuordnen**.

Wenn Sie einer EC2-Instanz eine öffentliche IP-Adresse zuweisen, bleibt diese nur zugewiesen, bis die Instanz gestoppt wird. Danach wird die Adresse an den Pool zurückgegeben. Wenn Sie die Instanz neu starten, wird eine neue öffentliche IP-Adresse zugewiesen.

Im Gegensatz dazu bleibt eine elastische IP-Adresse (EIP) zugewiesen, bis die Adresse von einer Instanz getrennt wird.

Weisen Sie eine elastische IP für die Management-NIC zu und ordnen Sie sie zu. Weitere Informationen zum Zuweisen und Zuordnen elastischer IP-Adressen finden Sie in diesen Themen:

- Zuweisen einer elastischen IP-Adresse
- Zuordnen einer elastischen IP-Adresse zu einer laufenden Instanz

Diese Schritte schließen das Verfahren zum Erstellen einer NetScaler VPX-Instanz auf AWS ab. Es kann einige Minuten dauern, bis die Instanz bereit ist. Überprüfen Sie, ob Ihre Instanz ihre Statusprüfungen bestanden hat. Diese Informationen können Sie in der Spalte **Statusprüfungen** auf der Seite Instanzen anzeigen.

**Schritt 10: Mit der VPX-Instanz verbinden**.

Nachdem Sie die VPX-Instanz erstellt haben, verbinden Sie sich mit der Instanz über die GUI und einen SSH-Client.

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

- GUI

Die folgenden Standard-Administratoranmeldeinformationen gelten für den Zugriff auf eine NetScaler VPX-Instanz

Benutzername: `nsroot`

Passwort: Das Standardpasswort für das ns-Root-Konto ist auf die AWS-Instanz-ID der NetScaler VPX-Instanz festgelegt. Bei der ersten Anmeldung werden Sie aus Sicherheitsgründen aufgefordert, das Passwort zu ändern. Nach dem Ändern des Passworts müssen Sie die Konfiguration speichern. Wenn die Konfiguration nicht gespeichert wird und die Instanz neu startet, müssen Sie sich mit dem Standardpasswort anmelden. Ändern Sie das Passwort erneut bei der Aufforderung.

- SSH-Client

Wählen Sie in der AWS-Managementkonsole die NetScaler VPX-Instanz aus und klicken Sie auf **Verbinden**. Befolgen Sie die Anweisungen auf der Seite **Mit Ihrer Instanz verbinden**.

Weitere Informationen zum Bereitstellen einer eigenständigen NetScaler VPX-Instanz in AWS mithilfe der AWS-Webkonsole finden Sie unter Szenario: eigenständige Instanz

## Konfigurieren einer NetScaler VPX-Instanz mithilfe der Citrix CloudFormation-Vorlage

Sie können die von Citrix bereitgestellte CloudFormation-Vorlage verwenden, um den Start der VPX-Instanz zu automatisieren. Die Vorlage bietet Funktionen zum Starten einer einzelnen NetScaler VPX-Instanz oder zum Erstellen einer Hochverfügbarkeitsumgebung mit einem Paar von NetScaler VPX-Instanzen.

Sie können die Vorlage über AWS Marketplace oder GitHub starten.

Die CloudFormation-Vorlage erfordert eine vorhandene VPC-Umgebung und startet eine VPX-Instanz mit drei elastischen Netzwerkschnittstellen (ENIs). Bevor Sie die CloudFormation-Vorlage starten, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Eine AWS Virtual Private Cloud (VPC)
- Drei Subnetze innerhalb der VPC: eines für die Verwaltung, eines für den Client-Traffic und eines für Back-End-Server
- Ein EC2-Schlüsselpaar, um den SSH-Zugriff auf die Instanz zu ermöglichen
- Eine Sicherheitsgruppe mit offenen UDP 3003-, TCP 3009–3010-, HTTP- und SSH-Ports

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

Weitere Informationen zum Abschluss der Voraussetzungen finden Sie im Abschnitt „Bereitstellen einer NetScaler VPX-Instanz auf AWS mithilfe der AWS-Webkonsole“ oder in der AWS-Dokumentation.

Des Weiteren konfigurieren und starten Sie eine eigenständige NetScaler VPX Express-Instanz mithilfe der Citrix CloudFormation-Vorlage, die auf GitHub verfügbar ist:

`<https://github.com/citrix/citrix-adc-aws-cloudformation/tree/master/templates/standalone/>`

Eine IAM-Rolle ist für eine eigenständige Bereitstellung nicht zwingend erforderlich. Citrix empfiehlt jedoch, eine IAM-Rolle mit den erforderlichen Berechtigungen für die Instanz zu erstellen und anzuhängen, um zukünftigen Anforderungen gerecht zu werden. Die IAM-Rolle stellt sicher, dass die eigenständige Instanz bei Bedarf problemlos in einen Hochverfügbarkeitsknoten mit SR-IOV umgewandelt werden kann.

Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter Konfigurieren von NetScaler VPX-Instanzen zur Verwendung der SR-IOV-Netzwerkschnittstelle.

**HINWEIS:**

Wenn Sie eine NetScaler VPX-Instanz auf AWS mithilfe der AWS-Webkonsole bereitstellen, ist der CloudWatch-Dienst standardmäßig aktiviert. Wenn Sie eine NetScaler VPX-Instanz mithilfe der Citrix CloudFormation-Vorlage bereitstellen, ist die Standardoption „Ja“. Wenn Sie den CloudWatch-Dienst deaktivieren möchten, wählen Sie „Nein“. Weitere Informationen finden Sie unter Überwachen Ihrer Instanzen mit Amazon CloudWatch

### Konfigurieren einer NetScaler VPX-Instanz mithilfe der AWS CLI

Sie können die AWS CLI verwenden, um Instanzen zu starten. Weitere Informationen finden Sie in der AWS Command Line Interface Documentation.

## Szenario: eigenständige Instanz

Dieses Szenario veranschaulicht, wie eine eigenständige NetScaler VPX EC2-Instanz in AWS mithilfe der AWS-GUI bereitgestellt wird. Erstellen Sie eine eigenständige VPX-Instanz mit drei NICs. Die Instanz, die als virtueller Lastausgleichsserver konfiguriert ist, kommuniziert mit Back-End-Servern (der Serverfarm). Richten Sie für diese Konfiguration die erforderlichen

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

Kommunikationsrouten zwischen der Instanz und den Back-End-Servern sowie zwischen der Instanz und den externen Hosts im öffentlichen Internet ein.

Weitere Informationen zum Verfahren zur Bereitstellung einer VPX-Instanz finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz in AWS.

Erstellen Sie drei NICs. Jede NIC kann mit einem Paar IP-Adressen (öffentlich und privat) konfiguriert werden. Die NICs dienen den folgenden Zwecken.

| NIC | ZWECK | ZUGEORDNET ZU |
|---|---|---|
| eth0 | Dient dem Management-Traffic (NSIP) | Eine öffentliche IP-Adresse und eine private IP-Adresse |
| eth1 | Dient dem clientseitigen Traffic (VIP) | Eine öffentliche IP-Adresse und eine private IP-Adresse |
| eth2 | Kommuniziert mit Back-End-Servern (SNIP) | Eine öffentliche IP-Adresse (Private IP-Adresse nicht zwingend erforderlich) |

Schritt 1: Eine VPC erstellen.

1. Melden Sie sich bei der AWS-Webkonsole an und navigieren Sie zu **Networking & Content Delivery** \> **VPC**. Klicken Sie auf **Start VPC Wizard**.
2. Wählen Sie **VPC with a Single Public Subnet** aus und klicken Sie auf **Select**.
3. Stellen Sie den IP-CIDR-Block für dieses Szenario auf 10.0.0.0/16 ein.
4. Geben Sie der VPC einen Namen.
5. Stellen Sie das öffentliche Subnetz auf 10.0.0.0/24 ein. (Dies ist das Management-Netzwerk).
6. Wählen Sie eine Verfügbarkeitszone aus.
7. Geben Sie dem Subnetz einen Namen.
8. Klicken Sie auf **VPC** erstellen.

Schritt 2: Zusätzliche Subnetze erstellen.

1. Öffnen Sie die Amazon VPC-Konsole unter `<https://console.aws.amazon.com/vpc/>`.
2. Wählen Sie im Navigationsbereich „Subnetze“, „Subnetz erstellen“, nachdem Sie die folgenden Details eingegeben haben.

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

- Name-Tag: Geben Sie einen Namen für Ihr Subnetz an.
- VPC: Wählen Sie die VPC aus, für die Sie das Subnetz erstellen.
- Verfügbarkeitszone: Wählen Sie die Verfügbarkeitszone aus, in der Sie die VPC in Schritt 1 erstellt haben.
- IPv4-CIDR-Block: Geben Sie einen IPv4-CIDR-Block für Ihr Subnetz an. Wählen Sie für dieses Szenario 10.0.1.0/24.

3. Wiederholen Sie die Schritte, um ein weiteres Subnetz für Back-End-Server zu erstellen.

Schritt 3: Erstellen Sie eine Routing-Tabelle.

1. Öffnen Sie die Amazon VPC-Konsole unter `<https://console.aws.amazon.com/vpc/>`.
2. Wählen Sie im Navigationsbereich **Routing-Tabellen** > **Routing-Tabelle erstellen.**
3. Fügen Sie im Fenster „Routing-Tabelle erstellen“ einen Namen hinzu und wählen Sie die VPC aus, die Sie in Schritt 1 erstellt haben.
4. Klicken Sie auf **Ja, erstellen**.

   Die Routing-Tabelle wird allen Subnetzen zugewiesen, die Sie für diese VPC erstellt haben, damit der Datenverkehr von einer Instanz in einem Subnetz eine Instanz in einem anderen Subnetz erreichen kann.
5. Klicken Sie auf **Subnetz-Zuordnungen** und dann auf **Bearbeiten**.
6. Klicken Sie auf das Management- und Client-Subnetz und dann auf Speichern. Dadurch wird eine Routing-Tabelle nur für den Internetverkehr erstellt.
7. Klicken Sie auf **Routen > Bearbeiten > Weitere Route hinzufügen**.
8. Fügen Sie im Feld „Ziel“ 0.0.0.0/0 hinzu und klicken Sie auf das Feld „Ziel“, um igw-\<xxxx\> das Internet-Gateway auszuwählen, das der VPC-Assistent automatisch erstellt hat.
9. Klicken Sie auf **Speichern**.
10. Führen Sie die Schritte aus, um eine Routing-Tabelle für den serverseitigen Datenverkehr zu erstellen.

Schritt 4: Eine NetScaler VPX-Instanz erstellen.

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

1. Melden Sie sich an der AWS Management Console an und klicken Sie unter **Compute** auf **EC2**.
2. Klicken Sie auf AWS Marketplace. Geben Sie in der Suchleiste von AWS Marketplace „NetScaler VPX“ ein und drücken Sie die Eingabetaste. Die verfügbaren NetScaler VPX-Editionen werden angezeigt.
3. Klicken Sie auf **Auswählen**, um die gewünschte NetScaler VPX-Edition auszuwählen. Der EC2-Instanz-Assistent wird gestartet.
4. Wählen Sie auf der Seite **Instanztyp auswählen** die Option **m4. Xlarge** (empfohlen) und klicken Sie auf **Weiter: Instanzdetails konfigurieren**.
5. Wählen Sie auf der Seite „Instanzdetails konfigurieren“ Folgendes aus und klicken Sie dann auf **Weiter: Speicher hinzufügen**.

   - Anzahl der Instanzen: 1
   - Netzwerk: die in Schritt 1 erstellte VPC
   - Subnetz: das Management-Subnetz
   - Öffentliche IP automatisch zuweisen: Aktivieren

6. Wählen Sie auf der Seite „Speicher hinzufügen“ die Standardoption aus und klicken Sie auf **Weiter: Tags hinzufügen**.
7. Geben Sie auf der Seite „Tags hinzufügen“ einen Namen für die Instanz ein und klicken Sie auf **Weiter: Sicherheitsgruppe konfigurieren**.
8. Wählen Sie auf der Seite „Sicherheitsgruppe konfigurieren“ die Standardoption (die von AWS Marketplace generiert wird und auf den empfohlenen Einstellungen von Citrix® Systems basiert) und klicken Sie dann auf **Überprüfen und starten > Starten**.
9. Sie werden aufgefordert, ein vorhandenes Schlüsselpaar auszuwählen oder ein neues Schlüsselpaar zu erstellen. Wählen Sie aus der Dropdown-Liste „Schlüsselpaar auswählen“ das Schlüsselpaar aus, das Sie als Voraussetzung erstellt haben (siehe Abschnitt „Voraussetzung“).
10. Aktivieren Sie das Kontrollkästchen, um das Schlüsselpaar zu bestätigen, und klicken Sie auf **Instanzen starten**.

Der Assistent zum Starten von Instanzen zeigt den Startstatus an, und die Instanz wird in der Liste der Instanzen angezeigt, sobald sie vollständig gestartet ist.

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

Um die Instanz zu überprüfen, gehen Sie zur AWS-Konsole und klicken Sie auf **EC2 > Laufende Instanzen**. Wählen Sie die Instanz aus und fügen Sie einen Namen hinzu. Stellen Sie sicher, dass der Instanzstatus „running“ (wird ausgeführt) ist und die Statusprüfungen abgeschlossen sind.

Schritt 5: Weitere Netzwerkschnittstellen erstellen und anfügen.

Als Sie die VPC erstellt haben, war nur eine Netzwerkschnittstelle damit verbunden. Fügen Sie nun zwei weitere Netzwerkschnittstellen zur VPC hinzu, für VIP und SNIP.

1. Öffnen Sie die Amazon EC2-Konsole unter `<https://console.aws.amazon.com/ec2/>`.
2. Wählen Sie im Navigationsbereich „Netzwerkschnittstellen“.
3. Wählen Sie Netzwerk-Schnittstelle erstellen.
4. Geben Sie unter **Beschreibung** einen aussagekräftigen Namen ein.
5. Wählen Sie unter **Subnetz** das Subnetz aus, das Sie zuvor für die VIP erstellt haben.
6. Lassen Sie unter **Private IP** die Standardoption unverändert.
7. Wählen Sie unter **Sicherheitsgruppen** die Gruppe aus.
8. Klicken Sie auf **Ja, erstellen**.

9. Nachdem die Netzwerkschnittstelle erstellt wurde, weisen Sie der Schnittstelle einen Namen zu.
10. Wiederholen Sie die Schritte, um eine Netzwerkschnittstelle für den serverseitigen Datenverkehr zu erstellen.

**Netzwerkschnittstellen anfügen**:

1. Wählen Sie im Navigationsbereich Netzwerk-Schnittstellen.
2. Wählen Sie die Netzwerkschnittstelle aus und klicken Sie auf **Anfügen**.
3. Wählen Sie im Dialogfeld Netzwerkschnittstelle anfügen die Instanz aus und klicken Sie auf **Anfügen**.

Schritt 6: Eine elastische IP an die NSIP anfügen.

1. Gehen Sie in der AWS-Managementkonsole zu **NETZWERK & SICHERHEIT > Elastic IPs**.
2. Prüfen Sie, ob eine freie EIP zum Anfügen verfügbar ist. Falls nicht, klicken Sie auf **Neue Adresse zuweisen**.

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

3. Wählen Sie die neu zugewiesene IP-Adresse aus und wählen Sie **Aktionen > Adresse zuordnen**.
4. Klicken Sie auf das Optionsfeld **Netzwerkschnittstelle**.
5. Wählen Sie aus der Dropdown-Liste „Netzwerkschnittstelle“ die Management-NIC aus.
6. Wählen Sie aus dem Dropdown-Menü **Private IP** die von AWS generierte IP-Adresse aus.
7. Aktivieren Sie das Kontrollkästchen **Neu zuordnen**.
8. Klicken Sie auf **Zuordnen**.

**Auf die VPX-Instanz zugreifen**:

Nachdem Sie eine eigenständige NetScaler VPX-Instanz mit drei NICs konfiguriert haben, melden Sie sich bei der VPX-Instanz an, um die NetScaler-seitige Konfiguration abzuschließen. Verwenden Sie die folgenden Optionen:

- GUI: Geben Sie die öffentliche IP der Management-NIC in den Browser ein. Melden Sie sich mit `nsroot` als Benutzernamen und der Instanz-ID (i-0c1ffe1d987817522) als Kennwort an.

**HINWEIS:**

Bei der ersten Anmeldung werden Sie aus Sicherheitsgründen aufgefordert, das Kennwort zu ändern. Nachdem Sie das Kennwort geändert haben, müssen Sie die Konfiguration speichern. Wenn die Konfiguration nicht gespeichert wird und die Instanz neu startet, müssen Sie sich mit dem Standardkennwort anmelden. Ändern Sie das Kennwort erneut bei der Aufforderung und speichern Sie die Konfiguration.

- SSH: Öffnen Sie einen SSH-Client und geben Sie Folgendes ein:

```
ssh -i \<location of your private key\> ns root@\<public DNS of the instance\>
```

Um den öffentlichen DNS zu finden, klicken Sie auf die Instanz und klicken Sie auf **Verbinden**.

**Verwandte Informationen**:

- Um die NetScaler-eigenen IP-Adressen (NSIP, VIP und SNIP) zu konfigurieren, siehe Konfigurieren von NetScaler-eigenen IP-Adressen.
- Sie haben eine BYOL-Version der NetScaler VPX Appliance konfiguriert; weitere Informationen finden Sie im VPX Licensing Guide unter `<https://support.citrix.com/s/article/`

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

`CTX255959-how-to-allocate-and-install-citrix-netscaler-vpx-licenses?language=en_US>`

# NetScaler VPX-Lizenz herunterladen

Nach dem Start einer NetScaler VPX-Instanz mit Kundenlizenz vom AWS Marketplace ist eine Lizenz erforderlich. Weitere Informationen zur VPX-Lizenzierung finden Sie unter Lizenzierungsübersicht.

Sie müssen:

1. Verwenden Sie das Lizenzierungsportal auf der Citrix®-Website, um eine gültige Lizenz zu generieren.
2. Laden Sie die Lizenz auf die Instanz hoch.

Wenn es sich um eine **kostenpflichtige** Marketplace-Instanz handelt, müssen Sie keine Lizenz installieren. Der korrekte Funktionsumfang und die Leistung werden automatisch aktiviert.

Wenn Sie eine NetScaler VPX-Instanz mit einer Modellnummer verwenden, die höher als VPX 5000 ist, entspricht der Netzwerkdurchsatz möglicherweise nicht dem in der Instanzlizenz angegebenen Wert. Andere Funktionen, wie z. B. der SSL-Durchsatz und die SSL-Transaktionen pro Sekunde, können sich jedoch verbessern.

Eine Netzwerkbandbreite von 5 Gbit/s wird im Instanztyp `c4.8xlarge` beobachtet.

## So migrieren Sie das AWS-Abonnement zu BYOL

Dieser Abschnitt beschreibt das Verfahren zur Migration von einem AWS-Abonnement zu Bring your own license (BYOL) und umgekehrt.

Führen Sie die folgenden Schritte aus, um ein AWS-Abonnement zu BYOL zu migrieren:

**HINWEIS:**

**Schritt 2** und **Schritt 3** werden auf der NetScaler VPX-Instanz ausgeführt, und alle anderen Schritte werden im AWS-Portal ausgeführt.

1. Erstellen Sie eine BYOL EC2-Instanz mit NetScaler VPX - Customer Licensed in derselben Availability Zone wie die alte EC2-Instanz, die dieselbe Sicherheitsgruppe, IAM-Rolle und dasselbe Subnetz hat. Die neue EC2-Instanz darf nur eine ENI-Schnittstelle haben.

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

2. Um die Daten auf der alten EC2-Instanz über die NetScaler GUI zu sichern, führen Sie die folgenden Schritte aus.

   a. Navigieren Sie zu **System > Backup and Restore**.

   b. Klicken Sie auf der Seite **Welcome** auf **Backup/Import**, um den Vorgang zu starten.

   c. Geben Sie auf der Seite **Backup/Import** die folgenden Details ein:

      - **Name** – Name der Sicherungsdatei.
      - **Level** – Wählen Sie die Sicherungsstufe als **Full**.
      - **Comment** – Geben Sie eine kurze Beschreibung der Sicherung an.

   d. Klicken Sie auf **Backup**. Sobald die Sicherung abgeschlossen ist, können Sie die Datei auswählen und auf Ihren lokalen Computer herunterladen.

3. Führen Sie die folgenden Schritte aus, um die Daten auf der neuen EC2-Instanz über die NetScaler-GUI wiederherzustellen:

   a. Navigieren Sie zu **System > Backup and Restore**.

   b. Klicken Sie auf **Backup/Import**, um den Vorgang zu starten.

   c. Wählen Sie die Option **Import** und laden Sie die Sicherungsdatei hoch.

   d. Wählen Sie die Datei aus.

   e. Wählen Sie im Dropdown-Menü **Aktion auswählen** die Option **Wiederherstellen**.

   f. Überprüfen Sie auf der Seite **Wiederherstellen** die Dateidetails und klicken Sie auf **Wiederherstellen**.

   g. Starten Sie nach der Wiederherstellung die EC2-Instanz neu.

4. Verschieben Sie alle Schnittstellen (außer der Verwaltungsschnittstelle, an die die NSIP-Adresse gebunden ist) von der alten EC2-Instanz auf die neue EC2-Instanz. Um eine

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

Netzwerkschnittstelle von einer EC2-Instanz zu einer anderen zu verschieben, gehen Sie wie folgt vor:

a. Stoppen Sie im **AWS-Portal** sowohl die alte als auch die neue EC2-Instanz.
b. Navigieren Sie zu **Netzwerkschnittstellen** und wählen Sie die Netzwerkschnittstelle aus, die an die alte EC2-Instanz angehängt ist.
c. Trennen Sie die EC2-Instanz, indem Sie auf **Aktionen > Trennen** klicken.

d. Fügen Sie die Netzwerkschnittstelle an die neue EC2-Instanz an, indem Sie auf **Aktionen > Anfügen** klicken. Geben Sie den Namen der EC2-Instanz ein, an die die Netzwerkschnittstelle angefügt werden soll.

e. Führen Sie **Schritt 1** bis **Schritt 4** für alle anderen angehängten Schnittstellen aus. Achten Sie darauf, die Reihenfolge einzuhalten und die Schnittstellenreihenfolge beizubehalten. Das heißt, trennen Sie zuerst Schnittstelle 2 und fügen Sie sie an, dann trennen Sie Schnittstelle 3 und fügen Sie sie an, und so weiter.

5. Sie können die Verwaltungsschnittstelle nicht von einer alten EC2-Instanz trennen. Verschieben Sie daher alle sekundären IP-Adressen (falls vorhanden) auf der Verwaltungsschnittstelle (primäre Netzwerkschnittstelle) der alten EC2-Instanz auf die neue EC2-Instanz. Um eine IP-Adresse von einer Schnittstelle zu einer anderen zu verschieben, gehen Sie wie folgt vor:

   a. Im **AWS-Portal** stellen Sie sicher, dass sowohl die alte als auch die neue EC2-Instanz den Status **Gestoppt** haben.
   b. Navigieren Sie zu **Netzwerkschnittstellen**, und wählen Sie die Verwaltungsschnittstelle aus, die an die alte EC2-Instanz angehängt ist.
   c. Klicken Sie auf **Aktionen > IP-Adresse verwalten**, und notieren Sie sich alle zugewiesenen sekundären IP-Adressen (falls vorhanden).
   d. Navigieren Sie zur Verwaltungsschnittstelle oder primären Schnittstelle der neuen EC2-Instanz.
   e. Klicken Sie auf **Aktionen > IP-Adressen verwalten**.
   f. Unter **IPv4-Adressen** klicken Sie auf **Neue IP-Adresse zuweisen**.
   g. Geben Sie die IP-Adressen ein, die in **Schritt 3** notiert wurden.

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

h. Aktivieren Sie das Kontrollkästchen **Sekundäre private IP-Adressen neu zuweisen zulassen**.

i. Klicken Sie auf **Speichern**.

6. Starten Sie die neue EC2-Instanz und überprüfen Sie die Konfiguration. Nachdem die gesamte Konfiguration verschoben wurde, können Sie die alte EC2-Instanz nach Bedarf löschen oder behalten.
7. Wenn eine EIP-Adresse an die NSIP-Adresse der alten EC2-Instanz angehängt ist, verschieben Sie die NSIP-Adresse der alten Instanz auf die NSIP-Adresse der neuen Instanz.
8. Wenn Sie zur alten Instanz zurückkehren möchten, führen Sie die gleichen Schritte in umgekehrter Reihenfolge zwischen der alten und der neuen Instanz aus.
9. Nachdem Sie von einer Abonnement-Instanz zu einer BYOL-Instanz gewechselt haben, ist eine Lizenz erforderlich. Um eine Lizenz zu installieren, gehen Sie wie folgt vor:

   - Verwenden Sie das Lizenzierungsportal auf der Citrix-Website, um eine gültige Lizenz zu generieren.
   - Laden Sie die Lizenz auf die Instanz hoch.

**HINWEIS:**

Wenn Sie eine BYOL-Instanz in eine Abonnement-Instanz (kostenpflichtige Marketplace-Instanz) verschieben, müssen Sie die Lizenz nicht installieren. Der korrekte Funktionsumfang und die Leistung werden automatisch aktiviert.

### Einschränkungen

Die Verwaltungsschnittstelle kann nicht auf die neue EC2-Instanz verschoben werden. Citrix empfiehlt daher, die Verwaltungsschnittstelle manuell zu konfigurieren. Weitere Informationen finden Sie unter **Schritt 5** im vorhergehenden Verfahren. Eine neue EC2-Instanz wird als exakte Replik der alten EC2-Instanz erstellt, aber nur die NSIP-Adresse hat eine neue IP-Adresse.

## Lastverteilung von Servern in verschiedenen Verfügbarkeitszonen

Eine VPX-Instanz kann verwendet werden, um Server, die in derselben Verfügbarkeitszone ausgeführt werden, oder in den folgenden Fällen eine Lastverteilung durchzuführen:

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

- Einer anderen Verfügbarkeitszone (AZ) in derselben AWS VPC
- Einer anderen AWS-Region
- AWS EC2 in einer VPC

Um einer VPX-Instanz zu ermöglichen, Server außerhalb der AWS VPC, in der sich die VPX-Instanz befindet, mit Lastverteilung zu versorgen, konfigurieren Sie die Instanz so, dass sie EIPs verwendet, um den Datenverkehr über das Internet-Gateway zu leiten, wie folgt:

1. Konfigurieren Sie eine SNIP auf der NetScaler VPX-Instanz mithilfe der NetScaler CLI oder der GUI.
2. Ermöglichen Sie das Routing des Datenverkehrs aus der AZ, indem Sie ein öffentliches Subnetz für den serverseitigen Datenverkehr erstellen.
3. Fügen Sie der Routing-Tabelle eine Internet-Gateway-Route hinzu, indem Sie die AWS GUI-Konsole verwenden.
4. Verknüpfen Sie die aktualisierte Routing-Tabelle mit dem serverseitigen Subnetz.
5. Verknüpfen Sie eine EIP mit der privaten serverseitigen IP-Adresse, die einer NetScaler SNIP-Adresse zugeordnet ist.

## So funktioniert Hochverfügbarkeit auf AWS

Sie können zwei NetScaler VPX-Instanzen auf AWS als Hochverfügbarkeits-Paar (HA) im Aktiv-Passiv-Modus konfigurieren. Wenn Sie eine Instanz als primären Knoten und die andere als sekundären Knoten konfigurieren, akzeptiert der primäre Knoten Verbindungen und verwaltet Server. Der sekundäre Knoten überwacht den primären Knoten. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen akzeptieren kann, übernimmt der sekundäre Knoten.

In AWS werden die folgenden Bereitstellungstypen für VPX-Instanzen unterstützt:

- Hochverfügbarkeit innerhalb derselben Zone
- Hochverfügbarkeit über verschiedene Zonen hinweg

**HINWEIS:**

Damit Hochverfügbarkeit funktioniert, stellen Sie sicher, dass beide NetScaler VPX-Instanzen mit IAM-Rollen verbunden und mit der Elastic IP (EIP)-Adresse für die NSIP zugewiesen sind. Sie müssen keine EIP auf NSIP zuweisen, wenn die NSIP über die NAT-Instanz das Internet erreichen kann.

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

## Hochverfügbarkeit innerhalb derselben Zonen

Bei einer Hochverfügbarkeitsbereitstellung innerhalb derselben Zonen müssen beide VPX-Instanzen ähnliche Netzwerkkonfigurationen aufweisen.

Beachten Sie diese beiden Regeln:

Regel 1. Jede NIC auf einer VPX-Instanz muss sich im selben Subnetz befinden wie die entsprechende NIC in der anderen VPX. Beide Instanzen müssen Folgendes haben:

- Managementschnittstelle im selben Subnetz (als Management-Subnetz bezeichnet)
- Clientschnittstelle im selben Subnetz (als Client-Subnetz bezeichnet)
- Serverschnittstelle im selben Subnetz (als Server-Subnetz bezeichnet)

Regel 2. Die Reihenfolge von Management-NIC, Client-NIC und Server-NIC auf beiden Instanzen muss gleich sein. Zum Beispiel wird das folgende Szenario nicht unterstützt.

VPX-Instanz 1

NIC 0: Verwaltung NIC 1: Client NIC 2: Server

VPX-Instanz 2

NIC 0: Verwaltung

NIC 1: Server

NIC 2: Client

In diesem Szenario befindet sich NIC 1 von Instanz 1 im Client-Subnetz, während sich NIC 1 von Instanz 2 im Server-Subnetz befindet. Damit HA funktioniert, muss NIC 1 beider Instanzen entweder im Client-Subnetz oder im Server-Subnetz sein.

Ab 13.0 41.xx kann Hochverfügbarkeit durch die Migration sekundärer privater IP-Adressen erreicht werden, die an die NICs (Client- und serverseitige NICs) des primären HA-Knotens angehängt sind, zum sekundären HA-Knoten nach einem Failover. In dieser Bereitstellung:

- Beide VPX-Instanzen haben die gleiche Anzahl von NICs und Subnetz-Zuordnung gemäß der NIC-Aufzählung.
- Jede VPX-NIC hat eine zusätzliche private IP-Adresse, außer der ersten NIC, die der Management-IP-Adresse entspricht. Die zusätzliche private IP-Adresse erscheint als primäre private IP-Adresse in der AWS-Webkonsole. In unserem Dokument bezeichnen wir diese zusätzliche IP-Adresse als Dummy-IP-Adresse).

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

- Die Dummy-IP-Adressen dürfen auf der NetScaler-Instanz nicht als VIP und SNIP konfiguriert werden.
- Andere sekundäre private IP-Adressen müssen bei Bedarf erstellt und als VIP und SNIP konfiguriert werden.
- Beim Failover sucht der neue primäre Knoten nach konfigurierten SNIPs und VIPs und verschiebt sie von den NICs, die an den vorherigen primären Knoten angehängt waren, zu den entsprechenden NICs auf dem neuen primären Knoten.
- NetScaler-Instanzen benötigen IAM-Berechtigungen, damit HA funktioniert. Fügen Sie die folgenden IAM-Berechtigungen zur IAM-Richtlinie hinzu, die jeder Instanz hinzugefügt wurde.

`"iam:GetRole"` `"ec2:DescribeInstances"` `"ec2:DescribeNetworkInterfaces"` `"ec2:AssignPrivateIpAddresses"`

**HINWEIS:**

`unassignPrivateIpAddress` ist nicht erforderlich.

Diese Methode ist schneller als die ältere Methode. Bei der älteren Methode hängt HA von der Migration der elastischen AWS-Netzwerkschnittstellen des primären Knotens zum sekundären Knoten ab.

Für die ältere Methode sind die folgenden Richtlinien erforderlich:

`"iam:GetRole"` `"ec2:DescribeInstances"` `"ec2:DescribeAddresses"` `"ec2:AssociateAddress"` `"ec2:DisassociateAddress"`

Weitere Informationen finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.

## Hochverfügbarkeit über verschiedene Zonen hinweg

Sie können zwei NetScaler VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen als Hochverfügbarkeits-Aktiv-Passiv-Paar im Independent Network Configuration (INC)-Modus konfigurieren. Beim Failover migriert die EIP (Elastic IP) der VIP der primären Instanz zur sekundären Instanz, die dann als neue primäre Instanz fungiert. Im Failover-Prozess führt die AWS-API folgende Schritte aus:

- Überprüft die virtuellen Server, denen `IPSets` zugewiesen ist.

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

- Findet die IP-Adresse mit einer zugeordneten öffentlichen IP aus den beiden IP-Adressen, auf denen der virtuelle Server lauscht. Eine, die direkt an den virtuellen Server angehängt ist, und eine, die über den IP-Satz angehängt ist.
- Ordnet die öffentliche IP (EIP) der privaten IP neu zu, die zur neuen primären VIP gehört.

Für HA über verschiedene Zonen hinweg sind die folgenden Richtlinien erforderlich:

`"iam:GetRole"` `"ec2:DescribeInstances"` `"ec2:DescribeAddresses"` `"ec2:AssociateAddress"` `"ec2:DisassociateAddress"`

Weitere Informationen finden Sie unter Hochverfügbarkeit über AWS-Verfügbarkeitszonen hinweg.

### Vor Beginn Ihrer Bereitstellung

Bevor Sie eine HA-Bereitstellung auf AWS starten, lesen Sie das folgende Dokument:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien
- Bereitstellen einer NetScaler VPX-Instanz auf AWS
- Hochverfügbarkeit

### Fehlerbehebung

Um Fehler während eines HA-Failovers einer NetScaler VPX-Instanz in der AWS Cloud zu beheben, überprüfen Sie die `cloud-ha-daemon.log` Datei, die am `/var/log/` Speicherort gespeichert ist.

## Bereitstellen eines VPX HA-Paares in derselben AWS-Verfügbarkeitszone

**HINWEIS:**

Ab NetScaler Release 13.1 Build 27.x unterstützt das VPX HA-Paar in derselben AWS-Verfügbarkeitszone IPv6-Adressen.

Sie können zwei NetScaler VPX-Instanzen in AWS als HA-Paar in derselben AWS-Zone konfigurieren, wobei sich beide VPX-Instanzen im selben Subnetz befinden. HA wird erreicht, indem sekundäre private IP-Adressen, die an die NICs (Client- und serverseitige NICs) des primären HA-Knotens angehängt sind, nach einem Failover auf den sekundären HA-Knoten

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

migriert werden. Alle mit den sekundären privaten IP-Adressen verbundenen Elastic IP-Adressen werden ebenfalls migriert.

Das NetScaler VPX HA-Paar unterstützt sowohl IPv4- als auch IPv6-Adressen in derselben AWS-Verfügbarkeitszone.

Die folgende Abbildung zeigt ein HA-Failover-Szenario durch Migration sekundärer privater IP-Adressen.

Abbildung 1. Ein NetScaler VPX HA-Paar in AWS unter Verwendung der privaten IP-Migration

Bevor Sie Ihr Dokument beginnen, lesen Sie die folgenden Dokumente:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien
- Bereitstellen einer NetScaler VPX-Instanz in AWS
- Hochverfügbarkeit

## So stellen Sie ein VPX HA-Paar in derselben Zone bereit

Hier ist eine Zusammenfassung der Schritte zur Bereitstellung eines VPX HA-Paares in derselben Zone:

1. Erstellen Sie zwei VPX-Instanzen in AWS, jede mit drei NICs.
2. Weisen Sie dem VIP und SNIP des primären Knotens eine sekundäre private AWS-IP-Adresse zu.
3. Konfigurieren Sie VIP und SNIP auf dem primären Knoten mithilfe sekundärer privater AWS-IP-Adressen.
4. Konfigurieren Sie HA auf beiden Knoten.

### Schritt 1. Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) unter Verwendung desselben VPC, jede mit drei NICs (Ethernet 0, Ethernet 1, Ethernet 2)

Befolgen Sie die Schritte unter Bereitstellen einer NetScaler VPX-Instanz in AWS mithilfe der AWS-Webkonsole.

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

### Schritt 2. Weisen Sie auf dem primären Knoten private IP-Adressen für Ethernet 1 (Client-IP oder VIP) und Ethernet 2 (Back-End-Server-IP oder SNIP) zu

Die AWS-Konsole weist den konfigurierten NICs automatisch primäre private IP-Adressen zu. Weisen Sie VIP und SNIP weitere private IP-Adressen zu, die als sekundäre private IP-Adressen bezeichnet werden.

Um einer Netzwerkschnittstelle eine private IP-Adresse zuzuweisen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Amazon EC2-Konsole unter `<https://console.aws.amazon.com/ec2/>`.
2. Wählen Sie im Navigationsbereich **Netzwerkschnittstellen** und dann die an die Instanz angehängte Netzwerkschnittstelle aus.
3. Wählen Sie **Aktionen > IP-Adressen verwalten**.
4. Wählen Sie je nach Anforderung **IPv4-Adressen** oder **IPv6-Adressen** aus.
5. Für IPv4-Adressen:
    a. Wählen Sie **Neue IP zuweisen**.
    b. Geben Sie eine spezifische IPv4-Adresse ein, die sich innerhalb des Subnetzbereichs für die Instanz befindet, oder lassen Sie das Feld leer, damit Amazon eine IP-Adresse für Sie auswählt.
    c. (Optional) Wählen Sie **Neuzuordnung zulassen**, um die Neuzuordnung der sekundären privaten IP-Adresse zu ermöglichen, falls diese bereits einer anderen Netzwerkschnittstelle zugewiesen ist.
6. Für IPv6-Adressen:
    a. Wählen Sie **Neue IP zuweisen**.
    b. Geben Sie eine spezifische IPv6-Adresse ein, die sich innerhalb des Subnetzbereichs für die Instanz befindet, oder lassen Sie das Feld leer, damit Amazon eine IP-Adresse für Sie auswählt.
    c. (Optional) Wählen Sie **Neuzuordnung zulassen**, um die Neuzuordnung der primären oder sekundären privaten IP-Adresse zu ermöglichen, falls diese bereits einer anderen Netzwerkschnittstelle zugewiesen ist.
7. Wählen Sie **Ja > Aktualisieren**.

Unter der **Instanzbeschreibung** werden die zugewiesenen privaten IP-Adressen angezeigt.

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

**HINWEIS:**

Bei einer IPv4-HA-Paar-Bereitstellung können Sie nur die sekundären IPv4-Adressen auf der Schnittstelle zuweisen und diese als VIP- und SNIP-Adressen verwenden. Bei einer IPv6-HA-Paar-Bereitstellung können Sie jedoch entweder die primären IPv6- oder sekundären IPv6-Adressen auf der Schnittstelle zuweisen und diese als VIP- und SNIP-Adressen verwenden.

### Schritt 3. Konfigurieren Sie VIP und SNIP auf dem primären Knoten unter Verwendung sekundärer privater IP-Adressen

Greifen Sie über SSH auf den primären Knoten zu. Öffnen Sie einen SSH-Client und geben Sie Folgendes ein:

```
ssh -i <location of your private key> nsroot@<public DNS of the instance>
```

Als Nächstes konfigurieren Sie VIP und SNIP.

Für VIP geben Sie Folgendes ein:

```
add ns ip <IPAddress> <netmask> -type <type>
```

Für SNIP geben Sie Folgendes ein:

```
add ns ip <IPAddress> <netmask> -type SNIP
```

Geben Sie `save config` ein, um zu speichern.

Um die konfigurierten IP-Adressen anzuzeigen, geben Sie den folgenden Befehl ein:

```
show ns ip
```

Weitere Informationen finden Sie in den folgenden Themen:

- Konfigurieren und Verwalten von virtuellen IP-Adressen (VIP-Adressen)
- Konfigurieren der NSIP-Adresse

### Schritt 4: HA auf beiden Instanzen konfigurieren

Öffnen Sie auf dem primären Knoten einen Shell-Client und geben Sie den folgenden Befehl ein:

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

```
add ha node <id> <private IP address of the management NIC of the
secondary node>
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein:

```
add ha node <id> <private IP address of the management NIC of the primary
node>
```

Geben Sie `save config` ein, um die Konfiguration zu speichern.

Um die konfigurierten HA-Knoten anzuzeigen, geben Sie `show ha node` ein.

Nach einem Failover werden die sekundären privaten IP-Adressen, die als VIP und SNIP auf dem vorherigen primären Knoten konfiguriert wurden, auf den neuen primären Knoten migriert.

Um ein Failover auf einem Knoten zu erzwingen, geben Sie `force HA` failover ein.

## Migrieren eines älteren HA-Paares zu einem neuen HA-Paar basierend auf der Migration sekundärer privater IP-Adressen

**HINWEIS:**

Die ältere Methode zur Bereitstellung eines VPX HA-Paares, die auf der ENI-Migration basiert, ist veraltet. Daher empfehlen wir Ihnen, die Bereitstellung des HA-Paares basierend auf der Migration sekundärer privater IP-Adressen zu verwenden.

Um eine nahtlose Migration von einem älteren HA-Paar zu einem neuen HA-Paar basierend auf der Migration sekundärer privater IPs zu ermöglichen, stellen Sie Folgendes sicher:

1. Sowohl der primäre als auch der sekundäre Knoten müssen die gleiche Anzahl von Schnittstellen haben, und diese Schnittstellen müssen sich in denselben Subnetzen befinden.
2. Die VIP und SNIP, die in der älteren Methode als primäre private IP-Adresse konfiguriert wurden, müssen in der neuen Methode zu einer sekundären privaten IP-Adresse migriert werden.
3. Die für die neue HA-Bereitstellung erforderlichen IAM-Berechtigungen müssen den primären und sekundären NetScaler®-Instanzen hinzugefügt werden.
4. Starten Sie beide primären und sekundären NetScaler-Instanzen neu.

Weitere Informationen finden Sie unter Hochverfügbarkeit innerhalb derselben Zonen.

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

## Bereitstellen eines Hochverfügbarkeitspaars mithilfe der Citrix CloudFormation-Vorlage

Bevor Sie die CloudFormation-Vorlage starten, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Eine VPC
- Drei Subnetze innerhalb der VPC
- Eine Sicherheitsgruppe mit offenen UDP 3003-, TCP 3009–3010-, HTTP- und SSH-Ports
- Ein Schlüsselpaar
- Ein Internet-Gateway erstellen
- Routing-Tabellen für Client- und Management-Netzwerke bearbeiten, um auf das Internet-Gateway zu verweisen

**HINWEIS:**

Das Citrix CloudFormation-Template erstellt automatisch eine IAM-Rolle. Vorhandene IAM-Rollen werden nicht im Template angezeigt.

**So starten Sie das Citrix CloudFormation-Template**:

1. Melden Sie sich mit Ihren AWS-Anmeldeinformationen bei dem AWS Marketplace an.
2. Geben Sie im Suchfeld **NetScaler VPX** ein, um nach dem NetScaler AMI zu suchen, und klicken Sie auf **Go**.
3. Klicken Sie auf der Suchergebnisseite auf das gewünschte NetScaler VPX-Angebot.
4. Klicken Sie auf die Registerkarte **Pricing**, um zu **Pricing Information** zu gelangen.
5. Wählen Sie die Region und **Fulfillment Option** als **NetScaler VPX – Customer Licensed** aus.
6. Klicken Sie auf **Continue to Subscribe**.
7. Überprüfen Sie die Details auf der Seite **Subscribe** und klicken Sie auf **Continue to Configuration**.
8. Wählen Sie **Delivery Method** als **CloudFormation Template** aus.
9. Wählen Sie das erforderliche CloudFormation-Template aus.
10. Wählen Sie **Software Version** und **Region** aus und klicken Sie auf **Continue to Launch**.

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

11. Wählen Sie unter **Choose Action** die Option **Launch CloudFormation** aus und klicken Sie auf **Launch**. Die Seite **Create stack** wird angezeigt.
12. Klicken Sie auf **Next**.

13. Die Seite **Stack-Details angeben** wird angezeigt. Geben Sie die folgenden Details ein.
    - Geben Sie einen **Stack-Namen** ein. Der Name darf maximal 25 Zeichen lang sein.
    - Unter **Netzwerkkonfiguration** führen Sie Folgendes aus:
        - Wählen Sie **Verwaltungs-Subnetzwerk**, **Client-Subnetzwerk** und **Server-Subnetzwerk** aus. Stellen Sie sicher, dass Sie die richtigen Subnetzwerke auswählen, die Sie innerhalb der VPC erstellt haben, die Sie unter VPC-ID ausgewählt haben.
        - Fügen Sie **Primäre Verwaltungs-IP**, **Sekundäre Verwaltungs-IP**, **Client-IP** und **Server-IP** hinzu. Die IP-Adressen müssen zu denselben Subnetzen der jeweiligen Subnetzwerke gehören. Alternativ können Sie die IP-Adressen automatisch vom Template zuweisen lassen.
        - Wählen Sie **default** für **VPCTenancy** aus.
    - Unter **NetScaler-Konfiguration** führen Sie Folgendes aus:
        - Wählen Sie **m5.xlarge** für den **Instanztyp** aus.
        - Wählen Sie das Schlüsselpaar, das Sie bereits erstellt haben, aus dem Menü für **Schlüsselpaar** aus.
        - Standardmäßig ist die Option **Benutzerdefinierte Metriken in CloudWatch veröffentlichen?** auf **Ja** eingestellt. Wenn Sie diese Option deaktivieren möchten, wählen Sie **Nein**.

          Weitere Informationen zu CloudWatch-Metriken finden Sie unter (#monitor-your-instances-using-amazon-cloudWatch).
    - Unter **Optionale Konfiguration** führen Sie Folgendes aus:
        - Standardmäßig ist die Option **Soll publicIP(EIP) den Verwaltungsschnittstellen zugewiesen werden?** auf **Nein** eingestellt.
        - Standardmäßig ist die Option **Soll publicIP(EIP) der Client-Schnittstelle zugewiesen werden?** auf **Nein** eingestellt.

14. Klicken Sie auf **Weiter**.

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

15. Die Seite **Stack-Optionen konfigurieren** wird angezeigt. Dies ist eine optionale Seite.

16. Klicken Sie auf **Weiter**.
17. Die Seite **Optionen** wird angezeigt. (Dies ist eine optionale Seite.) Klicken Sie auf **Weiter**.
18. Die Seite **Überprüfen** wird angezeigt. Nehmen Sie sich einen Moment Zeit, um die Einstellungen zu überprüfen und gegebenenfalls Änderungen vorzunehmen.
19. Aktivieren Sie das Kontrollkästchen **Ich bestätige, dass AWS CloudFormation IAM-Ressourcen erstellen könnte.**, und klicken Sie dann auf **Stack erstellen**.
20. Der Status **CREATE-IN-PROGRESS** wird angezeigt. Warten Sie, bis der Status **CREATE-COMPLETE** lautet. Wenn sich der Status nicht in **COMPLETE** ändert, überprüfen Sie die Registerkarte **Ereignisse** auf den Grund des Fehlers und erstellen Sie die Instanz mit den richtigen Konfigurationen neu.

21. Nachdem eine IAM-Ressource erstellt wurde, navigieren Sie zu **EC2 Management Console > Instances**. Sie finden zwei VPX-Instanzen, die mit einer IAM-Rolle erstellt wurden. Die primären und sekundären Knoten werden jeweils mit drei privaten IP-Adressen und drei Netzwerkschnittstellen erstellt.
22. Melden Sie sich am primären Knoten mit dem Benutzernamen `nsroot` und der Instanz-ID als Kennwort an. Navigieren Sie in der GUI zu **System > Hochverfügbarkeit > Knoten**. Das NetScaler VPX ist bereits durch die CloudFormation-Vorlage als HA-Paar konfiguriert.
23. Das NetScaler VPX HA-Paar wird angezeigt.

## Überwachen Sie Ihre Instanzen mit Amazon CloudWatch

Sie können den Amazon CloudWatch-Dienst verwenden, um eine Reihe von NetScaler VPX-Metriken wie CPU- und Speicherauslastung sowie Durchsatz zu überwachen. CloudWatch überwacht Ressourcen und Anwendungen, die auf AWS ausgeführt werden, in Echtzeit. Sie können auf das Amazon CloudWatch-Dashboard über die AWS Management Console zugreifen. Weitere Informationen finden Sie unter Amazon CloudWatch.

### Hinweise

- Wenn Sie eine NetScaler VPX-Instanz auf AWS mithilfe der AWS-Webkonsole bereitstellen, ist der CloudWatch-Dienst standardmäßig aktiviert.

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

- Wenn Sie eine NetScaler VPX-Instanz mithilfe der Citrix CloudFormation-Vorlage bereitstellen, ist die Standardoption „Ja“. Wenn Sie den CloudWatch-Dienst deaktivieren möchten, wählen Sie „Nein“.
- Metriken sind verfügbar für CPU (Management- und Paket-CPU-Nutzung), Arbeitsspeicher und Durchsatz (eingehend und ausgehend).

### So zeigen Sie CloudWatch-Metriken an

Um CloudWatch-Metriken für Ihre Instanz anzuzeigen, führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei **AWS Management Console > EC2 > Instances** an.
2. Wählen Sie die Instanz aus.
3. Klicken Sie auf **Monitoring**.
4. Klicken Sie auf **Alle CloudWatch-Metriken anzeigen**.

5. Klicken Sie unter „Alle Metriken“ auf Ihre Instanz-ID.

6. Klicken Sie auf die Metriken, die Sie anzeigen möchten, legen Sie die Dauer fest (nach Minuten, Stunden, Tagen, Wochen, Monaten).
7. Klicken Sie auf **Graphed metrics**, um die Nutzungsstatistiken anzuzeigen. Verwenden Sie die **Graph options**, um Ihr Diagramm anzupassen.

Abbildung. Diagrammierte Metriken für die CPU-Auslastung

## Konfigurieren von SR-IOV in einer Hochverfügbarkeitskonfiguration

Die Unterstützung für SR-IOV-Schnittstellen in einer Hochverfügbarkeitskonfiguration ist ab NetScaler Release 12.0 57.19 verfügbar. Weitere Informationen zur Konfiguration von SR-IOV finden Sie unter Konfigurieren von NetScaler VPX-Instanzen zur Verwendung der SR-IOV-Netzwerkschnittstelle.

### Verwandte Ressourcen

So funktioniert Hochverfügbarkeit in AWS

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

# Hochverfügbarkeit über verschiedene AWS-Verfügbarkeitszonen hinweg

Sie können zwei NetScaler VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen als ein Hochverfügbarkeits-Aktiv-Passiv-Paar im Modus für unabhängige Netzwerkkonfiguration (INC) konfigurieren. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen annehmen kann, übernimmt der sekundäre Knoten.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit. Weitere Informationen zu INC finden Sie unter Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen.

## Hinweise

- Lesen Sie die folgenden Dokumente, bevor Sie Ihre Bereitstellung starten:
  - AWS-Terminologie
  - Voraussetzungen
  - Einschränkungen und Nutzungsrichtlinien
- Das VPX-Hochverfügbarkeitspaar kann entweder in derselben Verfügbarkeitszone in einem anderen Subnetz oder in zwei verschiedenen AWS-Verfügbarkeitszonen liegen.
- Citrix® empfiehlt, dass Sie verschiedene Subnetze für die Verwaltung (NSIP), den Client-Datenverkehr (VIP) und den Backend-Server (SNIP) verwenden.
- Hochverfügbarkeit muss im Modus für unabhängige Netzwerkkonfiguration (INC) eingestellt werden, damit ein Failover funktioniert.
- Die beiden Instanzen müssen Port 3003 für UDP-Verkehr geöffnet haben, da dieser für Heartbeats verwendet wird.
- Die Verwaltungssubnetze beider Knoten müssen Zugang zum Internet oder zum AWS API-Server über internes NAT haben, damit die REST-APIs funktionsfähig sind.
- Die IAM-Rolle muss E2-Berechtigungen für die Migration öffentlicher IPs oder Elastic IPs (EIP) und EC2-Routingtabellenberechtigungen für die Migration privater IPs haben.

Sie können Hochverfügbarkeit über AWS-Verfügbarkeitszonen hinweg auf folgende Weisen bereitstellen:

- Verwenden von elastischen IP-Adressen
- Verwenden von privaten IP-Adressen

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

### Weitere Referenzen

Weitere Informationen zu NetScaler Application Delivery Management (ADM) für AWS finden Sie unter Installieren des NetScaler ADM-Agenten auf AWS.

## Bereitstellen eines VPX-Hochverfügbarkeitspaares mit elastischen IP-Adressen über verschiedene AWS-Zonen hinweg

Sie können zwei NetScaler VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen mithilfe von elastischen IP-Adressen (EIP) im INC-Modus konfigurieren.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit. Weitere Informationen zu INC finden Sie unter Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen.

### So funktioniert HA mit EIP-Adressen über verschiedene AWS-Zonen hinweg

Beim Failover migriert die EIP der VIP der primären Instanz zur sekundären Instanz, die als neue primäre Instanz übernimmt. Im Failover-Prozess führt die AWS-API folgende Schritte aus:

1. Überprüft die virtuellen Server, an die `IPSets` angehängt ist.
2. Findet die IP-Adresse, die eine zugeordnete öffentliche IP hat, aus den beiden IP-Adressen, auf denen der virtuelle Server lauscht. Eine, die direkt an den virtuellen Server angehängt ist, und diejenige, die über den IP-Satz angehängt ist.
3. Ordnet die öffentliche IP (EIP) der privaten IP neu zu, die zur neuen primären VIP gehört.

**HINWEIS:**

Um Ihr Netzwerk vor Angriffen wie Denial-of-Service (DoS) zu schützen, können Sie bei Verwendung einer EIP Sicherheitsgruppen in AWS erstellen, um den IP-Zugriff einzuschränken. Für Hochverfügbarkeit können Sie je nach Ihren Bereitstellungen von EIP zu einer Lösung für die private IP-Verschiebung wechseln.

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

## So stellen Sie ein VPX-Hochverfügbarkeitspaar mit elastischen IP-Adressen über verschiedene AWS-Zonen hinweg bereit

Im Folgenden finden Sie eine Zusammenfassung der Schritte zum Bereitstellen eines VPX-Paares in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen.

1. Erstellen Sie eine Amazon Virtual Private Cloud.
2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Verfügbarkeitszonen oder in derselben Zone, aber in verschiedenen Subnetzen bereit.
3. Hochverfügbarkeit konfigurieren
    a. Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.
    b. Fügen Sie in beiden Instanzen ein IP-Set hinzu.
    c. Binden Sie das IP-Set in beiden Instanzen an die VIP.
    d. Fügen Sie in der primären Instanz einen virtuellen Server hinzu.

Verwenden Sie für die Schritte 1 und 2 die AWS-Konsole. Verwenden Sie für Schritt 3 die NetScaler VPX GUI oder die CLI.

**Schritt 1.** Erstellen Sie eine Amazon Virtual Private Cloud (VPC).

**Schritt 2.** Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Verfügbarkeitszonen oder in derselben Zone, aber in verschiedenen Subnetzen bereit. Weisen Sie der VIP der primären VPX eine EIP zu.

Weitere Informationen zum Erstellen einer VPC und zum Bereitstellen einer VPX-Instanz auf AWS finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS und Szenario: eigenständige Instanz

**Schritt 3.** Konfigurieren Sie Hochverfügbarkeit. Sie können die NetScaler VPX CLI oder die GUI verwenden, um Hochverfügbarkeit einzurichten.

### Hochverfügbarkeit mithilfe der CLI konfigurieren

1. Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.

    **Auf dem primären Knoten:**

    ```
    add ha node 1 <sec_ip> -inc ENABLED
    ```

    **Auf dem sekundären Knoten:**

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

`add ha node 1 <prim_ip> -inc ENABLED`

`<sec_ip>` bezieht sich auf die private IP-Adresse der Management-NIC des sekundären Knotens

`<prim_ip>` bezieht sich auf die private IP-Adresse der Management-NIC des primären Knotens

2. Fügen Sie den IP-Satz in beiden Instanzen hinzu.

   Geben Sie den folgenden Befehl auf beiden Instanzen ein.

   `add ipset <ipsetname>`

3. Binden Sie den IP-Satz an den VIP-Satz auf beiden Instanzen.

   Geben Sie den folgenden Befehl auf beiden Instanzen ein:

   `add ns ip <secondary vip> <subnet> -type VIP`

   `bind ipset <ipsetname> <secondary VIP>`

   **HINWEIS:**

   Sie können den IP-Satz an die primäre VIP oder an die sekundäre VIP binden. Wenn Sie den IP-Satz jedoch an die primäre VIP binden, verwenden Sie die sekundäre VIP, um sie dem virtuellen Server hinzuzufügen, und umgekehrt.

4. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

   Geben Sie den folgenden Befehl ein:

   `add <server_type> vserver <vserver_name> <protocol> <primary_vip> <port> -ipset \<ipset_name>`

### Hochverfügbarkeit über die GUI konfigurieren

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.
2. Melden Sie sich am primären Knoten mit dem Benutzernamen `nsroot` und der Instanz-ID als Kennwort an.
3. Gehen Sie in der GUI zu **Configuration** (Konfiguration) > **System** (System) > **High Availability** (Hochverfügbarkeit). Klicken Sie auf **Add** (Hinzufügen).

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

4. Geben Sie im Feld **Remote Node IP address** (IP-Adresse des Remote-Knotens) die private IP-Adresse der Management-NIC des sekundären Knotens ein.
5. Wählen Sie den Modus **Turn on NIC (Independent Network Configuration)** (NIC (unabhängige Netzwerkkonfiguration) einschalten) auf dem Selbstknoten aus.
6. Fügen Sie unter **Remote System Login Credential** (Anmeldeinformationen für Remote-System) den Benutzernamen und das Kennwort für den sekundären Knoten hinzu und klicken Sie auf **Create** (Erstellen).
7. Wiederholen Sie die Schritte im sekundären Knoten.
8. Fügen Sie einen IP-Satz hinzu und binden Sie den IP-Satz an den VIP-Satz auf beiden Instanzen.
9. Navigieren Sie in der GUI zu **System** > **Network** (Netzwerk) > **IPs** > **Add** (Hinzufügen).
10. Fügen Sie die erforderlichen Werte für IP-Adresse, Netzmaske, IP-Typ (virtuelle IP) hinzu und klicken Sie auf **Create** (Erstellen).
11. Navigieren Sie zu **System** > **Network** (Netzwerk) > **IP Sets** (IP-Sätze) > **Add** (Hinzufügen). Fügen Sie einen IP-Satznamen hinzu und klicken Sie auf **Insert** (Einfügen).
12. Wählen Sie auf der Seite IPV4s die virtuelle IP aus und klicken Sie auf **Insert** (Einfügen). Klicken Sie auf **Create** (Erstellen), um den IP-Satz zu erstellen.
13. Fügen Sie einen virtuellen Server in der primären Instanz hinzu.

    Gehen Sie in der GUI zu **Configuration** (Konfiguration) > **Traffic Management** (Datenverkehrsverwaltung) > **Virtual Servers** (Virtuelle Server) > **Add** (Hinzufügen).

## Szenario

In diesem Szenario wird eine einzelne VPC erstellt. In dieser VPC werden zwei VPX-Instanzen in zwei Verfügbarkeitszonen erstellt. Jede Instanz verfügt über drei Subnetze – eines für die Verwaltung, eines für den Client und eines für den Back-End-Server. Eine EIP wird an die VIP des primären Knotens angehängt.

Diagramm: Dieses Diagramm veranschaulicht die NetScaler VPX Hochverfügbarkeits-Einrichtung im INC-Modus auf AWS.

Verwenden Sie für dieses Szenario die CLI, um Hochverfügbarkeit zu konfigurieren.

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

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

Geben Sie die folgenden Befehle auf dem primären und dem sekundären Knoten ein.

**Auf primär:**

```
add ha node 1 192.168.6.82 -inc enabled
```

Hier bezieht sich 192.168.6.82 auf die private IP-Adresse der Management-NIC des sekundären Knotens.

**Auf sekundär:**

```
add ha node 1 192.168.1.108 -inc enabled
```

Hier bezieht sich 192.168.1.108 auf die private IP-Adresse der Management-NIC des primären Knotens.

2. Fügen Sie einen IP-Satz hinzu und binden Sie den IP-Satz an die VIP auf beiden Instanzen.

   **Auf primär**:

   ```
   add ipset ipset123
   ```

   ```
   add ns ip 192.168.7.68 255.255.255.0 -type VIP
   ```

   ```
   bindipset ipset123 192.168.7.68
   ```

   **Auf dem sekundären Gerät**:

   ```
   add ipset ipset123
   ```

   ```
   add ns ip 192.168.7.68 255.255.255.0 -type VIP
   ```

   ```
   bind ipset ipset123 192.168.7.68
   ```

3. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

   Der folgende Befehl:

   ```
   add lbvserver vserver1 http 192.168.2.129 80 -ipset ipset123
   ```

4. Speichern Sie die Konfiguration.

   ☐

5. Nach einem erzwungenen Failover wird das sekundäre Gerät zum neuen primären Gerät.

   ☐

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

# Bereitstellen eines VPX-Hochverfügbarkeitspaares mit privaten IP-Adressen über verschiedene AWS-Zonen hinweg

Sie können zwei NetScaler VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen unter Verwendung privater IP-Adressen im INC-Modus konfigurieren. Diese Lösung lässt sich leicht in das bestehende Multizonen-(/de-de/vpx/current-release/deploy-aws/vpx-ha-eip-different-aws-zones.html) integrieren. Daher können Sie beide Lösungen zusammen verwenden.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter (/de-de/citrix-adc/current-release/system/high-availability-introduction.html). Weitere Informationen zu INC finden Sie unter (/de-de/citrix-adc/current-release/system/high-availability-introduction/configuring-high-availability-nodes-different-subnets.html).

**HINWEIS:**

Diese Bereitstellung wird ab NetScaler Release 13.0 Build 67.39 unterstützt. Diese Bereitstellung ist mit AWS Transit Gateway kompatibel.

## Hochverfügbarkeitspaar mit privaten IP-Adressen unter Verwendung einer nicht freigegebenen AWS VPC

### Voraussetzungen

Stellen Sie sicher, dass die IAM-Rolle, die Ihrem AWS-Konto zugeordnet ist, die folgenden IAM-Berechtigungen besitzt:

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Action": [

                "ec2:DescribeInstances",
```

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

```
                "ec2:DescribeAddresses",

                "ec2:AssociateAddress",

                "ec2:DisassociateAddress",

                "ec2:DescribeRouteTables",

                "ec2:DeleteRoute",

                "ec2:CreateRoute",

                "ec2:ModifyNetworkInterfaceAttribute",

                "iam:SimulatePrincipalPolicy",

                "iam:GetRole"

            ],

            "Resource": "*",

            "Effect": "Allow"

        }

    ]

}
```

### Bereitstellen eines VPX HA-Paares mit privaten IP-Adressen unter Verwendung einer nicht freigegebenen AWS VPC

Im Folgenden finden Sie eine Zusammenfassung der Schritte zur Bereitstellung eines VPX-Paares in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen unter Verwendung privater IP-Adressen.

1. Erstellen Sie eine Amazon Virtual Private Cloud.
2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Verfügbarkeitszonen bereit.
3. Hochverfügbarkeit konfigurieren

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

a. Richten Sie in beiden Instanzen Hochverfügbarkeit im INC-Modus ein.

b. Fügen Sie die entsprechenden Routing-Tabellen in der VPC hinzu, die auf die Client-Schnittstelle verweisen.

c. Fügen Sie einen virtuellen Server in der primären Instanz hinzu.

Verwenden Sie für die Schritte 1, 2 und 3b die AWS-Konsole. Verwenden Sie für die Schritte 3a und 3c die NetScaler VPX GUI oder die CLI.

**Schritt 1.** Erstellen Sie eine Amazon Virtual Private Cloud (VPC).

**Schritt 2.** Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Availability Zones mit der gleichen Anzahl von ENI (Network Interface) bereit.

Weitere Informationen zum Erstellen einer VPC und zum Bereitstellen einer VPX-Instanz in AWS finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz in AWS und Szenario: eigenständige Instanz

**Schritt 3.** Konfigurieren Sie die ADC-VIP-Adressen, indem Sie ein Subnetz wählen, das sich nicht mit den Amazon VPC-Subnetzen überschneidet. Wenn Ihre VPC 192.168.0.0/16 ist, können Sie zur Konfiguration der ADC-VIP-Adressen ein beliebiges Subnetz aus diesen IP-Adressbereichen wählen:

- 0.0.0.0 - 192.167.0.0
- 192.169.0.0 - 254.255.255.0

In diesem Beispiel wurde das Subnetz 10.10.10.0/24 gewählt und VIPs in diesem Subnetz erstellt. Sie können jedes Subnetz außer dem VPC-Subnetz (192.168.0.0/16) wählen.

**Schritt 4.** Fügen Sie eine Route hinzu, die vom VPC-Routentabelle auf die Client-Schnittstelle (VIP) des primären Knotens zeigt.

Geben Sie in der AWS CLI den folgenden Befehl ein:

```
aws ec2 create-route --route-table-id rtb-2272532 --destination-cidr-block
10.10.10.0/24 --gateway-id <eni-client-primary>
```

Führen Sie in der AWS GUI die folgenden Schritte aus, um eine Route hinzuzufügen:

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich **Route Tables** und dann die Routing-Tabelle aus.

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

3. Wählen Sie **Actions** und klicken Sie auf **Edit routes**.
4. Um eine Route hinzuzufügen, wählen Sie **Route hinzufügen**. Geben Sie für **Ziel** den Ziel-CIDR-Block, eine einzelne IP-Adresse oder die ID einer Präfixliste ein. Wählen Sie für die Gateway-ID die ENI einer Client-Schnittstelle des primären Knotens aus.

**HINWEIS:**

Sie müssen die **Quell-/Zielprüfung** auf der Client-ENI der primären Instanz deaktivieren.

Um die Quell-/Zielprüfung für eine Netzwerkschnittstelle über die Konsole zu deaktivieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich **Netzwerkschnittstellen** aus.
3. Wählen Sie die Netzwerkschnittstelle einer primären Client-Schnittstelle aus, wählen Sie **Aktionen** aus und klicken Sie auf **Quell-/Zielprüfung ändern**.
4. Wählen Sie im Dialogfeld **Deaktiviert** aus, klicken Sie auf **Speichern**.

**Schritt 5.** Konfigurieren Sie Hochverfügbarkeit. Sie können die NetScaler VPX CLI oder die GUI verwenden, um Hochverfügbarkeit einzurichten.

### Hochverfügbarkeit mithilfe der CLI konfigurieren

1. Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.

   Auf dem primären Knoten:

   ```
   add ha node 1 \<sec\_ip\> -inc ENABLED
   ```

   Auf dem sekundären Knoten:

   ```
   add ha node 1 \<prim\_ip\> -inc ENABLED
   ```

   \<sec_ip\> bezieht sich auf die private IP-Adresse der Management-NIC des sekundären Knotens.

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

\<prim_ip\> bezieht sich auf die private IP-Adresse der Management-NIC des primären Knotens.

2. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu. Sie müssen ihn aus dem gewählten Subnetz hinzufügen, zum Beispiel 10.10.10.0/24.

   Geben Sie den folgenden Befehl ein:

   ```
   add \<server\_type\> vserver \<vserver\_name\> \<protocol\>
   \<primary\_vip\> \<port\>
   ```

### Hochverfügbarkeit über die GUI konfigurieren

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.
2. Melden Sie sich am primären Knoten mit dem Benutzernamen `nsroot` und der Instanz-ID als Kennwort an.
3. Navigieren Sie zu **Configuration** > **System** > **High Availability** und klicken Sie auf **Add**.
4. Geben Sie im Feld **Remote Node IP address** die private IP-Adresse der Management-NIC des sekundären Knotens ein.
5. Wählen Sie den Modus **Turn on NIC (Independent Network Configuration)** auf dem eigenen Knoten aus.
6. Fügen Sie unter **Remote System Login Credential** den Benutzernamen und das Kennwort für den sekundären Knoten hinzu und klicken Sie auf **Create**.
7. Wiederholen Sie die Schritte im sekundären Knoten.
8. Fügen Sie einen virtuellen Server in der primären Instanz hinzu.

   Navigieren Sie zu **Configuration** > **Traffic Management** > **Virtual Servers** > **Add**.

## Bereitstellen eines VPX HA-Paares mit privaten IP-Adressen unter Verwendung von AWS Shared VPC

In einem AWS Shared VPC-Modell teilt das Konto, dem die VPC gehört (Eigentümer), ein oder mehrere Subnetze mit anderen Konten (Teilnehmern). Daher gibt es ein VPC-Eigentümerkonto und ein Teilnehmerkonto. Nachdem ein Subnetz freigegeben wurde, können die Teilnehmer ihre Anwendungsressourcen in den mit ihnen geteilten Subnetzen anzeigen, erstellen, ändern und

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

löschen. Teilnehmer können keine Ressourcen anzeigen, ändern oder löschen, die anderen Teilnehmern oder dem VPC-Eigentümer gehören.

Informationen zu AWS Shared VPC finden Sie in der AWS-Dokumentation.

**HINWEIS:**

Die Konfigurationsschritte für die Bereitstellung eines VPX HA-Paares mit privaten IP-Adressen unter Verwendung von AWS Shared VPC sind die gleichen wie bei der Bereitstellung eines VPX HA-Paares mit privaten IP-Adressen unter Verwendung von AWS Non-Shared VPC mit folgender Ausnahme:

- Die Routing-Tabellen in der VPC, die auf die Client-Schnittstelle zeigen, müssen vom *VPC-Eigentümerkonto* hinzugefügt werden.

### Voraussetzungen

- Stellen Sie sicher, dass die IAM-Rolle, die der NetScaler VPX-Instanz im AWS-Teilnehmerkonto zugeordnet ist, die folgenden IAM-Berechtigungen besitzt:

```
"Version": "2012-10-17",

    "Statement": [

        {

            "Sid": "VisualEditor0",

            "Effect": "Allow",

            "Action": [

                "ec2:DisassociateAddress",

                "iam:GetRole",

                "iam:SimulatePrincipalPolicy",

                "ec2:DescribeInstances",

                "ec2:DescribeAddresses",
```

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

```
                "ec2:ModifyNetworkInterfaceAttribute",

                “ec2:AssociateAddress”,

                "sts:AssumeRole"

        ],

            "Resource": "*"

        }

    ]

}
```

**HINWEIS:**

Die **AssumeRole** ermöglicht es der NetScaler VPX-Instanz, die kontoübergreifende IAM-Rolle zu übernehmen, die vom VPC-Eigentümerkonto erstellt wird.

- Stellen Sie sicher, dass das VPC-Eigentümerkonto dem Teilnehmerkonto die folgenden IAM-Berechtigungen über eine kontoübergreifende IAM-Rolle bereitstellt:

```
{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Sid": "VisualEditor0",

            "Effect": "Allow",

            "Action": [

                "ec2:CreateRoute",
```

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

```
                "ec2:DeleteRoute",

                "ec2:DescribeRouteTables"

            ],

            "Resource": "*"

        }

    ]

}
```

### Kontoübergreifende IAM-Rolle erstellen

1. Melden Sie sich bei der AWS-Webkonsole an.
2. Navigieren Sie auf der Registerkarte **IAM** zu **Rollen** und wählen Sie dann **Rolle erstellen**.
3. Wählen Sie **Anderes AWS-Konto**.

4. Geben Sie die 12-stellige Konto-ID-Nummer des Teilnehmerkontos ein, dem Sie Administratorzugriff gewähren möchten.

### Cross-Account-IAM-Rolle mithilfe der NetScaler CLI festlegen

Der folgende Befehl ermöglicht es der NetScaler VPX-Instanz, die Cross-Account-IAM-Rolle zu übernehmen, die im VPC-Besitzerkonto existiert.

```
set cloud awsParam -roleARN <string>
```

### Cross-Account-IAM-Rolle mithilfe der NetScaler GUI festlegen

1. Melden Sie sich bei der NetScaler Appliance an und navigieren Sie zu **Configuration > AWS > Change cloud parameters**.

2. Auf der Seite **Configure AWS Cloud Parameters** geben Sie den Wert für das Feld **RoleARN** ein.

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

## Szenario

In diesem Szenario wird eine einzelne VPC erstellt. In dieser VPC werden zwei VPX-Instanzen in zwei Verfügbarkeitszonen erstellt. Jede Instanz verfügt über drei Subnetze – eines für die Verwaltung, eines für den Client und eines für den Back-End-Server.

Die folgenden Diagramme veranschaulichen die NetScaler VPX-Hochverfügbarkeitskonfiguration im INC-Modus auf AWS. Das benutzerdefinierte Subnetz 10.10.10.10, das nicht Teil der VPC ist, wird als VIP verwendet. Daher kann das Subnetz 10.10.10.10 über Verfügbarkeitszonen hinweg verwendet werden.

Für dieses Szenario verwenden Sie die CLI, um Hochverfügbarkeit zu konfigurieren.

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

   Geben Sie die folgenden Befehle auf dem primären und dem sekundären Knoten ein.

   Auf dem primären Knoten:

   ```
   add ha node 1 192.168.4.10 -inc enabled
   ```

   Hier bezieht sich 192.168.4.10 auf die private IP-Adresse der Management-NIC des sekundären Knotens.

   Auf dem sekundären Knoten:

   ```
   add ha node 1 192.168.1.10 -inc enabled
   ```

   Hier bezieht sich 192.168.1.10 auf die private IP-Adresse der Management-NIC des primären Knotens.
2. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

   Geben Sie den folgenden Befehl ein:

   ```
   add lbvserver vserver1 http 10.10.10.10 80
   ```
3. Speichern Sie die Konfiguration.
4. Nach einem erzwungenen Failover:

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

- Die sekundäre Instanz wird zur neuen primären Instanz.
- Die VPC-Route, die auf die primäre ENI zeigt, migriert zur sekundären Client-ENI.
- Der Client-Datenverkehr wird auf der neuen primären Instanz fortgesetzt.

## AWS Transit Gateway-Konfiguration für HA-Lösung mit privater IP

Sie benötigen AWS Transit Gateway, um das private VIP-Subnetz innerhalb des internen Netzwerks, über AWS-VPCs, Regionen und lokale Netzwerke hinweg routingfähig zu machen. Die VPC muss mit AWS Transit Gateway verbunden sein. Eine statische Route für das VIP-Subnetz oder den IP-Pool innerhalb der AWS Transit Gateway-Routingtabelle wird erstellt und auf die VPC gerichtet.

Um AWS Transit Gateway zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Amazon VPC-Konsole.
2. Wählen Sie im Navigationsbereich **Transit Gateway-Routingtabellen**.
3. Wählen Sie die Registerkarte **Routen** und klicken Sie auf **Statische Route erstellen**.

4. Erstellen Sie eine statische Route, bei der CIDR auf Ihr privates VIPS-Subnetz verweist und die Anbindung auf die VPC mit NetScaler VPX.

5. Klicken Sie auf **Statische Route erstellen** und wählen Sie dann **Schließen**.

## Fehlerbehebung

Wenn bei der Konfiguration der HA-Lösung für private IPs über Multizonen-HA hinweg Probleme auftreten, überprüfen Sie die folgenden wichtigen Punkte zur Fehlerbehebung:

- Sowohl der primäre als auch der sekundäre Knoten verfügen über denselben Satz von IAM-Berechtigungen.
- Der INC-Modus ist auf sowohl dem primären als auch dem sekundären Knoten aktiviert.
- Sowohl der primäre als auch der sekundäre Knoten verfügen über die gleiche Anzahl von Schnittstellen.
- Beim Erstellen einer Instanz befolgen Sie die gleiche Reihenfolge beim Anfügen von Schnittstellen an sowohl primären als auch sekundären Knoten, basierend auf der Geräteindexnummer. Angenommen, an einem primären Knoten wird zuerst die Client-

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

Schnittstelle und dann die Server-Schnittstelle angefügt. Befolgen Sie dieselbe Reihenfolge auch am sekundären Knoten. Falls es eine Diskrepanz gibt, trennen Sie die Schnittstellen und fügen Sie sie in der richtigen Reihenfolge erneut an.

- Sie können die Reihenfolge der Schnittstellen überprüfen, indem Sie diesem Navigationspfad folgen: **AWS-Konsole > Netzwerk & Sicherheit > ENI > Gerätexindexnummer**. Standardmäßig werden den folgenden Schnittstellen die folgenden Gerätexindexnummern zugewiesen:
  - Managementschnittstelle – 0
  - Clientschnittstelle – 1
  - Serverschnittstelle – 2
- Wenn die Reihenfolge der Gerätexindexnummern auf der primären ENI 0, 1, 2 ist, muss die sekundäre ENI ebenfalls dieselbe Reihenfolge der Gerätexindexnummern einhalten: 0, 1, 2.

  Wenn es eine Diskrepanz in der Reihenfolge der Gerätexindexnummern gibt, werden alle nicht übereinstimmenden Routen an Index 0, die Managementschnittstelle, übertragen, um Routenverluste zu vermeiden. Sie müssen die Schnittstellen jedoch trotzdem trennen und in der richtigen Reihenfolge wieder anschließen, um die Verschiebung von Routen zur Managementschnittstelle zu vermeiden, da dies zu Verkehrsüberlastungen führen kann.
- Wenn der Datenverkehr nicht fließt, stellen Sie sicher, dass die Option „Source/dest. Check“ auf der Clientschnittstelle des primären Knotens zum ersten Mal deaktiviert ist.
- Stellen Sie sicher, dass der Befehl `cloudhadaemon` (`ps -aux | grep cloudha`) in der Shell ausgeführt wird.
- Stellen Sie sicher, dass die NetScaler-Firmware-Version 13.0 Build 70.x oder höher ist.
- Bei Problemen mit dem Failover-Prozess überprüfen Sie die Protokolldatei unter: `/var/log/cloud-ha-daemon.log`

# Bereitstellen einer NetScaler VPX-Instanz auf AWS Outposts

AWS Outposts ist ein Pool von AWS-Rechen- und Speicherkapazitäten, die an Ihrem Standort bereitgestellt werden. Outposts bietet AWS-Infrastruktur und -Dienste an Ihrem lokalen Standort. AWS betreibt, überwacht und verwaltet diese Kapazität als Teil einer AWS-Region. Sie können dieselben NetScaler VPX-Instanzen, AWS-APIs, Tools und Infrastruktur sowohl lokal als auch in der AWS Cloud für eine konsistente hybride Erfahrung verwenden.

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

Sie können Subnetze auf Ihren Outposts erstellen und diese angeben, wenn Sie AWS-Ressourcen wie EC2-Instanzen, EBS-Volumes, ECS-Cluster und RDS-Instanzen erstellen. Instanzen in den Outposts-Subnetzen kommunizieren mit anderen Instanzen in der AWS-Region über private IP-Adressen, alle innerhalb derselben Amazon Virtual Private Cloud (VPC).

Weitere Informationen finden Sie im AWS Outposts-Benutzerhandbuch.

## So funktioniert AWS Outposts

AWS Outposts ist darauf ausgelegt, mit einer konstanten und konsistenten Verbindung zwischen Ihren Outposts und einer AWS-Region zu arbeiten. Um diese Verbindung zur Region und zu den lokalen Workloads in Ihrer lokalen Umgebung herzustellen, müssen Sie Ihr Outpost mit Ihrem lokalen Netzwerk verbinden. Ihr lokales Netzwerk muss WAN-Zugriff zurück zur Region und zum Internet bereitstellen. Das Internet muss auch LAN- oder WAN-Zugriff auf das lokale Netzwerk bereitstellen, in dem sich Ihre lokalen Workloads oder Anwendungen befinden.

## Voraussetzung

- Sie müssen ein AWS Outposts an Ihrem Standort installieren.
- Die Rechen- und Speicherkapazität der AWS Outposts muss zur Verfügung stehen.

Weitere Informationen zur Bestellung von AWS Outposts finden Sie in der folgenden AWS-Dokumentation: `<https://aws.amazon.com/blogs/aws/aws-outposts-now-available-order-your-racks-today/>`

## Bereitstellen einer NetScaler VPX-Instanz auf AWS Outposts mithilfe der AWS-Webkonsole

Die folgende Abbildung zeigt eine einfache Bereitstellung von NetScaler VPX-Instanzen auf den Outposts. Das im AWS Marketplace vorhandene NetScaler AMI wird ebenfalls in den Outposts bereitgestellt.

Melden Sie sich bei der AWS-Webkonsole an und führen Sie die folgenden Schritte aus, um NetScaler VPX EC2-Instanzen auf Ihren AWS Outposts bereitzustellen.

1. Erstellen Sie ein Schlüsselpaar.
2. Erstellen Sie eine Virtual Private Cloud (VPC).
3. Fügen Sie weitere Subnetze hinzu.
4. Erstellen Sie Sicherheitsgruppen und Sicherheitsregeln.

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

5. Fügen Sie Routing-Tabellen hinzu.
6. Erstellen Sie ein Internet-Gateway.
7. Erstellen Sie eine NetScaler VPX-Instanz mithilfe des AWS EC2-Dienstes. Navigieren Sie im AWS-Dashboard zu **Compute > EC2 > Launch Instance > AWS Marketplace**.
8. Erstellen und verbinden Sie weitere Netzwerkschnittstellen.
9. Weisen Sie der Management-NIC elastische IPs zu.
10. Verbinden Sie sich mit der VPX-Instanz.

Detaillierte Anweisungen zu den einzelnen Schritten finden Sie unter Bereitstellen einer NetScaler VPX-Instanz auf AWS mithilfe der AWS-Webkonsole.

Informationen zur Hochverfügbarkeit innerhalb derselben Verfügbarkeitszone finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.

## Bereitstellen einer NetScaler VPX-Instanz in einer Hybrid Cloud mit AWS Outposts

Sie können eine NetScaler VPX-Instanz in einer Hybrid Cloud in einer AWS-Umgebung bereitstellen, die AWS Outposts enthält. Sie können den Mechanismus zur Anwendungsbereitstellung mithilfe der NetScaler Global Server Load Balancing (GSLB)-Lösung vereinfachen. Die GSLB-Lösung verteilt den Anwendungsverkehr über mehrere Rechenzentren in Hybrid Clouds, die mithilfe von AWS-Regionen und der AWS Outposts-Infrastruktur aufgebaut sind.

NetScaler GSLB unterstützt sowohl die Bereitstellungstypen Active-Active als auch Active-Passive, um verschiedene Anwendungsfälle abzudecken. Neben diesen flexiblen Bereitstellungsoptionen und Anwendungsbereitstellungsmechanismen sichert NetScaler das gesamte Netzwerk- und Anwendungsportfolio, unabhängig davon, ob Anwendungen nativ in der AWS Cloud oder auf AWS Outposts bereitgestellt werden.

Das folgende Diagramm veranschaulicht eine Anwendungsbereitstellung mit einer NetScaler Appliance in einer Hybrid Cloud mit AWS.

Bei einer Aktiv-Aktiv-Bereitstellung steuert der NetScaler den Datenverkehr global über eine verteilte Umgebung. Alle Standorte in der Umgebung tauschen Metriken über ihre Verfügbarkeit und den Zustand der Ressourcen über das Metrics Exchange Protocol (MEP) aus. Die NetScaler Appliance verwendet diese Informationen, um den Datenverkehr über Standorte hinweg auszugleichen und Client-Anfragen an den am besten geeigneten GSLB-Standort zu senden, der

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

durch die definierte Methode (Round Robin, Least Connection und statische Nähe) in der GSLB-Konfiguration bestimmt wird.

Sie können die Aktiv-Aktiv-GSLB-Bereitstellung verwenden, um:

- Die Ressourcennutzung zu optimieren, wobei alle Knoten aktiv sind.
- Die Benutzererfahrung zu verbessern, indem Anfragen an den Standort geleitet werden, der jedem einzelnen Benutzer am nächsten ist.
- Anwendungen in einem benutzerdefinierten Tempo in die Cloud zu migrieren.

Sie können die Aktiv-Passiv-GSLB-Bereitstellung verwenden für:

- Notfallwiederherstellung
- Cloud Burst

### Referenzen

- Bereitstellen einer NetScaler VPX-Instanz auf AWS
- Bereitstellen einer NetScaler VPX-Instanz auf AWS Outposts mithilfe der AWS-Webkonsole
- Konfigurieren von GSLB auf NetScaler VPX-Instanzen

## AWS API Gateway mithilfe der NetScaler Web App Firewall schützen

Sie können eine NetScaler Appliance vor Ihrem AWS API Gateway bereitstellen und das API Gateway vor externen Bedrohungen schützen. Die NetScaler Web App Firewall (WAF) kann Ihre API gegen OWASP Top 10 Bedrohungen und Zero-Day-Angriffe verteidigen. Die NetScaler Web App Firewall verwendet eine einzige Codebasis über alle ADC-Formfaktoren hinweg. Daher können Sie Sicherheitsrichtlinien in jeder Umgebung konsistent anwenden und durchsetzen. Die NetScaler Web App Firewall ist einfach bereitzustellen und als Einzellizenz verfügbar. Die NetScaler Web App Firewall bietet Ihnen die folgenden Funktionen:

- Vereinfachte Konfiguration
- Bot-Verwaltung
- Ganzheitliche Transparenz
- Daten aus mehreren Quellen zusammenführen und auf einem einheitlichen Bildschirm anzeigen

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

Zusätzlich zum API-Gateway-Schutz können Sie auch die anderen NetScaler-Funktionen nutzen. Weitere Informationen finden Sie unter NetScaler-Dokumentation. Um Rechenzentrumsausfälle zu vermeiden und Ausfallzeiten zu minimieren, können Sie ADC in Hochverfügbarkeit innerhalb oder über Verfügbarkeitszonen hinweg platzieren. Sie können auch Clustering mit der Autoscale-Funktion verwenden oder konfigurieren.

Früher unterstützte AWS API Gateway nicht die erforderlichen Schutzmaßnahmen, um die dahinter liegenden Anwendungen zu sichern. Ohne die Schutzmaßnahmen der Web Application Firewall (WAF) waren APIs anfällig für Sicherheitsbedrohungen.

## NetScaler Appliance vor dem AWS API Gateway bereitstellen

Im folgenden Beispiel wird eine NetScaler Appliance vor dem AWS API Gateway bereitgestellt.

ADC vor dem AWS API Gateway bereitstellen(/en-us/vpx/media/vpx-aws-api-gateway.png)

Nehmen wir an, es gibt eine echte API-Anfrage für den AWS Lambda-Dienst. Diese Anfrage kann für jeden der API-Dienste sein, wie in der Amazon API Gateway-Dokumentation erwähnt. Wie im vorhergehenden Diagramm gezeigt, ist der Datenverkehrsfluss wie folgt:

1. Der Client sendet eine Anfrage an die AWS Lambda-Funktion (XYZ). Diese Client-Anfrage wird an den virtuellen NetScaler-Server (192.168.1.1) gesendet.
2. Der virtuelle Server inspiziert das Paket und prüft auf bösartigen Inhalt.
3. Die NetScaler Appliance löst eine Rewrite-Richtlinie aus, um den Hostnamen und die URL in einer Client-Anfrage zu ändern. Zum Beispiel möchten Sie `https://restapi.citrix.com/default/LamdaFunctionXYZ` in `https://citrix.execute-api.<region>.amazonaws.com/default/LambdaFunctionXYZ` ändern.
4. Die NetScaler Appliance leitet diese Anfrage an das AWS API Gateway weiter.
5. Das AWS API Gateway sendet die Anfrage weiter an den Lambda-Dienst und ruft die Lambda-Funktion „XYZ“ auf.
6. Gleichzeitig, wenn ein Angreifer eine API-Anfrage mit bösartigem Inhalt sendet, landet die bösartige Anfrage auf der NetScaler Appliance.
7. Die NetScaler Appliance inspiziert die Pakete und verwirft sie basierend auf der konfigurierten Aktion.

## NetScaler Appliance mit aktiviertem WAF konfigurieren

Um WAF auf einer NetScaler Appliance zu aktivieren, führen Sie die folgenden Schritte aus:

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

1. Fügen Sie einen Content Switching oder einen Lastausgleichs-Virtual Server hinzu. Nehmen wir an, die IP-Adresse des virtuellen Servers ist 192.168.1.1, die zu einem Domänennamen (restapi.citrix.com) aufgelöst wird.
2. Aktivieren Sie die WAF-Richtlinie auf dem NetScaler Virtual Server. Weitere Informationen finden Sie unter Konfigurieren der Web App Firewall.
3. Aktivieren Sie die Rewrite-Richtlinie, um den Domänennamen zu ändern. Nehmen wir an, Sie möchten, dass die eingehende Anfrage an den Load Balancer unter dem Domänennamen „restapi.citrix.com“ auf das Backend AWS API Gateway unter dem Domänennamen „citrix.execute-api.`<region>`.amazonaws“ umgeschrieben wird.
4. Aktivieren Sie den L3-Modus auf der NetScaler Appliance, damit sie als Proxy fungiert. Verwenden Sie den folgenden Befehl:

```
enable ns mode L3
```

In Schritt 3 des vorhergehenden Beispiels möchte der Website-Administrator, dass die NetScaler Appliance den Domänennamen „restapi.citrix.com“ durch „citrix.execute-api.`<region>`.amazonaws.com“ und die URL durch „default/lambda/XYZ“ ersetzt.

Die folgende Prozedur beschreibt, wie der Hostname und die URL in einer Client-Anfrage mithilfe der Rewrite-Funktion geändert werden:

1. Melden Sie sich über SSH bei der NetScaler Appliance an.
2. Rewrite-Aktionen hinzufügen.

```
add rewrite action rewrite_host_hdr_act replace
"HTTP.REQ.HEADER(\"Host\")" "\"citrix.execute-
api.<region>.amazonaws.com\""



add rewrite action rewrite_url_act replace HTTP.REQ.URL.PATH_AND_QUERY
"\"/default/lambda/XYZ\""
```

3. Rewrite-Richtlinien für die Rewrite-Aktionen hinzufügen.

```
add rewrite policy rewrite_host_hdr_pol
"HTTP.REQ.HEADER(\"Host\").CONTAINS(\"restapi.citrix.com\")
"rewrite_host_hdr_act
```

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

```
add rewrite policy rewrite_url_pol
"HTTP.REQ.HEADER(\"Host\").CONTAINS(\"restapi.citrix.com\")
"rewrite_url_act
```

4. Binden Sie die Rewrite-Richtlinien an einen virtuellen Server.

```
bind lb vserver LB_API_Gateway -policyName rewrite_host_hdr_pol
-priority 10 -gotoPriorityExpression 20 -type REQUEST



bind lb vserver LB_API_Gateway -policyName rewrite_url_pol -priority 20
-gotoPriorityExpression END -type REQUEST
```

Weitere Informationen finden Sie unter Rewrite konfigurieren, um den Hostnamen und die URL in Clientanforderungen auf der NetScaler Appliance zu ändern.

## NetScaler-Funktionen und -Möglichkeiten

Die NetScaler Appliance sichert nicht nur die Bereitstellung, sondern kann die Anforderung auch basierend auf den Benutzeranforderungen verbessern. Die NetScaler Appliance bietet die folgenden Hauptfunktionen.

- **Lastverteilung des API-Gateways:** Wenn Sie mehr als ein API-Gateway haben, können Sie mehrere API-Gateways mit der NetScaler Appliance lastverteilen und das Verhalten der API-Anforderung definieren.
  - Es stehen verschiedene Lastverteilungsmethoden zur Verfügung. Zum Beispiel vermeidet die Methode der geringsten Verbindungen eine Überlastung des API-Gateway-Limits, die benutzerdefinierte Lastmethode hält eine bestimmte Last auf einem bestimmten API-Gateway aufrecht und so weiter. Weitere Informationen finden Sie unter Lastverteilungsalgorithmen.
  - SSL-Offloading wird ohne Unterbrechung des Datenverkehrs konfiguriert.
  - Der USIP-Modus (Use Source IP) ist aktiviert, um die Client-IP-Adresse beizubehalten.
  - Benutzerdefinierte SSL-Einstellungen: Sie können Ihren eigenen virtuellen SSL-Server mit Ihren eigenen signierten Zertifikaten und Algorithmen verwenden.

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

    - Backup-Virtual-Server: Wenn das API-Gateway nicht erreichbar ist, können Sie die Anforderung zur weiteren Bearbeitung an einen Backup-Virtual-Server senden.
    - Viele weitere Lastverteilungsfunktionen sind verfügbar. Weitere Informationen finden Sie unter Datenverkehr auf einer NetScaler Appliance lastverteilen.

- **Authentifizierung, Autorisierung und Auditierung:** Sie können Ihre eigenen Authentifizierungsmethoden wie LDAP, SAML, RADIUS definieren und die API-Anforderungen autorisieren und auditieren.
- **Responder:** Sie können API-Anforderungen während der Abschaltzeit an ein anderes API-Gateway umleiten.
- **Ratenbegrenzung:** Sie können die Ratenbegrenzungsfunktion konfigurieren, um eine Überlastung eines API-Gateways zu vermeiden.
- **Bessere Verfügbarkeit:** Sie können eine NetScaler Appliance in einem Hochverfügbarkeits-Setup oder einem Cluster-Setup konfigurieren, um eine bessere Verfügbarkeit für Ihren AWS API-Datenverkehr zu gewährleisten.
- **REST-API:** Unterstützt die REST-API, die zur Automatisierung der Arbeit in Cloud-Produktionsumgebungen verwendet werden kann.
- **Daten überwachen:** Überwacht und protokolliert die Daten zur Referenz.

Die NetScaler Appliance bietet viele weitere Funktionen, die in das AWS API Gateway integriert werden können. Weitere Informationen finden Sie in der NetScaler-Dokumentation.

## Back-End-AWS-Autoscaling-Dienst hinzufügen

Ein effizientes Hosting von Anwendungen in einer Cloud beinhaltet eine einfache und kostengünstige Verwaltung von Ressourcen, abhängig vom Anwendungsbedarf. Um steigende Anforderungen zu erfüllen, müssen Sie Netzwerkressourcen nach oben skalieren. Wenn die Nachfrage nachlässt, müssen Sie die Skalierung reduzieren, um unnötige Kosten für ungenutzte Ressourcen zu vermeiden. Sie können die Kosten für den Betrieb der Anwendungen minimieren, indem Sie zu jedem Zeitpunkt nur so viele Instanzen bereitstellen, wie nötig sind. Um dies zu erreichen, müssen Sie ständig den Datenverkehr, den Speicher- und CPU-Verbrauch usw. überwachen. Die manuelle Überwachung des Datenverkehrs ist jedoch umständlich. Damit die Anwendungsumgebung dynamisch skaliert werden kann, müssen Sie die Prozesse zur Überwachung des Datenverkehrs und zur Skalierung von Ressourcen bei Bedarf automatisieren.

Integriert mit dem AWS Auto Scaling-Dienst bietet die NetScaler VPX-Instanz die folgenden Vorteile:

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

- **Lastenausgleich und Verwaltung**: Automatische Konfiguration von Servern zum Hoch- und Herunterskalieren, je nach Bedarf. Die VPX-Instanz erkennt Autoscale™-Gruppen im Back-End-Subnetz automatisch und ermöglicht einem Benutzer die Auswahl der Autoscale-Gruppen zum Lastenausgleich. All dies geschieht durch die automatische Konfiguration der virtuellen und Subnetz-IP-Adressen auf der VPX-Instanz.
- **Hohe Verfügbarkeit**: Erkennt Autoscale-Gruppen, die sich über mehrere Verfügbarkeitszonen erstrecken, und gleicht die Last der Server aus.
- **Bessere Netzwerkverfügbarkeit**: Die VPX-Instanz unterstützt:
  - Back-End-Server in verschiedenen VPCs durch VPC-Peering
  - Back-End-Server in denselben Platzierungsgruppen
  - Back-End-Server in verschiedenen Verfügbarkeitszonen
- **Graceful Connection Termination**: Entfernt Autoscale-Server ordnungsgemäß, wodurch der Verlust von Client-Verbindungen bei Skalierungsaktivitäten durch die Funktion „Graceful Timeout“ vermieden wird.
- **Verbindungsentleerung für Standby-Server**: Verhindert das Senden neuer Client-Verbindungen an den Server im Standby-Zustand. Die Standby-Server sind jedoch weiterhin Teil der Autoscaling-Gruppe und bearbeiten weiterhin die bestehenden Client-Verbindungen, bis diese geschlossen werden. Wenn der Server wieder in den InService-Zustand wechselt, nimmt er die Bearbeitung neuer Verbindungen wieder auf. Sie können den Standby-Zustand verwenden, um Server zu aktualisieren, zu ändern oder Fehler zu beheben oder um je nach Anforderung zu skalieren. Weitere Informationen finden Sie in der AWS-Dokumentation.

**Diagramm**: AWS Autoscaling-Dienst mit einer NetScaler VPX-Instanz

Dieses Diagramm veranschaulicht, wie der AWS Autoscaling-Dienst mit einer NetScaler VPX-Instanz (Load Balancing Virtual Server) kompatibel ist. Weitere Informationen finden Sie in den folgenden AWS-Themen.

- Autoscaling-Gruppen
- CloudWatch
- Simple Notification Service (SNS)
- Simple Queue Service (Amazon SQS)

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

## Bevor Sie beginnen

Bevor Sie Autoscaling mit Ihrer NetScaler VPX-Instanz verwenden, müssen Sie die folgenden Aufgaben erledigen.

- Lesen Sie die folgenden Themen:
  - Voraussetzungen
  - Einschränkungen und Nutzungsrichtlinien
- Erstellen Sie eine NetScaler VPX-Instanz auf AWS entsprechend Ihren Anforderungen.
  - Weitere Informationen zum Erstellen einer eigenständigen NetScaler VPX-Instanz finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS und Szenario: eigenständige Instanz
  - Weitere Informationen zur Bereitstellung von VPX-Instanzen im HA-Modus finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.

  **HINWEIS:**

  Wir empfehlen Folgendes:

  - Verwenden Sie die CloudFormation-Vorlage zum Erstellen von NetScaler VPX-Instanzen auf AWS.
  - Erstellen Sie drei separate Schnittstellen: eine für die Verwaltung (NSIP), eine für den clientseitigen LB Virtual Server (VIP) und eine für die Subnetz-IP (NSIP).
- Erstellen Sie eine AWS Autoscale-Gruppe. Wenn Sie keine vorhandene Autoscaling-Konfiguration haben, müssen Sie:

  a. Eine Startkonfiguration erstellen

  b. Eine Autoscaling-Gruppe erstellen

  c. Die Autoscaling-Gruppe überprüfen

  Weitere Informationen finden Sie unter `<http://docs.aws.amazon.com/autoscaling/latest/userguide/GettingStartedTutorial.html>`.
- Ab NetScaler-Release 14.1-12.x müssen Sie in einer AWS Autoscale-Gruppe eine Scale-Down-Richtlinie nur dann angeben, wenn Sie die Option „Graceful“ aktiviert haben. In

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

NetScaler-Releases vor 14.1-12.x mussten Sie mindestens eine Scale-Down-Richtlinie angeben, unabhängig davon, ob die Option „Graceful“ aktiviert war oder nicht.

Die NetScaler VPX-Instanz unterstützt nur die Schrittskalierungsrichtlinie. Die einfache Skalierungsrichtlinie und die Zielverfolgungsskalierungsrichtlinie werden für die Autoscale-Gruppe nicht unterstützt.

- Stellen Sie sicher, dass Ihr AWS-Konto über die folgenden IAM-Berechtigungen verfügt:

```
{

    "Version": "2012-10-17",

    "Statement": \[

     {

            "Action": \[

                "ec2:DescribeInstances",

                "ec2:DescribeNetworkInterfaces",

                "ec2:DetachNetworkInterface",

                "ec2:AttachNetworkInterface",

                "ec2:StartInstances",

                "ec2:StopInstances",

                "ec2:RebootInstances",

                "autoscaling:\*",

                "sns:\*",

                "sqs:\*"



            “iam: SimulatePrincipalPolicy”
```

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

```
            “iam: GetRole”

            \],

            "Resource": "\*",

            "Effect": "Allow"

        }

    \]

}
```

## Den AWS Autoscaling-Dienst zu einer NetScaler VPX-Instanz hinzufügen

Führen Sie die folgenden Schritte aus, um den Autoscaling-Dienst zu einer VPX-Instanz hinzuzufügen:

1. Melden Sie sich mit Ihren Anmeldeinformationen für `nsroot` bei der VPX-Instanz an.
2. Navigieren Sie zu **System > AWS > Cloud Profile** und klicken Sie auf **Hinzufügen**.

   Die Konfigurationsseite **Cloud-Profil erstellen** wird angezeigt.

   **Wichtige Hinweise beim Erstellen eines Cloud-Profils**:

   - Die IP-Adresse des virtuellen Servers wird automatisch aus der freien IP-Adresse ausgefüllt, die der VPX-Instanz zur Verfügung steht. Weitere Informationen finden Sie unter Mehrere IP-Adressen verwalten.
   - Geben Sie den genauen Namen der Autoscaling-Gruppe ein, die Sie in Ihrem AWS-Konto konfiguriert haben. Weitere Informationen finden Sie unter AWS Auto Scaling-Gruppen.
   - Bei der Auswahl des Protokolls und Ports der Autoscaling-Gruppe stellen Sie sicher, dass Ihre Server auf diesen Protokollen und Ports lauschen und dass Sie den richtigen Monitor in der Dienstgruppe binden. Standardmäßig wird der TCP-Monitor verwendet.
   - Für Autoscaling vom Typ SSL-Protokoll scheint nach dem Erstellen des Cloud-Profils der virtuelle Lastausgleichsserver oder die Dienstgruppe aufgrund eines fehlenden Zertifikats

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

ausgefallen zu sein. Sie können das Zertifikat manuell an den virtuellen Server oder die Dienstgruppe binden.

- Wählen Sie **Graceful** aus und geben Sie einen Timeout-Wert im Feld **Verzögerung** an, um die Autoscaling-Server ordnungsgemäß zu entfernen. Diese Option initiiert ein Scale-Down-Ereignis. Die VPX-Instanz entfernt den Server nicht sofort, sondern markiert einen der Server zur ordnungsgemäßen Löschung. Während dieses Zeitraums lässt die VPX-Instanz keine neuen Verbindungen zu diesem Server zu. Bestehende Verbindungen werden bedient, bis der Timeout eintritt. Nach dem Timeout entfernt die VPX-Instanz den Server.

  Wenn Sie die Option **Graceful** nicht auswählen, wird der Server in der Autoscaling-Gruppe sofort entfernt, nachdem die Last sinkt. Dies kann zu Dienstunterbrechungen für die bestehenden verbundenen Clients führen.

Nachdem Sie das Cloud-Profil erstellt haben, wird ein virtueller NetScaler-Lastausgleichsserver und eine Dienstgruppe mit den Servern der Autoscaling-Gruppe als Mitglieder erstellt. Ihre Backend-Server müssen über die auf der VPX-Instanz konfigurierte SNIP erreichbar sein.

**HINWEIS:**

- Um Autoscaling-bezogene Informationen in der AWS-Konsole anzuzeigen, navigieren Sie zu **EC2** > **Dashboard** > **Auto Scaling** > **Auto Scaling Group**.
- Sie können verschiedene Cloud-Profile für verschiedene Dienste (unter Verwendung unterschiedlicher Ports) mit derselben Autoscaling-Gruppe (ASG) in AWS erstellen. Somit unterstützt die NetScaler VPX-Instanz mehrere Dienste mit derselben Autoscaling-Gruppe in der Public Cloud.

## NetScaler GSLB auf AWS bereitstellen

Die Einrichtung von GSLB für NetScaler auf AWS besteht im Wesentlichen darin, NetScaler so zu konfigurieren, dass der Datenverkehr auf Server verteilt wird, die sich außerhalb der VPC befinden, zu der NetScaler gehört, z. B. innerhalb einer anderen VPC in einer anderen Verfügbarkeitsregion oder einem lokalen Rechenzentrum.

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

## DBS-Übersicht

Die NetScaler GSLB-Unterstützung mittels Domain-name Based Services (DBS) für Cloud-Lastenausgleichsdienste ermöglicht die automatische Erkennung dynamischer Cloud-Dienste mithilfe einer Cloud-Lastenausgleichslösung. Diese Konfiguration ermöglicht es NetScaler, Global Server Load Balancing Domain-Name Based Services (GSLB DBS) in einer Active-Active-Umgebung zu implementieren. DBS ermöglicht die Skalierung von Backend-Ressourcen in AWS-Umgebungen durch DNS-Erkennung.

Dieser Abschnitt behandelt Integrationen zwischen NetScaler in AWS AutoScaling-Umgebungen. Der letzte Abschnitt des Dokuments beschreibt die Möglichkeit, ein HA-Paar von NetScaler ADCs einzurichten, das sich über zwei verschiedene Availability Zones (AZs) erstreckt, die spezifisch für eine AWS-Region sind.

### DBS mit ELB

GSLB DBS nutzt den FQDN des Elastic Load Balancers (ELB) des Benutzers, um die GSLB-Dienstgruppen dynamisch zu aktualisieren und die Backend-Server einzuschließen, die in AWS erstellt und gelöscht werden. Die Backend-Server oder Instanzen in AWS können so konfiguriert werden, dass sie je nach Netzwerkanforderung oder CPU-Auslastung skaliert werden. Um diese Funktion zu konfigurieren, richten Sie NetScaler auf den ELB aus, um dynamisch zu verschiedenen Servern in AWS zu routen, ohne NetScaler jedes Mal manuell aktualisieren zu müssen, wenn eine Instanz in AWS erstellt und gelöscht wird. Die NetScaler DBS-Funktion für GSLB-Dienstgruppen verwendet eine DNS-basierte Dienstermittlung, um die Mitgliedsdienstressourcen des in der Autoscale-Gruppe identifizierten DBS-Namespace zu bestimmen.

NetScaler GSLB DBS Autoscale-Komponenten mit Cloud-Lastenausgleichsdiensten:

## AWS-Komponenten konfigurieren

### Sicherheitsgruppen

**HINWEIS:**

Wir empfehlen Ihnen, verschiedene Sicherheitsgruppen für ELB, NetScaler GSLB-Instanz und Linux-Instanz zu erstellen, da der für jede dieser Entitäten erforderliche Regelsatz unterschiedlich ist. Dieses Beispiel enthält der Kürze halber eine konsolidierte Sicherheitsgruppenkonfiguration.

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

Um die ordnungsgemäße Konfiguration der virtuellen Firewall sicherzustellen, siehe Sicherheitsgruppen für Ihre VPC.

1. Melden Sie sich bei der Benutzer-**AWS-Ressourcengruppe** an und navigieren Sie zu **EC2 > NETWORK & SECURITY > Security Groups**.
2. Klicken Sie auf **Create Security Group** und geben Sie einen Namen und eine Beschreibung ein. Diese Sicherheitsgruppe umfasst NetScaler- und Linux-Back-End-Webserver.
3. Fügen Sie die Regeln für eingehende Ports aus dem folgenden Screenshot hinzu.

   **HINWEIS:**

   Die Beschränkung des Zugriffs auf Quell-IPs wird für eine detaillierte Härtung empfohlen. Weitere Informationen finden Sie unter Webserver-Regeln.

4. Amazon Linux Back-End-Webdienste

   a. Melden Sie sich bei der Benutzer-**AWS-Ressourcengruppe** an und navigieren Sie zu **EC2 > Instances**.

   b. Klicken Sie auf **Launch Instance** und verwenden Sie die folgenden Details, um die **Amazon Linux**-Instanz zu konfigurieren.

   Geben Sie die Details zur Einrichtung eines Webservers oder Back-End-Dienstes auf dieser Instanz ein.

5. NetScaler-Konfiguration

   a. Melden Sie sich bei der Benutzer-**AWS-Ressourcengruppe** an und navigieren Sie zu **EC2 > Instances**.

   b. Klicken Sie auf **Launch Instance** und verwenden Sie die folgenden Details, um die **Amazon AMI**-Instanz zu konfigurieren.

6. Elastic IP-Konfiguration

   **HINWEIS:**

   NetScaler kann bei Bedarf auch mit einer einzigen Elastic IP betrieben werden, um Kosten zu senken, indem keine öffentliche IP für die NSIP verwendet wird. Stattdessen weisen Sie dem SNIP eine Elastic IP zu, die den Verwaltungszugriff auf die Box abdecken kann, zusätzlich zur GSLB-Site-IP und ADNS-IP.

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

a. Melden Sie sich bei der **AWS-Ressourcengruppe** des Benutzers an und navigieren Sie zu **EC2 > NETWORK & SECURITY > Elastic IPs**.

b. Klicken Sie auf **Neue Adresse zuweisen**, um eine Elastic IP-Adresse zu erstellen.

c. Konfigurieren Sie die Elastic IP so, dass sie auf die vom Benutzer ausgeführte NetScaler-Instanz in AWS zeigt.

d. Konfigurieren Sie eine zweite Elastic IP und lassen Sie sie erneut auf die vom Benutzer ausgeführte NetScaler-Instanz zeigen.

7. Elastischer Lastausgleich

a. Melden Sie sich bei der **AWS-Ressourcengruppe** des Benutzers an und navigieren Sie zu **EC2 > LOAD BALANCING > Load Balancers**.

b. Klicken Sie auf **Load Balancer erstellen**, um einen klassischen Load Balancer zu konfigurieren.

Die Elastic Load Balancer des Benutzers ermöglichen es Benutzern, den Lastausgleich für ihre Backend-Amazon-Linux-Instanzen durchzuführen und gleichzeitig auch den Lastausgleich für andere Instanzen zu übernehmen, die bei Bedarf gestartet werden.

## Konfigurieren von Domainnamen-basierten Diensten für den globalen Server-Lastausgleich

Für Konfigurationen des Datenverkehrsmanagements siehe NetScaler GSLB-Domain-basierten Dienst konfigurieren.

## Bereitstellungstypen

Bereitstellung mit drei NICs

- Typische Bereitstellungen
  - GSLB StyleBook
  - Mit ADM
  - Mit GSLB (Route53 mit Domänenregistrierung)
  - Lizenzierung – Pooled/Marketplace
- Anwendungsfälle
  - Bereitstellungen mit drei NICs werden verwendet, um eine echte Isolation des Daten- und Verwaltungsdatenverkehrs zu erreichen.

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

- Bereitstellungen mit drei NICs verbessern auch die Skalierbarkeit und Leistung des ADC.
- Bereitstellungen mit drei NICs werden in Netzwerkanwendungen verwendet, bei denen der Durchsatz typischerweise 1 Gbit/s oder höher ist, und eine Bereitstellung mit drei NICs wird empfohlen.

## CFT-Bereitstellung

Kunden würden CloudFormation-Vorlagen verwenden, wenn sie ihre Bereitstellungen anpassen oder automatisieren.

## Bereitstellungsschritte

Im Folgenden sind die Bereitstellungsschritte aufgeführt:

1. Bereitstellung mit drei NICs für GSLB
2. Lizenzierung
3. Bereitstellungsoptionen

### Bereitstellung mit drei NICs für GSLB

Die NetScaler VPX-Instanz ist als Amazon Machine Image (AMI) auf dem AWS Marketplace verfügbar und kann als Elastic Compute Cloud (EC2)-Instanz innerhalb einer AWS VPC gestartet werden. Der minimale EC2-Instanztyp, der als unterstütztes AMI auf NetScaler VPX zugelassen ist, ist m4.large. Eine NetScaler VPX AMI-Instanz erfordert mindestens 2 virtuelle CPUs und 2 GB Arbeitsspeicher. Eine innerhalb einer AWS VPC gestartete EC2-Instanz kann auch die mehreren Schnittstellen, mehrere IP-Adressen pro Schnittstelle sowie öffentliche und private IP-Adressen bereitstellen, die für die VPX-Konfiguration erforderlich sind. Jede VPX-Instanz benötigt mindestens drei IP-Subnetze:

- Ein Management-Subnetz
- Ein clientseitiges Subnetz (VIP)
- Ein Back-End-Subnetz (SNIP)

NetScaler empfiehlt drei Netzwerkschnittstellen für eine Standard-VPX-Instanz bei der AWS-Installation.

AWS stellt die Multi-IP-Funktionalität derzeit nur Instanzen zur Verfügung, die innerhalb einer AWS VPC ausgeführt werden. Eine VPX-Instanz in einer VPC kann zum Lastenausgleich von Servern verwendet werden, die in EC2-Instanzen ausgeführt werden. Eine Amazon VPC ermöglicht

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

Benutzern die Erstellung und Steuerung einer virtuellen Netzwerkumgebung, einschließlich ihres eigenen IP-Adressbereichs, Subnetze, Routing-Tabellen und Netzwerk-Gateways.

**HINWEIS:**

Standardmäßig können Benutzer bis zu 5 VPC-Instanzen pro AWS-Region für jedes AWS-Konto erstellen. Benutzer können höhere VPC-Limits anfordern, indem sie das Antragsformular von Amazon hier einreichen: Amazon VPC Request.

### Lizenzierung

Eine NetScaler VPX-Instanz auf AWS erfordert eine Lizenz. Die folgenden Lizenzierungsoptionen sind für NetScaler VPX-Instanzen, die auf AWS ausgeführt werden, verfügbar:

- Kostenlos (unbegrenzt)
- Stündlich
- Jährlich
- Eigene Lizenz mitbringen
- Kostenlose Testversion (alle NetScaler VPX-AWS Abonnementangebote für 21 Tage kostenlos im AWS Marketplace).

### Bereitstellungsoptionen

Benutzer können eine eigenständige NetScaler VPX-Instanz auf AWS bereitstellen. Weitere Informationen finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS

## NetScaler Global Server Load Balancing für Hybrid- und Multi-Cloud-Bereitstellungen

Die NetScaler Hybrid- und Multi-Cloud-Lösung für globales Server-Lastenausgleich (GSLB) ermöglicht es Benutzern, den Anwendungsverkehr über mehrere Rechenzentren in Hybrid-Clouds, Multi-Clouds und lokalen Bereitstellungen zu verteilen. Die NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung hilft Benutzern, ihre Lastenausgleichskonfiguration in Hybrid- oder Multi-Cloud-Umgebungen zu verwalten, ohne die bestehende Konfiguration zu ändern. Wenn Benutzer eine lokale Konfiguration haben, können sie einige ihrer Dienste in der Cloud mit der NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung testen, bevor sie vollständig in die Cloud migrieren. Zum Beispiel können Benutzer nur einen kleinen Prozentsatz ihres Datenverkehrs in die Cloud leiten und den Großteil des Datenverkehrs lokal verarbeiten. Die NetScaler Hybrid- und Multi-Cloud-GSLB-

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

Lösung ermöglicht es Benutzern 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 Gesamtleistung des Unternehmens verbessern, indem sie „Vendor Lock-in“ vermeidet und unterschiedliche Infrastrukturen nutzt, um die Anforderungen von Benutzerpartnern und Kunden zu erfüllen. Mit der Multi-Cloud-Architektur können Benutzer ihre Infrastrukturkosten besser verwalten, da sie jetzt nur noch für das bezahlen müssen, was sie nutzen. Benutzer können ihre Anwendungen auch besser skalieren, da sie die Infrastruktur jetzt bei Bedarf nutzen. Es bietet auch die Möglichkeit, schnell von einer Cloud zur anderen zu wechseln, um die besten Angebote jedes Anbieters zu nutzen.

NetScaler GSLB-Knoten übernehmen die DNS-Namensauflösung. Jeder dieser GSLB-Knoten kann DNS-Anfragen von jedem Client-Standort empfangen. Der GSLB-Knoten, der die DNS-Anfrage empfängt, gibt die IP-Adresse des virtuellen Load-Balancer-Servers zurück, die gemäß der konfigurierten Lastenausgleichsmethode ausgewählt wurde. Metriken (Standort-, Netzwerk- und Persistenzmetriken) werden zwischen den GSLB-Knoten über das Metrikaustauschprotokoll (MEP) ausgetauscht, einem proprietären NetScaler-Protokoll. Weitere Informationen zum MEP-Protokoll finden Sie unter Metrikaustauschprotokoll konfigurieren.

Der im GSLB-Knoten konfigurierte Monitor überwacht den Integritätsstatus des virtuellen Lastenausgleichsservers im selben Rechenzentrum. In einer Parent-Child-Topologie werden Metriken zwischen den GSLB- und NetScaler-Knoten über MEP ausgetauscht. Das Konfigurieren von Monitor-Probes zwischen einem GSLB- und NetScaler-LB-Knoten ist in einer Parent-Child-Topologie jedoch optional.

Der NetScaler-Agent ermöglicht die Kommunikation zwischen dem NetScaler ADM und den verwalteten Instanzen im Benutzerrechenzentrum. Weitere Informationen zu NetScaler-Agenten und deren Installation finden Sie unter Erste Schritte.

**HINWEIS:**

Dieses Dokument geht von folgenden Annahmen aus:

- Wenn Benutzer eine bestehende Lastenausgleichskonfiguration haben, ist diese betriebsbereit.
- Auf jedem NetScaler GSLB-Knoten ist eine SNIP-Adresse oder eine GSLB-Site-IP-Adresse konfiguriert. Diese IP-Adresse wird als Quell-IP-Adresse des Rechenzentrums verwendet, wenn Metriken mit anderen Rechenzentren ausgetauscht werden.
- Ein ADNS- oder ADNS-TCP-Dienst ist auf jeder NetScaler GSLB-Instanz konfiguriert, um den DNS-Verkehr zu empfangen.

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

- Die erforderlichen Firewall- und Sicherheitsgruppen sind bei den Cloud-Dienstanbietern konfiguriert.

### Konfiguration der Sicherheitsgruppen

Benutzer müssen die erforderliche Firewall-/Sicherheitsgruppenkonfiguration bei den Cloud-Dienstanbietern einrichten. Weitere Informationen zu den AWS-Sicherheitsfunktionen finden Sie unter AWS/Dokumentation/Amazon VPC/Benutzerhandbuch/Sicherheit.

Außerdem müssen Benutzer auf dem GSLB-Knoten Port 53 für den ADNS-Dienst/die IP-Adresse des DNS-Servers und Port 3009 für die GSLB-Site-IP-Adresse für den MEP-Verkehrsaustausch öffnen. Auf dem Lastenausgleichsknoten müssen Benutzer die entsprechenden Ports öffnen, um den Anwendungsverkehr zu empfangen. Beispielsweise müssen Benutzer 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 NetScaler-Agenten und NetScaler ADM.

Für die GSLB-Methode mit dynamischer Roundtrip-Zeit müssen Benutzer 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, daher muss diese Einstellung für Sicherheitsgruppen vorgenommen werden, die an das serverseitige Subnetz gebunden sind.

## Funktionen der hybriden und Multi-Cloud-GSLB-Lösung von NetScaler

Einige der Funktionen der hybriden und Multi-Cloud-GSLB-Lösung von NetScaler werden in diesem Abschnitt beschrieben.

### Kompatibilität mit anderen Lastenausgleichslösungen

Die hybride und Multi-Cloud-GSLB-Lösung von NetScaler unterstützt verschiedene Lastenausgleichslösungen wie NetScaler Load Balancer, NGINX, HAProxy und andere Lastenausgleichslösungen von Drittanbietern.

**HINWEIS:**

Lastenausgleichslösungen, die nicht von NetScaler stammen, werden nur unterstützt, wenn proximitätsbasierte und nicht-metrikbasierte GSLB-Methoden verwendet werden und wenn keine Parent-Child-Topologie konfiguriert ist.

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

### GSLB-Methoden

Die hybride und Multi-Cloud-GSLB-Lösung von NetScaler unterstützt die folgenden GSLB-Methoden.

- Metrikbasierte GSLB-Methoden. Metrikbasierte GSLB-Methoden sammeln Metriken von den anderen NetScaler-Knoten über das Metrikaustauschprotokoll.
  - Geringste Verbindungen (Least Connection): Die Client-Anfrage wird an den Lastenausgleich weitergeleitet, der die wenigsten aktiven Verbindungen hat.
  - Geringste Bandbreite (Least Bandwidth): Die Client-Anfrage wird an den Lastenausgleich weitergeleitet, der derzeit die geringste Menge an Datenverkehr bedient.
  - Geringste Pakete (Least Packets): Die Client-Anfrage wird an den Lastenausgleich weitergeleitet, der in den letzten 14 Sekunden die wenigsten Pakete empfangen hat.
- Nicht-metrikbasierte GSLB-Methoden
  - Round Robin: Die Client-Anfrage wird an die IP-Adresse des Lastenausgleichs weitergeleitet, der ganz oben in der Liste der Lastenausgleicher steht. Dieser Lastenausgleicher rückt dann an das Ende der Liste.
  - Source IP Hash: Diese Methode verwendet den Hash-Wert der Client-IP-Adresse, um einen Lastenausgleicher auszuwählen.
- Proximity-basierte GSLB-Methoden
  - Statische Proximity: Die Client-Anfrage wird an den Lastenausgleicher 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 funktionierenden Lastenausgleichs auszuwählen.

Weitere Informationen zu den Lastenausgleichsmethoden finden Sie unter Lastenausgleichsalgorithmen.

### GSLB-Topologien

Die NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung unterstützt die Aktiv-Passiv-Topologie und die Parent-Child-Topologie.

- Aktiv-Passiv-Topologie – Bietet Disaster Recovery und gewährleistet die kontinuierliche Verfügbarkeit von Anwendungen durch Schutz vor Ausfallpunkten. Fällt das primäre

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

Rechenzentrum aus, wird das passive Rechenzentrum betriebsbereit. Weitere Informationen zur GSLB-Aktiv-Passiv-Topologie finden Sie unter GSLB für Disaster Recovery konfigurieren.

- Parent-Child-Topologie – Kann verwendet werden, wenn Kunden die metrikbasierten GSLB-Methoden zur Konfiguration von GSLB- und Lastenausgleichsknoten verwenden und wenn die Lastenausgleichsknoten auf einer anderen NetScaler-Instanz bereitgestellt werden. In einer Parent-Child-Topologie muss 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-GSLB-Lösung unterstützt auch IPv6.

### Überwachung

Die NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung unterstützt integrierte Monitore mit der Option, eine sichere Verbindung zu aktivieren. Wenn jedoch LB- und GSLB-Konfigurationen auf derselben NetScaler-Instanz vorhanden sind oder eine Parent-Child-Topologie verwendet wird, ist die Konfiguration von Monitoren optional.

### Persistenz

Die NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung unterstützt Folgendes:

- Sitzungen mit Quell-IP-basierter Persistenz, sodass mehrere Anfragen desselben Clients an denselben Dienst weitergeleitet werden, wenn sie innerhalb des konfigurierten Zeitfensters eintreffen. Wenn der Zeitüberschreitungswert 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 GSLB-Knoten ein Rechenzentrum zur Verarbeitung einer Client-Anfrage auswählt und die IP-Adresse des ausgewählten Rechenzentrums für alle nachfolgenden DNS-Anfragen weiterleitet. Wenn die konfigurierte Persistenz für einen DOWN-Status einer Site gilt, verwendet der GSLB-Knoten eine GSLB-Methode, um eine neue Site auszuwählen, und die neue Site wird für nachfolgende Anfragen des Clients persistent.

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

## Konfiguration mithilfe von NetScaler ADM StyleBooks

Kunden können das standardmäßige Multi-Cloud-GSLB-StyleBook auf NetScaler ADM verwenden, um NetScaler-Instanzen mit Hybrid- und Multi-Cloud-GSLB-Konfigurationen zu konfigurieren.

Kunden können das standardmäßige Multi-Cloud-GSLB-StyleBook für das Lastausgleichs-Knoten-StyleBook verwenden, um NetScaler-Lastausgleichsknoten zu konfigurieren, die die untergeordneten Sites in einer Parent-Child-Topologie sind, die den Anwendungsverkehr verarbeiten. Verwenden Sie dieses StyleBook nur, wenn Benutzer Lastausgleichsknoten in einer Parent-Child-Topologie konfigurieren möchten. Jeder LB-Knoten muss jedoch separat mit diesem StyleBook konfiguriert werden.

## Workflow der NetScaler Hybrid- und Multi-Cloud-GSLB-Lösungskonfiguration

Kunden können das mitgelieferte Multi-Cloud-GSLB-StyleBook auf NetScaler ADM verwenden, um NetScaler-Instanzen mit Hybrid- und Multi-Cloud-GSLB-Konfigurationen zu konfigurieren.

Das folgende Diagramm zeigt den Workflow für die Konfiguration einer NetScaler Hybrid- und Multi-Cloud-GSLB-Lösung. Die Schritte im Workflow-Diagramm werden nach dem Diagramm detaillierter erläutert.

Führen Sie die folgenden Aufgaben als Cloud-Administrator aus:

1. Registrieren Sie sich für ein NetScaler Cloud-Konto.

   Um NetScaler ADM nutzen zu können, erstellen Sie ein NetScaler Cloud-Unternehmenskonto oder treten Sie einem bestehenden bei, das von jemandem in Ihrem Unternehmen erstellt wurde.
2. Nachdem sich Benutzer bei NetScaler Cloud angemeldet haben, klicken Sie auf **Manage** auf der Kachel **NetScaler Application Delivery Management**, um den ADM-Dienst zum ersten Mal einzurichten.
3. Laden Sie mehrere NetScaler ADM-Dienst-Agenten herunter und installieren Sie diese.

   Benutzer müssen den NetScaler ADM-Dienst-Agenten in ihrer Netzwerkumgebung installieren und konfigurieren, um die Kommunikation zwischen NetScaler ADM und den verwalteten Instanzen in ihrem Rechenzentrum oder ihrer Cloud zu ermöglichen. Installieren Sie einen Agenten in jeder Region, damit sie LB- und GSLB-Konfigurationen auf den verwalteten Instanzen konfigurieren können. Die LB- und GSLB-Konfigurationen können einen einzigen

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

Agenten gemeinsam nutzen. Weitere Informationen zu den oben genannten drei Aufgaben finden Sie unter Erste Schritte.

4. Stellen Sie Lastenausgleichsmodule in der Microsoft AWS Cloud/in lokalen Rechenzentren bereit.

   Je nach Art der Lastenausgleichsmodule, die Benutzer in der Cloud und lokal bereitstellen, stellen Sie diese entsprechend bereit. Benutzer können beispielsweise NetScaler VPX-Instanzen in einer virtuellen privaten Cloud von Amazon Web Services (AWS) und in lokalen Rechenzentren bereitstellen. Konfigurieren Sie NetScaler-Instanzen so, dass sie als LB- oder GSLB-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:

   - NetScaler VPX unter AWS.
   - Konfigurieren einer NetScaler VPX Standalone-Instanz.

5. Führen Sie Sicherheitskonfigurationen durch.

   Konfigurieren Sie Netzwerksicherheitsgruppen und Netzwerk-ACLs in ARM und in AWS, um den eingehenden und ausgehenden Datenverkehr für Benutzerinstanzen und Subnetze zu steuern.

6. Fügen Sie NetScaler-Instanzen in NetScaler ADM hinzu.

   NetScaler-Instanzen sind Netzwerk-Appliances oder virtuelle Appliances, die Benutzer von NetScaler ADM aus erkennen, verwalten und überwachen möchten. Um diese Instanzen zu verwalten und zu überwachen, müssen Benutzer die Instanzen zum Dienst hinzufügen und sowohl LB- (wenn Benutzer NetScaler für LB verwenden) als auch GSLB-Instanzen registrieren. Weitere Informationen zum Hinzufügen von NetScaler-Instanzen in NetScaler ADM finden Sie unter Erste Schritte

7. Implementieren Sie die GSLB- und LB-Konfigurationen mithilfe der Standard-NetScaler ADM StyleBooks.

   - Verwenden Sie das Multi-Cloud GSLB StyleBook, um die GSLB-Konfiguration auf den ausgewählten GSLB NetScaler-Instanzen auszuführen.
   - Implementieren Sie die Lastenausgleichskonfiguration. (Benutzer können diesen Schritt überspringen, wenn sie bereits LB-Konfigurationen auf den verwalteten Instanzen haben.) Benutzer können Lastenausgleichsmodule auf NetScaler-Instanzen auf zwei Arten konfigurieren:

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

- Konfigurieren Sie die Instanzen manuell für den Lastenausgleich der Anwendungen. Weitere Informationen zum manuellen Konfigurieren der Instanzen finden Sie unter Grundlegenden Lastenausgleich einrichten.
- Verwenden Sie StyleBooks. Benutzer können eines der NetScaler ADM StyleBooks (HTTP/SSL-Lastverteilungs-StyleBook oder HTTP/SSL-Lastverteilungs-StyleBook (mit Monitoren)) verwenden, um die Lastverteilerkonfiguration auf der ausgewählten NetScaler-Instanz zu erstellen. Benutzer können auch ihre eigenen StyleBooks erstellen. Weitere Informationen zu StyleBooks finden Sie unter StyleBooks.

8. Verwenden Sie das Multi-Cloud-GSLB-StyleBook für LB-Knoten, um die GSLB-Parent-Child-Topologie in einem der folgenden Fälle zu konfigurieren:

   - Wenn Benutzer die metrikbasierten GSLB-Algorithmen (geringste Pakete, geringste Verbindungen, geringste Bandbreite) verwenden, um GSLB- und Lastverteilungsknoten zu konfigurieren, und wenn die Lastverteilungsknoten auf einer anderen NetScaler-Instanz bereitgestellt werden.
   - Wenn Site-Persistenz erforderlich ist.

### Verwenden von StyleBooks zur Konfiguration von GSLB auf NetScaler-Lastverteilungsknoten

Kunden können das **Multi-Cloud-GSLB-StyleBook für LB-Knoten** verwenden, wenn sie die metrikbasierten GSLB-Algorithmen (geringste Pakete, geringste Verbindungen, geringste Bandbreite) verwenden, um GSLB- und Lastverteilungsknoten zu konfigurieren, und wenn die Lastverteilungsknoten auf einer anderen NetScaler-Instanz bereitgestellt werden.

Benutzer können dieses StyleBook auch verwenden, um weitere 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 GSLB-Konfiguration auf die untergeordneten Sites an. Benutzer können maximal 1024 untergeordnete Sites konfigurieren.

**HINWEIS:**

Verwenden Sie das Multi-Cloud-GSLB-StyleBook, um die übergeordneten Sites zu konfigurieren.

Dieses StyleBook geht von folgenden Annahmen aus:

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

- Eine SNIP-Adresse oder eine GSLB-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-GSLB-StyleBooks für LB-Knoten

1. Navigieren Sie zu **Applications > Configuration > Create New**.
2. Navigieren Sie zu **Applications** > **Configuration**, und klicken Sie auf **Create New**.

   Das StyleBook wird als Benutzeroberfläche angezeigt, auf der Benutzer die Werte für alle in diesem StyleBook definierten Parameter eingeben können.

   **HINWEIS:**

   Die Begriffe Rechenzentrum und Standorte werden in diesem Dokument synonym verwendet.

3. Legen Sie die folgenden Parameter fest:

   - **Anwendungsname**. Geben Sie den Namen der GSLB-Anwendung ein, die auf den GSLB-Standorten bereitgestellt wird, für die Sie untergeordnete Standorte erstellen möchten.
   - **Protokoll**. Wählen Sie das Anwendungsprotokoll der bereitgestellten Anwendung aus der Dropdown-Liste aus.
   - **LB-Integritätsprüfung** (Optional)
   - **Typ der Integritätsprüfung**. Wählen Sie aus der Dropdown-Liste den Sondentyp aus, der zur Überprüfung der Integrität der Load Balancer VIP-Adresse verwendet wird, die die Anwendung an einem Standort darstellt.
   - **Sicherer Modus**. (Optional) Wählen Sie **Ja** aus, um diesen Parameter zu aktivieren, wenn SSL-basierte Integritätsprüfungen erforderlich sind.
   - **HTTP-Anfrage**. (Optional) Wenn Benutzer HTTP als Typ der Integritätsprüfung ausgewählt haben, geben Sie die vollständige HTTP-Anfrage ein, die zum Abfragen der VIP-Adresse verwendet wird.
   - **Liste der HTTP-Status-Antwortcodes**. (Optional) Wenn Benutzer HTTP als Typ der Integritätsprüfung ausgewählt haben, geben Sie die Liste der erwarteten HTTP-Statuscodes in den Antworten auf HTTP-Anfragen ein, wenn die VIP fehlerfrei ist.

4. Konfigurieren des übergeordneten Standorts.

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

- Geben Sie die Details des übergeordneten Standorts (GSLB-Knoten) an, unter dem Sie den untergeordneten Standort (LB-Knoten) erstellen möchten.
  - **Standortname**. Geben Sie den Namen des übergeordneten Standorts ein.
  - **Standort-IP-Adresse**. Geben Sie die IP-Adresse ein, die der übergeordnete Standort als Quell-IP-Adresse verwendet, wenn er Metriken mit anderen Standorten austauscht. Es wird davon ausgegangen, dass diese IP-Adresse bereits auf dem GSLB-Knoten an jedem Standort konfiguriert ist.
  - **Öffentliche IP-Adresse des Standorts**. (Optional) Geben Sie die öffentliche IP-Adresse des übergeordneten Standorts ein, die zum Austausch von Metriken verwendet wird, falls die IP-Adresse dieses Standorts NAT-ed ist.

5. Konfigurieren des untergeordneten Standorts.
   - Geben Sie die Details des untergeordneten Standorts an.
     - **Standortname**. Geben Sie den Namen des Standorts ein.
     - **IP-Adresse des 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 untergeordneten Standorts ein, die zum Austausch von Metriken verwendet wird, falls die IP-Adresse dieses Standorts NAT-ed ist.
6. Konfigurieren aktiver GSLB-Dienste (optional)
   - Konfigurieren Sie aktive GSLB-Dienste nur, wenn die IP-Adresse des virtuellen LB-Servers keine öffentliche IP-Adresse ist. Dieser Abschnitt ermöglicht Benutzern die Konfiguration der Liste der lokalen GSLB-Dienste an den Standorten, an denen die Anwendung bereitgestellt wird.
     - **Dienst-IP**. Geben Sie die IP-Adresse des virtuellen Lastausgleichsservers an diesem Standort ein.
     - **Öffentliche IP-Adresse des Dienstes**. Wenn die virtuelle IP-Adresse privat ist und eine öffentliche IP-Adresse darauf NAT-ed ist, geben Sie die öffentliche IP-Adresse an.
     - **Dienstport**. Geben Sie den Port des GSLB-Dienstes an diesem Standort ein.
     - **Standortname**. Geben Sie den Namen des Standorts ein, an dem sich der GSLB-Dienst befindet.

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

7. Klicken Sie auf **Target Instances** und wählen Sie NetScaler-Instanzen aus, die als GSLB-Instanzen an jedem Standort konfiguriert sind, an dem die GSLB-Konfiguration bereitgestellt werden soll.
8. Klicken Sie auf **Create**, um die LB-Konfiguration auf der ausgewählten NetScaler-Instanz (LB-Knoten) zu erstellen. Benutzer können auch auf **Dry Run** klicken, um die Objekte zu überprüfen, die in den Zielinstanzen erstellt würden. Die von Benutzern erstellte StyleBook-Konfiguration wird in der Liste der Konfigurationen auf der Seite „Configurations“ angezeigt. Benutzer können diese Konfiguration über die NetScaler ADM GUI überprüfen, aktualisieren oder entfernen.

## Bereitstellung der CloudFormation-Vorlage

NetScaler VPX ist als Amazon Machine Images (AMI) im AWS Marketplace verfügbar. Bevor ein CloudFormation-Template zur Bereitstellung eines NetScaler VPX in AWS verwendet wird, muss der AWS-Benutzer die Bedingungen akzeptieren und das AWS Marketplace-Produkt abonnieren. Jede Edition von NetScaler VPX im Marketplace erfordert diesen Schritt.

Jedes Template im CloudFormation-Repository verfügt über eine begleitende Dokumentation, die die Verwendung und Architektur des Templates beschreibt. Die Templates versuchen, die empfohlene Bereitstellungsarchitektur von NetScaler VPX zu kodifizieren, den Benutzer in NetScaler einzuführen oder eine bestimmte Funktion, Edition oder Option zu demonstrieren. Benutzer können die Templates wiederverwenden, ändern oder erweitern, um sie an ihre spezifischen Produktions- und Testanforderungen anzupassen. Die meisten Templates erfordern vollständige EC2-Berechtigungen zusätzlich zu den Berechtigungen zum Erstellen von IAM-Rollen.

Die CloudFormation-Templates enthalten AMI-IDs, die spezifisch für eine bestimmte Version von NetScaler VPX (z. B. Version 12.0-56.20) und Edition (z. B. NetScaler VPX Platinum Edition – 10 Mbit/s) ODER NetScaler BYOL sind. Um eine andere Version/Edition von NetScaler VPX mit einem CloudFormation-Template zu verwenden, muss der Benutzer das Template bearbeiten und die AMI-IDs ersetzen.

Die neuesten NetScaler AWS-AMI-IDs finden Sie hier: NetScaler AWS CloudFormation Master.

### CFT-Bereitstellung mit drei NICs

Dieses Template stellt eine VPC mit 3 Subnetzen (Management, Client, Server) für 2 Availability Zones bereit. Es stellt ein Internet Gateway mit einer Standardroute in den öffentlichen Subnetzen bereit. Dieses Template erstellt auch ein HA-Paar über Availability Zones hinweg mit zwei Instanzen von NetScaler: 3 ENIs, die 3 VPC-Subnetzen (Management, Client, Server) auf dem primären und 3 ENIs, die 3 VPC-Subnetzen (Management, Client, Server) auf dem sekundären

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

zugeordnet sind. Alle von diesem CFT erstellten Ressourcennamen werden mit einem tagName des Stack-Namens präfixiert.

Die Ausgabe des CloudFormation-Templates umfasst:

- PrimaryCitrixADCManagementURL – HTTPS-URL zur Management-GUI des primären VPX (verwendet selbstsigniertes Zertifikat)
- PrimaryCitrixADCManagementURL2 – HTTP-URL zur Management-GUI des primären VPX
- PrimaryCitrixADCInstanceID – Instanz-ID der neu erstellten primären VPX-Instanz
- PrimaryCitrixADCPublicVIP – Elastic IP-Adresse der primären VPX-Instanz, die dem VIP zugeordnet ist
- PrimaryCitrixADCPrivateNSIP – Private IP (NS IP) für die Verwaltung des primären VPX
- PrimaryCitrixADCPublicNSIP – Öffentliche IP (NS IP) für die Verwaltung des primären VPX
- PrimaryCitrixADCPrivateVIP – Private IP-Adresse der primären VPX-Instanz, die dem VIP zugeordnet ist
- PrimaryCitrixADCSNIP – Private IP-Adresse der primären VPX-Instanz, die dem SNIP zugeordnet ist
- SecondaryCitrixADCManagementURL – HTTPS-URL zur Management-GUI des sekundären VPX (verwendet selbstsigniertes Zertifikat)
- SecondaryCitrixADCManagementURL2 – HTTP-URL zur Management-GUI des sekundären VPX
- SecondaryCitrixADCInstanceID – Instanz-ID der neu erstellten sekundären VPX-Instanz
- SecondaryCitrixADCPrivateNSIP – Private IP (NS IP), die für die Verwaltung des sekundären VPX verwendet wird
- SecondaryCitrixADCPublicNSIP – Öffentliche IP (NS IP), die für die Verwaltung des sekundären VPX verwendet wird
- SecondaryCitrixADCPrivateVIP – Private IP-Adresse der sekundären VPX-Instanz, die mit dem VIP verknüpft ist
- SecondaryCitrixADCSNIP – Private IP-Adresse der sekundären VPX-Instanz, die mit dem SNIP verknüpft ist
- SecurityGroup – Sicherheitsgruppen-ID, zu der der VPX gehört

Bei der Eingabe in das CFT bedeutet das `*` bei jedem Parameter im CFT, dass es sich um ein Pflichtfeld handelt. Zum Beispiel ist `VPC ID*` ein Pflichtfeld.

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

Die folgenden Voraussetzungen müssen erfüllt sein. Die CloudFormation-Vorlage erfordert ausreichende Berechtigungen zum Erstellen von IAM-Rollen, die über normale EC2-Vollzugriffsrechte hinausgehen. Der Benutzer dieser Vorlage muss außerdem die Bedingungen akzeptieren und das AWS Marketplace-Produkt abonnieren, bevor er diese CloudFormation-Vorlage verwendet.

Folgendes sollte ebenfalls vorhanden sein:

- Schlüsselpaar
- 3 nicht zugewiesene EIPs
- Primäres Management
- Client-VIP
- Sekundäres Management

Weitere Informationen zur Bereitstellung von NetScaler VPX-Instanzen auf AWS finden Sie unter Bereitstellen von NetScaler VPX-Instanzen auf AWS.

Informationen zum Konfigurieren von GSLB mit StyleBooks finden Sie unter Verwenden von StyleBooks zum Konfigurieren von GSLB

## Notfallwiederherstellung (DR)

Eine Katastrophe ist eine plötzliche Unterbrechung der Geschäftsfunktionen, die durch Naturkatastrophen oder von Menschen verursachte Ereignisse hervorgerufen wird. Katastrophen beeinträchtigen den Rechenzentrumsbetrieb, wonach Ressourcen und die am Katastrophenort verlorenen Daten vollständig wiederhergestellt werden müssen. Der Datenverlust oder die Ausfallzeit im Rechenzentrum ist kritisch und gefährdet die Geschäftskontinuität.

Eine der Herausforderungen, vor denen Kunden heute stehen, ist die Entscheidung, wo sie ihren DR-Standort einrichten sollen. Unternehmen suchen nach Konsistenz und Leistung, unabhängig von der zugrunde liegenden Infrastruktur oder Netzwerkfehlern.

Informationen zur Bereitstellung von GSLB für die Notfallwiederherstellung finden Sie unter Bereitstellen einer eigenständigen NetScaler VPX-Instanz auf AWS

## Weitere Ressourcen

NetScaler ADM GSLB für Hybrid- und Multi-Cloud-Bereitstellungen.

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

# Bereitstellen von NetScaler Web App Firewall auf AWS

Die NetScaler Web App Firewall kann entweder als Layer-3-Netzwerkgerät oder als Layer-2-Netzwerkbrücke zwischen Kundenservern und Kundenbenutzern installiert werden, normalerweise hinter dem Router oder der Firewall des Kundenunternehmens. Die NetScaler Web App Firewall muss an einem Ort installiert werden, an dem sie den Datenverkehr zwischen den Webservern und dem Hub oder Switch abfangen kann, über den Benutzer auf diese Webserver zugreifen. Benutzer konfigurieren dann das Netzwerk so, dass Anfragen an die Web Application Firewall gesendet werden, anstatt direkt an ihre Webserver, und Antworten an die Web Application Firewall, anstatt direkt an ihre Benutzer. Die Web Application Firewall filtert diesen Datenverkehr, bevor sie ihn an sein endgültiges Ziel weiterleitet, wobei sie sowohl ihren internen Regelsatz als auch die Benutzerergänzungen und -änderungen verwendet. Sie blockiert oder macht jede Aktivität unschädlich, die sie als schädlich erkennt, und leitet dann den verbleibenden Datenverkehr an den Webserver weiter. Die vorhergehende Abbildung bietet einen Überblick über den Filterprozess.

Weitere Informationen finden Sie unter Funktionsweise der NetScaler Web App Firewall.

## Architektur für NetScaler Web App Firewall auf AWS für die Produktionsbereitstellung

Die Abbildung zeigt eine Virtual Private Cloud (VPC) mit **Standardparametern**, die eine NetScaler Web App Firewall-Umgebung in der AWS Cloud aufbaut.

In einer Produktionsbereitstellung werden die folgenden Parameter für die NetScaler Web App Firewall-Umgebung eingerichtet:

- Diese Architektur setzt die Verwendung einer AWS CloudFormation-Vorlage voraus.
- Eine VPC, die sich über zwei Availability Zones erstreckt und gemäß den AWS-Best Practices mit zwei öffentlichen und vier privaten Subnetzen konfiguriert ist, um Ihnen Ihr eigenes virtuelles Netzwerk auf AWS mit einem /16 Classless Inter-Domain Routing (CIDR)-Block (ein Netzwerk mit 65.536 privaten IP-Adressen) bereitzustellen.
- Zwei Instanzen der NetScaler Web App Firewall (Primär und Sekundär), jeweils eine in jeder Availability Zone.
- **Drei Sicherheitsgruppen**, eine für jede Netzwerkschnittstelle (Management, Client, Server), die als virtuelle Firewalls fungieren, um den Datenverkehr für ihre zugehörigen Instanzen zu steuern.
- **Drei Subnetze**, für jede Instanz – eines für Management, eines für Client und eines für den Back-End-Server.

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

- Ein an die VPC angeschlossenes **Internet-Gateway** und eine Routing-Tabelle für öffentliche Subnetze, die mit öffentlichen Subnetzen verknüpft ist, um den Zugriff auf das Internet zu ermöglichen. Dieses Gateway wird vom Web App Firewall-Host verwendet, um Datenverkehr zu senden und zu empfangen. Weitere Informationen zu Internet-Gateways finden Sie unter: Internet-Gateways.
- **5 Routing-Tabellen** – eine öffentliche Routing-Tabelle, die den Client-Subnetzen sowohl der primären als auch der sekundären Web App Firewall zugeordnet ist. Die restlichen 4 Routing-Tabellen sind mit jedem der 4 privaten Subnetze (Management- und serverseitige Subnetze der primären und sekundären Web App Firewall) verknüpft.
- AWS Lambda in der Web App Firewall kümmert sich um Folgendes:
  - Konfigurieren von zwei Web App Firewalls in jeder Verfügbarkeitszone des HA-Modus
  - Erstellen eines Beispiel-Web App Firewall-Profils und anschließendes Übertragen dieser Konfiguration in Bezug auf die Web App Firewall
- AWS Identity and Access Management (IAM) zur sicheren Steuerung des Zugriffs auf AWS-Dienste und -Ressourcen für Ihre Benutzer. Standardmäßig erstellt die CloudFormation-Vorlage (CFT) die erforderliche IAM-Rolle. Benutzer können jedoch ihre eigene IAM-Rolle für NetScaler ADC-Instanzen bereitstellen.
- In den öffentlichen Subnetzen zwei verwaltete Network Address Translation (NAT)-Gateways, um ausgehenden Internetzugang für Ressourcen in öffentlichen Subnetzen zu ermöglichen.

**HINWEIS:**

Die CFT Web App Firewall-Vorlage, die die NetScaler Web App Firewall in eine bestehende VPC bereitstellt, überspringt die mit Sternchen gekennzeichneten Komponenten und fordert Benutzer zur Eingabe ihrer bestehenden VPC-Konfiguration auf.

Backend-Server werden nicht von der CFT bereitgestellt.

## Kosten und Lizenzierung

Benutzer sind für die Kosten der AWS-Dienste verantwortlich, die bei der Ausführung von AWS-Bereitstellungen verwendet werden. Die AWS CloudFormation-Vorlagen, die für diese Bereitstellung verwendet werden können, enthalten Konfigurationsparameter, die Benutzer bei Bedarf anpassen können. Einige dieser Einstellungen, wie z. B. der Instanztyp, beeinflussen die Bereitstellungskosten. Für Kostenschätzungen sollten Benutzer die Preisübersichten für jeden von ihnen verwendeten AWS-Dienst konsultieren. Die Preise können sich ändern.

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

Eine NetScaler Web App Firewall auf AWS erfordert eine Lizenz. Um die NetScaler Web App Firewall zu lizenzieren, müssen Benutzer den Lizenzschlüssel in einem S3-Bucket ablegen und dessen Speicherort beim Start der Bereitstellung angeben.

**HINWEIS:**

Wenn Benutzer das Lizenzierungsmodell „Bring your own license (BYOL)“ wählen, sollten sie sicherstellen, dass die AppFlow-Funktion aktiviert ist. Weitere Informationen zur BYOL-Lizenzierung finden Sie unter: AWS Marketplace/Citrix VPX – Customer Licensed.

Die folgenden Lizenzierungsoptionen sind für Citrix® ADC Web App Firewall unter AWS verfügbar. Benutzer können ein AMI (Amazon Machine Image) basierend auf einem einzelnen Faktor wie dem Durchsatz auswählen.

- **Lizenzmodell**: Pay as You Go (PAYG, für die Produktionslizenzen) oder Bring Your Own License (BYOL, für das vom Kunden lizenzierte AMI – Citrix ADC Pooled Capacity). Weitere Informationen zu Citrix ADC Pooled Capacity finden Sie unter: Citrix ADC Pooled Capacity.
    - Für BYOL gibt es 3 Lizenzierungsmodi:
        - NetScaler Pooled Capacity konfigurieren: Citrix ADC Pooled Capacity konfigurieren
        - NetScaler VPX Check-in- und Check-out-Lizenzierung (CICO): Citrix ADC VPX Check-in- und Check-out-Lizenzierung

        **TIPP:**

        Wenn Benutzer die CICO-Lizenzierung mit dem Anwendungstyp VPX-200, VPX-1000, VPX-3000, VPX-5000 oder VPX-8000 wählen, sollten sie sicherstellen, dass sie dieselbe Durchsatzlizenz auf ihrem NetScaler Console-Lizenzserver haben.

        - NetScaler virtuelle CPU-Lizenzierung: NetScaler virtuelle CPU-Lizenzierung

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

**HINWEIS:**

Wenn Benutzer die Bandbreite einer VPX-Instanz dynamisch ändern möchten, sollten sie eine BYOL-Option wählen, z. B. **NetScaler Pooled Capacity**, bei der sie die Lizenzen von NetScaler Console zuweisen können, oder sie können die Lizenzen von NetScaler entsprechend der minimalen und maximalen Kapazität der Instanz bei Bedarf und ohne Neustart auschecken. Ein Neustart ist nur erforderlich, wenn Benutzer die Lizenzedition ändern möchten.

- **Durchsatz**: 200 Mbit/s oder 1 Gbit/s
- **Bundle**: Premium

## Bereitstellungsoptionen

Dieser Bereitstellungsleitfaden bietet zwei Bereitstellungsoptionen:

- Die erste Option ist die Bereitstellung mithilfe eines Quick Start Guide-Formats und der folgenden Optionen:
  - **NetScaler Web App Firewall in einem neuen VPC bereitstellen (End-to-End-Bereitstellung)**. Diese Option erstellt eine neue AWS-Umgebung, die aus VPC, Subnetzen, Sicherheitsgruppen und anderen Infrastrukturkomponenten besteht, und stellt dann NetScaler Web App Firewall in diesem neuen VPC bereit.
  - **NetScaler Web App Firewall in einem vorhandenen VPC bereitstellen**. Diese Option stellt NetScaler Web App Firewall in der vorhandenen AWS-Infrastruktur des Benutzers bereit.
- Die zweite Option ist die Bereitstellung mithilfe von Web App Firewall StyleBooks über NetScaler Console

## AWS Quick Start

### Schritt 1: Beim AWS-Benutzerkonto anmelden

- Melden Sie sich bei AWS bei Ihrem Benutzerkonto an: AWS mit einer IAM-Benutzerrolle (Identity and Access Management), die über die erforderlichen Berechtigungen zum Erstellen eines Amazon-Kontos (falls erforderlich) oder zum Anmelden bei einem Amazon-Konto verfügt.

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

- Verwenden Sie die Regionsauswahl in der Navigationsleiste, um die AWS-Region auszuwählen, in der Benutzer Hochverfügbarkeit über AWS-Verfügbarkeitszonen hinweg bereitstellen möchten.
- Stellen Sie sicher, dass das AWS-Benutzerkonto korrekt konfiguriert ist. Weitere Informationen finden Sie im Abschnitt „Technische Anforderungen“ dieses Dokuments.

### Schritt 2: NetScaler Web App Firewall AMI abonnieren

- Diese Bereitstellung erfordert ein Abonnement für das AMI für NetScaler Web App Firewall im AWS Marketplace.
- Melden Sie sich bei Ihrem AWS-Benutzerkonto an.
- Öffnen Sie die Seite für das NetScaler Web App Firewall-Angebot, indem Sie einen der Links in der folgenden Tabelle auswählen.
    - Wenn Benutzer den Quick Start Guide starten, um NetScaler Web App Firewall in Schritt 3 unten bereitzustellen, verwenden sie den Parameter **NetScaler Web App Firewall Image**, um das Bundle und die Durchsatzoption auszuwählen, die ihrem AMI-Abonnement entsprechen. Die folgende Liste zeigt die AMI-Optionen und die entsprechenden Parametereinstellungen. Die VPX AMI-Instanz erfordert mindestens 2 virtuelle CPUs und 2 GB Arbeitsspeicher.

**HINWEIS:**

Um die AMI-ID abzurufen, lesen Sie die Seite NetScaler Products on AWS Marketplace auf GitHub: Citrix Products on AWS Marketplace.

- AWS Marketplace AMI
    - NetScaler Web Application Firewall (Web App Firewall) – 200 Mbit/s: Citrix Web App Firewall (Web App Firewall) - 200 Mbps
    - NetScaler Web Application Firewall (Web App Firewall) – 1000 Mbit/s: Citrix Web App Firewall (Web App Firewall) - 1000 Mbps
- Auf der AMI-Seite wählen Sie **Weiter zum Abonnement**.

- Überprüfen Sie die Nutzungsbedingungen für die Software und wählen Sie dann **Bedingungen akzeptieren**.

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

**HINWEIS:**

Benutzer erhalten eine Bestätigungsseite, und eine E-Mail-Bestätigung wird an den Kontoinhaber gesendet. Detaillierte Abonnementanweisungen finden Sie unter Erste Schritte in der AWS Marketplace-Dokumentation: Erste Schritte.

- Wenn der Abonnementprozess abgeschlossen ist, verlassen Sie den AWS Marketplace ohne weitere Maßnahmen. Stellen Sie die Software nicht über den AWS Marketplace bereit – Benutzer werden das AMI mit dem Quick Start Guide bereitstellen.

### Schritt 3: AWS Quick Start starten

- Melden Sie sich bei Ihrem AWS-Konto an und wählen Sie eine der folgenden Optionen, um die AWS CloudFormation-Vorlage zu starten. Hilfe bei der Auswahl einer Option finden Sie unter Bereitstellungsoptionen weiter oben in diesem Handbuch.
  - Stellen Sie NetScaler VPX in einer neuen VPC auf AWS bereit, indem Sie eine der hier befindlichen AWS CloudFormation-Vorlagen verwenden:
    - Citrix/Citrix-ADC-AWS-CloudFormation/Templates/High-Availability/Across-Availability-Zone
    - Citrix/Citrix-ADC-AWS-CloudFormation/Templates/High-Availability/Same-Availability-Zone

**WICHTIG:**

Wenn Benutzer NetScaler Web App Firewall in einer vorhandenen VPC bereitstellen, müssen sie sicherstellen, dass ihre VPC zwei Availability Zones umfasst, mit einem öffentlichen und zwei privaten Subnetzen in jeder Availability Zone für die Workload-Instanzen, und dass die Subnetze nicht gemeinsam genutzt werden. Dieses Bereitstellungshandbuch unterstützt keine gemeinsam genutzten Subnetze, siehe Arbeiten mit gemeinsam genutzten VPCs: Arbeiten mit gemeinsam genutzten VPCs. Diese Subnetze benötigen NAT-Gateways in ihren Routing-Tabellen, damit die Instanzen Pakete und Software herunterladen können, ohne sie dem Internet auszusetzen. Weitere Informationen zu NAT-Gateways finden Sie unter NAT-Gateways. Konfigurieren Sie die Subnetze so, dass es keine Überlappung von Subnetzen gibt.

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

Benutzer sollten außerdem sicherstellen, dass die Domänennamenoption in den DHCP-Optionen wie in der Amazon VPC-Dokumentation hier beschrieben konfiguriert ist: DHCP-Optionssätze DHCP-Optionssätze. Benutzer werden beim Starten des Quick Start Guide nach ihren VPC-Einstellungen gefragt.

- Jede Bereitstellung dauert etwa 15 Minuten.
- Überprüfen Sie die AWS-Region, die in der oberen rechten Ecke der Navigationsleiste angezeigt wird, und ändern Sie sie bei Bedarf. Hier wird die Netzwerkinfrastruktur für Citrix Web App Firewall aufgebaut. Die Vorlage wird standardmäßig in der Region USA Ost (Ohio) gestartet.

**HINWEIS:**

Diese Bereitstellung umfasst NetScaler Web App Firewall, die derzeit nicht in allen AWS-Regionen unterstützt wird. Eine aktuelle Liste der unterstützten Regionen finden Sie unter AWS Service Endpoints: AWS Service Endpoints.

- Behalten Sie auf der Seite **Select Template** die Standardeinstellung für die Vorlagen-URL bei und wählen Sie dann Weiter.
- Geben Sie auf der Seite **Specify Details** den Stack-Namen nach Belieben des Benutzers an. Überprüfen Sie die Parameter für die Vorlage. Geben Sie Werte für die Parameter an, die eine Eingabe erfordern. Überprüfen Sie für alle anderen Parameter die Standardeinstellungen und passen Sie diese bei Bedarf an.
- In der folgenden Tabelle sind die Parameter nach Kategorie aufgeführt und für die Bereitstellungsoption separat beschrieben:
- Parameter zur Bereitstellung von NetScaler Web App Firewall in einem neuen oder bestehenden VPC (Bereitstellungsoption 1)
- Wenn Benutzer die Überprüfung und Anpassung der Parameter abgeschlossen haben, sollten sie Weiter wählen.

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

## Parameter zur Bereitstellung von NetScaler Web App Firewall in einem neuen VPC

### VPC-Netzwerkkonfiguration

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| **Primäre Verfügbarkeitszone (PrimaryAvailabilityZone)** | Eingabe erforderlich | Die Verfügbarkeitszone für die Bereitstellung der primären NetScaler Web App Firewall |
| **Sekundäre Verfügbarkeitszone (SecondaryAvailabilityZone)** | Eingabe erforderlich | Die Verfügbarkeitszone für die Bereitstellung der sekundären NetScaler Web App Firewall |
| **VPC CIDR** (VPCCIDR) | 10.0.0.0/16 | Der CIDR-Block für die VPC. Muss ein gültiger IP-CIDR-Bereich der Form x.x.x.x/x sein. |
| **Remote SSH CIDR IP(Management)** (RestrictedSSHCIDR) | Eingabe erforderlich | Der IP-Adressbereich, der per SSH auf die EC2-Instanz zugreifen kann (Port: 22). |
| | Beispiel: Die Verwendung von 0.0.0.0/0 ermöglicht allen IP-Adressen den Zugriff auf die Benutzerinstanz über SSH oder RDP. Hinweis: Autorisieren Sie nur eine bestimmte IP-Adresse oder einen Adressbereich für den Zugriff auf die Benutzerinstanz, da die Verwendung in der Produktion unsicher ist. | |
| **Remote HTTP CIDR IP(Client)** (RestrictedWebAppCIDR) | 0.0.0.0/0 | Der IP-Adressbereich, der per HTTP auf die EC2-Instanz zugreifen kann (Port: 80). |

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

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| **Remote-HTTP-CIDR-IP (Client)** (RestrictedWebAppCIDR) | 0.0.0.0/0 | Der IP-Adressbereich, der HTTP-Verbindungen zur EC2-Instanz herstellen kann (Port: 80) |
| **Primäres privates Management-Subnetz-CIDR** (PrimaryManagementPrivate SubnetCIDR) | 10.0.1.0/24 | Der CIDR-Block für das primäre Management-Subnetz in Verfügbarkeitszone 1. |
| **Primäre private Management-IP** (PrimaryManagementPrivateI P) | — | Private IP, die dem primären Management-ENI zugewiesen ist (das letzte Oktett muss zwischen 5 und 254 liegen), aus dem primären Management-Subnetz-CIDR. |
| **Primäres öffentliches Client-Subnetz-CIDR** (PrimaryClientPublicSubnetCI DR) | 10.0.2.0/24 | Der CIDR-Block für das primäre Client-Subnetz in Verfügbarkeitszone 1. |
| **Primäre private Client-IP** (PrimaryClientPrivateIP) | — | Private IP, die dem primären Client-ENI zugewiesen ist (das letzte Oktett muss zwischen 5 und 254 liegen), aus dem primären Client-Subnetz-CIDR. |
| **Privates Subnetz-CIDR des primären Servers** (PrimaryServerPrivateSubnet CIDR) | 10.0.3.0/24 | Der CIDR-Block für den primären Server in Verfügbarkeitszone 1. |
| **Private IP des primären Servers** (PrimaryServerPrivateIP) | — | Private IP, die der ENI des primären Servers zugewiesen ist (das letzte Oktett muss zwischen 5 und 254 liegen) |

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

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| | | aus dem Subnetz-CIDR des primären Servers. |
| **Privates Subnetz-CIDR der sekundären Verwaltung** (SecondaryManagementPrivateSubnetCIDR) | 10.0.4.0/24 | Der CIDR-Block für das Subnetz der sekundären Verwaltung in Verfügbarkeitszone 2. |
| **Private IP der sekundären Verwaltung** (SecondaryManagementPrivateIP) | — | Private IP, die der ENI der sekundären Verwaltung zugewiesen ist (das letzte Oktett muss zwischen 5 und 254 liegen). Sie würde die IP der sekundären Verwaltung aus dem Subnetz-CIDR der sekundären Verwaltung zuweisen. |
| **Öffentliches Subnetz-CIDR des sekundären Clients** (SecondaryClientPublicSubnetCIDR) | 10.0.5.0/24 | Der CIDR-Block für das Subnetz des sekundären Clients in Verfügbarkeitszone 2. |
| **Sekundäre private Client-IP** (SecondaryClientPrivateIP) | — | Private IP, die der sekundären Client-ENI zugewiesen ist (das letzte Oktett muss zwischen 5 und 254 liegen). Sie würde die sekundäre Client-IP aus dem sekundären Client-Subnetz-CIDR zuweisen. |
| **Sekundäres privates Server-Subnetz-CIDR** (SecondaryServerPrivateSubnetCIDR) | 10.0.6.0/24 | Der CIDR-Block für das sekundäre Server-Subnetz in Verfügbarkeitszone 2. |
| **Sekundäre private Server-IP** (SecondaryServerPrivateIP) | — | Private IP, die der sekundären Server-ENI zugewiesen ist (das letzte Oktett muss zwischen 5 und |

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

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| | | 254 liegen). Sie würde die sekundäre Server-IP aus dem sekundären Server-Subnetz-CIDR zuweisen. |
| **VPC-Tenancy-Attribut** (`VPCTenancy`) | Standard | Die zulässige Tenancy von Instanzen, die in der VPC gestartet werden. Wählen Sie Dedicated Tenancy, um EC2-Instanzen zu starten, die einem einzelnen Kunden gewidmet sind. |

### Bastion-Host-Konfiguration

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| **Bastion-Host erforderlich** (LinuxBastionHostEIP) | Nein | Standardmäßig wird kein Bastion-Host konfiguriert. Wenn Benutzer jedoch eine Sandbox-Bereitstellung wünschen, wählen Sie **Ja** aus dem Menü, wodurch ein **Linux Bastion Host** im öffentlichen Subnetz mit einer EIP bereitgestellt wird, der Benutzern den Zugriff auf die Komponenten im privaten und öffentlichen Subnetz ermöglicht. |

### NetScaler Web App Firewall Konfiguration

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| **Schlüsselpaarname** (KeyPairName) | Eingabe erforderlich | Ein öffentliches/privates Schlüsselpaar, das Benutzern eine sichere Verbindung zur Benutzerinstanz nach deren |

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

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| | | Start ermöglicht. Dies ist das Schlüsselpaar, das Benutzer in ihrer bevorzugten AWS Region erstellt haben; siehe Abschnitt Technische Anforderungen. |
| **NetScaler Instanztyp** (CitrixADCInstanceType) | m4.xlarge | Der EC2-Instanztyp, der für die ADC-Instanzen verwendet werden soll. Stellen Sie sicher, dass der gewählte Instanztyp mit den im AWS Marketplace verfügbaren Instanztypen übereinstimmt, andernfalls könnte die CFT fehlschlagen. |
| **NetScaler ADC AMI-ID** (CitrixADCImageID) | — | Das AWS Marketplace AMI, das für die Bereitstellung der NetScaler Web App Firewall verwendet werden soll. Dies muss mit dem AMI übereinstimmen, das Benutzer in Schritt 2 abonniert haben. |
| **NetScaler ADC VPX IAM-Rolle** (`iam:GetRole`) | — | Diese Vorlage: AWS-Quickstart/Quickstart-Citrix-ADC-VPX/Templates erstellt die IAM-Rolle und das Instance-Profil, die für NetScaler VPX erforderlich sind. Wenn leer gelassen, erstellt CFT die erforderliche IAM-Rolle. |
| **Client PublicIP(EIP)** (ClientPublicEIP) | Nein | Wählen Sie „Ja“, wenn Benutzer eine öffentliche EIP der Client-Netzwerkschnittstelle zuweisen möchten. |

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

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| | | Andernfalls haben Benutzer auch nach der Bereitstellung immer noch die Möglichkeit, sie bei Bedarf später zuzuweisen. |

### Konfiguration der Pool-Lizenzierung

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| **NetScaler Console Pool-Lizenzierung** | Nein | Wenn Sie die BYOL-Option für die Lizenzierung wählen, wählen Sie **Ja** aus der Liste. Dies ermöglicht Benutzern, ihre bereits erworbenen Lizenzen hochzuladen. Bevor Benutzer beginnen, sollten sie die NetScaler ADC Pool-Kapazität konfigurieren, um sicherzustellen, dass die NetScaler Console Pool-Lizenzierung verfügbar ist, siehe NetScaler Pool-Kapazität konfigurieren |
| **Erreichbare NetScaler Console / NetScaler Console Agent IP** | Eingabe erforderlich | Für die Option „Kundenlizenziert“ stellen Sie sicher, dass eine erreichbare |

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

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| | | NetScaler Console IP-Adresse vorhanden ist, die dann als Eingabeparameter verwendet wird, unabhängig davon, ob Benutzer NetScaler Console lokal oder einen Agenten in der Cloud bereitstellen. |
| **Lizenzierungsmodus** | Optional | Benutzer können aus den 3 Lizenzierungsmodi wählen:* Konfigurieren Sie die NetScaler Pooled Capacity. Weitere Informationen finden Sie unter Citrix ADC Pooled Capacity konfigurieren* NetScaler VPX Check-in- und Check-out-Lizenzierung (CICO). Weitere Informationen finden Sie unter Citrix ADC VPX Check-in- und Check-out-Lizenzierung* NetScaler virtuelle CPU-Lizenzierung. Weitere Informationen finden Sie unter Citrix ADC |

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

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| | | virtuelle CPU-Lizenzierung |
| **Lizenzbandbreite in MBit/s** | 0 MBit/s | Dieses Feld wird nur relevant, wenn der Lizenzierungsmodus „Pooled-Licensing“ ist. Es weist eine anfängliche Bandbreite der Lizenz in MBit/s zu, die nach der Erstellung der BYOL ADCs zugewiesen werden soll. Es sollte ein Vielfaches von 10 MBit/s sein. |
| **Lizenz-Edition** | Premium | Die Lizenz-Edition für den Pooled Capacity Licensing Mode ist **Premium**. |
| **Appliance-Plattformtyp** | Optional | Wählen Sie den erforderlichen Appliance-Plattformtyp **nur** aus, wenn Benutzer den CICO-Lizenzierungsmodus wählen. Benutzern stehen folgende Optionen zur Verfügung: VPX-200, VPX-1000, VPX-3000, VPX-5000, VPX-8000. |

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

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| **Lizenz-Edition** | Premium | Die Lizenz-Edition für die vCPU-basierte Lizenzierung ist **Premium**. |

### AWS Quick Start-Konfiguration

**HINWEIS:**

Wir empfehlen Benutzern, die Standardeinstellungen für die folgenden beiden Parameter beizubehalten, es sei denn, sie passen die Quick Start Guide-Vorlagen für ihre eigenen Bereitstellungsprojekte an. Das Ändern der Einstellungen dieser Parameter aktualisiert automatisch Code-Referenzen, um auf einen neuen Quick Start Guide-Speicherort zu verweisen. Weitere Informationen finden Sie im AWS Quick Start Guide Contributor's Guide hier: AWS Quick Starts/Option 1 - Adopt a Quick Start.

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| **Quick Start-Anleitung S3 Bucket-Name** (QSS3BucketName) | `aws-quickstart` | Der S3-Bucket, den Benutzer für ihre Kopie der Quick Start Guide-Assets erstellt haben, wenn Benutzer sich entscheiden, den Quick Start Guide für ihre eigene Nutzung anzupassen oder zu erweitern. Der Bucket-Name kann Zahlen, Kleinbuchstaben, Großbuchstaben und Bindestriche enthalten, sollte aber nicht mit einem Bindestrich beginnen oder enden. |

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

| PARAMETERBEZEICHNUNG (NAME) | STANDARD | BESCHREIBUNG |
|---|---|---|
| **S3-Schlüsselpräfix des Quick Start Guide** (QSS3KeyPrefix) | quickstart-citrix-adc-vpx/ | Das S3-Schlüsselnamenpräfix aus dem Objekt-Schlüssel und Metadaten: Objekt-Schlüssel und Metadaten, wird verwendet, um einen Ordner für die Benutzerkopie der Quick Start Guide-Assets zu simulieren, wenn Benutzer sich entscheiden, den Quick Start Guide für ihre eigene Nutzung anzupassen oder zu erweitern. Dieses Präfix kann Zahlen, Kleinbuchstaben, Großbuchstaben, Bindestriche und Schrägstriche enthalten. |

- Auf der Seite **Optionen** können Benutzer ein Ressourcen-Tag oder ein Schlüssel-Wert-Paar für Ressourcen in Ihrem Stack angeben und erweiterte Optionen festlegen. Weitere Informationen zu Ressourcen-Tags finden Sie unter Ressourcen-Tag. Weitere Informationen zum Festlegen von AWS CloudFormation Stack-Optionen finden Sie unter Festlegen von AWS CloudFormation Stack-Optionen. Wenn Benutzer fertig sind, sollten sie **Weiter** wählen.
- Auf der Seite **Überprüfen** überprüfen und bestätigen Sie die Vorlageneinstellungen. Unter **Funktionen** aktivieren Sie die beiden Kontrollkästchen, um zu bestätigen, dass die Vorlage IAM-Ressourcen erstellt und dass sie möglicherweise die Fähigkeit zum automatischen erweiternieren von Makros erfordert.
- Wählen Sie **Erstellen**, um den Stack bereitzustellen.
- Überwachen Sie den Status des Stacks. Wenn der Status **CREATE_COMPLETE** ist, ist die NetScaler Web App Firewall-Instanz bereit.
- Verwenden Sie die URLs, die auf der Registerkarte **Ausgaben** für den Stack angezeigt werden, um die erstellten Ressourcen anzuzeigen.

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

### Schritt 4: Bereitstellung testen

Wir bezeichnen die Instanzen in dieser Bereitstellung als **primär** und **sekundär**. Jede Instanz hat unterschiedliche IP-Adressen, die ihr zugeordnet sind. Wenn der Quick Start erfolgreich bereitgestellt wurde, läuft der Datenverkehr über die primäre NetScaler Web App Firewall-Instanz, die in Verfügbarkeitszone 1 konfiguriert ist. Unter Failover-Bedingungen, wenn die primäre Instanz nicht auf Client-Anfragen reagiert, übernimmt die sekundäre Web App Firewall-Instanz.

Die Elastic IP-Adresse der virtuellen IP-Adresse der primären Instanz migriert zur sekundären Instanz, die als neue primäre Instanz übernimmt.

Im Failover-Prozess führt NetScaler Web App Firewall Folgendes aus:

- NetScaler Web App Firewall prüft die virtuellen Server, denen IP-Sets zugeordnet sind.
- NetScaler Web App Firewall findet die IP-Adresse, der eine öffentliche IP-Adresse zugeordnet ist, aus den beiden IP-Adressen, auf denen der virtuelle Server lauscht. Eine, die direkt an den virtuellen Server angehängt ist, und eine, die über das IP-Set angehängt ist.
- NetScaler Web App Firewall ordnet die öffentliche Elastic IP-Adresse der privaten IP-Adresse neu zu, die zur neuen primären virtuellen IP-Adresse gehört.

Um die Bereitstellung zu validieren, führen Sie Folgendes aus:

- Verbindung zur primären Instanz herstellen

Zum Beispiel mit einem Proxy-Server, Jump-Host (einer Linux-/Windows-/FW-Instanz, die in AWS läuft, oder dem Bastion-Host) oder einem anderen Gerät, das über diese VPC oder eine Direct Connect-Verbindung erreichbar ist, wenn es um lokale Konnektivität geht.

- Führen Sie eine Auslöseaktion aus, um ein Failover zu erzwingen und zu prüfen, ob die sekundäre Instanz übernimmt.

**TIPP:**

Um die Konfiguration bezüglich NetScaler Web App Firewall weiter zu validieren, führen Sie den folgenden Befehl aus, nachdem Sie sich mit der **primären NetScaler Web App Firewall-Instanz** verbunden haben:

```
Sh appfw profile QS-Profile
```

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

### Verbindung zu NetScaler Web App Firewall HA-Paar mithilfe eines Bastion-Hosts herstellen

Wenn Benutzer sich für eine Sandbox-Bereitstellung entscheiden (z. B. als Teil von CFT, entscheiden sich Benutzer für die Konfiguration eines Bastion-Hosts), wird ein in einem öffentlichen Subnetz bereitgestellter Linux-Bastion-Host für den Zugriff auf die Web App Firewall-Schnittstellen konfiguriert.

Wählen Sie in der AWS CloudFormation-Konsole, auf die Sie sich hier anmelden können: Anmelden, den Master-Stack aus, und suchen Sie auf der Registerkarte **Outputs** den Wert von **LinuxBastionHostEIP1**.

- Der Wert des Schlüssels **PrivateManagementPrivateNSIP** und **PrimaryADCInstanceID** wird in den späteren Schritten verwendet, um sich per SSH mit dem ADC zu verbinden.
- Wählen Sie **Services**.
- Wählen Sie auf der Registerkarte **Compute** die Option **EC2**.
  - Wählen Sie unter **Resources** die Option **Running Instances**.
  - Notieren Sie auf der Registerkarte **Description** der primären Web App Firewall-Instanz die **öffentliche IPv4-Adresse**. Benutzer benötigen diese IP-Adresse, um den SSH-Befehl zu erstellen.

- Um den Schlüssel im Benutzerschlüsselbund zu speichern, führen Sie den Befehl `ssh-add -K [your-key-pair].pem` aus.

Unter Linux müssen Benutzer möglicherweise das Flag -K weglassen.

- Melden Sie sich mit dem folgenden Befehl beim Bastion-Host an, wobei Sie den Wert für **LinuxBastionHostEIP1** verwenden, den Sie in Schritt 1 notiert haben.

```
ssh -A ubuntu@[LinuxBastionHostEIP1]
```

- Vom Bastion-Host aus können Benutzer sich per SSH mit der primären Web App Firewall-Instanz verbinden.

```
ssh nsroot@[Primary Management Private NSIP]
```

Passwort:

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

Benutzer sind nun mit der primären NetScaler Web App Firewall Instanz verbunden. Um die verfügbaren Befehle anzuzeigen, können Benutzer den Befehl „help“ ausführen. Um die aktuelle HA-Konfiguration anzuzeigen, können Benutzer den Befehl „show HA node“ ausführen.

## NetScaler Console

Der NetScaler Application Delivery Management Service bietet eine einfache und skalierbare Lösung zur Verwaltung von NetScaler-Bereitstellungen, die NetScaler MPX, NetScaler VPX, NetScaler Gateway, NetScaler Secure Web Gateway, NetScaler SDX, NetScaler ADC CPX und NetScaler SD-WAN Appliances umfassen, die On-Premises oder in der Cloud bereitgestellt werden.

Die Dokumentation zum NetScaler Console Service enthält Informationen zum Einstieg in den Dienst, eine Liste der vom Dienst unterstützten Funktionen und die spezifische Konfiguration für diese Dienstlösung.

Weitere Informationen finden Sie unter NetScaler Console – Übersicht.

## Bereitstellen von NetScaler VPX-Instanzen auf AWS mit NetScaler Console

Wenn Kunden ihre Anwendungen in die Cloud verlagern, nehmen die Komponenten ihrer Anwendung zu, werden verteilter und müssen dynamisch verwaltet werden.

Weitere Informationen finden Sie unter Bereitstellen von NetScaler VPX-Instanzen auf AWS.

## NetScaler Web App Firewall und OWASP Top 10 – 2017

Das Open Web Application Security Project: OWASP veröffentlichte die OWASP Top 10 für 2017 für die Sicherheit von Webanwendungen. Diese Liste dokumentiert die häufigsten Schwachstellen von Webanwendungen und ist ein guter Ausgangspunkt, um die Websicherheit zu bewerten. Hier beschreiben wir, wie die NetScaler Web App Firewall (Web App Firewall) konfiguriert wird, um diese Schwachstellen zu mindern. Die Web App Firewall ist als integriertes Modul im NetScaler (Premium Edition) sowie als vollständige Palette von Appliances verfügbar.

Das vollständige OWASP Top 10-Dokument ist unter OWASP Top Ten verfügbar.

Signaturen bieten die folgenden Bereitstellungsoptionen, um Benutzern zu helfen, den Schutz ihrer Anwendungen zu optimieren:

- Negatives Sicherheitsmodell: Mit dem negativen Sicherheitsmodell verwenden Benutzer eine Vielzahl vorkonfigurierter Signaturregeln, um die Leistungsfähigkeit des Musterabgleichs zur

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

Erkennung von Angriffen und zum Schutz vor Anwendungsschwachstellen zu nutzen. Benutzer blockieren nur das, was sie nicht wollen, und erlauben den Rest. Benutzer können ihre eigenen Signaturregeln basierend auf den spezifischen Sicherheitsanforderungen ihrer Anwendungen hinzufügen, um ihre eigenen maßgeschneiderten Sicherheitslösungen zu entwerfen.

- Hybrides Sicherheitsmodell: Zusätzlich zur Verwendung von Signaturen können Benutzer positive Sicherheitsprüfungen verwenden, um eine Konfiguration zu erstellen, die ideal für Benutzeranwendungen geeignet ist. Verwenden Sie Signaturen, um unerwünschte Inhalte zu blockieren, und positive Sicherheitsprüfungen, um das zu erzwingen, was erlaubt ist.

Um Benutzeranwendungen mithilfe von Signaturen zu schützen, müssen Benutzer ein oder mehrere Profile konfigurieren, die ihr Signaturobjekt verwenden. In einer hybriden Sicherheitskonfiguration werden die SQL-Injection- und Cross-Site-Scripting-Muster sowie die SQL-Transformationsregeln im Benutzersignaturobjekt nicht nur von den Signaturregeln, sondern auch von den positiven Sicherheitsprüfungen verwendet, die im Web Application Firewall-Profil konfiguriert sind, das das Signaturobjekt verwendet.

Die Web Application Firewall untersucht den Datenverkehr zu benutzergeschützten Websites und Webdiensten, um Datenverkehr zu erkennen, der einer Signatur entspricht. Eine Übereinstimmung wird nur ausgelöst, wenn jedes Muster in der Regel mit dem Datenverkehr übereinstimmt. Wenn eine Übereinstimmung auftritt, werden die angegebenen Aktionen für die Regel aufgerufen. Benutzer können eine Fehlerseite oder ein Fehlerobjekt anzeigen, wenn eine Anforderung blockiert wird. Protokollmeldungen können Benutzern helfen, Angriffe zu identifizieren, die gegen Benutzeranwendungen gestartet werden. Wenn Benutzer Statistiken aktivieren, verwaltet die Web Application Firewall Daten über Anforderungen, die einer Web Application Firewall-Signatur oder Sicherheitsprüfung entsprechen.

Wenn der Datenverkehr sowohl einer Signatur als auch einer positiven Sicherheitsprüfung entspricht, wird die restriktivere der beiden Aktionen erzwungen. Wenn beispielsweise eine Anforderung einer Signaturregel entspricht, für die die Blockierungsaktion deaktiviert ist, die Anforderung aber auch einer positiven SQL-Injection-Sicherheitsprüfung entspricht, für die die Aktion Blockieren ist, wird die Anforderung blockiert. In diesem Fall kann die Signaturverletzung als protokolliert werden, obwohl die Anforderung durch die SQL-Injection-Prüfung blockiert wird.

**Anpassung**: Bei Bedarf können Benutzer dem Signaturobjekt eigene Regeln hinzufügen. Benutzer können auch die SQL/XSS-Muster anpassen. Die Möglichkeit, eigene Signaturregeln basierend auf den spezifischen Sicherheitsanforderungen von Benutzeranwendungen hinzuzufügen, gibt Benutzern die Flexibilität, eigene maßgeschneiderte Sicherheitslösungen zu entwerfen. Benutzer blockieren nur das, was sie nicht wollen, und erlauben den Rest. Ein spezifisches Fast-Match-Muster an einem bestimmten Ort kann den Verarbeitungsaufwand

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

erheblich reduzieren, um die Leistung zu optimieren. Benutzer können SQL-Injection- und Cross-Site-Scripting-Muster hinzufügen, ändern oder entfernen. Integrierte RegEx- und Ausdruckseditoren helfen Benutzern, Benutzermuster zu konfigurieren und deren Genauigkeit zu überprüfen.

## NetScaler Web App Firewall

Die Web App Firewall ist eine Unternehmenslösung, die modernste Schutzfunktionen für moderne Anwendungen bietet. Die NetScaler Web App Firewall mindert Bedrohungen für öffentlich zugängliche Assets, einschließlich Websites, Webanwendungen und APIs. Sie umfasst IP-Reputations-basiertes Filtern, Bot-Minderung, Schutz vor OWASP Top 10 Anwendungsbedrohungen, Layer-7-DDoS-Schutz und mehr. Ebenfalls enthalten sind Optionen zur Erzwingung von Authentifizierung, starken SSL/TLS-Chiffren, TLS 1.3, Ratenbegrenzung und Rewrite-Richtlinien. Durch die Verwendung sowohl grundlegender als auch erweiterter Schutzfunktionen der Web App Firewall bietet sie umfassenden Schutz für Ihre Anwendungen mit beispielloser Benutzerfreundlichkeit. Die Inbetriebnahme dauert nur wenige Minuten. Darüber hinaus spart die NetScaler Web App Firewall den Benutzern durch ein automatisiertes Lernmodell, das als dynamisches Profiling bezeichnet wird, wertvolle Zeit. Indem sie automatisch lernt, wie eine geschützte Anwendung funktioniert, passt sich die Web App Firewall der Anwendung an, selbst wenn Entwickler die Anwendungen bereitstellen und ändern. Die NetScaler Web App Firewall hilft bei der Einhaltung aller wichtigen regulatorischen Standards und Vorschriften, einschließlich PCI-DSS, HIPAA und mehr. Mit unseren CloudFormation-Vorlagen war es noch nie einfacher, schnell einsatzbereit zu sein. Mit der automatischen Skalierung können Benutzer sicher sein, dass ihre Anwendungen geschützt bleiben, selbst wenn ihr Datenverkehr zunimmt.

## Web App Firewall Bereitstellungsstrategie

Der erste Schritt zur Bereitstellung der Web Application Firewall besteht darin, zu bewerten, welche Anwendungen oder spezifischen Daten den maximalen Sicherheitsschutz benötigen, welche weniger anfällig sind und für welche die Sicherheitsprüfung sicher umgangen werden kann. Dies hilft Benutzern, eine optimale Konfiguration zu finden und geeignete Richtlinien und Bindungspunkte zu entwerfen, um den Datenverkehr zu trennen. Beispielsweise möchten Benutzer möglicherweise eine Richtlinie konfigurieren, um die Sicherheitsprüfung von Anforderungen für statische Webinhalte wie Bilder, MP3-Dateien und Filme zu umgehen, und eine andere Richtlinie konfigurieren, um erweiterte Sicherheitsprüfungen auf Anforderungen für dynamische Inhalte anzuwenden. Benutzer können mehrere Richtlinien und Profile verwenden, um verschiedene Inhalte derselben Anwendung zu schützen.

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

Der nächste Schritt ist die Basislinienbestimmung der Bereitstellung. Beginnen Sie mit der Erstellung eines virtuellen Servers und leiten Sie Testdatenverkehr darüber, um eine Vorstellung von der Rate und Menge des Datenverkehrs zu erhalten, der durch das Benutzersystem fließt.

Stellen Sie dann die Web App Firewall bereit. Verwenden Sie die NetScaler-Konsole und das Web App Firewall StyleBook, um die Web App Firewall zu konfigurieren. Details finden Sie im Abschnitt StyleBook weiter unten in diesem Handbuch.

Nachdem die Web App Firewall bereitgestellt und mit dem Web App Firewall StyleBook konfiguriert wurde, wäre ein nützlicher nächster Schritt die Implementierung der NetScaler ADC Web App Firewall und OWASP Top 10.

Schließlich sind drei der Web App Firewall-Schutzfunktionen besonders wirksam gegen gängige Arten von Webangriffen und werden daher häufiger verwendet als alle anderen. Daher sollten sie in der Erstbereitstellung implementiert werden.

## NetScaler-Konsole

Die NetScaler-Konsole bietet eine skalierbare Lösung zur Verwaltung von NetScaler ADC-Bereitstellungen, die NetScaler ADC MPX, NetScaler ADC VPX, NetScaler Gateway, NetScaler Secure Web Gateway, NetScaler ADC SDX, NetScaler ADC CPX und NetScaler SD-WAN-Appliances umfassen, die On-Premises oder in der Cloud bereitgestellt werden.

### NetScaler Console Anwendungsanalyse- und Verwaltungsfunktionen

Die auf der NetScaler Console unterstützten Funktionen sind entscheidend für die Rolle der NetScaler Console in der App-Sicherheit.

Weitere Informationen zu den Funktionen finden Sie unter Funktionen und Lösungen.

## Voraussetzungen

Bevor Benutzer versuchen, eine VPX-Instanz in AWS zu erstellen, sollten sie sicherstellen, dass die Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter Voraussetzungen:

## Einschränkungen und Nutzungsrichtlinien

Die unter Einschränkungen und Nutzungsrichtlinien verfügbaren Einschränkungen und Nutzungsrichtlinien gelten bei der Bereitstellung einer Citrix ADC VPX-Instanz in AWS.

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

## Technische Anforderungen

Bevor Benutzer den Quick Start Guide starten, um eine Bereitstellung zu beginnen, muss das Benutzerkonto wie in der folgenden Ressourcentabelle angegeben konfiguriert werden. Andernfalls könnte die Bereitstellung fehlschlagen.

### Ressourcen

Melden Sie sich bei Bedarf bei Ihrem Amazon-Konto an und beantragen Sie hier eine Erhöhung der Dienstlimits für die folgenden Ressourcen: AWS/Anmelden. Dies kann erforderlich sein, wenn Sie bereits eine bestehende Bereitstellung haben, die diese Ressourcen nutzt, und Sie der Meinung sind, dass Sie mit dieser Bereitstellung die Standardlimits überschreiten könnten. Die Standardlimits finden Sie in der AWS-Dokumentation unter AWS Service Quotas: AWS Service Quotas.

Der AWS Trusted Advisor, hier zu finden: AWS/Anmelden, bietet eine Überprüfung der Dienstlimits, die die Nutzung und Limits für einige Aspekte bestimmter Dienste anzeigt.

| RESSOURCE | DIESE BEREITSTELLUNG VERWENDET |
|---|---|
| VPCs | 1 |
| Elastische IP-Adressen | 0/1 (für Bastion-Host) |
| IAM-Sicherheitsgruppen | 3 |
| IAM-Rollen | 1 |
| Subnetze | 6 (3/Verfügbarkeitszone) |
| Internet-Gateway | 1 |
| Routing-Tabellen | 5 |
| Web App Firewall VPX-Instanzen | 2 |
| Bastion-Host | 0/1 |
| NAT-Gateway | 2 |

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

### Regionen

NetScaler Web App Firewall unter AWS wird derzeit nicht in allen AWS-Regionen unterstützt. Eine aktuelle Liste der unterstützten Regionen finden Sie unter AWS Service Endpoints in der AWS-Dokumentation: AWS Service Endpoints.

Weitere Informationen zu AWS-Regionen und warum Cloud-Infrastruktur wichtig ist, finden Sie unter: Globale Infrastruktur.

### Schlüsselpaar

Stellen Sie sicher, dass mindestens ein Amazon EC2-Schlüsselpaar im AWS-Konto des Benutzers in der Region vorhanden ist, in der Benutzer die Bereitstellung mithilfe des Quick Start Guide planen. Notieren Sie sich den Namen des Schlüsselpaars. Benutzer werden während der Bereitstellung nach diesen Informationen gefragt. Um ein Schlüsselpaar zu erstellen, befolgen Sie die Anweisungen für Amazon EC2-Schlüsselpaare und Linux-Instanzen in der AWS-Dokumentation: Amazon EC2-Schlüsselpaare und Linux-Instanzen.

Wenn Benutzer den Quick Start Guide zu Test- oder Proof-of-Concept-Zwecken bereitstellen, empfehlen wir, ein neues Schlüsselpaar zu erstellen, anstatt ein Schlüsselpaar anzugeben, das bereits von einer Produktionsinstanz verwendet wird.

## Referenzen

- HTML-SQL-Injection-Prüfung
- XML-SQL-Injection-Prüfung
- Konfigurieren der HTML-Cross-Site-Scripting-Prüfung über die Befehlszeile
- XML-Cross-Site-Scripting-Prüfung
- Verwenden der Befehlszeile zum Konfigurieren der Pufferüberlauf-Sicherheitsprüfung
- Hinzufügen oder Entfernen eines Signaturobjekts
- Konfigurieren oder Ändern eines Signaturobjekts
- Aktualisieren eines Signaturobjekts
- Snort-Regelintegration
- Bot-Erkennung
- Bereitstellen einer NetScaler VPX-Instanz auf Microsoft Azure

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

# NetScaler VPX-Instanz zur Verwendung der SR-IOV-Netzwerkschnittstelle konfigurieren

**HINWEIS:**

Die Unterstützung für SR-IOV-Schnittstellen in einer Hochverfügbarkeitskonfiguration ist ab NetScaler Release 12.0 57.19 verfügbar.

Nachdem Sie eine NetScaler VPX-Instanz in AWS erstellt haben, können Sie die virtuelle Appliance so konfigurieren, dass sie SR-IOV-Netzwerkschnittstellen verwendet, indem Sie die AWS CLI nutzen.

In allen NetScaler VPX-Modellen, mit Ausnahme der NetScaler VPX AWS Marketplace Editions von 3G und 5G, ist SR-IOV in der Standardkonfiguration einer Netzwerkschnittstelle nicht aktiviert.

Bevor Sie mit der Konfiguration beginnen, lesen Sie die folgenden Themen:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien

Dieser Abschnitt enthält die folgenden Themen:

- Schnittstellentyp in SR-IOV ändern
- SR-IOV in einer Hochverfügbarkeitskonfiguration einrichten

## Schnittstellentyp in SR-IOV ändern

Sie können den Befehl show interface summary ausführen, um die Standardkonfiguration einer Netzwerkschnittstelle zu überprüfen.

**Beispiel 1:** Der folgende CLI-Screenshot zeigt die Konfiguration einer Netzwerkschnittstelle, bei der SR-IOV standardmäßig auf NetScaler VPX AWS Marketplace Editions von 3G und 5G aktiviert ist.

**Beispiel 2:** Der folgende CLI-Screenshot zeigt die Standardkonfiguration einer Netzwerkschnittstelle, bei der SR-IOV nicht aktiviert ist.

Weitere Informationen zum Ändern des Schnittstellentyps in SR-IOV finden Sie unter `<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sriov-networking.html>`

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

### So ändern Sie den Schnittstellentyp in SR-IOV

1. Fahren Sie die NetScaler VPX-Instanz herunter, die unter AWS ausgeführt wird.
2. Um SR-IOV auf der Netzwerkschnittstelle zu aktivieren, geben Sie den folgenden Befehl in der AWS CLI ein.

   ```
   $ aws ec2 modify-instance-attribute --instance-id \<instance\_id\> --sriov-net-support simple
   ```

3. Um zu überprüfen, ob SR-IOV aktiviert wurde, geben Sie den folgenden Befehl in der AWS CLI ein.

   ```
   $ aws ec2 describe-instance-attribute --instance-id \<instance\_id\> --attribute sriovNetSupport
   ```

   **Beispiel 3:** Netzwerkschnittstellentyp in SR-IOV geändert, mithilfe der AWS CLI.

   Wenn SR-IOV nicht aktiviert ist, ist der Wert für SriovNetSupport nicht vorhanden.

   **Beispiel 4:** Im folgenden Beispiel ist die SR-IOV-Unterstützung nicht aktiviert.

4. Schalten Sie die VPX-Instanz ein. Um den geänderten Status der Netzwerkschnittstelle anzuzeigen, geben Sie „show interface summary“ in der CLI ein.

   **Beispiel 5:** Der folgende Screenshot zeigt die Netzwerkschnittstellen mit aktiviertem SR-IOV. Die Schnittstellen 10/1, 10/2, 10/3 sind SR-IOV-fähig.

Diese Schritte schließen das Verfahren zur Konfiguration von VPX-Instanzen zur Verwendung von SR-IOV-Netzwerkschnittstellen ab.

## SR-IOV in einem Hochverfügbarkeits-Setup konfigurieren

Hochverfügbarkeit wird mit SR-IOV-Schnittstellen ab NetScaler Release 12.0 Build 57.19 unterstützt.

Wenn das Hochverfügbarkeits-Setup manuell oder mithilfe der Citrix CloudFormation-Vorlage für NetScaler Version 12.0 56.20 und niedriger bereitgestellt wurde, muss die an das Hochverfügbarkeits-Setup angehängte IAM-Rolle die folgenden Berechtigungen haben:

- ec2:DescribeInstances

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

- ec2:DescribeNetworkInterfaces
- ec2:DetachNetworkInterface
- ec2:AttachNetworkInterface
- ec2:StartInstances
- ec2:StopInstances
- ec2:RebootInstances
- automatische Skalierung:*
- sns:alle
- SQS:*
- IAM:SimulatePrincipalPolicy
- IAM:GetRole

Standardmäßig fügt die Citrix CloudFormation-Vorlage für NetScaler Version 12.0 57.19 die erforderlichen Berechtigungen automatisch zur IAM-Rolle hinzu.

**HINWEIS:**

Ein Hochverfügbarkeits-Setup mit SR-IOV-Schnittstellen führt zu einer Ausfallzeit von etwa 100 Sekunden.

**Verwandte Ressourcen**:

Weitere Informationen zu IAM-Rollen finden Sie in der AWS-Dokumentation.

## Konfigurieren einer NetScaler VPX-Instanz zur Verwendung von Enhanced Networking mit AWS ENA

Nachdem Sie eine NetScaler VPX-Instanz auf AWS erstellt haben, können Sie die virtuelle Appliance so konfigurieren, dass sie Enhanced Networking mit AWS Elastic Network Adapter (ENA) unter Verwendung der AWS CLI nutzt.

In Verbindung mit AWS ENA bietet Enhanced Networking eine höhere Bandbreite, eine höhere Paket-pro-Sekunde (PPS)-Leistung und durchweg geringere Latenzzeiten zwischen Instanzen.

Bevor Sie mit der Konfiguration beginnen, lesen Sie die folgenden Themen:

- Voraussetzungen

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

- Einschränkungen und Nutzungsrichtlinien

Die folgenden HA-Konfigurationen werden für ENA-fähige Instanzen unterstützt:

- Private IP-Adressen können innerhalb derselben Verfügbarkeitszone verschoben werden.
- Elastische IP-Adressen können über Verfügbarkeitszonen hinweg verschoben werden.

# Eine NetScaler VPX-Instanz auf AWS aktualisieren

Sie können den EC2-Instanztyp, den Durchsatz, die Software-Edition und die Systemsoftware einer auf AWS ausgeführten NetScaler VPX aktualisieren. Für bestimmte Arten von Upgrades empfiehlt Citrix die Verwendung der Hochverfügbarkeitskonfiguration, um Ausfallzeiten zu minimieren.

**HINWEIS:**

- NetScaler Software-Release 10.1.e-124.1308.e oder höher für ein NetScaler VPX AMI (einschließlich Utility-Lizenz und Kundenlizenz) unterstützt die Instanzfamilien M1 und M2 nicht.
- Aufgrund von Änderungen in der VPX-Instanzunterstützung wird ein Downgrade von 10.1.e-124 oder einer späteren Version auf 10.1.123.x oder eine frühere Version nicht unterstützt.
- Die meisten Upgrades erfordern keinen Start eines neuen AMI, und das Upgrade kann auf der aktuellen NetScaler AMI-Instanz durchgeführt werden. Wenn Sie auf eine neue NetScaler AMI-Instanz aktualisieren möchten, verwenden Sie die Methode der Hochverfügbarkeitskonfiguration.

## Change the EC2 instance type of a NetScaler VPX instance on AWS

If your NetScaler VPX instances are running release 10.1.e-124.1308.e or later, you can change the EC2 instance type from the AWS console as follows:

1. Die VPX-Instanz anhalten.
2. Ändern Sie den EC2-Instanztyp über die AWS-Konsole.
3. Die Instanz starten.

Sie können das oben beschriebene Verfahren auch verwenden, um den EC2-Instanztyp für ein Release zu ändern, das älter ist als 10.1.e-124.1308.e, es sei denn, Sie möchten den Instanztyp

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

auf M3 ändern. In diesem Fall müssen Sie zuerst das Standard-NetScaler-Upgrade-Verfahren, unter, befolgen, um die NetScaler-Software auf 10.1.e-124 oder ein späteres Release zu aktualisieren, und dann die oben genannten Schritte ausführen.

## Aktualisieren des Durchsatzes oder der Software-Edition einer NetScaler VPX-Instanz auf AWS

Um die Software-Edition (z. B. um von der Standard- auf die Premium-Edition zu aktualisieren) oder den Durchsatz (z. B. um von 200 Mbit/s auf 1000 Mbit/s zu aktualisieren), hängt die Methode von der Lizenz der Instanz ab.

### Verwenden einer Kundenlizenz (Bring-Your-Own-License)

Wenn Sie eine Kundenlizenz verwenden, können Sie die neue Lizenz von der Citrix®-Website erwerben und herunterladen und dann auf der VPX-Instanz installieren. Weitere Informationen zum Herunterladen und Installieren einer Lizenz von der Citrix-Website finden Sie im VPX-Lizenzierungshandbuch.

### Verwenden einer Utility-Lizenz (Utility-Lizenz mit stündlicher Gebühr)

AWS unterstützt keine direkten Upgrades für kostenpflichtige Instanzen. Um die Software-Edition oder den Durchsatz einer kostenpflichtigen NetScaler VPX-Instanz zu aktualisieren, starten Sie ein neues AMI mit der gewünschten Lizenz und Kapazität und migrieren Sie die Konfiguration der älteren Instanz auf die neue Instanz. Dies kann durch die Verwendung einer NetScaler Hochverfügbarkeitskonfiguration erreicht werden, wie im Unterabschnitt auf dieser Seite beschrieben.

## Aktualisieren der Systemsoftware einer NetScaler VPX-Instanz auf AWS

Wenn Sie eine VPX-Instanz aktualisieren müssen, die 10.1.e-124.1308.e oder eine spätere Version ausführt, befolgen Sie das Standard-NetScaler-Upgrade-Verfahren unter Upgrade und Downgrade einer NetScaler Appliance.

Wenn Sie eine VPX-Instanz, die eine ältere Version als 10.1.e-124.1308.e ausführt, auf 10.1.e-124.1308.e oder eine spätere Version aktualisieren müssen, aktualisieren Sie zuerst die Systemsoftware und ändern Sie dann den Instanztyp auf M3 wie folgt:

1. Stoppen Sie die VPX-Instanz.
2. Ändern Sie den EC2-Instanztyp über die AWS-Konsole.
3. Starten Sie die Instanz.

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

## Upgrade auf eine neue NetScaler AMI-Instanz mithilfe einer NetScaler Hochverfügbarkeitskonfiguration

Um die Hochverfügbarkeitsmethode für das Upgrade auf eine neue NetScaler AMI-Instanz zu verwenden, führen Sie die folgenden Aufgaben aus:

- Erstellen Sie eine neue Instanz mit dem gewünschten EC2-Instanztyp, der Software-Edition, dem Durchsatz oder der Softwareversion vom AWS Marketplace.
- Konfigurieren Sie Hochverfügbarkeit zwischen der alten Instanz (die aktualisiert werden soll) und der neuen Instanz. Nachdem die Hochverfügbarkeit zwischen der alten und der neuen Instanz konfiguriert wurde, wird die Konfiguration von der alten Instanz mit der neuen Instanz synchronisiert.
- Erzwingen Sie ein HA-Failover von der alten Instanz auf die neue Instanz. Dadurch wird die neue Instanz primär und beginnt, Datenverkehr zu empfangen.
- Stoppen und rekonfigurieren oder entfernen Sie die alte Instanz aus AWS.

## Voraussetzungen und zu berücksichtigende Punkte

- Stellen Sie sicher, dass Sie verstehen, wie Hochverfügbarkeit zwischen zwei NetScaler VPX-Instanzen auf AWS funktioniert. Weitere Informationen zur Hochverfügbarkeitskonfiguration zwischen zwei NetScaler VPX-Instanzen auf AWS finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.
- Sie müssen die neue Instanz in derselben Verfügbarkeitszone wie die alte Instanz erstellen, mit exakt derselben Sicherheitsgruppe und demselben Subnetz.
- Für die Einrichtung der Hochverfügbarkeit sind Zugriffs- und geheime Schlüssel erforderlich, die dem AWS Identity and Access Management (IAM)-Konto des Benutzers für beide Instanzen zugeordnet sind. Wenn die korrekten Schlüsselinformationen beim Erstellen von VPX-Instanzen nicht verwendet werden, schlägt die HA-Einrichtung fehl. Weitere Informationen zum Erstellen eines IAM-Kontos für eine VPX-Instanz finden Sie unter Voraussetzungen.
    - Sie müssen die EC2-Konsole verwenden, um die neue Instanz zu erstellen. Sie können den AWS 1-Click-Launch nicht verwenden, da er die Zugriffs- und geheimen Schlüssel nicht als Eingabe akzeptiert.
    - Die neue Instanz darf nur eine ENI-Schnittstelle haben.

Um eine NetScaler VPX-Instanz mithilfe einer Hochverfügbarkeitskonfiguration zu aktualisieren, führen Sie die folgenden Schritte aus:

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

1. Konfigurieren Sie Hochverfügbarkeit zwischen der alten und der neuen Instanz. Um Hochverfügbarkeit zwischen zwei NetScaler VPX-Instanzen zu konfigurieren, geben Sie an der Eingabeaufforderung jeder Instanz Folgendes ein:

   - `add ha node <nodeID> <IPaddress of the node to be added>`
   - `save config`

   **Beispiel**:

   Geben Sie an der Eingabeaufforderung der alten Instanz Folgendes ein:

   ```
   add ha node 30 192.0.2.30

   Done
   ```

   Geben Sie an der Eingabeaufforderung der neuen Instanz Folgendes ein:

   ```
   add ha node 10 192.0.2.10

   Done
   ```

   Beachten Sie Folgendes:

   - In der HA-Einrichtung ist die alte Instanz der primäre Knoten und die neue Instanz der sekundäre Knoten.
   - Die NSIP-IP-Adresse wird nicht von der alten Instanz auf die neue Instanz kopiert. Daher hat Ihre neue Instanz nach dem Upgrade eine andere Verwaltungs-IP-Adresse als die vorherige.
   - Das `nsroot`-Kontopasswort der neuen Instanz wird nach der HA-Synchronisierung auf das der alten Instanz gesetzt.

   Weitere Informationen zur Hochverfügbarkeitskonfiguration zwischen zwei NetScaler VPX-Instanzen auf AWS finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.

2. Erzwingen Sie ein HA-Failover. Um ein Failover in einer Hochverfügbarkeitskonfiguration zu erzwingen, geben Sie an der Eingabeaufforderung einer der Instanzen Folgendes ein:

   ```
   force HA failover
   ```

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

Als Ergebnis des erzwungenen Failovers werden die ENIs der alten Instanz auf die neue Instanz migriert, und der Datenverkehr fließt über die neue Instanz (den neuen primären Knoten). Die alte Instanz (der neue sekundäre Knoten) wird neu gestartet.

Wenn die folgende Warnmeldung angezeigt wird, geben Sie N ein, um den Vorgang abzubrechen:

```
[WARNING]:Force Failover may cause configuration loss, peer health not
optimum. Reason(s):

HA version mismatch

HA heartbeats not seen on some interfaces

Please confirm whether you want force-failover (Y/N)?
```

Die Warnmeldung wird angezeigt, da die Systemsoftware der beiden VPX-Instanzen nicht HA-kompatibel ist. Infolgedessen kann die Konfiguration der alten Instanz bei einem erzwungenen Failover nicht automatisch mit der neuen Instanz synchronisiert werden.

Im Folgenden wird die Problemumgehung für dieses Problem beschrieben:

a. Geben Sie an der NetScaler-Shell-Eingabeaufforderung der alten Instanz den folgenden Befehl ein, um eine Sicherung der Konfigurationsdatei (`ns.conf`) zu erstellen:

   `copy /nsconfig/ns.conf to /nsconfig/ns.conf.bkp`

b. Entfernen Sie die folgende Zeile aus der Sicherungskonfigurationsdatei (`ns.conf.bkp`):

   - `set ns config -IPAddress <IP> -netmask <MASK>`

   Zum Beispiel, `set ns config -IPAddress 192.0.2.10 -netmask 255.255.255.0`

c. Kopieren Sie die Sicherungskonfigurationsdatei der alten Instanz (`ns.conf.bkp`) in das Verzeichnis `/nsconfig` der neuen Instanz.

d. Geben Sie an der NetScaler-Shell-Eingabeaufforderung der neuen Instanz den folgenden Befehl ein, um die Konfigurationsdatei der alten Instanz (`ns.conf.bkp`) auf der neuen Instanz zu laden:

   - `batch -f /nsconfig/ns.conf.bkp`

e. Speichern Sie die Konfiguration auf der neuen Instanz.

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

- `save conifg`

f. Geben Sie an der Eingabeaufforderung eines der Knoten den folgenden Befehl ein, um ein Failover zu erzwingen, und geben Sie dann Y für die Warnmeldung ein, um den erzwungenen Failover-Vorgang zu bestätigen:

- `force ha failover`

**Beispiel**:

```
        > force ha failover



WARNING]:Force Failover may cause configuration loss, peer health not
optimum.

        Reason(s):

        HA version mismatch

        HA heartbeats not seen on some interfaces

        Please confirm whether you want force-failover (Y/N)? Y
```

3. Entfernen Sie die HA-Konfiguration, sodass die beiden Instanzen nicht mehr in einer HA-Konfiguration sind. Entfernen Sie zuerst die HA-Konfiguration vom sekundären Knoten und dann die HA-Konfiguration vom primären Knoten.

   Um eine HA-Konfiguration zwischen zwei NetScaler VPX-Instanzen zu entfernen, geben Sie an der Eingabeaufforderung jeder Instanz Folgendes ein:

```
> remove ha node \<nodeID\>

>  save config
```

   Weitere Informationen zur Hochverfügbarkeitskonfiguration zwischen zwei VPX-Instanzen auf AWS finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.

   **Beispiel**:

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

Geben Sie an der Eingabeaufforderung der alten Instanz (neuer sekundärer Knoten) Folgendes ein:

```
> remove ha node 30

  Done

> save config

  Done
```

Geben Sie an der Eingabeaufforderung der neuen Instanz (neuer primärer Knoten) Folgendes ein:

```
> remove ha node 10

  Done

> save config

  Done
```

## Fehlerbehebung bei einer VPX-Instanz auf AWS

Amazon bietet keinen Konsolenzugriff auf eine NetScaler VPX-Instanz. Zur Fehlerbehebung müssen Sie die AWS-GUI verwenden, um das Aktivitätsprotokoll anzuzeigen. Sie können nur Fehler beheben, wenn das Netzwerk verbunden ist. Um das Systemprotokoll einer Instanz anzuzeigen, klicken Sie mit der rechten Maustaste auf die Instanz und wählen Sie „Systemprotokoll“.

NetScaler bietet Unterstützung für über den AWS Marketplace lizenzierte NetScaler VPX-Instanzen (Utility-Lizenz mit stündlicher Gebühr) auf AWS. Um einen Supportfall zu eröffnen, suchen Sie Ihre AWS-Kontonummer und Ihren Support-PIN-Code und rufen Sie den NetScaler-Support an. Sie werden auch nach Ihrem Namen und Ihrer E-Mail-Adresse gefragt. Um den Support-PIN zu finden, melden Sie sich bei der VPX-GUI an und navigieren Sie zur Systemseite.

Hier ist ein Beispiel einer Systemseite, die den Support-PIN anzeigt.

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

# AWS FAQs

- **Unterstützt eine NetScaler VPX-Instanz die verschlüsselten Volumes in AWS?**

  Verschlüsselung und Entschlüsselung erfolgen auf Hypervisor-Ebene und funktionieren daher nahtlos mit jeder Instanz. Weitere Informationen zu den verschlüsselten Volumes finden Sie im folgenden AWS-Dokument:

  `<https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html>`

- **Wie kann eine NetScaler VPX-Instanz am besten in AWS bereitgestellt werden?**

  Sie können eine NetScaler VPX-Instanz in AWS auf eine der folgenden Arten bereitstellen:

  - AWS CloudFormation Template (CFT) im AWS Marketplace
  - NetScaler ADM
  - AWS Quick Starts
  - Citrix® AWS CFTs in GitHub
  - Citrix Terraform-Skripte in GitHub
  - Citrix Ansible Playbooks in GitHub
  - AWS EC2 Start-Workflow

  Sie können eine der aufgeführten Optionen basierend auf dem von Ihnen verwendeten Automatisierungstool auswählen.

  Weitere Details zu den Optionen finden Sie unter NetScaler VPX auf AWS.

- **Wie wird eine NetScaler VPX-Instanz in AWS aktualisiert?**

  Um die NetScaler VPX-Instanz in AWS zu aktualisieren, können Sie die Systemsoftware aktualisieren oder auf ein neues NetScaler VPX Amazon Machine Image (AMI) aktualisieren, indem Sie die Vorgehensweise unter Upgrade a NetScaler VPX instance on AWS befolgen.

  Die empfohlene Methode zum Aktualisieren einer NetScaler VPX-Instanz ist die Verwendung des ADM-Dienstes, indem Sie die Vorgehensweise unter Use jobs to upgrade NetScaler instances befolgen.

- **Wie lange dauert der HA-Failover für NetScaler VPX in AWS?**

  - Der HA-Failover von NetScaler VPX innerhalb der AWS-Verfügbarkeitszone dauert etwa 3 Sekunden.

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

    - Der HA-Failover von NetScaler VPX über AWS-Verfügbarkeitszonen hinweg dauert etwa 5 Sekunden.

- **Welche Art von Support wird für NetScaler VPX Marketplace-Abonnementkunden bereitgestellt, die die technische Support-PIN angeben?**

  Standardmäßig wird der Dienst „Select for Software“ Kunden bereitgestellt, die die technische Support-PIN angeben.

- **Müssen wir bei der Bereitstellung von** High availability across different zones using Elastic IP **mehrere IP-Sets für jede Anwendung erstellen?**

  Ja. Wenn es mehrere Anwendungen mit mehreren VIPs gibt, die mehreren EIPs zugeordnet sind, sind mehrere IP-Sets erforderlich. Daher werden beim HA-Failover alle primären VIP-Zuordnungen von EIPs auf sekundäre (neue primäre) VIPs geändert.

- **Warum ist der INC-Modus bei Hochverfügbarkeit über verschiedene Zonenbereitstellungen hinweg aktiviert?**

  HA-Paare über Verfügbarkeitszonen hinweg befinden sich in verschiedenen Netzwerken. Für die HA-Synchronisierung darf die Netzwerkkonfiguration nicht synchronisiert werden. Dies wird durch die Aktivierung des INC-Modus auf dem HA-Paar erreicht.

- **Kann ein HA-Knoten in einer Verfügbarkeitszone mit Backend-Servern in einer anderen Verfügbarkeitszone kommunizieren, vorausgesetzt, diese Verfügbarkeitszonen befinden sich im selben VPC?**

  Ja, Subnetze in verschiedenen Verfügbarkeitszonen desselben VPC sind erreichbar, indem eine zusätzliche Route hinzugefügt wird, die über SNIP auf das Backend-Server-Subnetz verweist. Wenn beispielsweise das SNIP-Subnetz des ADC in AZ1 192.168.3.0/24 und das Backend-Server-Subnetz in AZ2 192.168.6.0/24 ist, muss eine Route in der in AZ1 vorhandenen NetScaler-Appliance als 192.168.6.0 255.255.255.0 192.168.3.1 hinzugefügt werden.

- **Können** High availability across different zones using Elastic IP **und** High availability across different zones using Private IP **Bereitstellungen zusammenarbeiten?**

  Ja, beide Konfigurationen können auf demselben HA-Paar angewendet werden.

- **Bei der Bereitstellung von** Hochverfügbarkeit über verschiedene Zonen hinweg mit privater IP**, wenn es in einer VPC mehrere Subnetze mit mehreren Routing-Tabellen gibt, wie weiß ein sekundärer Knoten in einem HA-Paar, welche Routing-Tabelle während eines HA-Failovers überprüft werden muss?**

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

Der sekundäre Knoten kennt die primären NICs und durchsucht alle Routing-Tabellen in einer VPC.

- **Wie groß ist die `/var`-Partition bei Verwendung des Standard-Images für VPX auf AWS? Wie kann der Festplattenspeicher erhöht werden?**

  Die Größe der Root-Festplatte ist auf 20 GB begrenzt, um das Festplatten-Image klein zu halten.

  Wenn Sie den `/var/core/`- oder den `/var/crash/`-Verzeichnisspeicherplatz erhöhen möchten, schließen Sie eine zusätzliche Festplatte an. Um die `/var`-Größe zu erhöhen, müssen Sie derzeit eine zusätzliche Festplatte anschließen und einen symbolischen Link zu `/var` erstellen, nachdem Sie die kritischen Inhalte auf die neue Festplatte kopiert haben.

- **Wie viele Paket-Engines werden aktiviert und vCPUs zugewiesen?**

  Die Paket-Engines (PEs) sind durch die Anzahl der lizenzierten vCPUs begrenzt. Die NetScaler-Daemons sind nicht an eine bestimmte vCPU gebunden und können auf jeder der Nicht-PE-vCPUs ausgeführt werden. Laut AWS ist die C5.9xlarge eine 36-vCPU-Instanz mit 72 GB Arbeitsspeicher. Bei der Pooled-Lizenzierung wird die NetScaler VPX-Instanz mit der maximalen Anzahl von PEs bereitgestellt. In diesem Fall laufen 19 PEs auf den Kernen 1–19. Die ADC-Verwaltungsprozesse laufen jedoch auf den CPUs 20–31.

- **Wie wählt man die richtige AWS-Instanz für ADC aus?**

  a. Verstehen Sie Ihren Anwendungsfall und Ihre Anforderungen wie Durchsatz, PPS, SSL-Anforderung und durchschnittliche Paketgröße.

  b. Wählen Sie das richtige ADC-Angebot und die Lizenzierung, die Ihren Anforderungen entsprechen, wie z. B. VPX-Bandbreitenangebote oder vCPU-basierte Lizenzierung.

  c. Wählen Sie basierend auf dem gewählten Angebot die AWS-Instanz aus.

  **Beispiel:**

  Eine 5-Gbit/s-Lizenz ermöglicht 5 Datenpaket-Engines. Daher beträgt die vCPU-Anforderung 6 (5+1 für die Verwaltung). Eine 6-vCPU-Instanz ist jedoch nicht verfügbar. Eine 8-vCPU-Instanz ist also ausreichend, um diesen Durchsatz zu erreichen, vorausgesetzt, Sie wählen ein Netzwerk, das eine 5-Gbit/s-Bandbreite unterstützt. Sie müssen beispielsweise m5.2xlarge für eine 5-Gbit/s-Bandbreitenlizenz wählen, um die maximale PE-Zuweisung für die 5-Gbit/s-Lizenz zu ermöglichen. Wenn Sie jedoch eine vCPU-Lizenz verwenden, die nicht durch den Durchsatz begrenzt ist, können Sie möglicherweise einen 5-Gbit/s-Durchsatz mit der m5.xlarge-Instanz selbst erzielen.

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

- **Ist die Bereitstellung mit drei NICs und drei Subnetzen für ADC in AWS obligatorisch?**

  Die Bereitstellung mit drei NICs und drei Subnetzen ist die empfohlene Bereitstellung, wobei jeweils eine für das Management-, Client- und Servernetzwerk vorgesehen ist. Diese Bereitstellung bietet eine bessere Datenverkehrsisolierung und VPX-Leistung. Zwei NICs und zwei Subnetze sowie eine NIC und ein Subnetz sind die anderen verfügbaren Optionen. Es wird nicht empfohlen, dass mehrere NICs ein Subnetz in AWS gemeinsam nutzen, wie z. B. eine Bereitstellung mit zwei NICs und einem Subnetz. Dieses Szenario kann Netzwerkprobleme wie asymmetrisches Routing verursachen. Weitere Informationen finden Sie unter Best Practices für die Konfiguration von Netzwerkschnittstellen in AWS.

- **Warum zeigt ein ENA-Treiber in AWS immer eine Verbindungsgeschwindigkeit von 1 Gbit/s (1/1) an, unabhängig von den Netzwerkfunktionen der Instanz?**

  Die angezeigte Geschwindigkeit eines AWS Elastic Network Adapters (ENA) wird oft als 1 Gbit/s (1/1) angezeigt, unabhängig vom ausgewählten Instanztyp. Dies liegt daran, dass die angezeigte Geschwindigkeit nicht direkt die tatsächliche Netzwerkleistung widerspiegelt. Im Gegensatz zu herkömmlichen Netzwerkschnittstellen können sich ENA-Geschwindigkeiten dynamisch an die Anforderungen und die Arbeitslast der Instanz anpassen. Die wahre Netzwerkleistung wird hauptsächlich durch den Instanztyp und die Größe bestimmt. Daher kann der tatsächliche Netzwerkdurchsatz je nach spezifischem Instanztyp und der aktuellen Netzwerklast erheblich variieren.

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

# Bereitstellen einer NetScaler VPX-Instanz in Microsoft Azure

Wenn Sie eine NetScaler VPX-Instanz in Microsoft Azure Resource Manager (ARM) bereitstellen, können Sie beide der folgenden Funktionssätze verwenden, um Ihre Geschäftsanforderungen zu erfüllen:

- Azure Cloud-Computing-Funktionen
- NetScaler Lastenausgleichs- und Datenverkehrsmanagement-Funktionen

Sie können NetScaler VPX-Instanzen in ARM entweder als eigenständige Instanzen oder als Hochverfügbarkeitspaare im Aktiv-Standby-Modus bereitstellen.

Sie können eine NetScaler VPX-Instanz in Microsoft Azure auf zwei Arten bereitstellen:

- Über den Azure Marketplace. Die virtuelle NetScaler VPX-Appliance ist als Image im Microsoft Azure Marketplace verfügbar.
- Mithilfe der NetScaler Azure Resource Manager (ARM) JSON-Vorlage, die auf GitHub verfügbar ist. Weitere Informationen finden Sie im GitHub-Repository für NetScaler-Lösungsvorlagen.

**HINWEIS:**

Azure beschränkt den Zugriff auf Datenverkehr, der von außerhalb von Azure stammt, und blockiert diesen. Um den Zugriff zu ermöglichen, aktivieren Sie den Dienst oder Port, indem Sie eine eingehende Regel in der Netzwerksicherheitsgruppe hinzufügen, die an die NIC der VM angehängt ist, an die eine öffentliche IP-Adresse angehängt ist. Weitere Informationen finden Sie in der Azure-Dokumentation zu eingehenden NAT-Regeln.

## Voraussetzung

Sie benötigen einige Vorkenntnisse, bevor Sie eine NetScaler VPX-Instanz in Azure bereitstellen.

- Vertrautheit mit der Azure-Terminologie und Netzwerkdetails. Weitere Informationen finden Sie unter Azure-Terminologie.

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

- Kenntnisse einer NetScaler-Appliance. Detaillierte Informationen zur NetScaler-Appliance finden Sie unter NetScaler
- Kenntnisse der NetScaler-Netzwerkfunktionen. Siehe das Thema Netzwerkfunktionen.

## So funktioniert eine NetScaler VPX-Instanz in Azure

Bei einer lokalen Bereitstellung benötigt eine NetScaler VPX-Instanz mindestens drei IP-Adressen:

- Management-IP-Adresse, genannt NSIP-Adresse
- Subnetz-IP-Adresse (SNIP) für die Kommunikation mit der Serverfarm
- Virtuelle Server-IP-Adresse (VIP) zum Akzeptieren von Clientanfragen

Weitere Informationen finden Sie unter Netzwerkarchitektur für NetScaler VPX-Instanzen in Microsoft Azure.

**HINWEIS:**

Die NetScaler VPX-Instanz unterstützt sowohl Intel- als auch AMD-Prozessoren. VPX-virtuelle Appliances können auf jedem Instanztyp bereitgestellt werden, der zwei oder mehr virtualisierte Kerne und mehr als 2 GB Arbeitsspeicher besitzt. Weitere Informationen zu den Systemanforderungen finden Sie im NetScaler VPX-Datenblatt.

Bei einer Azure-Bereitstellung können Sie eine NetScaler VPX-Instanz in Azure auf drei Arten bereitstellen:

- Multi-NIC-Multi-IP-Architektur
- Single-NIC-Multi-IP-Architektur
- Single-NIC-Single-IP

Je nach Ihren Anforderungen können Sie jeden dieser unterstützten Architekturtypen verwenden.

### Multi-NIC-Multi-IP-Architektur

Bei diesem Bereitstellungstyp können Sie mehr als eine Netzwerkschnittstelle (NIC) an eine VPX-Instanz anschließen. Jede NIC kann eine oder mehrere IP-Konfigurationen haben – statische oder dynamische öffentliche und private IP-Adressen, die ihr zugewiesen sind.

Weitere Informationen finden Sie in den folgenden Anwendungsfällen:

- Einrichten einer Hochverfügbarkeitskonfiguration mit mehreren IP-Adressen und NICs

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

- Einrichten einer Hochverfügbarkeitskonfiguration mit mehreren IP-Adressen und NICs mithilfe von PowerShell-Befehlen

**HINWEIS:**

Um MAC-Verschiebungen und Schnittstellenstummschaltungen in Azure-Umgebungen zu vermeiden, empfiehlt Citrix, für jede Datenschnittstelle (ohne Tag) der NetScaler VPX-Instanz ein VLAN zu erstellen und die primäre IP der NIC in Azure zu binden. Weitere Informationen finden Sie im Artikel CTX224626.

### Einzel-NIC-Multi-IP-Architektur

Bei diesem Bereitstellungstyp ist eine Netzwerkschnittstelle (NIC) mit mehreren IP-Konfigurationen verknüpft – statische oder dynamische öffentliche und private IP-Adressen sind ihr zugewiesen. Weitere Informationen finden Sie in den folgenden Anwendungsfällen:

- Konfigurieren mehrerer IP-Adressen für eine eigenständige NetScaler VPX-Instanz
- Konfigurieren mehrerer IP-Adressen für eine eigenständige NetScaler VPX-Instanz mithilfe von PowerShell-Befehlen

### Einzel-NIC-Einzel-IP

Bei diesem Bereitstellungstyp ist eine Netzwerkschnittstelle (NIC) mit einer einzelnen IP-Adresse verknüpft, die zur Ausführung der Funktionen von NSIP, SNIP und VIP verwendet wird.

Weitere Informationen finden Sie unter Konfigurieren einer eigenständigen NetScaler VPX-Instanz.

**HINWEIS:**

Der Einzel-IP-Modus ist nur in Azure-Bereitstellungen verfügbar. Dieser Modus ist für eine NetScaler VPX-Instanz vor Ort, auf AWS oder in anderen Bereitstellungstypen nicht verfügbar.

## NetScaler VPX-Lizenzierung

Eine NetScaler VPX-Instanz in Azure erfordert eine gültige Lizenz. Die für NetScaler VPX-Instanzen, die in Azure ausgeführt werden, verfügbaren Lizenzierungsoptionen sind:

- **Eigene Lizenz mitbringen (BYOL)**: Um die BYOL-Option zu verwenden, führen Sie die folgenden Schritte aus:

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

- Verwenden Sie das Lizenzierungsportal auf der NetScaler®-Website, um eine gültige Lizenz zu generieren.
- Laden Sie die generierte Lizenz auf die Instanz hoch.

- **NetScaler VPX Check-in- und Check-out-Lizenz**: Dieses Lizenzierungsmodell ermöglicht es Ihnen, eine Lizenz aus einem Pool verfügbarer Lizenzen auszuchecken und sie wieder einzuchecken, wenn sie nicht mehr benötigt wird. Weitere Informationen und detaillierte Anweisungen finden Sie unter NetScaler VPX Check-in- und Check-out-Lizenz.

**HINWEIS:**

- Die Lizenzierung über Marketplace-Abonnements wird für NetScaler VPX-Instanzen in Azure nicht mehr unterstützt.
- Führen Sie einen Warmstart durch, bevor Sie Konfigurationsänderungen an der NetScaler VPX-Instanz vornehmen, um die korrekte NetScaler VPX-Lizenz zu aktivieren.

## VPX-Leistung und empfohlene Azure-Instanztypen

Für die gewünschte VPX-Leistung werden die folgenden Azure-Instanztypen empfohlen.

| VPX-LEISTUNG | AZURE-INSTANZTYPEN | | |
|---|---|---|---|
| | VPX 1 NIC/2 NIC | VPX 3 NIC | VPX BIS ZU 8 NIC |
| Bis zu 200 Mbit/s | Standard_D2s_v5 | Standard_D8s_v5 | Standard_D16_v5 |
| Bis zu 1 Gbit/s | Standard_D4s_v5 | Standard_D8s_v5 | Standard_D16_v5 |
| Bis zu 5 Gbit/s | Standard_D8ds_v5 | Standard_D8ds_v5 | Standard_D16_v5 |
| Bis zu 10 Gbit/s | Standard_D8s_v5 | Standard_D8s_v5 | Standard_D16_v5 |

**HINWEIS:**

Microsoft Azure Network Adapter (MANA) wird ab NetScaler Version 14.1-51.x und höher unterstützt. Weitere Informationen finden Sie in der Microsoft-Dokumentation.

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

## Wichtige Hinweise

- Azure unterstützt einen VPX-Durchsatz von bis zu 10 Gbit/s. Weitere Informationen finden Sie im NetScaler VPX-Datenblatt.
- Um eine optimale Leistung auf NetScaler VPX-Instanzen mit einem Durchsatz von über 1 Gbit/s zu erzielen, müssen Sie das beschleunigte Azure-Netzwerk aktivieren. Es wird empfohlen, hierfür einen Azure-Instanztyp zu verwenden, der beschleunigtes Netzwerk unterstützt. Weitere Informationen zur Konfiguration des beschleunigten Netzwerks finden Sie unter Konfigurieren einer NetScaler VPX-Instanz zur Verwendung des beschleunigten Azure-Netzwerks.
- Wenn Sie erwarten, dass Sie die virtuelle NetScaler VPX-Maschine jederzeit herunterfahren und vorübergehend die Zuordnung aufheben müssen, weisen Sie beim Erstellen der virtuellen Maschine eine statische interne IP-Adresse zu. Wenn Sie keine statische interne IP-Adresse zuweisen, weist Azure der virtuellen Maschine bei jedem Neustart möglicherweise eine andere IP-Adresse zu, und die virtuelle Maschine könnte unzugänglich werden.
- Für die Bereitstellung von Citrix Virtual Apps and Desktops kann ein virtueller VPN-Server auf einer VPX-Instanz in den folgenden Modi konfiguriert werden:
  - Basismodus, bei dem der `ICAOnly` VPN-Virtual-Server-Parameter auf ON gesetzt ist. Der Basismodus funktioniert vollständig auf einer nicht lizenzierten NetScaler VPX-Instanz.
  - SmartAccess-Modus, bei dem der `ICAOnly` VPN-Virtual-Server-Parameter auf OFF gesetzt ist. Der SmartAccess-Modus funktioniert nur für fünf NetScaler AAA-Sitzungsbenutzer auf einer nicht lizenzierten NetScaler VPX-Instanz.

**HINWEIS:**

Um die SmartControl-Funktion zu konfigurieren, müssen Sie eine Premium-Lizenz auf die NetScaler VPX-Instanz anwenden.

## IPv6-Unterstützung für NetScaler VPX-Instanz in Azure

Die eigenständige NetScaler VPX-Instanz unterstützt IPv6-Adressen in Azure. Sie können die IPv6-Adressen als VIP- und SNIP-Adressen auf der eigenständigen NetScaler VPX-Instanz in der Azure-Cloud konfigurieren.

Informationen zum Aktivieren von IPv6 in Azure finden Sie in der folgenden Azure-Dokumentation:

- Was ist IPv6 für Azure Virtual Network?
- Hinzufügen von IPv6 zu einer IPv4-Anwendung in einem virtuellen Azure-Netzwerk – Azure CLI

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

- Adresstypen

Informationen dazu, wie die NetScaler-Appliance IPv6 unterstützt, finden Sie unter Internetprotokoll Version 6.

**IPv6-Einschränkungen:**

- IPv6-Bereitstellungen in NetScaler unterstützen derzeit keine Azure-Backend-Autoskalierung.
- IPv6 wird für die NetScaler VPX HA-Bereitstellung nicht unterstützt.

## Einschränkungen

Der Betrieb der NetScaler VPX Lastverteilungslösung auf ARM unterliegt den folgenden Einschränkungen:

- Die Azure-Architektur unterstützt die folgenden NetScaler-Funktionen nicht:
  - Gratuitous ARP (GARP)
  - L2-Modus
  - Tagged VLAN
  - Dynamisches Routing
  - virtuelle MAC
  - USIP
  - Clustering
- Bei Verwendung einer NetScaler VPX-Instanz mit einem Durchsatz von mehr als 3 Gbit/s stimmt der tatsächliche Netzwerkdurchsatz möglicherweise nicht mit dem in der Lizenz der Instanz angegebenen Durchsatz überein. Andere Funktionen wie der SSL-Durchsatz und die SSL-Transaktionen pro Sekunde können sich jedoch verbessern.
- Die Bereitstellungs-ID, die Azure während der Bereitstellung virtueller Maschinen generiert, ist für den Benutzer in ARM nicht sichtbar. Sie können die Bereitstellungs-ID nicht verwenden, um die NetScaler VPX-Appliance auf ARM bereitzustellen.

## Azure-Terminologie

Einige der in der NetScaler VPX Azure-Dokumentation verwendeten Azure-Begriffe sind unten aufgeführt.

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

1. Azure Load Balancer – Ein Azure Load Balancer ist eine Ressource, die eingehenden Datenverkehr auf Computer in einem Netzwerk verteilt. Der Datenverkehr wird auf virtuelle Maschinen verteilt, die in einem Load-Balancer-Set definiert sind. Ein Load Balancer kann extern oder internetseitig sein, oder er kann intern sein.
2. Azure Resource Manager (ARM) – ARM ist das neue Verwaltungs-Framework für Dienste in Azure. Azure Load Balancer wird mithilfe von ARM-basierten APIs und Tools verwaltet.
3. Back-End-Adresspool – Dies sind IP-Adressen, die der NIC (Netzwerkschnittstellenkarte) der virtuellen Maschine zugeordnet sind, auf die die Last verteilt wird.
4. BLOB - Binary Large Object – Jedes binäre Objekt wie eine Datei oder ein Bild, das im Azure-Speicher gespeichert werden kann.
5. Front-End-IP-Konfiguration – Ein Azure Load Balancer kann eine oder mehrere Front-End-IP-Adressen enthalten, auch bekannt als virtuelle IPs (VIPs). Diese IP-Adressen dienen als Eingang für den Datenverkehr.
6. Instanzebene öffentliche IP (ILPIP) – Eine ILPIP ist eine öffentliche IP-Adresse, die Sie direkt Ihrer virtuellen Maschine oder Rolleninstanz zuweisen können, anstatt dem Cloud-Dienst, in dem sich Ihre virtuelle Maschine oder Rolleninstanz befindet. Dies ersetzt nicht die VIP (virtuelle IP), die Ihrem Cloud-Dienst zugewiesen ist. Vielmehr ist es eine zusätzliche IP-Adresse, die Sie verwenden können, um sich direkt mit Ihrer virtuellen Maschine oder Rolleninstanz zu verbinden.

   **HINWEIS:**

   Früher wurde eine ILPIP als PIP bezeichnet, was für öffentliche IP steht.

7. Eingehende NAT-Regeln – Dies enthält Regeln, die einen öffentlichen Port auf dem Load Balancer einem Port für eine bestimmte virtuelle Maschine im Back-End-Adresspool zuordnen.
8. IP-Konfiguration – Sie kann als ein IP-Adresspaar (öffentliche IP und private IP) definiert werden, das einer einzelnen NIC zugeordnet ist. In einer IP-Konfiguration kann die öffentliche IP-Adresse NULL sein. Jede NIC kann mehrere IP-Konfigurationen zugeordnet haben, bis zu 255.
9. Lastenausgleichsregeln – Eine Regeleigenschaft, die eine gegebene Front-End-IP- und Port-Kombination einem Satz von Back-End-IP-Adressen und Port-Kombinationen zuordnet. Mit einer einzigen Definition einer Load-Balancer-Ressource können Sie mehrere Lastenausgleichsregeln definieren, wobei jede Regel eine Kombination aus einer Front-End-IP

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

und einem Port sowie einer Back-End-IP und einem Port widerspiegelt, die virtuellen Maschinen zugeordnet sind.

10. Netzwerksicherheitsgruppe – Enthält eine Liste von Zugriffssteuerungslisten (ACL)-Regeln, die den Netzwerkverkehr zu Ihren virtuellen Maschineninstanzen in einem virtuellen Netzwerk zulassen oder verweigern. NSGs können entweder Subnetzen oder einzelnen virtuellen Maschineninstanzen innerhalb dieses Subnetzes zugeordnet werden. Wenn eine Netzwerksicherheitsgruppe einem Subnetz zugeordnet ist, gelten die ACL-Regeln für alle virtuellen Maschineninstanzen in diesem Subnetz. Darüber hinaus kann der Datenverkehr zu einer einzelnen virtuellen Maschine weiter eingeschränkt werden, indem eine Netzwerksicherheitsgruppe direkt dieser virtuellen Maschine zugeordnet wird.
11. Private IP-Adressen – Werden für die Kommunikation innerhalb eines virtuellen Azure-Netzwerks und Ihres lokalen Netzwerks verwendet, wenn Sie ein VPN-Gateway nutzen, um Ihr Netzwerk auf Azure zu erweitern. Private IP-Adressen ermöglichen Azure-Ressourcen die Kommunikation mit anderen Ressourcen in einem virtuellen Netzwerk oder einem lokalen Netzwerk über ein VPN-Gateway oder eine ExpressRoute-Verbindung, ohne eine über das Internet erreichbare IP-Adresse zu verwenden. Im Azure Resource Manager-Bereitstellungsmodell ist eine private IP-Adresse den folgenden Typen von Azure-Ressourcen zugeordnet: virtuelle Maschinen, interne Lastenausgleichsmodule (ILBs) und Anwendungsgateways.
12. Probes – Dies enthält Integritätstests, die verwendet werden, um die Verfügbarkeit von Instanzen virtueller Maschinen im Backend-Adresspool zu überprüfen. Wenn eine bestimmte virtuelle Maschine für einige Zeit nicht auf Integritätstests reagiert, wird sie aus der Datenverkehrsverteilung entfernt. Probes ermöglichen es Ihnen, den Zustand virtueller Instanzen zu überwachen. Wenn ein Integritätstest fehlschlägt, wird die virtuelle Instanz automatisch aus der Rotation genommen.
13. Öffentliche IP-Adressen (PIP) – PIP wird für die Kommunikation mit dem Internet verwendet, einschließlich öffentlicher Azure-Dienste, und ist virtuellen Maschinen, Internet-orientierten Lastenausgleichsmodulen, VPN-Gateways und Anwendungsgateways zugeordnet.
14. Region – Ein Bereich innerhalb einer Geografie, der keine nationalen Grenzen überschreitet und ein oder mehrere Rechenzentren enthält. Preise, regionale Dienste und Angebotstypen werden auf Regionsebene angezeigt. Eine Region wird typischerweise mit einer anderen Region gepaart, die bis zu mehrere hundert Meilen entfernt sein kann, um ein regionales Paar zu bilden. Regionale Paare können als Mechanismus für Notfallwiederherstellung und Hochverfügbarkeitsszenarien verwendet werden. Wird auch allgemein als Standort bezeichnet.

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

15. Ressourcengruppe – Ein Container im Resource Manager enthält zusammengehörige Ressourcen für eine Anwendung. Die Ressourcengruppe kann alle Ressourcen für eine Anwendung oder nur diejenigen Ressourcen enthalten, die logisch zusammengefasst sind.
16. Speicherkonto – Ein Azure-Speicherkonto bietet Ihnen Zugriff auf die Azure Blob-, Warteschlangen-, Tabellen- und Dateidienste in Azure Storage. Ihr Speicherkonto stellt den eindeutigen Namespace für Ihre Azure-Speicherdatenobjekte bereit.
17. Virtuelle Maschine – Die Softwareimplementierung eines physischen Computers, der ein Betriebssystem ausführt. Mehrere virtuelle Maschinen können gleichzeitig auf derselben Hardware ausgeführt werden. In Azure sind virtuelle Maschinen in verschiedenen Größen verfügbar.
18. Virtuelles Netzwerk – Ein virtuelles Azure-Netzwerk ist eine Darstellung Ihres eigenen Netzwerks in der Cloud. Es ist eine logische Isolation der Azure-Cloud, die Ihrem Abonnement gewidmet ist. Sie können die IP-Adressblöcke, DNS-Einstellungen, Sicherheitsrichtlinien und Routingtabellen innerhalb dieses Netzwerks vollständig steuern. Sie können Ihr VNet auch weiter in Subnetze segmentieren und virtuelle Azure IaaS-Maschinen und Cloud-Dienste (PaaS-Rolleninstanzen) starten. Zusätzlich können Sie das virtuelle Netzwerk über eine der in Azure verfügbaren Konnektivitätsoptionen mit Ihrem lokalen Netzwerk verbinden. Im Wesentlichen können Sie Ihr Netzwerk auf Azure erweiternieren, mit vollständiger Kontrolle über IP-Adressblöcke und dem Vorteil der von Azure bereitgestellten Unternehmensskalierung.

## Netzwerkarchitektur für NetScaler VPX-Instanzen auf Microsoft Azure

Im Azure Resource Manager (ARM) befindet sich eine virtuelle NetScaler VPX-Maschine (VM) in einem virtuellen Netzwerk. Eine einzelne Netzwerkschnittstelle kann in einem bestimmten Subnetz des virtuellen Netzwerks erstellt und an die VPX-Instanz angehängt werden. Sie können den Netzwerkverkehr zu und von einer VPX-Instanz in einem virtuellen Azure-Netzwerk mit einer Netzwerksicherheitsgruppe filtern. Eine Netzwerksicherheitsgruppe enthält Sicherheitsregeln, die eingehenden oder ausgehenden Netzwerkverkehr zu oder von einer VPX-Instanz zulassen oder verweigern. Weitere Informationen finden Sie unter Sicherheitsgruppen.

Die Netzwerksicherheitsgruppe filtert die Anfragen an die NetScaler VPX-Instanz, und die VPX-Instanz sendet diese an die Server. Die Antwort eines Servers folgt dem gleichen Pfad in umgekehrter Richtung. Die Netzwerksicherheitsgruppe kann so konfiguriert werden, dass sie eine

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

einzelne VPX-VM filtert oder, mit Subnetzen und virtuellen Netzwerken, den Datenverkehr bei der Bereitstellung mehrerer VPX-Instanzen filtert.

Die NIC enthält Netzwerkkonfigurationsdetails wie das virtuelle Netzwerk, Subnetze, interne IP-Adresse und öffentliche IP-Adresse.

Im ARM ist es gut, die folgenden IP-Adressen zu kennen, die für den Zugriff auf VMs verwendet werden, die mit einer einzelnen NIC und einer einzelnen IP-Adresse bereitgestellt wurden:

- Die öffentliche IP-Adresse (PIP) ist die direkt auf der virtuellen NIC der NetScaler® VM konfigurierte, dem Internet zugewandte IP-Adresse. Dies ermöglicht Ihnen den direkten Zugriff auf eine VM aus dem externen Netzwerk.
- Die NetScaler IP-Adresse (auch bekannt als NSIP) ist die auf der VM konfigurierte interne IP-Adresse. Sie ist nicht routingfähig.
- Die virtuelle IP-Adresse (VIP) wird unter Verwendung der NSIP und einer Portnummer konfiguriert. Clients greifen über die PIP-Adresse auf NetScaler-Dienste zu, und wenn die Anfrage die NIC der NetScaler VPX™ VM oder den Azure Load Balancer erreicht, wird die VIP in die interne IP (NSIP) und interne Portnummer übersetzt.
- Die interne IP-Adresse ist die private interne IP-Adresse der VM aus dem Adressraumpool des virtuellen Netzwerks. Diese IP-Adresse kann vom externen Netzwerk aus nicht erreicht werden. Diese IP-Adresse ist standardmäßig dynamisch, es sei denn, Sie legen sie als statisch fest. Der Datenverkehr aus dem Internet wird gemäß den in der Netzwerksicherheitsgruppe erstellten Regeln an diese Adresse weitergeleitet. Die Netzwerksicherheitsgruppe integriert sich mit der NIC, um den richtigen Datenverkehrstyp selektiv an den richtigen Port auf der NIC zu senden, was von den auf der VM konfigurierten Diensten abhängt.

Die folgende Abbildung zeigt, wie der Datenverkehr von einem Client zu einem Server über eine im ARM bereitgestellte NetScaler VPX-Instanz fließt.

## Datenfluss durch Netzwerkadressübersetzung

Sie können auch eine öffentliche IP-Adresse (PIP) für Ihre NetScaler VPX-Instanz (Instanzebene) anfordern. Wenn Sie diese direkte PIP auf VM-Ebene verwenden, müssen Sie keine eingehenden und ausgehenden Regeln definieren, um den Netzwerkverkehr abzufangen. Die eingehende Anfrage aus dem Internet wird direkt auf der VM empfangen. Azure führt eine Netzwerkadressübersetzung (NAT) durch und leitet den Datenverkehr an die interne IP-Adresse der VPX-Instanz weiter.

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

Die folgende Abbildung zeigt, wie Azure eine Netzwerkadressübersetzung durchführt, um die interne NetScaler IP-Adresse zuzuordnen.

In diesem Beispiel ist die der Netzwerksicherheitsgruppe zugewiesene öffentliche IP-Adresse 140.x.x.x und die interne IP-Adresse 10.x.x.x. Wenn die Eingangs- und Ausgangsregeln definiert sind, wird der öffentliche HTTP-Port 80 als der Port definiert, an dem die Clientanfragen empfangen werden, und ein entsprechender privater Port, 10080, wird als der Port definiert, an dem die NetScaler VPX-Instanz lauscht. Die Clientanfrage wird an der öffentlichen IP-Adresse (140.x.x.x) empfangen. Azure führt eine Netzwerkadressübersetzung durch, um die PIP der internen IP-Adresse 10.x.x.x auf Port 10080 zuzuordnen, und leitet die Clientanfrage weiter.

**HINWEIS:**

NetScaler VPX VMs in Hochverfügbarkeit werden von externen oder internen Lastenausgleichsmodulen gesteuert, die Eingangsregeln definiert haben, um den Lastenausgleichsverkehr zu steuern. Der externe Datenverkehr wird zuerst von diesen Lastenausgleichsmodulen abgefangen, und der Datenverkehr wird gemäß den konfigurierten Lastenausgleichsregeln umgeleitet, die Backend-Pools, NAT-Regeln und Integritätstests auf den Lastenausgleichsmodulen definiert haben.

## Richtlinien zur Portnutzung

Sie können weitere Eingangs- und Ausgangsregeln in der Netzwerksicherheitsgruppe konfigurieren, während Sie die NetScaler VPX-Instanz erstellen oder nachdem die virtuelle Maschine bereitgestellt wurde. Jede Eingangs- und Ausgangsregel ist einem öffentlichen Port und einem privaten Port zugeordnet.

Beachten Sie vor dem Konfigurieren von Netzwerksicherheitsgruppenregeln die folgenden Richtlinien bezüglich der Portnummern, die Sie verwenden können:

1. Die NetScaler VPX-Instanz reserviert die folgenden Ports. Sie können diese nicht als private Ports definieren, wenn Sie die öffentliche IP-Adresse für Anfragen aus dem Internet verwenden.

   Ports 21, 22, 80, 443, 8080, 67, 161, 179, 500, 520, 3003, 3008, 3009, 3010, 3011, 4001, 5061, 9000, 7000.

   Wenn Sie jedoch internetseitige Dienste wie den VIP einen Standardport (z. B. Port 443) verwenden lassen möchten, müssen Sie eine Portzuordnung mithilfe der

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

Netzwerksicherheitsgruppe erstellen. Der Standardport wird dann einem anderen Port zugeordnet, der auf dem NetScaler für diesen VIP-Dienst konfiguriert ist.

Zum Beispiel könnte ein VIP-Dienst auf Port 8443 auf der VPX-Instanz laufen, aber dem öffentlichen Port 443 zugeordnet sein. Wenn der Benutzer also über die öffentliche IP auf Port 443 zugreift, wird die Anfrage an den privaten Port 8443 weitergeleitet.

2. Die öffentliche IP-Adresse unterstützt keine Protokolle, bei denen die Portzuordnung dynamisch geöffnet wird, wie z. B. passives FTP oder ALG.
3. Hochverfügbarkeit funktioniert nicht für Datenverkehr, der eine öffentliche IP-Adresse (PIP) verwendet, die einer VPX-Instanz zugeordnet ist, anstatt einer auf dem Azure Load Balancer konfigurierten PIP.

**HINWEIS:**

Im Azure Resource Manager ist eine NetScaler VPX-Instanz mit zwei IP-Adressen verknüpft – einer öffentlichen IP-Adresse (PIP) und einer internen IP-Adresse. Während der externe Datenverkehr sich mit der PIP verbindet, ist die interne IP-Adresse oder die NSIP nicht routingfähig. Um VIP in VPX zu konfigurieren, verwenden Sie die interne IP-Adresse und einen der verfügbaren freien Ports. Verwenden Sie die PIP nicht zur Konfiguration von VIP.

# Eine NetScaler VPX Standalone-Instanz konfigurieren

Sie können eine einzelne NetScaler VPX Instanz im Azure Resource Manager (ARM)-Portal im Standalone-Modus bereitstellen, indem Sie die virtuelle Maschine erstellen und andere Ressourcen konfigurieren.

## Bevor Sie beginnen

Stellen Sie sicher, dass Folgendes vorhanden ist:

- Ein Microsoft Azure-Benutzerkonto
- Zugriff auf Microsoft Azure Resource Manager
- Microsoft Azure SDK
- Microsoft Azure PowerShell

Melden Sie sich auf der Seite Microsoft Azure Portal beim Azure Resource Manager-Portal an, indem Sie Ihren Benutzernamen und Ihr Kennwort eingeben.

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

**HINWEIS:**

Im ARM-Portal öffnet das Klicken auf eine Option in einem Bereich einen neuen Bereich auf der rechten Seite. Navigieren Sie von einem Bereich zum nächsten, um Ihr Gerät zu konfigurieren.

## Zusammenfassung der Konfigurationsschritte

1. Eine Ressourcengruppe konfigurieren
2. Eine Netzwerksicherheitsgruppe konfigurieren
3. Virtuelles Netzwerk und seine Subnetze konfigurieren
4. Speicherkonto konfigurieren
5. Verfügbarkeitsgruppe konfigurieren
6. Eine NetScaler VPX-Instanz konfigurieren.

## Ressourcengruppe konfigurieren

Erstellen Sie eine neue Ressourcengruppe, die ein Container für alle Ihre Ressourcen ist. Verwenden Sie die Ressourcengruppe, um Ihre Ressourcen als Gruppe bereitzustellen, zu verwalten und zu überwachen.

1. Klicken Sie auf **Neu** > **Verwaltung** > **Ressourcengruppe**.
2. Geben Sie im Bereich **Ressourcengruppe** die folgenden Details ein:
   - Name der Ressourcengruppe
   - Speicherort der Ressourcengruppe
3. Klicken Sie auf **Erstellen**.

## Netzwerksicherheitsgruppe konfigurieren

Erstellen Sie eine Netzwerksicherheitsgruppe, um eingehende und ausgehende Regeln zuzuweisen, um den eingehenden und ausgehenden Datenverkehr innerhalb des virtuellen Netzwerks zu steuern. Eine Netzwerksicherheitsgruppe ermöglicht es Ihnen, Sicherheitsregeln für eine einzelne virtuelle Maschine und auch für ein Subnetz eines virtuellen Netzwerks zu definieren.

1. Klicken Sie auf **Neu** > **Netzwerk** > **Netzwerksicherheitsgruppe**.

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

2. Geben Sie im Bereich **Netzwerksicherheitsgruppe erstellen** die folgenden Details ein und klicken Sie dann auf **Erstellen**.

   - Name – geben Sie einen Namen für die Sicherheitsgruppe ein
   - Ressourcengruppe – wählen Sie die Ressourcengruppe aus der Dropdown-Liste aus

**HINWEIS:**

Stellen Sie sicher, dass Sie den richtigen Standort ausgewählt haben. Die Liste der Ressourcen, die in der Dropdown-Liste angezeigt werden, ist für verschiedene Standorte unterschiedlich.

## Ein virtuelles Netzwerk und Subnetze konfigurieren

Virtuelle Netzwerke in ARM bieten eine Sicherheits- und Isolationsschicht für Ihre Dienste. VMs und Dienste, die Teil desselben virtuellen Netzwerks sind, können aufeinander zugreifen.

Führen Sie diese Schritte aus, um ein virtuelles Netzwerk und Subnetze zu erstellen.

1. Klicken Sie auf **Neu** > **Netzwerk** > **Virtuelles Netzwerk**.
2. Stellen Sie im Bereich **Virtuelles Netzwerk** sicher, dass der Bereitstellungsmodus **Resource Manager** ist, und klicken Sie auf **Erstellen**.

3. Geben Sie im Bereich **Virtuelles Netzwerk erstellen** die folgenden Werte ein und klicken Sie dann auf **Erstellen**.

   - Name des virtuellen Netzwerks
   - Adressraum – geben Sie den reservierten IP-Adressblock für das virtuelle Netzwerk ein
   - Subnetz – geben Sie den Namen des ersten Subnetzes ein (das zweite Subnetz erstellen Sie später in diesem Schritt)
   - Subnetz-Adressbereich – Geben Sie den reservierten IP-Adressblock des Subnetzes ein
   - Ressourcengruppe – Wählen Sie die zuvor erstellte Ressourcengruppe aus der Dropdown-Liste aus

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

### Zweites Subnetz konfigurieren

1. Wählen Sie das neu erstellte virtuelle Netzwerk aus dem Bereich **Alle Ressourcen** aus, und klicken Sie im Bereich **Einstellungen** auf **Subnetze**.

2. Klicken Sie auf **+Subnetz**, und erstellen Sie das zweite Subnetz, indem Sie die folgenden Details eingeben.

   - Name des zweiten Subnetzes
   - Adressbereich – Geben Sie den reservierten IP-Adressblock des zweiten Subnetzes ein
   - Netzwerksicherheitsgruppe – Wählen Sie die Netzwerksicherheitsgruppe aus der Dropdown-Liste aus

3. Klicken Sie auf **Erstellen**.

## Speicherkonto konfigurieren

Der ARM IaaS-Infrastrukturspeicher umfasst alle Dienste, in denen wir Daten in Form von Blobs, Tabellen, Warteschlangen und Dateien speichern können. Sie können auch Anwendungen mit diesen Formen von Speicherdaten in ARM erstellen.

Erstellen Sie ein Speicherkonto, um alle Ihre Daten zu speichern.

1. Klicken Sie auf **+Neu** > **Daten + Speicher** > **Speicherkonto**.
2. Geben Sie im Bereich **Speicherkonto erstellen** die folgenden Details ein:

   - Name des Kontos
   - Bereitstellungsmodus – stellen Sie sicher, dass Sie **Resource Manager** auswählen
   - Kontotyp – wählen Sie **Allgemein** aus der Dropdown-Liste aus
   - Replikation – wählen Sie **Lokal redundanter Speicher** aus der Dropdown-Liste aus
   - Ressourcengruppe – wählen Sie die neu erstellte Ressourcengruppe aus der Dropdown-Liste aus

3. Klicken Sie auf **Erstellen**.

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

## Eine Verfügbarkeitsgruppe konfigurieren

Eine Verfügbarkeitsgruppe garantiert, dass mindestens eine VM im Falle geplanter oder ungeplanter Wartungsarbeiten betriebsbereit bleibt. Zwei oder mehr VMs innerhalb derselben „Verfügbarkeitsgruppe“ werden auf verschiedenen Fehlerdomänen platziert, um redundante Dienste zu gewährleisten.

1. Klicken Sie auf **+Neu**.
2. Klicken Sie im Bereich MARKETPLACE auf **Alle anzeigen** und klicken Sie auf **Virtuelle Computer**.
3. Suchen Sie nach Verfügbarkeitsgruppe, und wählen Sie dann die Entität **Verfügbarkeitsgruppe** aus der angezeigten Liste aus.

4. Klicken Sie auf **Erstellen,** und geben Sie im Bereich **Verfügbarkeitsgruppe erstellen** die folgenden Details ein:

   - Name des Sets
   - Ressourcengruppe – wählen Sie die neu erstellte Ressourcengruppe aus der Dropdown-Liste
5. Klicken Sie auf **Erstellen**.

## Eine NetScaler VPX-Instanz konfigurieren

Erstellen Sie eine Instanz von NetScaler VPX im virtuellen Netzwerk. Beziehen Sie das NetScaler VPX-Image vom Azure Marketplace, und verwenden Sie dann das Azure Resource Manager-Portal, um eine NetScaler VPX-Instanz zu erstellen.

Bevor Sie mit der Erstellung der NetScaler VPX-Instanz beginnen, stellen Sie sicher, dass Sie ein virtuelles Netzwerk mit den erforderlichen Subnetzen erstellt haben, in dem sich die Instanz befindet. Sie können virtuelle Netzwerke während der VM-Bereitstellung erstellen, jedoch ohne die Flexibilität, verschiedene Subnetze zu erstellen.

Konfigurieren Sie optional DNS-Server- und VPN-Konnektivität, die einer virtuellen Maschine den Zugriff auf Internetressourcen ermöglicht.

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

**HINWEIS:**

Citrix empfiehlt, dass Sie Ressourcengruppe, Netzwerksicherheitsgruppe, virtuelles Netzwerk und andere Entitäten erstellen, bevor Sie die NetScaler VPX-VM bereitstellen, damit die Netzwerkinformationen während der Bereitstellung verfügbar sind.

1. Klicken Sie auf **+Neu** \> **Netzwerk**.
2. Klicken Sie auf **Alle anzeigen** und klicken Sie im Bereich Netzwerk auf **NetScaler 13.0**.
3. Wählen Sie **NetScaler 13.0 VPX Bring Your Own License** aus der Liste der Softwarepläne aus.

   Um schnell eine Entität im ARM-Portal zu finden, können Sie auch den Namen der Entität in das Suchfeld des Azure Marketplace eingeben und die \<Eingabetaste\> drücken. Geben Sie NetScaler in das Suchfeld ein, um die NetScaler-Images zu finden.

   **HINWEIS:**

   Stellen Sie sicher, dass Sie das neueste Image auswählen. Ihr NetScaler®-Image könnte die Releasenummer im Namen enthalten.

4. Wählen Sie auf der Seite **NetScaler VPX Bring Your Own License** aus der Dropdown-Liste **Resource Manager** aus und klicken Sie auf **Create**.

5. Geben Sie im Bereich **Create virtual machine** in jedem Abschnitt die erforderlichen Werte ein, um eine virtuelle Maschine zu erstellen. Klicken Sie in jedem Abschnitt auf **OK**, um Ihre Konfiguration zu speichern.

**Grundlegend:**

- Name – Geben Sie einen Namen für die NetScaler VPX-Instanz an
- VM-Datenträgertyp – Wählen Sie SSD (Standardwert) oder HDD aus dem Dropdown-Menü
- Benutzername und Kennwort – Geben Sie einen Benutzernamen und ein Kennwort an, um auf die Ressourcen in der von Ihnen erstellten Ressourcengruppe zuzugreifen
- Authentifizierungstyp – Wählen Sie SSH Public Key oder Password

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

- Ressourcengruppe – Wählen Sie die von Ihnen erstellte Ressourcengruppe aus der Dropdown-Liste

Sie können hier eine Ressourcengruppe erstellen, aber Citrix® empfiehlt, dass Sie eine Ressourcengruppe über Resource groups in Azure Resource Manager erstellen und dann die Gruppe aus der Dropdown-Liste auswählen.

**HINWEIS:**

Geben Sie in einer Azure Stack-Umgebung zusätzlich zu den grundlegenden Parametern die folgenden Parameter an:

- Azure Stack-Domäne
- Azure Stack-Mandant (Optional)
- Azure-Client (Optional)
- Azure-Client-Geheimnis (Optional)

**Größe**:

Abhängig vom VM-Festplattentyp (SSD oder HDD), den Sie in den Grundeinstellungen ausgewählt haben, werden die Festplattengrößen angezeigt.

- Wählen Sie eine Festplattengröße entsprechend Ihren Anforderungen aus und klicken Sie auf **Auswählen**.

**Einstellungen**:

- Wählen Sie den Standard-Festplattentyp (Standard) aus.
- Speicherkonto – wählen Sie das Speicherkonto aus.
- Virtuelles Netzwerk – wählen Sie das virtuelle Netzwerk aus.
- Subnetz – legen Sie die Subnetzadresse fest.
- Öffentliche IP-Adresse – wählen Sie den Typ der IP-Adresszuweisung aus.
- Netzwerksicherheitsgruppe – wählen Sie die von Ihnen erstellte Sicherheitsgruppe aus. Stellen Sie sicher, dass in der Sicherheitsgruppe Eingangs- und Ausgangsregeln konfiguriert sind.
- Verfügbarkeitsgruppe – wählen Sie die Verfügbarkeitsgruppe aus dem Dropdown-Menü aus.

**Zusammenfassung**:

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

Die Konfigurationseinstellungen werden validiert, und die Zusammenfassungsseite zeigt das Ergebnis der Validierung an. Schlägt die Validierung fehl, zeigt die Zusammenfassungsseite den Grund des Fehlers an. Gehen Sie zurück zum entsprechenden Abschnitt und nehmen Sie die erforderlichen Änderungen vor. Ist die Validierung erfolgreich, klicken Sie auf **OK**.

**Kaufen**:

Überprüfen Sie die Angebotsdetails und rechtlichen Bedingungen auf der Kaufseite und klicken Sie auf **Kaufen**.

Für eine Bereitstellung mit hoher Verfügbarkeit erstellen Sie zwei unabhängige Instanzen von NetScaler VPX im selben Verfügbarkeitsset und in derselben Ressourcengruppe, um sie in einer Aktiv-Standby-Konfiguration bereitzustellen.

# Mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz konfigurieren

Dieser Abschnitt erklärt, wie eine eigenständige NetScaler VPX-Instanz mit mehreren IP-Adressen in Azure Resource Manager (ARM) konfiguriert wird. Die VPX-Instanz kann eine oder mehrere NICs angeschlossen haben, und jede NIC kann eine oder mehrere statische oder dynamische öffentliche und private IP-Adressen zugewiesen bekommen. Sie können mehrere IP-Adressen als NSIP, VIP, SNIP usw. zuweisen.

Weitere Informationen finden Sie in der Azure-Dokumentation Zuweisen mehrerer IP-Adressen zu virtuellen Maschinen über das Azure-Portal.

Wenn Sie PowerShell-Befehle verwenden möchten, siehe Konfigurieren mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus mithilfe von PowerShell-Befehlen.

## Anwendungsfall

In diesem Anwendungsfall wird eine eigenständige NetScaler VPX-Appliance mit einer einzelnen NIC konfiguriert, die mit einem virtuellen Netzwerk (VNET) verbunden ist. Die NIC ist drei IP-Konfigurationen (ipconfig) zugeordnet, die jeweils einem anderen Zweck dienen – wie in der Tabelle gezeigt.

| IP-KONFIGURATION | ZUGEORDNET ZU | ZWECK |
|---|---|---|
| ipconfig1 | Statische öffentliche IP-Adresse; statische private IP-Adresse | Dient dem Management-Traffic |

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

| IP-KONFIGURATION | ZUGEORDNET ZU | ZWECK |
|---|---|---|
| ipconfig2 | Statische öffentliche IP-Adresse; statische private IP-Adresse | Dient dem Client-seitigen Traffic |
| ipconfig3 | Statische private IP-Adresse | Kommuniziert mit Back-End-Servern |

**HINWEIS:**

`IPConfig-3` ist keiner öffentlichen IP-Adresse zugeordnet.

**Diagramm**: Topologie

Hier ist die visuelle Darstellung des Anwendungsfalls.

**HINWEIS:**

In einer Azure NetScaler VPX-Bereitstellung mit mehreren NICs und mehreren IPs wird die private IP, die der primären (ersten) `IPConfig` der primären (ersten) NIC zugeordnet ist, automatisch als Verwaltungs-NSIP der Appliance hinzugefügt. Die verbleibenden privaten IP-Adressen, die `IPConfigs` zugeordnet sind, müssen in der VPX-Instanz als VIP oder SNIP mithilfe des Befehls `add ns ip` gemäß Ihren Anforderungen hinzugefügt werden.

## Bevor Sie beginnen

Bevor Sie beginnen, erstellen Sie eine VPX-Instanz, indem Sie die Schritte unter diesem Link befolgen:

Konfigurieren einer NetScaler VPX Standalone-Instanz

Für diesen Anwendungsfall wird die NSDoc0330VM VPX-Instanz erstellt.

**Verfahren zum Konfigurieren mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus.**

Zum Konfigurieren mehrerer IP-Adressen für eine NetScaler VPX Appliance im Standalone-Modus:

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

1. IP-Adressen zur VM hinzufügen
2. NetScaler-eigene IP-Adressen konfigurieren

**Schritt 1**: IP-Adressen zur VM hinzufügen

1. Klicken Sie im Portal auf **Weitere Dienste > geben Sie virtuelle Maschinen** in das Filterfeld ein, und klicken Sie dann auf **Virtuelle Maschinen**.
2. Klicken Sie im Blade **Virtuelle Maschinen** auf die VM, der Sie IP-Adressen hinzufügen möchten. Klicken Sie im angezeigten Blade der virtuellen Maschine auf **Netzwerkeinstellungen**, und wählen Sie dann die Netzwerkschnittstelle aus.

Multi-IP-NIC(/en-us/vpx/media/multi-ip-nic.png)

Klicken Sie im Blade, das für die ausgewählte NIC angezeigt wird, auf **IP-Konfigurationen**. Die vorhandene IP-Konfiguration, die beim Erstellen der VM zugewiesen wurde, **ipconfig1**, wird angezeigt. Stellen Sie für diesen Anwendungsfall sicher, dass die mit ipconfig1 verknüpften IP-Adressen statisch sind. Erstellen Sie als Nächstes zwei weitere IP-Konfigurationen: ipconfig2 (VIP) und ipconfig3 (SNIP).

Um weitere `ipconfigs` zu erstellen, klicken Sie auf **Hinzufügen**.

Multi-IP-Konfiguration(/en-us/vpx/media/multi-ip-ipconfig.png)

Geben Sie im Fenster **IP-Konfiguration hinzufügen** einen **Namen** ein, geben Sie die Zuweisungsmethode als **Statisch** an, geben Sie eine IP-Adresse (192.0.0.5 für diesen Anwendungsfall) ein und aktivieren Sie die **Öffentliche IP-Adresse**.

**HINWEIS:**

Bevor Sie eine statische private IP-Adresse hinzufügen, überprüfen Sie die Verfügbarkeit der IP-Adresse und stellen Sie sicher, dass die IP-Adresse zu demselben Subnetz gehört, an das die NIC angeschlossen ist.

IP-Konfiguration hinzufügen(/en-us/vpx/media/addipconfig2.png)

Klicken Sie als Nächstes auf **Erforderliche Einstellungen konfigurieren**, um eine statische öffentliche IP-Adresse für ipconfig2 zu erstellen.

Standardmäßig sind öffentliche IPs dynamisch. Um sicherzustellen, dass die VM immer dieselbe öffentliche IP-Adresse verwendet, erstellen Sie eine statische öffentliche IP.

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

Fügen Sie im Blade „Öffentliche IP-Adresse erstellen“ einen Namen hinzu, klicken Sie unter „Zuweisung“ auf **Statisch**. Klicken Sie anschließend auf **OK**.

**HINWEIS:**

Auch wenn Sie die Zuweisungsmethode auf statisch setzen, können Sie die tatsächlich der öffentlichen IP-Ressource zugewiesene IP-Adresse nicht angeben. Stattdessen wird sie aus einem Pool verfügbarer IP-Adressen am Azure-Standort zugewiesen, an dem die Ressource erstellt wird.

Führen Sie die Schritte aus, um eine weitere IP-Konfiguration für ipconfig3 hinzuzufügen. Eine öffentliche IP ist nicht zwingend erforderlich.

### Schritt 2: NetScaler-eigene IP-Adressen konfigurieren

Konfigurieren Sie die NetScaler-eigenen IP-Adressen über die GUI oder den Befehl `add ns ip`. Weitere Informationen finden Sie unter Konfigurieren von NetScaler-eigenen IP-Adressen.

## Konfigurieren einer Hochverfügbarkeits-Einrichtung mit mehreren IP-Adressen und NICs

Bei einer Microsoft Azure-Bereitstellung wird eine Hochverfügbarkeitskonfiguration von zwei NetScaler VPX-Instanzen durch die Verwendung des Azure Load Balancers (ALB) erreicht. Dies wird durch die Konfiguration eines Health Probes auf dem ALB erreicht, der jede VPX-Instanz überwacht, indem er alle 5 Sekunden einen Health Probe an sowohl primäre als auch sekundäre Instanzen sendet.

In dieser Einrichtung antwortet nur der primäre Knoten auf Health Probes, der sekundäre nicht. Sobald der primäre Knoten die Antwort auf den Health Probe sendet, beginnt der ALB, den Datenverkehr an die Instanz zu senden. Wenn die primäre Instanz zwei aufeinanderfolgende Health Probes verpasst, leitet der ALB den Datenverkehr nicht an diese Instanz um. Beim Failover beginnt der neue primäre Knoten, auf Health Probes zu antworten, und der ALB leitet den Datenverkehr an ihn um. Die standardmäßige VPX-Hochverfügbarkeits-Failover-Zeit beträgt drei Sekunden. Die gesamte Failover-Zeit, die für die Verkehrsverlagerung benötigt werden kann, beträgt maximal 13 Sekunden.

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

Sie können ein Paar NetScaler VPX-Instanzen mit mehreren NICs in einer aktiv-passiven Hochverfügbarkeits-(HA)-Einrichtung in Azure bereitstellen. Jede NIC kann mehrere IP-Adressen enthalten.

Die folgenden Optionen sind für eine Hochverfügbarkeitsbereitstellung mit mehreren NICs verfügbar:

- Hochverfügbarkeit unter Verwendung eines Azure Availability Sets
- Hochverfügbarkeit unter Verwendung von Azure Availability Zones

Weitere Informationen zu Azure Availability Set und Availability Zones finden Sie in der Azure-Dokumentation Verwalten der Verfügbarkeit von virtuellen Linux-Computern.

## Hochverfügbarkeit unter Verwendung eines Availability Sets

Eine Hochverfügbarkeits-Einrichtung unter Verwendung eines Availability Sets muss die folgenden Anforderungen erfüllen:

- Eine HA Independent Network Configuration (INC)-Konfiguration
- Der Azure Load Balancer (ALB) im Direct Server Return (DSR)-Modus

Der gesamte Datenverkehr läuft über den primären Knoten. Der sekundäre Knoten bleibt im Standby-Modus, bis der primäre Knoten ausfällt.

**HINWEIS:**

Damit eine NetScaler VPX-Hochverfügbarkeitsbereitstellung in der Azure Cloud funktioniert, benötigen Sie eine Floating Public IP (PIP), die zwischen den beiden VPX-Knoten verschoben werden kann. Der Azure Load Balancer (ALB) stellt diese Floating PIP bereit, die im Falle eines Failovers automatisch auf den zweiten Knoten verschoben wird.

**Diagramm**: Beispiel einer Bereitstellungsarchitektur für Hochverfügbarkeit unter Verwendung eines Azure Availability Sets

In einer aktiv-passiven Bereitstellung werden die öffentlichen IP-Adressen (PIP) des ALB-Frontends als VIP-Adressen in jedem VPX-Knoten hinzugefügt. In der HA-INC-Konfiguration sind die VIP-Adressen schwebend und die SNIP-Adressen instanzspezifisch.

Sie können ein VPX-Paar im aktiv-passiven Hochverfügbarkeitsmodus auf zwei Arten bereitstellen, indem Sie Folgendes verwenden:

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

- **Standard-Hochverfügbarkeitsvorlage für NetScaler VPX**: Verwenden Sie diese Option, um ein HA-Paar mit der Standardoption von drei Subnetzen und sechs NICs zu konfigurieren.
- **Windows PowerShell-Befehle**: Verwenden Sie diese Option, um ein HA-Paar entsprechend Ihren Subnetz- und NIC-Anforderungen zu konfigurieren.

Dieses Thema beschreibt, wie ein VPX-Paar in einem aktiv-passiven HA-Setup mithilfe der Citrix-Vorlage bereitgestellt wird. Wenn Sie PowerShell-Befehle verwenden möchten, siehe Konfigurieren eines HA-Setups mit mehreren IP-Adressen und NICs mithilfe von PowerShell-Befehlen.

### HA-INC-Knoten mithilfe der NetScaler®-Hochverfügbarkeitsvorlage konfigurieren

Sie können schnell und effizient ein Paar VPX-Instanzen im HA-INC-Modus mithilfe der Standardvorlage bereitstellen. Die Vorlage erstellt zwei Knoten mit drei Subnetzen und sechs NICs. Die Subnetze sind für Management-, Client- und serverseitigen Datenverkehr vorgesehen, und jedes Subnetz verfügt über zwei NICs für beide VPX-Instanzen.

Sie können die NetScaler HA-Paar-Vorlage auf dem Azure Marketplace erhalten.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein hochverfügbares VPX-Paar mithilfe von Azure Availability Sets bereitzustellen.

1. Suchen Sie im Azure Marketplace nach **NetScaler**.

2. Klicken Sie auf **JETZT ERHALTEN**.
3. Wählen Sie die erforderliche HA-Bereitstellung zusammen mit der Lizenz aus und klicken Sie auf **Weiter**.

4. Die Seite **Grundlagen** wird angezeigt. Erstellen Sie eine Ressourcengruppe und wählen Sie **OK** aus.

5. Die Seite **Allgemeine Einstellungen** wird angezeigt. Geben Sie die Details ein und wählen Sie **OK** aus.

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

**HINWEIS:**

Standardmäßig ist die Option **Überwachungsmetriken veröffentlichen** auf **false** gesetzt. Wenn Sie diese Option aktivieren möchten, wählen Sie **true** aus. Erstellen Sie eine Azure Active Directory (ADD)-Anwendung und einen Dienstprinzipal, der auf Ressourcen zugreifen kann. Weisen Sie der neu erstellten AAD-Anwendung die Rolle „Mitwirkender“ zu. Weitere Informationen finden Sie unter Verwenden des Portals zum Erstellen einer Azure Active Directory-Anwendung und eines Dienstprinzipals, der auf Ressourcen zugreifen kann.

6. Die Seite **Netzwerkeinstellungen** wird angezeigt. Überprüfen Sie die VNet- und Subnetzkonfigurationen, bearbeiten Sie die erforderlichen Einstellungen und wählen Sie **OK** aus.

7. Die Seite **Zusammenfassung** wird angezeigt. Überprüfen Sie die Konfiguration und bearbeiten Sie sie entsprechend. Wählen Sie **OK** zur Bestätigung aus.
8. Die Seite **Kaufen** wird angezeigt. Wählen Sie **Kaufen** aus, um die Bereitstellung abzuschließen.

Es kann einen Moment dauern, bis die Azure-Ressourcengruppe mit den erforderlichen Konfigurationen erstellt ist. Wählen Sie nach Abschluss die **Ressourcengruppe** im Azure-Portal aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools und Integritätstests anzuzeigen. Das Hochverfügbarkeitspaar wird als ns-vpx0 und ns-vpx1 angezeigt.

Wenn weitere Änderungen für Ihr HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal tun.

Als Nächstes müssen Sie den virtuellen Lastausgleichsserver mit der **öffentlichen Frontend-IP-Adresse (PIP) des ALB** auf dem primären Knoten konfigurieren. Um die ALB-PIP zu finden, wählen Sie ALB \> **Frontend-IP-Konfiguration** aus.

Weitere Informationen zur Konfiguration des Lastenausgleichs-Virtual-Servers finden Sie im Abschnitt **Ressourcen**.

**Ressourcen**:

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

Die folgenden Links bieten zusätzliche Informationen zur HA-Bereitstellung und Virtual-Server-Konfiguration:

- Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen
- Grundlegenden Lastenausgleich einrichten

**Verwandte Ressourcen**:

- Einrichten einer Hochverfügbarkeitskonfiguration mit mehreren IP-Adressen und NICs mithilfe von PowerShell-Befehlen
- Konfigurieren von GSLB bei einer Active-Standby-HA-Bereitstellung in Azure

## Hochverfügbarkeit mithilfe von Verfügbarkeitszonen

Azure-Verfügbarkeitszonen sind fehlerisolierte Standorte innerhalb einer Azure-Region, die redundante Stromversorgung, Kühlung und Netzwerk bereitstellen und die Ausfallsicherheit erhöhen. Nur bestimmte Azure-Regionen unterstützen Verfügbarkeitszonen. Weitere Informationen zu Regionen, die Verfügbarkeitszonen unterstützen, finden Sie in der Azure-Dokumentation Was sind Verfügbarkeitszonen in Azure?.

Diagramm: Beispiel einer Hochverfügbarkeits-Bereitstellungsarchitektur unter Verwendung von Azure-Verfügbarkeitszonen

Sie können ein VPX-Paar im Hochverfügbarkeitsmodus bereitstellen, indem Sie die Vorlage „NetScaler 13.0 HA mit Verfügbarkeitszonen“ verwenden, die im Azure Marketplace verfügbar ist.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein Hochverfügbarkeits-VPX-Paar mithilfe von Azure-Verfügbarkeitszonen bereitzustellen.

1. Wählen Sie im Azure Marketplace die Citrix®-Lösungsvorlage aus und initiieren Sie diese.

2. Stellen Sie sicher, dass der Bereitstellungstyp „Resource Manager“ ist, und wählen Sie **Erstellen**.
3. Die Seite **Grundlagen** wird angezeigt. Geben Sie die Details ein und klicken Sie auf **OK**.

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

**HINWEIS:**

Stellen Sie sicher, dass Sie eine Azure-Region auswählen, die Verfügbarkeitszonen unterstützt. Weitere Informationen zu Regionen, die Verfügbarkeitszonen unterstützen, finden Sie in der Azure-Dokumentation Was sind Verfügbarkeitszonen in Azure?

4. Die Seite **Allgemeine Einstellungen** wird angezeigt. Geben Sie die Details ein und wählen Sie **OK**.
5. Die Seite **Netzwerkeinstellungen** wird angezeigt. Überprüfen Sie die VNet- und Subnetzkonfigurationen, bearbeiten Sie die erforderlichen Einstellungen und wählen Sie **OK**.
6. Die Seite **Zusammenfassung** wird angezeigt. Überprüfen Sie die Konfiguration und bearbeiten Sie sie entsprechend. Wählen Sie **OK** zur Bestätigung.
7. Die Seite **Kaufen** wird angezeigt. Wählen Sie **Kaufen**, um die Bereitstellung abzuschließen.

   Es kann einen Moment dauern, bis die Azure-Ressourcengruppe mit den erforderlichen Konfigurationen erstellt wird. Wählen Sie nach Abschluss die **Ressourcengruppe** aus, um die Konfigurationsdetails, wie z. B. LB-Regeln, Back-End-Pools, Integritätstests usw., im Azure-Portal anzuzeigen. Das Hochverfügbarkeitspaar wird als ns-vpx0 und ns-vpx1 angezeigt. Außerdem können Sie den Standort unter der Spalte **Standort** sehen.

Wenn weitere Änderungen an Ihrem HA-Setup erforderlich sind, wie z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal tun.

## Überwachen Sie Ihre Instanzen mithilfe von Metriken in Azure Monitor

Sie können Metriken in der Azure Monitor-Datenplattform verwenden, um eine Reihe von NetScaler VPX-Ressourcen wie CPU, Speicherauslastung und Durchsatz zu überwachen. Der Metrikdienst überwacht NetScaler VPX-Ressourcen, die in Azure ausgeführt werden, in Echtzeit. Sie können den **Metrik-Explorer** verwenden, um auf die gesammelten Daten zuzugreifen. Weitere Informationen finden Sie unter Übersicht über Azure Monitor-Metriken.

### Hinweise

- Wenn Sie eine NetScaler VPX-Instanz in Azure über das Azure Marketplace-Angebot bereitstellen, ist der Metrikdienst standardmäßig deaktiviert.

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

- Der Metrikdienst wird in Azure CLI nicht unterstützt.
- Metriken sind für CPU (CPU-Nutzung für Verwaltung und Pakete), Arbeitsspeicher und Durchsatz (eingehend und ausgehend) verfügbar.

### So zeigen Sie Metriken in Azure Monitor an

Um Metriken in Azure Monitor für Ihre Instanz anzuzeigen, führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei **Azure-Portal > Virtuelle Computer** an.
2. Wählen Sie den virtuellen Computer aus, der der primäre Knoten ist.
3. Klicken Sie im Abschnitt **Überwachung** auf **Metriken**.
4. Klicken Sie im Dropdown-Menü **Metrik-Namespace** auf **NetScaler**.
5. Klicken Sie unter **Alle Metriken** im Dropdown-Menü **Metriken** auf die Metriken, die Sie anzeigen möchten.
6. Klicken Sie auf **Metrik hinzufügen**, um eine weitere Metrik im selben Diagramm anzuzeigen. Verwenden Sie die Diagrammoptionen, um Ihr Diagramm anzupassen.

## Konfigurieren Sie ein Hochverfügbarkeits-Setup mit mehreren IP-Adressen und NICs mithilfe von PowerShell-Befehlen

Sie können ein Paar NetScaler VPX-Instanzen mit mehreren NICs in einem aktiv-passiven Hochverfügbarkeits-Setup (HA) in Azure bereitstellen. Jede NIC kann mehrere IP-Adressen enthalten.

Eine aktiv-passive Bereitstellung erfordert:

- Eine HA Independent Network Configuration (INC)-Konfiguration
- Den Azure Load Balancer (ALB) im Direct Server Return (DSR)-Modus

Der gesamte Datenverkehr läuft über den primären Knoten. Der sekundäre Knoten bleibt im Standby-Modus, bis der primäre Knoten ausfällt.

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

**HINWEIS:**

Damit eine NetScaler VPX-Hochverfügbarkeitsbereitstellung in einer Azure-Cloud funktioniert, benötigen Sie eine schwebende öffentliche IP (PIP), die zwischen den beiden Hochverfügbarkeitsknoten verschoben werden kann. Der Azure Load Balancer (ALB) stellt diese schwebende PIP bereit, die im Falle eines Failovers automatisch auf den zweiten Knoten verschoben wird.

**Diagramm**: Beispiel einer aktiv-passiven Bereitstellungsarchitektur

Bei einer aktiv-passiven Bereitstellung werden die schwebenden öffentlichen IP-Adressen (PIP) des ALB als VIP-Adressen in jedem VPX-Knoten hinzugefügt. In der HA-INC-Konfiguration sind die VIP-Adressen schwebend und die SNIP-Adressen instanzspezifisch.

ALB überwacht jede VPX-Instanz, indem es alle 5 Sekunden eine Integritätsprüfung sendet und den Datenverkehr nur an die Instanz umleitet, die regelmäßig auf Integritätsprüfungen antwortet. In einem HA-Setup antwortet der primäre Knoten auf Integritätsprüfungen, der sekundäre jedoch nicht. Wenn die primären Instanzen zwei aufeinanderfolgende Integritätsprüfungen verpassen, leitet ALB den Datenverkehr nicht an diese Instanz um. Beim Failover beginnt der neue primäre Knoten, auf Integritätsprüfungen zu antworten, und der ALB leitet den Datenverkehr an ihn um. Die standardmäßige VPX-Hochverfügbarkeits-Failoverzeit beträgt drei Sekunden. Die gesamte Failoverzeit, die für die Datenverkehrsumschaltung benötigt werden kann, beträgt maximal 13 Sekunden.

Sie können ein VPX-Paar in einem aktiv-passiven HA-Setup auf zwei Arten bereitstellen, indem Sie Folgendes verwenden:

- **NetScaler VPX Standard-Hochverfügbarkeitsvorlage**: Verwenden Sie diese Option, um ein HA-Paar mit der Standardoption von drei Subnetzen und sechs NICs zu konfigurieren.
- **Windows PowerShell-Befehle**: Verwenden Sie diese Option, um ein HA-Paar gemäß Ihren Subnetz- und NIC-Anforderungen zu konfigurieren.

Dieses Thema beschreibt, wie ein VPX-Paar in einem aktiv-passiven HA-Setup mithilfe von PowerShell-Befehlen bereitgestellt wird. Wenn Sie die NetScaler VPX Standard HA-Vorlage verwenden möchten, siehe Konfigurieren eines HA-Setups mit mehreren IP-Adressen und NICs.

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

# HA-INC-Knoten mithilfe von PowerShell-Befehlen konfigurieren

### Szenario: HA-INC PowerShell-Bereitstellung

In diesem Szenario stellen Sie ein NetScaler VPX-Paar mithilfe der in der Tabelle angegebenen Topologie bereit. Jede VPX-Instanz enthält drei NICs, wobei jede NIC in einem anderen Subnetz bereitgestellt wird. Jeder NIC wird eine IP-Konfiguration zugewiesen.

| ALB | VPX1 | VPX2 |
|---|---|---|
| ALB ist verknüpft mit öffentlicher IP 3 (pip3) | Management-IP ist mit IPConfig1 konfiguriert, die eine öffentliche IP (pip1) und eine private IP (12.5.2.24) enthält; nic1; Mgmtsubnet=12.5.2.0/24 | Management-IP ist mit IPConfig5 konfiguriert, die eine öffentliche IP (pip3) und eine private IP (12.5.2.26) enthält;nic4;Mgmtsubnet=12.5.2.0/24 |
| LB-Regeln und konfigurierter Port sind HTTP (80), SSL (443), Health-Probe (9000) | Client-seitige IP ist mit IPConfig3 konfiguriert, die eine private IP (12.5.1.27) enthält;nic2; FrontEndsubet=12.5.1.0/24 | Client-seitige IP ist mit IPConfig7 konfiguriert, die eine private IP (12.5.1.28) enthält;nic5;FrontEndsubet=12.5.1.0/24 |
| - | Server-seitige IP ist mit IPConfig4 konfiguriert, die eine private IP (12.5.3.24) enthält; nic3;BackendSubnet=12.5.3.0/24 | Die serverseitige IP ist mit IPConfig8 konfiguriert, die eine private IP (12.5.3.28);nic6;BackendSubnet=12.5.3.0/24 enthält |
| - | Regeln und Ports für NSG sind SSH (22), HTTP (80), HTTPS (443) | - |

## Parametereinstellungen

Die folgenden Parametereinstellungen werden in diesem Szenario verwendet:

```
$locName= "South east Asia"
```

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

```
$rgName = "MulitIP-MultiNIC-RG"

$nicName1= "VM1-NIC1"

$nicName2 = "VM1-NIC2"

$nicName3= "VM1-NIC3"

$nicName4 = "VM2-NIC1"

$nicName5= "VM2-NIC2"

$nicName6 = "VM2-NIC3"

$vNetName = "Azure-MultiIP-ALB-vnet"

$vNetAddressRange= "12.5.0.0/16"

$frontEndSubnetName= "frontEndSubnet"

$frontEndSubnetRange= "12.5.1.0/24"
```

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

```
$mgmtSubnetName= "mgmtSubnet"

$mgmtSubnetRange= "12.5.2.0/24"

$backEndSubnetName = "backEndSubnet"

$backEndSubnetRange = "12.5.3.0/24"

$prmStorageAccountName = "multiipmultinicbstorage"

$avSetName = "multiple-avSet"

$vmSize= "Standard\_DS4\_V2"

$publisher = "Citrix"

$offer = "netscalervpx-120"

$sku = "netscalerbyol"

$version="latest"
```

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

```
$pubIPName1="VPX1MGMT"

$pubIPName2="VPX2MGMT"

$pubIPName3="ALBPIP"

$domName1="vpx1dns"

$domName2="vpx2dns"

$domName3="vpxalbdns"

$vmNamePrefix="VPXMultiIPALB"

$osDiskSuffix1="osmultiipalbdiskdb1"

$osDiskSuffix2="osmultiipalbdiskdb2"

$lbName= "MultiIPALB"

$frontEndConfigName1= "FrontEndIP"
```

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

```
$backendPoolName1= "BackendPoolHttp"


$lbRuleName1= "LBRuleHttp"


$healthProbeName= "HealthProbe"


$nsgName="NSG-MultiIP-ALB"


$rule1Name="Inbound-HTTP"


$rule2Name="Inbound-HTTPS"


$rule3Name="Inbound-SSH"
```

Um die Bereitstellung abzuschließen, führen Sie die folgenden Schritte mithilfe von PowerShell-Befehlen aus:

1. Erstellen Sie eine Ressourcengruppe, ein Speicherkonto und eine Verfügbarkeitsgruppe
2. Erstellen Sie eine Netzwerksicherheitsgruppe und fügen Sie Regeln hinzu
3. Erstellen Sie ein virtuelles Netzwerk und drei Subnetze
4. Erstellen Sie öffentliche IP-Adressen
5. Erstellen Sie IP-Konfigurationen für VPX1
6. Erstellen Sie IP-Konfigurationen für VPX2
7. Erstellen Sie NICs für VPX1
8. Erstellen Sie NICs für VPX2

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

9. VPX1 erstellen
10. VPX2 erstellen
11. ALB erstellen

**Eine Ressourcengruppe, ein Speicherkonto und eine Verfügbarkeitsgruppe erstellen**.

```
New-AzureRmResourceGroup -Name $rgName -Location $locName




$prmStorageAccount=New-AzureRMStorageAccount -Name $prmStorageAccountName
-ResourceGroupName $rgName -Type Standard_LRS -Location $locName




$avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
$rgName -Location $locName
```

**Eine Netzwerksicherheitsgruppe erstellen und Regeln hinzufügen**.

```
$rule1 = New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name
-Description "Allow HTTP" -Access Allow -Protocol Tcp -Direction Inbound
-Priority 101




-SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
* -DestinationPortRange 80




$rule2 = New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name
-Description "Allow HTTPS" -Access Allow -Protocol Tcp -Direction Inbound
-Priority 110
```

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

```
-SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
* -DestinationPortRange 443




$rule3 = New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name
-Description "Allow SSH" -Access Allow -Protocol Tcp -Direction Inbound
-Priority 120




-SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
* -DestinationPortRange 22




$nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName
-Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,$rule3
```

**Ein virtuelles Netzwerk und drei Subnetze erstellen**.

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
$frontEndSubnetName -AddressPrefix $frontEndSubnetRange (this parameter
value should be as per your requirement)




$mgmtSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name $mgmtSubnetName
-AddressPrefix $mgmtSubnetRange
```

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

```
$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
$backEndSubnetName -AddressPrefix $backEndSubnetRange



$vnet =New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
$rgName -Location $locName -AddressPrefix $vNetAddressRange -Subnet
$frontendSubnet,$backendSubnet, $mgmtSubnet



$subnetName ="frontEndSubnet"



$subnet1=$vnet.Subnets|?{$_.Name -eq $subnetName}



$subnetName="backEndSubnet"



$subnet2=$vnet.Subnets|?{$_.Name -eq $subnetName}



$subnetName="mgmtSubnet"
```

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

```
$subnet3=$vnet.Subnets|?{$_.Name -eq $subnetName}
```

**Öffentliche IP-Adressen erstellen**.

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
$rgName -DomainNameLabel $domName1 -Location $locName -AllocationMethod
Dynamic



$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
$rgName -DomainNameLabel $domName2 -Location $locName -AllocationMethod
Dynamic



$pip3=New-AzureRmPublicIpAddress -Name $pubIPName3 -ResourceGroupName
$rgName -DomainNameLabel $domName3 -Location $locName -AllocationMethod
Dynamic
```

**IP-Konfigurationen für VPX1 erstellen**.

```
$IpConfigName1 = "IPConfig1"




$IPAddress = "12.5.2.24"




$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1
-Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip1
-Primary
```

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

```
$IPConfigName3="IPConfig-3"



$IPAddress="12.5.1.27"



$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3
-Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary



$IPConfigName4 = "IPConfig-4"



$IPAddress = "12.5.3.24"



$IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4
-Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

**IP-Konfigurationen für VPX2 erstellen**.

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

```
$IpConfigName5 = "IPConfig5"



$IPAddress="12.5.2.26"



$IPConfig5=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName5
-Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip2
-Primary



$IPConfigName7="IPConfig-7"



$IPAddress="12.5.1.28"



$IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7
-Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary



$IPConfigName8="IPConfig-8"
```

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

```
$IPAddress="12.5.3.28"



$IPConfig8=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName8
-Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

**NICs für VPX1 erstellen**.

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig1
-NetworkSecurityGroupId $nsg.Id



$nic2=New-AzureRmNetworkInterface -Name $nicName2 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig3
-NetworkSecurityGroupId $nsg.Id



$nic3=New-AzureRmNetworkInterface -Name $nicName3 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig4
-NetworkSecurityGroupId $nsg.Id
```

**NICs für VPX2 erstellen**.

```
$nic4=New-AzureRmNetworkInterface -Name $nicName4 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig5
-NetworkSecurityGroupId $nsg.Id
```

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

```
$nic5=New-AzureRmNetworkInterface -Name $nicName5 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig7
-NetworkSecurityGroupId $nsg.Id




$nic6=New-AzureRmNetworkInterface -Name $nicName6 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig8
-NetworkSecurityGroupId $nsg.Id
```

**VPX1 erstellen**.

Dieser Schritt umfasst die folgenden Unterschritte:

- VM-Konfigurationsobjekt erstellen
- Anmeldeinformationen, Betriebssystem und Image festlegen
- NICs hinzufügen
- Betriebssystemdatenträger angeben und VM erstellen

```
 $suffixNumber = 1



 $vmName=$vmNamePrefix + $suffixNumber



 $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize
-AvailabilitySetId $avSet.Id



 $cred=Get-Credential -Message "Type the name and password for VPX
login."



 $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux
-ComputerName $vmName -Credential $cred
```

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

```
 $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
$publisher -Offer $offer -Skus $sku -Version $version


 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id
-Primary


 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.Id


 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.Id


 $osDiskName=$vmName + "-" + $osDiskSuffix1


 $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() +
"vhds/" + $osDiskName + ".vhd"


 $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
$osVhdUri -CreateOption fromImage


 Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer
-Name $sku


 New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
$locName
```

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

**VPX2 erstellen**.

```
```

```
$suffixNumber=2
```

```
$vmName=$vmNamePrefix + $suffixNumber
```

```
$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize
-AvailabilitySetId $avSet.Id
```

```
$cred=Get-Credential -Message "Type the name and password for VPX login."
```

```
$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName
$vmName -Credential $cred
```

```
$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher
-Offer $offer -Skus $sku -Version $version
```

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

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic4.Id
-Primary



$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic5.Id



$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic6.Id



$osDiskName=$vmName + "-" + $osDiskSuffix2



$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/" +
$osDiskName + ".vhd"



$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
$osVhdUri -CreateOption fromImage



Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer
-Name $sku
```

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

```
New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location $locName
```

Um die den NICs zugewiesenen privaten und öffentlichen IP-Adressen anzuzeigen, geben Sie die folgenden Befehle ein:

```
$nic1.IPConfig

$nic2.IPConfig

$nic3.IPConfig

$nic4.IPConfig

$nic5.IPConfig

$nic6.IPConfig
```

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

```
```

**Azure Load Balancer (ALB) erstellen**.

Dieser Schritt umfasst die folgenden Unterschritte:

- Front-End-IP-Konfiguration erstellen
- Integritätstest erstellen
- Back-End-Adresspool erstellen
- Lastenausgleichsregeln erstellen (HTTP und SSL)
- ALB mit Front-End-IP-Konfiguration, Back-End-Adresspool und LB-Regel erstellen
- IP-Konfiguration mit Back-End-Pools verknüpfen

```
$frontEndIP1=New-AzureRmLoadBalancerFrontendIpConfig -Name
$frontEndConfigName1 -PublicIpAddress $pip3

$healthProbe=New-AzureRmLoadBalancerProbeConfig -Name $healthProbeName
-Protocol Tcp -Port 9000 –IntervalInSeconds 5 -ProbeCount 2

$beAddressPool1=New-AzureRmLoadBalancerBackendAddressPoolConfig -Name
$backendPoolName1

$lbRule1=New-AzureRmLoadBalancerRuleConfig -Name $lbRuleName1
-FrontendIpConfiguration $frontEndIP1 -BackendAddressPool $beAddressPool1
-Probe $healthProbe -Protocol Tcp -FrontendPort 80 -BackendPort 80
-EnableFloatingIP

$lb=New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name $lbName
-Location $locName -FrontendIpConfiguration $frontEndIP1 -LoadBalancingRule
$lbRule1 -BackendAddressPool $beAddressPool1 -Probe $healthProbe

$nic2.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb.BackendAddressPools[0

$nic5.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb.BackendAddressPools[0

$lb=$lb |Set-AzureRmLoadBalancer

$nic2=$nic2 | Set-AzureRmNetworkInterface

$nic5=$nic5 | Set-AzureRmNetworkInterface
```

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

Nachdem Sie das NetScaler VPX-Paar erfolgreich bereitgestellt haben, melden Sie sich bei jeder VPX-Instanz an, um HA-INC sowie SNIP- und VIP-Adressen zu konfigurieren.

1. Geben Sie den folgenden Befehl ein, um HA-Knoten hinzuzufügen.

   ```
   add ha node 1 PeerNodeNSIP -inc Enabled
   ```

2. Fügen Sie private IP-Adressen von clientseitigen NICs als SNIPs für VPX1 (NIC2) und VPX2 (NIC5) hinzu.

   ```
   add nsip privateIPofNIC2 255.255.255.0 -type SNIP
   ```
   ```
   add nsip privateIPofNIC5 255.255.255.0 -type SNIP
   ```

3. Fügen Sie auf dem primären Knoten einen Lastenausgleichs-Virtual-Server mit der Front-End-IP-Adresse (öffentliche IP) des ALB hinzu.

   ```
   add lb virtual server v1 HTTP FrontEndIPofALB 80
   ```

**Verwandte Ressourcen**:

Konfigurieren von GSLB in einer Active-Standby-HA-Bereitstellung in Azure

## Bereitstellen eines NetScaler-Hochverfügbarkeitspaars auf Azure mit ALB im Floating-IP-deaktivierten Modus

Sie können ein Paar NetScaler VPX-Instanzen mit mehreren NICs in einer aktiv-passiven Hochverfügbarkeits-(HA)-Einrichtung auf Azure bereitstellen. Jede NIC kann viele IP-Adressen enthalten.

Eine aktiv-passive Bereitstellung erfordert:

- Eine HA Independent Network Configuration (INC)-Konfiguration
- Den Azure Load Balancer (ALB) mit:
  - Floating-IP-aktiviertem Modus oder Direct Server Return (DSR)-Modus
  - Floating-IP-deaktiviertem Modus

Weitere Informationen zu den Floating-IP-Optionen von ALB finden Sie in der Azure-Dokumentation.

Wenn Sie ein VPX-Paar in einer aktiv-passiven HA-Einrichtung auf Azure mit aktiviertem ALB Floating IP bereitstellen möchten, siehe Konfigurieren einer Hochverfügbarkeitseinrichtung mit mehreren IP-Adressen und NICs mithilfe von PowerShell-Befehlen.

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

## HA-Bereitstellungsarchitektur mit ALB im Floating-IP-deaktivierten Modus

In einer aktiv-passiven Bereitstellung werden die privaten IP-Adressen der Client-Schnittstelle jeder Instanz als VIP-Adressen in jeder VPX-Instanz hinzugefügt. Konfigurieren Sie im HA-INC-Modus, wobei VIP-Adressen über IPSet geteilt werden und SNIP-Adressen instanzspezifisch sind. Der gesamte Datenverkehr läuft über die primäre Instanz. Die sekundäre Instanz befindet sich im Standby-Modus, bis die primäre Instanz ausfällt.

**Diagramm**: Beispiel einer aktiv-passiven Bereitstellungsarchitektur

## Voraussetzungen

Sie müssen mit den folgenden Informationen vertraut sein, bevor Sie eine NetScaler VPX-Instanz auf Azure bereitstellen.

- Azure-Terminologie und Netzwerkdetails. Weitere Informationen finden Sie unter Azure-Terminologie.
- Funktionsweise einer NetScaler-Appliance. Weitere Informationen finden Sie in der NetScaler-Dokumentation.
- NetScaler-Netzwerk. Weitere Informationen finden Sie unter ADC-Netzwerk.
- Azure Load Balancer und Konfiguration der Lastenausgleichsregel. Weitere Informationen finden Sie in der Azure ALB-Dokumentation.

## Bereitstellen eines VPX HA-Paares in Azure mit deaktivierter ALB Floating IP

Hier ist eine Zusammenfassung der HA- und ALB-Bereitstellungsschritte:

1. Stellen Sie zwei VPX-Instanzen (primäre und sekundäre Instanzen) in Azure bereit.
2. Fügen Sie Client- und Server-NICs zu beiden Instanzen hinzu.
3. Stellen Sie einen ALB mit einer Lastenausgleichsregel bereit, deren Floating-IP-Modus deaktiviert ist.
4. Konfigurieren Sie die HA-Einstellungen auf beiden Instanzen über die NetScaler-GUI.

**Schritt 1. Stellen Sie zwei VPX-Instanzen in Azure bereit.**

Erstellen Sie zwei VPX-Instanzen, indem Sie die folgenden Schritte ausführen:

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

1. Wählen Sie die NetScaler-Version aus dem Azure Marketplace aus (in diesem Beispiel wird NetScaler Release 13.1 verwendet).

2. Wählen Sie den erforderlichen ADC-Lizenzierungsmodus aus und klicken Sie auf **Erstellen**.

   Die Seite **Virtuellen Computer erstellen** wird geöffnet.

3. Geben Sie die erforderlichen Details in jedem Tab ein: Grundlagen, Datenträger, Netzwerk, Verwaltung, Überwachung, Erweitert und Tags, um eine erfolgreiche Bereitstellung zu gewährleisten.

   Erstellen Sie auf der Registerkarte **Netzwerk** ein neues virtuelles Netzwerk mit 3 Subnetzen, jeweils eines für: Management-, Client- und Server-NICs. Alternativ können Sie auch ein vorhandenes virtuelles Netzwerk verwenden. Die Management-NIC wird während der VM-Bereitstellung erstellt. Client- und Server-NICs werden nach der Erstellung der VM erstellt und angehängt. Für die Netzwerksicherheitsgruppe der NIC können Sie eine der folgenden Optionen wählen:

   - Wählen Sie **Erweitert** und verwenden Sie eine vorhandene Netzwerksicherheitsgruppe, die Ihren Anforderungen entspricht.
   - Wählen Sie **Basic** und die erforderlichen Ports aus.

   **HINWEIS:**

   Sie können die Einstellungen der Netzwerksicherheitsgruppe auch nach Abschluss der VM-Bereitstellung ändern.

4. Klicken Sie auf Weiter: **Überprüfen + erstellen >**.

   Nach erfolgreicher Validierung überprüfen Sie die Grundeinstellungen, VM-Konfigurationen, Netzwerk- und zusätzliche Einstellungen und klicken Sie auf **Erstellen**.

5. Nach Abschluss der Bereitstellung klicken Sie auf **Zu Ressource wechseln**, um die Konfigurationsdetails anzuzeigen.

   Stellen Sie in ähnlicher Weise eine zweite NetScaler VPX-Instanz bereit.

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

**Schritt 2. Client- und Server-NICs auf beiden Instanzen hinzufügen.**

**HINWEIS:**

Um weitere NICs anzuhängen, müssen Sie zuerst die VM anhalten. Wählen Sie im Azure-Portal die VM aus, die Sie anhalten möchten. Klicken Sie auf der Registerkarte **Übersicht** auf **Beenden**. Warten Sie, bis der Status als **Beendet** angezeigt wird.

Um eine Client-NIC auf der primären Instanz hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Networking > Attach Network Interface**.

   Sie können eine vorhandene NIC auswählen oder eine neue Schnittstelle erstellen und anhängen.
2. Für die NIC-Netzwerksicherheitsgruppe können Sie eine vorhandene Netzwerksicherheitsgruppe verwenden, indem Sie **Erweitert** auswählen, oder eine neue erstellen, indem Sie **Standard** auswählen.

Um eine Server-NIC hinzuzufügen, führen Sie die gleichen Schritte wie beim Hinzufügen einer Client-NIC aus.

Die NetScaler VPX-Instanz hat alle drei NICs (Management-NIC, Client-NIC und Server-NIC) angehängt.

Wiederholen Sie die vorherigen Schritte zum Hinzufügen von NICs auf der sekundären Instanz.

Nachdem Sie NICs auf beiden Instanzen erstellt und angehängt haben, starten Sie beide Instanzen neu, indem Sie zu **Übersicht > Starten** navigieren.

**HINWEIS:**

Sie müssen den Datenverkehr durch den Port in der eingehenden Client-NIC-Regel zulassen, der später zum Erstellen eines virtuellen Lastausgleichsservers bei der Konfiguration der NetScaler VPX-Instanz verwendet wird.

**Schritt 3. Stellen Sie einen ALB mit einer Lastenausgleichsregel bereit, deren Floating-IP-Modus deaktiviert ist.**

Um die Konfiguration des ALB zu starten, führen Sie die folgenden Schritte aus:

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

1. Gehen Sie zur Seite **Load Balancer** und klicken Sie auf **Erstellen**.
2. Geben Sie auf der Seite **Load Balancer erstellen** die erforderlichen Details an.

   Im folgenden Beispiel stellen wir einen regionalen öffentlichen Load Balancer der Standard-SKU bereit.

   **HINWEIS:**

   Alle öffentlichen IPs, die an die NetScaler-VMs angehängt sind, müssen dieselbe SKU wie die des ALB haben. Weitere Informationen zu ALB-SKUs finden Sie in der Dokumentation zu Azure Load Balancer SKUs.
3. Erstellen Sie auf der Registerkarte **Frontend-IP-Konfiguration** entweder eine IP-Adresse oder verwenden Sie eine vorhandene IP-Adresse.

4. Wählen Sie auf der Registerkarte **Backend-Pools** die NIC-basierte Backend-Pool-Konfiguration aus und fügen Sie die Client-NICs beider NetScaler-VMs hinzu.

5. Klicken Sie auf der Registerkarte **Eingehende Regeln** auf **Lastenausgleichsregel hinzufügen** und geben Sie die in den vorherigen Schritten erstellte Frontend-IP-Adresse und den Backend-Pool an. Wählen Sie das Protokoll und den Port entsprechend Ihren Anforderungen aus. Erstellen oder verwenden Sie einen vorhandenen Integritätstest. Deaktivieren Sie das Kontrollkästchen **Floating IP aktivieren**.

6. Klicken Sie auf **Überprüfen + Erstellen**. Nachdem die Validierung erfolgreich war, klicken Sie auf **Erstellen**.

   Validierung des Lastenausgleichs erfolgreich(/en-us/vpx/media/alb-floating-ip-lb-validation-passed.png)

**Schritt 4. Konfigurieren Sie die HA-Einstellungen auf beiden NetScaler VPX-Instanzen über die NetScaler GUI.**

Nachdem Sie die NetScaler VPX-Instanzen in Azure erstellt haben, können Sie HA über die NetScaler GUI konfigurieren.

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

**Schritt 1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.**

Auf der primären Instanz führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und dem bei der Bereitstellung der Instanz angegebenen Kennwort an.
2. Navigieren Sie zu **Configuration > System > High Availability > Nodes**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **Remote Node IP address** die private IP-Adresse der Management-NIC der sekundären Instanz ein, zum Beispiel: 10.4.1.5.
4. Aktivieren Sie das Kontrollkästchen **Turn on INC (Independent Network Configuration) mode on self node**.
5. Klicken Sie auf **Erstellen**.

Primäre Instanz für Hochverfügbarkeit(/en-us/vpx/media/alb-floating-ip-ha-primary-node.png)

Auf der sekundären Instanz führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und dem bei der Bereitstellung der Instanz angegebenen Kennwort an.
2. Navigieren Sie zu **Configuration > System > High Availability > Nodes**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **Remote Node IP address** die private IP-Adresse der Management-NIC der primären Instanz ein, zum Beispiel: 10.4.1.4.
4. Aktivieren Sie das Kontrollkästchen **Turn on INC (Independent Network Configuration) mode on self node**.
5. Klicken Sie auf **Create**.

Sekundäre Hochverfügbarkeitsinstanz(/en-us/vpx/media/alb-floating-ip-ha-secondary-node.png)

Bevor Sie fortfahren, stellen Sie sicher, dass der **Synchronization state** der sekundären Instanz als **SUCCESS** auf der Seite **Nodes** angezeigt wird.

**HINWEIS:**

Die sekundäre Instanz hat nun die gleichen Anmeldeinformationen wie die primäre Instanz.

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

Synchronisierungsstatus der Hochverfügbarkeit(/en-us/vpx/media/alb-floating-ip-ha-sync-state.png)

**Schritt 2. Virtuelle IP-Adresse und Subnetz-IP-Adresse auf beiden Instanzen hinzufügen.**

Führen Sie auf der primären Instanz die folgenden Schritte aus:

1. Navigieren Sie zu **System > Network > IPs > IPv4s** und klicken Sie auf **Add**.
2. Fügen Sie eine primäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
    a. Geben Sie die private IP-Adresse der Client-NIC der primären Instanz und die für das Client-Subnetz in der VM-Instanz konfigurierte Netzmaske ein.
    b. Wählen Sie im Feld **IP Type** aus dem Dropdown-Menü **Virtual IP** aus.
    c. Klicken Sie auf **Create**.
3. Fügen Sie eine primäre SNIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
    a. Geben Sie die interne IP-Adresse der Server-NIC der primären Instanz und die für das Server-Subnetz in der primären Instanz konfigurierte Netzmaske ein.
    b. Wählen Sie im Feld **IP-Typ** im Dropdown-Menü die Option **Subnetz-IP** aus.
    c. Klicken Sie auf **Erstellen**.
4. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
    a. Geben Sie die interne IP-Adresse der Client-NIC der sekundären Instanz und die für das Client-Subnetz in der VM-Instanz konfigurierte Netzmaske ein.
    b. Wählen Sie im Feld **IP-Typ** im Dropdown-Menü die Option **Virtuelle IP** aus.
    c. Klicken Sie auf **Erstellen**.

    Primäre VIP und SNIP hinzufügen(/en-us/vpx/media/alb-floating-ip-primary-vip-snip.png)

Führen Sie auf der sekundären Instanz die folgenden Schritte aus:

1. Navigieren Sie zu **System > Network > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
    a. Geben Sie die interne IP-Adresse der Client-NIC der sekundären Instanz und die für das Client-Subnetz in der VM-Instanz konfigurierte Netzmaske ein.
    b. Wählen Sie im Feld **IP-Typ** im Dropdown-Menü die Option **Virtuelle IP** aus.
3. Fügen Sie eine sekundäre SNIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:

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

a. Geben Sie die interne IP-Adresse der Server-NIC der sekundären Instanz und die für das Server-Subnetz in der sekundären Instanz konfigurierte Netzmaske ein.

b. Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdown-Menü aus.

c. Klicken Sie auf **Erstellen**.

**Schritt 3. IP-Set hinzufügen und IP-Set an die sekundäre VIP auf beiden Instanzen binden.**

Führen Sie auf der primären Instanz die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IP-Sets > Hinzufügen**.
2. Geben Sie einen IP-Set-Namen ein und klicken Sie auf **Einfügen**.
3. Wählen Sie auf der Seite **IPV4s** die virtuelle IP (sekundäre VIP) aus und klicken Sie auf **Einfügen**.
4. Klicken Sie auf **Erstellen**, um das IP-Set zu erstellen.

Führen Sie auf der sekundären Instanz die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IP-Sets > Hinzufügen**.
2. Geben Sie einen IP-Set-Namen ein und klicken Sie auf **Einfügen**.
3. Wählen Sie auf der Seite **IPv4s** die virtuelle IP (sekundäre VIP) aus und klicken Sie auf **Einfügen**.
4. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.

**HINWEIS:**

Der IP-Satzname muss auf der primären und sekundären Instanz identisch sein.

**Schritt 4. Fügen Sie einen Lastausgleichs-virtuellen Server auf der primären Instanz hinzu.**

1. Navigieren Sie zu **Configuration > Traffic Management > Load Balancing > Virtual Servers > Add**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäre VIP) und Port hinzu.

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

3. Klicken Sie auf **More**. Navigieren Sie zu **IP Range IP Set Settings**, wählen Sie **IPset** aus dem Dropdown-Menü und geben Sie den in **Schritt 3** erstellten IPset an.
4. Klicken Sie auf **OK**, um den Lastausgleichs-virtuellen Server zu erstellen.

**Schritt 5. Fügen Sie einen Dienst oder eine Dienstgruppe auf der primären Instanz hinzu.**

1. Navigieren Sie zu **Configuration > Traffic Management > Load Balancing > Services > Add**.
2. Fügen Sie die erforderlichen Werte für Dienstname, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

**Schritt 6. Binden Sie den Dienst oder die Dienstgruppe an den Lastausgleichs-virtuellen Server auf der primären Instanz.**

1. Navigieren Sie zu **Configuration > Traffic Management > Load Balancing > Virtual Servers**.
2. Wählen Sie den in **Schritt 4** konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **Dienst und Dienstgruppen** auf **Keine Bindung des virtuellen Lastausgleichsserverdienstes**.
4. Wählen Sie den in **Schritt 5** konfigurierten Dienst aus und klicken Sie auf **Binden**.

**Schritt 7. Speichern Sie die Konfiguration.**

Andernfalls gehen alle Konfigurationen nach einem Neustart oder bei einem sofortigen Neustart verloren.

**Schritt 8. Überprüfen Sie die Konfiguration.**

Stellen Sie sicher, dass die ALB-Frontend-IP-Adresse nach einem Failover erreichbar ist.

1. Kopieren Sie die ALB-Frontend-IP-Adresse.
2. Fügen Sie die IP-Adresse in den Browser ein und stellen Sie sicher, dass die Back-End-Server erreichbar sind.
3. Führen Sie auf der primären Instanz ein Failover durch:

   Navigieren Sie in der NetScaler-GUI zu **Konfiguration > System > Hochverfügbarkeit > Aktion > Failover erzwingen**.

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

4. Stellen Sie sicher, dass die Back-End-Server nach dem Failover über die zuvor verwendete ALB-Frontend-IP erreichbar sind.

# Bereitstellen eines NetScaler® für eine private Azure DNS-Zone

Azure DNS ist ein Dienst in der Microsoft Azure-Infrastruktur zum Hosten von DNS-Domänen und zur Bereitstellung der Namensauflösung.

Private Azure DNS-Zonen sind ein Dienst, der sich auf die Auflösung von Domänennamen in einem privaten Netzwerk konzentriert. Mit privaten Zonen können Kunden ihre eigenen benutzerdefinierten Domänennamen verwenden, anstatt der heute verfügbaren von Azure bereitgestellten Namen.

NetScaler, die führende Lösung für die Anwendungsbereitstellung, eignet sich am besten, um Lastausgleichs- und GSLB-Funktionen für eine private Azure DNS-Zone bereitzustellen. Durch das Abonnieren der privaten Azure DNS-Zone kann das Unternehmen auf die Leistung und Intelligenz von NetScaler Global Server Load Balancing (GSLB) vertrauen, um den Intranet-Datenverkehr über Workloads in mehreren geografischen Regionen und Rechenzentren zu verteilen, die über sichere VPN-Tunnel verbunden sind. Diese Zusammenarbeit garantiert Unternehmen einen nahtlosen Zugriff auf den Teil ihrer Workload, den sie in die öffentliche Azure Cloud verschieben möchten.

## Übersicht über Azure DNS

Das Domain Name System (DNS) ist für die Übersetzung oder Auflösung eines Dienstnamens in seine IP-Adresse verantwortlich. Als Hosting-Dienst für DNS-Domänen bietet Azure DNS die Namensauflösung mithilfe der Microsoft Azure-Infrastruktur. Neben der Unterstützung von internetorientierten DNS-Domänen unterstützt Azure DNS jetzt auch private DNS-Domänen.

Azure DNS bietet einen zuverlässigen, sicheren DNS-Dienst zur Verwaltung und Auflösung von Domänennamen in einem virtuellen Netzwerk, ohne dass eine benutzerdefinierte DNS-Lösung erforderlich ist. Durch die Verwendung privater DNS-Zonen können Sie Ihre eigenen benutzerdefinierten Domänennamen anstelle der von Azure bereitgestellten Namen verwenden. Die Verwendung benutzerdefinierter Domänennamen hilft Ihnen, Ihre Architektur des virtuellen Netzwerks optimal an die Anforderungen Ihrer Organisation anzupassen. Es bietet Namensauflösung für virtuelle Maschinen (VMs) innerhalb eines virtuellen Netzwerks und zwischen virtuellen Netzwerken. Kunden können auch Zonennamen mit einer Split-Horizon-

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

Ansicht konfigurieren, die es einer privaten und einer öffentlichen DNS-Zone ermöglicht, einen Namen zu teilen.

## Warum NetScaler GSLB für private Azure DNS-Zonen?

In der heutigen Welt möchten Unternehmen ihre Workloads von lokalen Umgebungen in die Azure Cloud verlagern. Der Übergang zur Cloud ermöglicht es ihnen, Markteinführungszeiten, Investitionskosten/Preise, einfache Bereitstellung und Sicherheit zu optimieren. Der Azure DNS Private Zone Service bietet ein einzigartiges Angebot für Unternehmen, die einen Teil ihrer Workloads in die Azure Cloud verlagern. Diese Unternehmen können ihren privaten DNS-Namen, den sie jahrelang in lokalen Bereitstellungen hatten, verwenden, wenn sie den Private Zone Service nutzen. Bei diesem Hybridmodell, bei dem Intranet-Anwendungsserver lokal und in der Azure Cloud über sichere VPN-Tunnel verbunden sind, besteht die Herausforderung darin, einen nahtlosen Zugriff auf diese Intranet-Anwendungen zu gewährleisten. NetScaler löst diesen einzigartigen Anwendungsfall mit seiner globalen Lastausgleichsfunktion, die den Anwendungsverkehr zu den optimalsten verteilten Workloads/Servern entweder lokal oder in der Azure Cloud leitet und den Status der Anwendungsserver bereitstellt.

### Anwendungsfall

Benutzer in einem lokalen Netzwerk und in verschiedenen Azure VNets können sich mit den optimalsten Servern in einem internen Netzwerk verbinden, um auf die benötigten Inhalte zuzugreifen. Dies stellt sicher, dass die Anwendung immer verfügbar ist, die Kosten optimiert sind und die Benutzererfahrung gut ist. Azure Private Traffic Management (PTM) ist hier die primäre Anforderung. Azure PTM stellt sicher, dass die DNS-Abfragen der Benutzer zu einer geeigneten privaten IP-Adresse des Anwendungsservers aufgelöst werden.

### Lösung des Anwendungsfalls

NetScaler enthält die GSLB-Funktion (Global Server Load Balancing), um die Azure PTM-Anforderung zu erfüllen. GSLB fungiert als DNS-Server, der die DNS-Anfragen empfängt und die DNS-Anfrage in eine geeignete IP-Adresse auflöst, um Folgendes bereitzustellen:

- Nahtloses DNS-basiertes Failover.
- Phasenweise Migration von lokalen Umgebungen in die Cloud.
- A/B-Tests einer neuen Funktion.

Unter den vielen unterstützten Lastenausgleichsmethoden können die folgenden Methoden in dieser Lösung nützlich sein:

1. Round Robin

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

2. Statische Nähe (standortbasierte Serverauswahl). Sie kann auf zwei Arten bereitgestellt werden:

   a. EDNS Client Subnet (ECS) basierte GSLB auf NetScaler.

   b. Stellen Sie einen DNS-Forwarder für jedes virtuelle Netzwerk bereit.

## Topologie

Die folgende Abbildung zeigt die NetScaler GSLB-Bereitstellung für eine private Azure DNS-Zone.

Ein Benutzer kann auf jeden Anwendungsserver entweder in Azure oder On-Prem zugreifen, basierend auf der NetScaler GSLB-Methode in einer privaten Azure DNS-Zone. Der gesamte Datenverkehr zwischen On-Prem und dem virtuellen Azure-Netzwerk erfolgt ausschließlich über einen sicheren VPN-Tunnel. Anwendungsdatenverkehr, DNS-Datenverkehr und Überwachungsdatenverkehr sind in der vorhergehenden Topologie dargestellt. Je nach erforderlicher Redundanz können NetScaler und DNS-Forwarder in den virtuellen Netzwerken und Rechenzentren bereitgestellt werden. Der Einfachheit halber wird hier nur ein NetScaler gezeigt, aber wir empfehlen mindestens einen Satz NetScaler und DNS-Forwarder für die Azure-Region. Alle DNS-Abfragen der Benutzer gehen zuerst an den DNS-Forwarder, der Regeln für die Weiterleitung der Abfragen an einen geeigneten DNS-Server definiert hat.

### Konfigurieren von NetScaler für eine private Azure DNS-Zone

Getestete Produkte und Versionen:

| PRODUKT | VERSION |
|---|---|
| Azure | Cloud-Abonnement |
| NetScaler VPX | BYOL (Bring Your Own License) |

**HINWEIS:**

Die Bereitstellung wurde getestet und bleibt ab NetScaler Version 12.0 unverändert.

### Voraussetzungen

Im Folgenden sind die allgemeinen Voraussetzungen aufgeführt.

- Microsoft Azure Portal-Konto mit einem gültigen Abonnement.

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

- Stellen Sie die Konnektivität (sicherer VPN-Tunnel) zwischen der lokalen Umgebung und der Azure-Cloud sicher. Informationen zum Einrichten eines sicheren VPN-Tunnels in Azure finden Sie unter Schritt-für-Schritt: Konfigurieren eines Site-to-Site-VPN-Gateways zwischen Azure und lokalen Umgebungen.

## Lösungsbeschreibung

Wenn Sie eine Anwendung in einer privaten Azure DNS-Zone (rr.ptm.mysite.net) hosten möchten, die über HTTPS läuft und über Azure und lokale Umgebungen mit Intranetzugriff bereitgestellt wird, basierend auf der Round-Robin-GSLB-Lastverteilungsmethode. Um diese Bereitstellung zu erreichen, aktivieren Sie GSLB für die private Azure DNS-Zone mit NetScaler, die aus den folgenden Konfigurationen besteht:

1. Azure- und lokale Einrichtung konfigurieren.
2. NetScaler-Appliance im virtuellen Azure-Netzwerk.

## Azure- und lokale Einrichtung konfigurieren

Wie in der Topologie gezeigt, richten Sie das virtuelle Azure-Netzwerk (in diesem Fall VNet A, VNet B) und die lokale Einrichtung ein.

1. Erstellen Sie eine private Azure DNS-Zone mit dem Domänennamen (mysite.net).
2. Erstellen Sie zwei virtuelle Netzwerke (VNet A, VNet B) in einem Hub-and-Spoke-Modell in einer Azure-Region.
3. Stellen Sie App Server, DNS-Forwarder, Windows 10 Pro Client, NetScaler in VNet A bereit.
4. Stellen Sie einen App Server und einen DNS-Forwarder bereit, falls Clients in VNet B vorhanden sind.
5. Stellen Sie einen App-Server, einen DNS-Forwarder und einen Windows 10 Pro-Client lokal bereit.

### Private Azure DNS-Zone

Erstellen Sie eine private Azure DNS-Zone mit Domänennamen.

1. Melden Sie sich beim Azure-Portal an und wählen oder erstellen Sie ein Dashboard.
2. Klicken Sie auf **Ressource erstellen** und suchen Sie nach DNS-Zone, um eine private Azure DNS-Zone mit Domänennamen (in diesem Fall mysite.net) zu erstellen.

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

### Virtuelle Azure-Netzwerke (VNet A, VNet B) im Hub-and-Spoke-Modell

Erstellen Sie zwei virtuelle Netzwerke (VNet A, VNet B) in einem Hub-and-Spoke-Modell in einer Azure-Region.

1. Erstellen Sie zwei virtuelle Netzwerke.
2. Wählen Sie dasselbe Dashboard aus, klicken Sie auf **Ressource erstellen** und suchen Sie nach virtuellen Netzwerken, um zwei virtuelle Netzwerke, nämlich VNet A und VNet B, in derselben Region zu erstellen und diese zu koppeln, um ein Hub-and-Spoke-Modell zu bilden, wie in der folgenden Abbildung gezeigt. Weitere Informationen zum Einrichten einer Hub-and-Spoke-Topologie finden Sie unter Implementieren einer Hub-Spoke-Netzwerktopologie in Azure.

### VNet A-zu-VNet B-Peering

So peeren Sie VNet A und VNet B:

1. Klicken Sie im Menü **Einstellungen** von VNet A auf **Peerings** und peeren Sie VNet B.
2. Aktivieren Sie **Weitergeleiteten Datenverkehr zulassen** und **Gateway-Transit zulassen**, wie in der folgenden Abbildung gezeigt.

Die folgende Abbildung zeigt das erfolgreiche Peering von VNet A mit VNet B.

### VNet B-zu-VNet A-Peering

So peeren Sie VNet B und VNet A:

1. Klicken Sie im Menü **Einstellungen** von VNet B auf **Peerings** und peeren Sie VNet A.
2. Aktivieren Sie **Weitergeleiteten Datenverkehr zulassen** und verwenden Sie Remote-Gateways, wie in der folgenden Abbildung gezeigt.

Die folgende Abbildung zeigt das erfolgreiche Peering von VNet B mit VNet A.

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

### Bereitstellen von App-Server, DNS-Forwarder, Windows 10 Pro-Client, NetScaler in VNet A

Wir besprechen kurz den App-Server, den DNS-Forwarder, den Windows 10 Pro-Client und NetScaler in VNet A.

1. Wählen Sie dasselbe Dashboard aus, klicken Sie auf **Ressource erstellen**.
2. Suchen Sie nach den entsprechenden Instanzen und weisen Sie eine IP-Adresse aus dem VNet A-Subnetz zu.

#### App-Server

Ein App-Server ist nichts anderes als der Webserver (HTTP-Server), auf dem ein Ubuntu-Server 16.04 als Instanz auf der Azure- oder lokalen VM bereitgestellt wird. Um ihn als Webserver zu konfigurieren, geben Sie an der Eingabeaufforderung Folgendes ein:

```
sudo apt install apache2
```

#### Windows 10 Pro-Client

Starten Sie eine Windows 10 Pro-Instanz als Client-Maschine in VNet A und lokal.

#### NetScaler

NetScaler ergänzt die private Azure DNA-Zone durch Integritätsprüfungen und Analysen von NetScaler MAS. Starten Sie einen NetScaler aus dem Azure Marketplace basierend auf Ihren Anforderungen; hier haben wir NetScaler (BYOL) für diese Bereitstellung verwendet.

Detaillierte Schritte zur Bereitstellung von NetScaler auf Microsoft Azure finden Sie hier. Siehe Bereitstellen einer NetScaler VPX-Instanz in Microsoft Azure.

Nach der Bereitstellung verwenden Sie die NetScaler-IP, um NetScaler GSLB zu konfigurieren.

#### DNS-Forwarder

Er wird verwendet, um Client-Anfragen von gehosteten Domänen, die an NetScaler GSLB (ADNS IP) gebunden sind, weiterzuleiten. Starten Sie einen Ubuntu-Server 16.04 als Linux-Instanz (Ubuntu-Server 16.04) und beachten Sie die unten stehende URL, wie Sie ihn als DNS-Forwarder einrichten.

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

**HINWEIS:**

Für die Round-Robin-GSLB-Lastverteilungsmethode ist ein DNS-Forwarder pro Azure-Region ausreichend, aber für statische Proximity benötigen wir einen DNS-Forwarder pro virtuellem Netzwerk.

1. Nach der Bereitstellung des Forwarders ändern Sie die DNS-Server-Einstellungen des virtuellen Netzwerks A von Standard auf Benutzerdefiniert mit der IP-Adresse des VNet A DNS-Forwarders, wie in der folgenden Abbildung gezeigt.
2. Ändern Sie die Datei `named.conf.options` im VNet A DNS-Forwarder, um Weiterleitungsregeln für die Domäne (mysite.net) und Subdomäne (ptm.mysite.net) zur ADNS-IP von NetScaler GSLB hinzuzufügen.
3. Starten Sie den DNS-Forwarder neu, um die in der Datei `named.conf.options` vorgenommenen Änderungen zu übernehmen.

### VNet A DNS-Forwarder-Einstellungen

```
zone "mysite.net" {

           type forward;

forwarders { 168.63.129.16; };

};

zone "ptm.mysite.net" {

    type forward;

    forwarders { 10.8.0.5; };

};
```

**HINWEIS:**

Für die Zonen-IP-Adresse der Domäne ("mysite.net") verwenden Sie die DNS-IP-Adresse Ihrer Azure-Region. Für die Zonen-IP-Adresse der Subdomäne ("ptm.mysite.net") verwenden Sie alle ADNS-IP-Adressen Ihrer GSLB-Instanzen.

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

### App-Server und DNS-Forwarder bereitstellen, wenn sich Clients in VNet B befinden

1. Für das virtuelle Netzwerk B wählen Sie dasselbe Dashboard aus und klicken Sie auf **Ressource erstellen**.
2. Suchen Sie nach den entsprechenden Instanzen und weisen Sie eine IP-Adresse aus dem VNet B-Subnetz zu.
3. Starten Sie den App-Server und den DNS-Forwarder, wenn ein statisches Proximity-GSLB-Lastenausgleich ähnlich wie bei VNet A vorhanden ist.
4. Bearbeiten Sie die VNet B DNS-Forwarder-Einstellungen in `named.conf.options`, wie in der folgenden Einstellung gezeigt:

   VNet B DNS-Forwarder-Einstellungen:

```
zone "ptm.mysite.net" {

    type forward;

    forwarders { 10.8.0.5; };

};
```

Die folgende Abbildung zeigt die VNet B DNS-Forwarder-Einstellungen:

### App-Server, DNS-Forwarder und Windows 10 Pro-Client lokal bereitstellen

1. Für lokale Umgebungen starten Sie die VMs auf Bare Metal und stellen Sie den App-Server, den DNS-Forwarder und den Windows 10 Pro-Client ähnlich wie bei VNet A bereit.
2. Bearbeiten Sie die Einstellungen des lokalen DNS-Forwarders in `named.conf.options`, wie im folgenden Beispiel gezeigt.

#### Einstellungen des lokalen DNS-Forwarders

```
zone "mysite.net" {

           type forward;

           forwarders { 10.8.0.6; };

};
```

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

```
zone "ptm.mysite.net" {

    type forward;

    forwarders { 10.8.0.5; };

};
```

Für `mysite.net` haben wir die DNS-Forwarder-IP von VNet A anstelle der Azure Private DNS Zone Server-IP angegeben, da es sich um eine spezielle IP-Adresse handelt, die von lokalen Systemen nicht erreichbar ist. Daher ist diese Änderung in der DNS-Forwarder-Einstellung von lokalen Systemen erforderlich.

## NetScaler im virtuellen Azure-Netzwerk konfigurieren

Wie in der Topologie gezeigt, stellen Sie den NetScaler im virtuellen Azure-Netzwerk (in diesem Fall VNet A) bereit und greifen Sie über die NetScaler-GUI darauf zu.

### NetScaler GSLB konfigurieren

1. ADNS-Dienst erstellen.
2. Lokale und Remote-Sites erstellen.
3. Dienste für die lokalen virtuellen Server erstellen.
4. Virtuelle Server für die GSLB-Dienste erstellen.

### ADNS-Dienst hinzufügen

1. Melden Sie sich bei der NetScaler-GUI an.
2. Wählen Sie auf der Registerkarte **Configuration** die Option **Traffic Management > Load Balancing > Services**.
3. Fügen Sie einen Dienst hinzu. Wir empfehlen Ihnen, den ADNS-Dienst sowohl in TCP als auch in UDP zu konfigurieren, wie in der folgenden Abbildung gezeigt:

### GSLB-Sites hinzufügen

1. Fügen Sie lokale und Remote-Sites hinzu, zwischen denen GSLB konfiguriert werden soll.

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

2. Auf der Registerkarte **Konfiguration** navigieren Sie zu **Traffic Management > GSLB > GSLB Sites**. Fügen Sie eine Site wie im folgenden Beispiel gezeigt hinzu und wiederholen Sie den Vorgang für andere Sites.

### GSLB-Dienste hinzufügen

1. Fügen Sie GSLB-Dienste für die lokalen und Remote-virtuellen Server hinzu, die den Lastausgleich für App-Server durchführen.
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Traffic Management > GSLB > GSLB Services**.
3. Fügen Sie die Dienste wie in den folgenden Beispielen gezeigt hinzu.
4. Binden Sie den HTTP-Monitor, um den Serverstatus zu überprüfen.

5. Nachdem Sie den Dienst erstellt haben, wechseln Sie zur Registerkarte **Erweiterte Einstellungen** innerhalb des GSLB-Dienstes.
6. Klicken Sie auf **Monitor hinzufügen**, um den GSLB-Dienst mit einem HTTP-Monitor zu verbinden und den Dienststatus zu aktivieren.

7. Sobald Sie den HTTP-Monitor gebunden haben, wird der Status der Dienste als UP markiert, wie in der folgenden Abbildung gezeigt:

### Virtuellen GSLB-Server hinzufügen

Fügen Sie einen virtuellen GSLB-Server hinzu, über den die Alias-GSLB-Dienste der App-Server zugänglich sind.

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Traffic Management > GSLB > GSLB Virtual Servers**.
2. Fügen Sie die virtuellen Server hinzu, wie im folgenden Beispiel gezeigt.
3. Binden Sie GSLB-Dienste und Domänennamen daran.

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

4. Nachdem Sie den virtuellen GSLB-Server erstellt und die entsprechende Lastverteilungsmethode (in diesem Fall Round Robin) ausgewählt haben, binden Sie GSLB-Dienste und Domänen, um den Schritt abzuschließen.

5. Wechseln Sie zur Registerkarte **Erweiterte Einstellungen** innerhalb des virtuellen Servers und klicken Sie auf die Registerkarte **Domänen hinzufügen**, um eine Domäne zu binden.
6. Gehen Sie zu **Erweitert > Dienste** und klicken Sie auf den Pfeil, um einen GSLB-Dienst zu binden und alle drei Dienste (VNet A, VNet B, On-premises) an den virtuellen Server zu binden.

   Nachdem GSLB-Dienste und Domäne an den virtuellen Server gebunden wurden, wird es wie in der folgenden Abbildung gezeigt:

   Einstellungen für virtuelle GSLB-Server(/en-us/vpx/media/image-23.png)

Überprüfen Sie, ob der virtuelle GSLB-Server aktiv und zu 100 % fehlerfrei ist. Wenn der Monitor anzeigt, dass der Server aktiv und fehlerfrei ist, bedeutet dies, dass die Sites synchronisiert sind und die Backend-Dienste verfügbar sind.

Lastausgleich virtueller GSLB-Server(/en-us/vpx/media/image-24.png)

Um die Bereitstellung zu testen, greifen Sie über eine Cloud-Clientmaschine oder eine lokale Clientmaschine auf die Domain-URL `rr.ptm.mysite.net` zu. Wenn Sie über eine Cloud-Windows-Clientmaschine darauf zugreifen, stellen Sie sicher, dass der lokale App-Server in einer privaten DNS-Zone ohne die Notwendigkeit von Drittanbieter- oder benutzerdefinierten DNS-Lösungen aufgerufen wird.

## Konfigurieren einer NetScaler VPX-Instanz für Azure Accelerated Networking

Beschleunigtes Netzwerk ermöglicht die Single Root I/O Virtualization (SR-IOV) Virtual Function (VF) NIC für eine virtuelle Maschine, was die Netzwerkleistung verbessert. Sie können diese Funktion bei hohen Arbeitslasten verwenden, die Daten mit höherem Durchsatz, zuverlässigem Streaming und geringerer CPU-Auslastung senden oder empfangen müssen. Wenn eine NIC mit beschleunigtem Netzwerk aktiviert ist, bündelt Azure die vorhandene paravirtualisierte (PV) Schnittstelle der NIC mit einer SR-IOV VF-Schnittstelle. Die Unterstützung der SR-IOV VF-Schnittstelle ermöglicht und verbessert den Durchsatz der NetScaler VPX-Instanz.

Beschleunigtes Netzwerk bietet die folgenden Vorteile:

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

- Geringere Latenz
- Höhere Pakete pro Sekunde (pps)-Leistung
- Verbesserter Durchsatz
- Reduzierter Jitter
- Geringere CPU-Auslastung

**HINWEIS:**

Azure Accelerated Networking wird auf NetScaler VPX-Instanzen ab Release 13.0 Build 76.29 unterstützt.

## Voraussetzungen

- Stellen Sie sicher, dass Ihre VM-Größe den Anforderungen für Azure Accelerated Networking entspricht.
- Beenden Sie VMs (einzeln oder in einer Verfügbarkeitsgruppe), bevor Sie beschleunigtes Netzwerk auf einer beliebigen NIC aktivieren.

## Einschränkungen

Beschleunigtes Netzwerk kann nur für einige Instanztypen aktiviert werden. Weitere Informationen finden Sie unter Unterstützte Instanztypen.

## Für beschleunigtes Netzwerk unterstützte NICs

Azure stellt Mellanox ConnectX3-, ConnectX4- und ConnectX5-NICs im SR-IOV-Modus für beschleunigtes Netzwerk bereit.

Wenn beschleunigtes Netzwerk auf einer NetScaler VPX-Schnittstelle aktiviert ist, bündelt Azure entweder eine ConnectX3-, ConnectX4- oder ConnectX5-Schnittstelle mit der vorhandenen PV-Schnittstelle einer NetScaler VPX-Appliance.

Weitere Informationen zum Aktivieren des beschleunigten Netzwerks vor dem Anfügen einer Schnittstelle an eine VM finden Sie unter Erstellen einer Netzwerkschnittstelle mit beschleunigtem Netzwerk.

Weitere Informationen zum Aktivieren des beschleunigten Netzwerks auf einer vorhandenen Schnittstelle einer VM finden Sie unter Vorhandene Schnittstellen auf einer VM aktivieren.

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

## So aktivieren Sie beschleunigtes Netzwerk auf einer NetScaler VPX-Instanz über die Azure-Konsole

Sie können beschleunigtes Netzwerk auf einer bestimmten Schnittstelle über die Azure-Konsole oder Azure PowerShell aktivieren.

Führen Sie die folgenden Schritte aus, um beschleunigtes Netzwerk mithilfe von Azure-Verfügbarkeitsgruppen oder Verfügbarkeitszonen zu aktivieren.

1. Melden Sie sich beim Azure-Portal an und navigieren Sie zum **Azure Marketplace**.

2. Suchen Sie im **Azure Marketplace** nach **NetScaler**.

3. Wählen Sie einen Nicht-FIPS-NetScaler-Plan zusammen mit der Lizenz aus und klicken Sie auf **Erstellen**.

   Die Seite **NetScaler erstellen** wird angezeigt.

4. Erstellen Sie auf der Registerkarte **Grundlagen** eine Ressourcengruppe. Geben Sie auf der Registerkarte **Parameter** Details für Region, Administrator-Benutzername, Administrator-Passwort, Lizenztyp (VM SKU) und andere Felder ein.

5. Klicken Sie auf **Weiter: VM-Konfigurationen >**.

   Führen Sie auf der Seite **VM-Konfigurationen** Folgendes aus:

   a. Konfigurieren Sie ein Suffix für den öffentlichen IP-Domänennamen.

   b. Aktivieren oder deaktivieren Sie **Azure Monitoring Metrics**.

   c. Aktivieren oder deaktivieren Sie **Backend Autoscale™**.

6. Klicken Sie auf **Weiter: Netzwerk und zusätzliche Einstellungen >**.

   Erstellen Sie auf der Seite **Netzwerk und zusätzliche Einstellungen** ein Startdiagnosekonto und konfigurieren Sie die Netzwerkeinstellungen.

   Im Abschnitt **Beschleunigtes Netzwerk** haben Sie die Möglichkeit, das beschleunigte Netzwerk separat für die Verwaltungsschnittstelle, die Clientschnittstelle und die Serverschnittstelle zu aktivieren oder zu deaktivieren.

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

7. Klicken Sie auf **Weiter: Überprüfen + erstellen >**.

   Nach erfolgreicher Validierung überprüfen Sie die Grundeinstellungen, VM-Konfigurationen, Netzwerk- und zusätzlichen Einstellungen und klicken Sie auf **Erstellen**. Es kann einige Zeit dauern, bis die Azure-Ressourcengruppe mit den erforderlichen Konfigurationen erstellt wird.

8. Wählen Sie nach Abschluss der Bereitstellung die **Ressourcengruppe** aus, um die Konfigurationsdetails anzuzeigen.

9. Um die Konfigurationen für beschleunigtes Netzwerk zu überprüfen, wählen Sie **Virtuelle Maschine > Netzwerk**. Der Status des beschleunigten Netzwerks wird für jede NIC als **Aktiviert** oder **Deaktiviert** angezeigt.

## Beschleunigtes Netzwerk mit Azure PowerShell aktivieren

Wenn Sie das beschleunigte Netzwerk nach der VM-Erstellung aktivieren müssen, können Sie dies mit Azure PowerShell tun.

**HINWEIS:**

Stellen Sie sicher, dass Sie die VM anhalten, bevor Sie das beschleunigte Netzwerk mit Azure PowerShell aktivieren.

Führen Sie die folgenden Schritte aus, um das beschleunigte Netzwerk mit Azure PowerShell zu aktivieren.

1. Navigieren Sie zum **Azure-Portal** und klicken Sie auf das **PowerShell**-Symbol in der oberen rechten Ecke.

   **HINWEIS:**

   Wenn Sie sich im Bash-Modus befinden, wechseln Sie in den PowerShell-Modus.

2. Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

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

```
az network nic update --name <nic-name> --accelerated-networking [true
| false] --resource-group <resourcegroup-name>
```

Der Parameter für beschleunigtes Netzwerk akzeptiert einen der folgenden Werte:

- **Wahr:** Aktiviert Accelerated Networking auf der angegebenen NIC.
- **Falsch:** Deaktiviert Accelerated Networking auf der angegebenen NIC.

**So aktivieren Sie Accelerated Networking auf einer bestimmten NIC:**

```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-
networking true --resource-group rsgp1-aan
```

**So deaktivieren Sie Accelerated Networking auf einer bestimmten NIC:**

```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-
networking false --resource-group rsgp1-aan
```

3. Um den Status von Accelerated Networking nach Abschluss der Bereitstellung zu überprüfen, navigieren Sie zu **VM > Networking**.

   Im folgenden Beispiel sehen Sie, dass Accelerated Networking **aktiviert** ist.

   Im folgenden Beispiel sehen Sie, dass Accelerated Networking **deaktiviert** ist.

## So überprüfen Sie Accelerated Networking auf einer Schnittstelle mithilfe der FreeBSD-Shell von NetScaler

Sie können sich bei der FreeBSD-Shell von NetScaler anmelden und die folgenden Befehle ausführen, um den Status von Accelerated Networking zu überprüfen.

**Beispiel für ConnectX3 NIC:**

Das folgende Beispiel zeigt die Ausgabe des Befehls „ifconfig“ der Mellanox ConnectX3 NIC. „50/n“ bezeichnet die VF-Schnittstellen der Mellanox ConnectX3 NICs. 0/1 und 1/1 bezeichnen die PV-Schnittstellen der NetScaler VPX-Instanz. Sie können beobachten, dass sowohl die PV-Schnittstelle (1/1) als auch die CX3 VF-Schnittstelle (50/1) dieselben MAC-Adressen (00:22:48:1c:99:3e) haben. Dies deutet darauf hin, dass die beiden Schnittstellen gebündelt sind.

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

**Beispiel für ConnectX4 NIC:**

Das folgende Beispiel zeigt die Ausgabe des Befehls „ifconfig“ der Mellanox ConnectX4 NIC. „100/n“ bezeichnet die VF-Schnittstellen der Mellanox ConnectX4 NICs. 0/1, 1/1 und 1/2 bezeichnen die PV-Schnittstellen der NetScaler VPX-Instanz. Sie können beobachten, dass sowohl die PV-Schnittstelle (1/1) als auch die CX4 VF-Schnittstelle (100/1) dieselben MAC-Adressen (00:0d:3a:9b:f2:1d) haben. Dies deutet darauf hin, dass die beiden Schnittstellen gebündelt sind. Ähnlich haben die PV-Schnittstelle (1/2) und die CX4 VF-Schnittstelle (100/2) dieselben MAC-Adressen (00:0d:3a:1e:d2:23).

## So überprüfen Sie die beschleunigte Netzwerkanbindung auf einer Schnittstelle mithilfe der ADC-CLI

**Beispiel für ConnectX3 NIC:**

Die folgende Ausgabe des Befehls „show interface“ zeigt an, dass die PV-Schnittstelle 1/1 mit der virtuellen Funktion 50/1 gebündelt ist, die eine SR-IOV VF NIC ist. Die MAC-Adressen beider NICs 1/1 und 50/1 sind identisch. Nachdem die beschleunigte Netzwerkanbindung aktiviert wurde, werden die Daten der Schnittstelle 1/1 über den Datenpfad der Schnittstelle 50/1 gesendet, die eine ConnectX3-Schnittstelle ist. Sie können sehen, dass die Ausgabe von „show interface“ der PV-Schnittstelle (1/1) auf die VF (50/1) verweist. Ebenso verweist die Ausgabe von „show interface“ der VF-Schnittstelle (50/1) auf die PV-Schnittstelle (1/1).

**Beispiel für ConnectX4 NIC:**

Die folgende Ausgabe des Befehls „show interface“ zeigt an, dass die PV-Schnittstelle 1/1 mit der virtuellen Funktion 100/1 gebündelt ist, die eine SR-IOV VF NIC ist. Die MAC-Adressen beider NICs 1/1 und 100/1 sind identisch. Nachdem die beschleunigte Netzwerkanbindung aktiviert wurde, werden die Daten der Schnittstelle 1/1 über den Datenpfad der Schnittstelle 100/1 gesendet, die eine ConnectX4-Schnittstelle ist. Sie können sehen, dass die Ausgabe von „show interface“ der PV-Schnittstelle (1/1) auf die VF (100/1) verweist. Ebenso verweist die Ausgabe von „show interface“ der VF-Schnittstelle (100/1) auf die PV-Schnittstelle (1/1).

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

## Wichtige Hinweise in NetScaler

- Die PV-Schnittstelle gilt als primäre oder Hauptschnittstelle für alle notwendigen Operationen. Konfigurationen müssen nur auf PV-Schnittstellen durchgeführt werden.
- Alle „set“-Operationen auf einer VF-Schnittstelle sind blockiert, außer den folgenden:
  - Schnittstelle aktivieren
  - Schnittstelle deaktivieren
  - Schnittstelle zurücksetzen
  - Statistiken löschen

  **HINWEIS:**

  Citrix® empfiehlt, keine Operationen auf der VF-Schnittstelle durchzuführen.

- Sie können die Bindung der PV-Schnittstelle an die VF-Schnittstelle mit dem `show interface` Befehl überprüfen.
- Ab NetScaler-Release 13.1-33.x kann eine NetScaler VPX-Instanz dynamische NIC-Entfernungen und die erneute Anbindung der entfernten NICs in Azure Accelerated Networking nahtlos handhaben. Azure kann SR-IOV VF-NICs des Accelerated Networking für ihre Host-Wartungsaktivitäten entfernen. Immer wenn eine NIC von einer Azure VM entfernt wird, zeigt die NetScaler VPX-Instanz den Schnittstellenstatus als „Link Down“ an, und der Datenverkehr läuft nur über die virtuelle Schnittstelle. Nachdem die entfernte NIC wieder angefügt wurde, verwenden die VPX-Instanzen die wieder angefügte SR-IOV VF-NIC. Dieser Prozess erfolgt nahtlos und erfordert keine Konfiguration.

## Ein VLAN für eine PV-Schnittstelle konfigurieren

Wenn eine PV-Schnittstelle an ein VLAN gebunden ist, ist die zugehörige beschleunigte VF-Schnittstelle ebenfalls an dasselbe VLAN wie die PV-Schnittstelle gebunden. In diesem Beispiel ist die PV-Schnittstelle (1/1) an VLAN (20) gebunden. Die VF-Schnittstelle (100/1), die mit der PV-Schnittstelle (1/1) gebündelt ist, ist ebenfalls an VLAN 20 gebunden.

**Beispiel:**

1. Ein VLAN erstellen.

```
add vlan 20
```

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

2. Ein VLAN an die PV-Schnittstelle binden.

```
bind vlan 20 –ifnum 1/1


show vlan


1)  VLAN ID: 1
    Link-local IPv6 addr: fe80::20d:3aff:fe9b:f21d/64
    Interfaces : LO/1


2)  VLAN ID: 10     VLAN Alias Name:
    Interfaces : 0/1 100/1
    IPs : 10.0.1.29  Mask: 255.255.255.0


3)  VLAN ID: 20     VLAN Alias Name:
    Interfaces :  1/1 100/2
```

**HINWEIS:**

VLAN-Bindungsvorgänge sind auf einer beschleunigten VF-Schnittstelle nicht zulässig.

```
bind vlan 1 -ifnum 100/1

ERROR: Operation not permitted
```

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

# HA-INC-Knoten mithilfe der NetScaler® Hochverfügbarkeitsvorlage mit Azure ILB konfigurieren

Sie können ein Paar VPX-Instanzen im HA-INC-Modus schnell und effizient mithilfe der Standardvorlage für Intranet-Anwendungen bereitstellen. Der interne Azure Load Balancer (ILB) verwendet eine interne oder private IP-Adresse für das Frontend, wie in Abbildung 1 gezeigt. Die Vorlage erstellt zwei Knoten mit drei Subnetzen und sechs NICs. Die Subnetze sind für Management-, Client- und serverseitigen Datenverkehr vorgesehen, wobei jedes Subnetz zu einer anderen NIC auf jedem Gerät gehört.

Abbildung 1: NetScaler HA-Paar für Clients in einem internen Netzwerk

Sie können diese Bereitstellung auch verwenden, wenn das NetScaler HA-Paar hinter einer Firewall ist, wie in Abbildung 2 gezeigt. Die öffentliche IP-Adresse gehört zur Firewall und wird per NAT an die Frontend-IP-Adresse des ILB weitergeleitet.

Abbildung 2: NetScaler HA-Paar mit Firewall mit öffentlicher IP-Adresse

Sie können die NetScaler HA-Paar-Vorlage für Intranet-Anwendungen im Azure-Portal abrufen.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein Hochverfügbarkeits-VPX-Paar mithilfe von Azure Availability Sets bereitzustellen.

1. Navigieren Sie im Azure-Portal zur Seite **Benutzerdefinierte Bereitstellung**.
2. Die Seite **Grundlagen** wird angezeigt. Erstellen Sie eine Ressourcengruppe. Geben Sie unter der Registerkarte **Parameter** Details für Region, Administrator-Benutzernamen, Administrator-Passwort, Lizenztyp ( `VM sku` ) und andere Felder ein.

3. Klicken Sie auf **Weiter: Überprüfen + erstellen >**.

   Es kann einen Moment dauern, bis die Azure-Ressourcengruppe mit den erforderlichen Konfigurationen erstellt ist. Wählen Sie nach Abschluss die Ressourcengruppe im Azure-Portal aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools und Integritätstests anzuzeigen. Das Hochverfügbarkeitspaar wird als ADC-VPX-0 und ADC-VPX-1 angezeigt.

   Wenn weitere Änderungen für Ihr HA-Setup erforderlich sind, wie das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal tun.

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

Sobald die erforderliche Konfiguration abgeschlossen ist, werden die folgenden Ressourcen erstellt.

4. Melden Sie sich an den Knoten **ADC-VPX-0** und **ADC-VPX-1** an, um die folgende Konfiguration zu überprüfen:

   - Die NSIP-Adressen für beide Knoten müssen sich im Management-Subnetz befinden.
   - Auf dem primären (ADC-VPX-0) und sekundären (ADC-VPX-1) Knoten müssen Sie zwei SNIP-Adressen sehen. Eine SNIP (Client-Subnetz) wird für die Beantwortung von ILB-Probes verwendet, und die andere SNIP (Server-Subnetz) wird für die Kommunikation mit dem Back-End-Server verwendet.

   **HINWEIS:**

   Im HA-INC-Modus sind die SNIP-Adressen der ADC-VPX-0- und ADC-VPX-1-VMs unterschiedlich, obwohl sie sich im selben Subnetz befinden, im Gegensatz zur klassischen lokalen ADC-HA-Bereitstellung, bei der beide gleich sind. Um Bereitstellungen zu unterstützen, bei denen sich die VPX-Paar-SNIP in verschiedenen Subnetzen befindet, oder wenn die VIP nicht im selben Subnetz wie eine SNIP ist, müssen Sie entweder Mac-Based Forwarding (MBF) aktivieren oder eine statische Hostroute für jede VIP zu jedem VPX-Knoten hinzufügen.

   Auf dem primären Knoten (ADC-VPX-0)

   Auf dem sekundären Knoten (ADC-VPX-1)

5. Nachdem die primären und sekundären Knoten UP sind und der Synchronisierungsstatus **SUCCESS** lautet, müssen Sie den virtuellen Lastausgleichsserver oder den virtuellen Gateway-Server auf dem primären Knoten (ADC-VPX-0) mit der privaten Floating-IP-Adresse (FIP) des ADC Azure Load Balancers konfigurieren. Weitere Informationen finden Sie im Abschnitt Beispielkonfiguration.
6. Um die private IP-Adresse des ADC Azure Load Balancers zu finden, navigieren Sie zu **Azure-Portal > ADC Azure Load Balancer > Frontend-IP-Konfiguration**.

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

7. Auf der Konfigurationsseite des **Azure Load Balancers** hilft die Bereitstellung der ARM-Vorlage beim Erstellen der LB-Regel, Back-End-Pools und Integritätstests.

   - Die LB-Regel (LbRule1) verwendet standardmäßig Port 80.

   - Bearbeiten Sie die Regel, um Port 443 zu verwenden, und speichern Sie die Änderungen.

     **HINWEIS:**

     Für erhöhte Sicherheit empfiehlt Citrix®, SSL-Port 443 für den virtuellen LB-Server oder den virtuellen Gateway-Server zu verwenden.

Um weitere VIP-Adressen auf dem ADC hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Azure Load Balancer > Frontend-IP-Konfiguration**, und klicken Sie auf **Hinzufügen**, um eine neue interne Load Balancer-IP-Adresse zu erstellen.

2. Geben Sie auf der Seite **Frontend-IP-Adresse hinzufügen** einen Namen ein, wählen Sie das Client-Subnetz aus, weisen Sie entweder eine dynamische oder statische IP-Adresse zu und klicken Sie auf **Hinzufügen**.

3. Die Frontend-IP-Adresse wird erstellt, aber es ist keine LB-Regel zugeordnet. Erstellen Sie eine neue Lastenausgleichsregel und ordnen Sie sie der Frontend-IP-Adresse zu.

4. Auf der Seite **Azure Load Balancer** wählen Sie **Lastenausgleichsregeln** aus und klicken Sie dann auf **Hinzufügen**.

5. Erstellen Sie eine neue LB-Regel, indem Sie die neue Front-End-IP-Adresse und den Port auswählen. Das Feld **Floating IP** muss auf **Aktiviert** gesetzt werden.

6. Nun zeigt die **Frontend-IP-Konfiguration** die angewendete LB-Regel an.

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

## Beispielkonfiguration

Um einen Gateway-VPN-Virtual-Server und einen Lastenausgleichs-Virtual-Server zu konfigurieren, führen Sie die folgenden Befehle auf dem primären Knoten (ADC-VPX-0) aus. Die Konfiguration wird automatisch mit dem sekundären Knoten (ADC-VPX-1) synchronisiert.

Gateway-Beispielkonfiguration

```
enable feature aaa LB SSL SSLVPN

enable ns mode MBF

add vpn vserver vpn_ssl SSL 10.11.1.4 443

add ssl certKey ckp -cert wild-cgwsanity.cer -key wild-cgwsanity.key

bind ssl vserver vpn_ssl -certkeyName ckp
```

Lastenausgleichs-Beispielkonfiguration

```
enable feature LB SSL

enable ns mode MBF

add lb vserver lb_vs1 SSL 10.11.1.7 443

bind ssl vserver lb_vs1 -certkeyName ckp
```

Sie können nun auf den Lastenausgleichs- oder VPN-Virtual-Server zugreifen, indem Sie den vollqualifizierten Domänennamen (FQDN) verwenden, der der internen IP-Adresse des ILB zugeordnet ist.

Weitere Informationen zur Konfiguration des Lastenausgleichs-Virtual-Servers finden Sie im Abschnitt **Ressourcen**.

**Ressourcen**:

Die folgenden Links bieten zusätzliche Informationen zur HA-Bereitstellung und Virtual-Server-Konfiguration:

- Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen
- Einrichten des grundlegenden Lastenausgleichs

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

**Verwandte Ressourcen**:

- Konfigurieren einer Hochverfügbarkeits-Einrichtung mit mehreren IP-Adressen und NICs mithilfe von PowerShell-Befehlen
- Konfigurieren von GSLB in einer Active-Standby-HA-Bereitstellung in Azure

## HA-INC-Knoten mithilfe der NetScaler® Hochverfügbarkeitsvorlage für internetorientierte Anwendungen konfigurieren

Sie können schnell und effizient ein Paar VPX-Instanzen im HA-INC-Modus mithilfe der Standardvorlage für internetorientierte Anwendungen bereitstellen. Der Azure Load Balancer (ALB) verwendet eine öffentliche IP-Adresse für das Frontend. Die Vorlage erstellt zwei Knoten mit drei Subnetzen und sechs NICs. Die Subnetze sind für Management-, Client- und serverseitigen Datenverkehr vorgesehen. Jedes Subnetz verfügt über zwei NICs für beide VPX-Instanzen.

Sie können die NetScaler HA-Paar-Vorlage für internetorientierte Anwendungen im Azure Marketplace erhalten.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein Hochverfügbarkeits-VPX-Paar mithilfe von Azure-Verfügbarkeitsgruppen oder -Verfügbarkeitszonen bereitzustellen.

1. Suchen Sie im Azure Marketplace nach **NetScaler**.
2. Klicken Sie auf **JETZT ERHALTEN**.

3. Wählen Sie die erforderliche HA-Bereitstellung zusammen mit der Lizenz aus und klicken Sie auf **Weiter**.

4. Die Seite **Grundlagen** wird angezeigt. Erstellen Sie eine Ressourcengruppe. Geben Sie unter der Registerkarte **Parameter** Details für Region, Administrator-Benutzernamen, Administrator-Passwort, Lizenztyp (VM SKU) und andere Felder ein.

5. Klicken Sie auf **Weiter : VM-Konfigurationen >**.

6. Führen Sie auf der Seite **VM-Konfigurationen** Folgendes aus:

   - Suffix des öffentlichen IP-Domänennamens konfigurieren

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

- Aktivieren oder deaktivieren Sie **Azure Monitoring Metrics**
- Aktivieren oder deaktivieren Sie **Backend Autoscale™**

7. Klicken Sie auf **Weiter: Netzwerk und zusätzliche Einstellungen >**

8. Erstellen Sie auf der Seite **Netzwerk und zusätzliche Einstellungen** ein Startdiagnosekonto und konfigurieren Sie die Netzwerkeinstellungen.

9. Klicken Sie auf **Weiter: Überprüfen + erstellen >**.
10. Überprüfen Sie die Grundeinstellungen, die VM-Konfiguration, die Netzwerk- und zusätzlichen Einstellungen und klicken Sie auf **Erstellen**.

    Es kann einen Moment dauern, bis die Azure-Ressourcengruppe mit den erforderlichen Konfigurationen erstellt wird. Wählen Sie nach Abschluss die Ressourcengruppe im Azure-Portal aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools und Integritätstests anzuzeigen. Das Hochverfügbarkeitspaar wird als **citrix-adc-vpx-0** und **citrix-adc-vpx-1** angezeigt.

    Wenn weitere Änderungen für Ihr HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal tun.

    Sobald die erforderliche Konfiguration abgeschlossen ist, werden die folgenden Ressourcen erstellt.

11. Sie müssen sich bei den Knoten **citrix-adc-vpx-0** und **citrix-adc-vpx-1** anmelden, um die folgende Konfiguration zu überprüfen:

    - NSIP-Adressen für beide Knoten müssen sich im Verwaltungs-Subnetz befinden.
    - Auf den primären (citrix-adc-vpx-0) und sekundären (citrix-adc-vpx-1) Knoten müssen Sie zwei SNIP-Adressen sehen. Eine SNIP (Client-Subnetz) wird für die Beantwortung der ALB-Probes verwendet, und die andere SNIP (Server-Subnetz) wird für die Back-End-Serverkommunikation verwendet.

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

**HINWEIS:**

Im HA-INC-Modus sind die SNIP-Adressen der VMs citrix-adc-vpx-0 und citrix-adc-vpx-1 unterschiedlich, im Gegensatz zur klassischen lokalen ADC-Hochverfügbarkeitsbereitstellung, bei der beide gleich sind.

Auf dem primären Knoten (citrix-adc-vpx-0)

Auf dem sekundären Knoten (citrix-adc-vpx-1)

12. Nachdem die primären und sekundären Knoten UP sind und der Synchronisierungsstatus **SUCCESS** lautet, müssen Sie den virtuellen Lastausgleichsserver oder den virtuellen Gateway-Server auf dem primären Knoten (citrix-adc-vpx-0) mit der öffentlichen IP-Adresse des virtuellen ALB-Servers konfigurieren. Weitere Informationen finden Sie im Abschnitt Beispielkonfiguration.
13. Um die öffentliche IP-Adresse des virtuellen ALB-Servers zu finden, navigieren Sie zu **Azure-Portal > Azure Load Balancer > Frontend-IP-Konfiguration**.

14. Fügen Sie die eingehende Sicherheitsregel für den virtuellen Server-Port 443 in der Netzwerksicherheitsgruppe beider Client-Schnittstellen hinzu.

15. Konfigurieren Sie den ALB-Port, auf den Sie zugreifen möchten, und erstellen Sie eine eingehende Sicherheitsregel für den angegebenen Port. Der Backend-Port ist Ihr virtueller Lastausgleichsserver-Port oder der virtuelle VPN-Server-Port.

16. Jetzt können Sie auf den virtuellen Lastausgleichsserver oder den virtuellen VPN-Server mithilfe des vollqualifizierten Domänennamens (FQDN) zugreifen, der der öffentlichen IP-Adresse des ALB zugeordnet ist.

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

## Beispielkonfiguration

Um einen virtuellen Gateway-VPN-Server und einen virtuellen Lastausgleichsserver zu konfigurieren, führen Sie die folgenden Befehle auf dem primären Knoten (ADC-VPX-0) aus. Die Konfiguration wird automatisch mit dem sekundären Knoten (ADC-VPX-1) synchronisiert.

Gateway-Beispielkonfiguration

```
enable feature aaa LB SSL SSLVPN

add ip 52.172.55.197 255.255.255.0 -type VIP

add vpn vserver vpn_ssl SSL 52.172.55.197 443

add ssl certKey ckp -cert cgwsanity.cer -key cgwsanity.key

bind ssl vserver vpn_ssl -certkeyName ckp
```

Lastausgleichs-Beispielkonfiguration

```
enable feature LB SSL

enable ns mode MBF

add lb vserver lb_vs1 SSL 52.172.55.197 443

bind ssl vserver lb_vs1 -certkeyName ckp
```

Sie können jetzt auf den virtuellen Lastausgleichs- oder VPN-Server mithilfe des FQDN zugreifen, der der öffentlichen IP-Adresse des ALB zugeordnet ist.

Weitere Informationen zur Konfiguration des virtuellen Lastausgleichsservers finden Sie im Abschnitt **Ressourcen**.

**Ressourcen**:

Die folgenden Links bieten zusätzliche Informationen zur HA-Bereitstellung und virtuellen Serverkonfiguration:

- Virtuelle Server erstellen
- Grundlegenden Lastausgleich einrichten

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

# Konfigurieren eines Hochverfügbarkeits-Setups mit externen und internen Azure Load Balancern gleichzeitig

Das Hochverfügbarkeitspaar in Azure unterstützt gleichzeitig sowohl externe als auch interne Load Balancer.

Sie haben die folgenden zwei Optionen, um ein Hochverfügbarkeitspaar zu konfigurieren, das sowohl externe als auch interne Azure Load Balancer verwendet:

- Verwenden von zwei virtuellen LB-Servern auf der NetScaler Appliance.
- Verwenden eines virtuellen LB-Servers und eines IP-Sets. Der einzelne virtuelle LB-Server leitet den Datenverkehr an mehrere IPs weiter, die durch das IPset definiert sind.

Führen Sie die folgenden Schritte aus, um ein Hochverfügbarkeitspaar in Azure zu konfigurieren, das gleichzeitig sowohl externe als auch interne Load Balancer verwendet:

Für die Schritte 1 und 2 verwenden Sie das Azure-Portal. Für die Schritte 3 und 4 verwenden Sie die NetScaler VPX GUI oder die CLI.

**Schritt 1.** Konfigurieren Sie einen Azure Load Balancer, entweder einen externen Load Balancer oder einen internen Load Balancer.

Weitere Informationen zum Konfigurieren eines Hochverfügbarkeits-Setups mit externen Azure Load Balancern finden Sie unter Konfigurieren eines Hochverfügbarkeits-Setups mit mehreren IP-Adressen und NIC.

Weitere Informationen zum Konfigurieren eines Hochverfügbarkeits-Setups mit internen Azure Load Balancern finden Sie unter HA-INC-Knoten mithilfe der NetScaler-Hochverfügbarkeitsvorlage mit Azure ILB konfigurieren.

**Schritt 2.** Erstellen Sie einen zusätzlichen Load Balancer (ILB) in Ihrer Ressourcengruppe. Wenn Sie in Schritt 1 einen externen Load Balancer erstellt haben, erstellen Sie nun einen internen Load Balancer und umgekehrt.

- Um einen internen Load Balancer zu erstellen, wählen Sie den Load Balancer-Typ als **Intern**. Für das Feld **Subnetz** müssen Sie Ihr NetScaler-Client-Subnetz auswählen. Sie können eine statische IP-Adresse in diesem Subnetz angeben, sofern es keine Konflikte gibt. Andernfalls wählen Sie die dynamische IP-Adresse.

- Um einen externen Load Balancer zu erstellen, wählen Sie den Load Balancer-Typ als **Öffentlich** und erstellen Sie hier die öffentliche IP-Adresse.

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

1. Nachdem Sie den Azure Load Balancer erstellt haben, navigieren Sie zu **Frontend-IP-Konfiguration** und notieren Sie die hier angezeigte IP-Adresse. Sie müssen diese IP-Adresse beim Erstellen des virtuellen ADC-Lastausgleichsservers wie in Schritt 3 verwenden.

2. Auf der Seite **Azure Load Balancer-Konfiguration** hilft die ARM-Vorlagenbereitstellung beim Erstellen der LB-Regel, der Backend-Pools und der Integritätstests.
3. Fügen Sie die Client-NICs des Hochverfügbarkeitspaares zum Backend-Pool für den ILB hinzu.
4. Erstellen Sie einen Integritätstest (TCP, Port 9000)
5. Erstellen Sie zwei Lastausgleichsregeln:
   - Eine LB-Regel für HTTP-Datenverkehr (Webanwendungs-Anwendungsfall) auf Port 80. Die Regel muss auch den Backend-Port 80 verwenden. Wählen Sie den erstellten Backend-Pool und den Integritätstest aus. Floating IP muss aktiviert sein.
   - Eine weitere LB-Regel für HTTPS- oder CVAD-Datenverkehr auf Port 443. Der Prozess ist derselbe wie beim HTTP-Datenverkehr.

**Schritt 3.** Erstellen Sie auf dem primären Knoten der NetScaler-Appliance einen virtuellen Lastausgleichsserver für ILB.

1. Fügen Sie einen virtuellen Lastausgleichsserver hinzu.

```
add lb vserver <name> <serviceType> [<ILB Frontend IP address>]
[<port>]
```

**Beispiel:**

```
add lb vserver vserver_name HTTP 52.172.96.71 80
```

**HINWEIS:**

Verwenden Sie die Frontend-IP-Adresse des Load Balancers, die dem zusätzlichen Load Balancer zugeordnet ist, den Sie in Schritt 2 erstellen.

2. Binden Sie einen Dienst an einen virtuellen Lastausgleichsserver.

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

```
bind lb vserver <name> <serviceName>
```

**Beispiel:**

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
```

Weitere Informationen finden Sie unter Grundlegendes Lastenausgleich einrichten

**Schritt 4:** Als Alternative zu Schritt 3 können Sie einen virtuellen Lastausgleichsserver für ILB mithilfe von IPsets erstellen.

1. Fügen Sie eine IP-Adresse vom Typ virtuelle Server-IP (VIP) hinzu.

   ```
   add nsip <ILB Frontend IP address> -type <type>
   ```

   **Beispiel:**

   ```
   add nsip 52.172.96.71 -type vip
   ```

2. Fügen Sie ein IPset auf primären und sekundären Knoten hinzu.

   ```
   add ipset <name>
   ```

   **Beispiel:**

   ```
   add ipset ipset1
   ```

3. Binden Sie IP-Adressen an das IPset.

   ```
   bind ipset <name> <ILB Frontend IP address>
   ```

   **Beispiel:**

   ```
   bind ipset ipset1 52.172.96.71
   ```

4. Konfigurieren Sie den vorhandenen virtuellen LB-Server zur Verwendung des IPsets.

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

```
set lb vserver <vserver name> -ipset <ipset name>
```

**Beispiel:**

```
set lb vserver vserver_name -ipset ipset1
```

Weitere Informationen finden Sie unter Konfigurieren eines virtuellen Multi-IP-Servers.

## Bereitstellen eines NetScaler VPX HA-Paars in Azure unter Verwendung der sekundären IP-Konfigurationen

Sie können ein NetScaler VPX Hochverfügbarkeitspaar in Azure bereitstellen, wobei sich beide NetScaler VPX Instanzen im selben virtuellen Netzwerk (VNet) befinden und die sekundären IP-Konfigurationen der Netzwerkschnittstellen (NICs) verwendet werden. Diese HA-Bereitstellung macht den Azure Load Balancer (ALB) überflüssig. Während eines Failovers werden die sekundären privaten IP-Adressen, die den clientseitigen und serverseitigen NICs des primären Knotens zugewiesen sind, auf den sekundären Knoten migriert. Alle öffentlichen IP-Adressen, die mit diesen sekundären privaten IP-Adressen verknüpft sind, werden ebenfalls entsprechend verschoben.

**WICHTIG:**

Vor Beginn der Bereitstellung stellen Sie sicher, dass Ihre Azure-Umgebung die Voraussetzungen erfüllt, um Probleme während der Einrichtung zu vermeiden.

Im Folgenden sind einige der Vorteile der Verwendung sekundärer IP-Konfigurationen aufgeführt:

- **Vereinfachtes Failover:** Sekundäre IP-Adressen ermöglichen die automatische Migration von virtuellen IP-Adressen (VIPs) und Subnetz-IP-Adressen (SNIPs) zwischen HA-Knoten, wodurch ein nahtloses Failover ohne die Notwendigkeit eines externen Lastenausgleichs gewährleistet wird.
- **Skalierbarkeit:** Einer einzelnen NIC können mehrere IP-Adressen zugewiesen werden, was eine flexible Verkehrsführung und Skalierung von Diensten innerhalb derselben VM ermöglicht.
- **Ausfallsicherheit:** Die Möglichkeit, sekundäre private IP-Adressen zwischen Knoten zu verschieben, verbessert die Netzwerkverfügbarkeit und ermöglicht eine schnelle Wiederherstellung bei Knotenausfall.

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

- **Kosteneffizienz:** Durch den Wegfall eines ALB reduzieren Sie die Infrastrukturkosten, während Sie Hochverfügbarkeit und Verkehrsmanagement innerhalb desselben Subnetzes aufrechterhalten.

Die folgende Abbildung zeigt ein HA-Failover-Szenario durch die Migration sekundärer privater IP-Adressen.

## Voraussetzungen für die Bereitstellung eines NetScaler VPX™ HA-Paars unter Verwendung von Azure sekundären IP-Konfigurationen

- Verwenden Sie NetScaler Version 14.1–34.42 oder höher.
- Stellen Sie sicher, dass in Ihrem Abonnement die neue Azure-Steuerungsebene aktiviert ist.

**HINWEIS:**

Wenn die neue Azure-Steuerungsebene für Ihr Abonnement nicht aktiviert ist, können Hochverfügbarkeitsbereitstellungen eine längere Failover-Dauer aufweisen. Wenden Sie sich in solchen Fällen an den Azure-Support, um Unterstützung bei der Aktivierung der neuen Steuerungsebene zu erhalten.

## Bereitstellen eines NetScaler VPX HA-Paares mithilfe sekundärer Azure IP-Konfigurationen

Um ein NetScaler VPX HA-Paar mithilfe der sekundären IP-Konfigurationen in Azure bereitzustellen, führen Sie die folgenden Schritte aus:

1. Stellen Sie zwei NetScaler VPX-Instanzen in Azure bereit, jede mit drei Netzwerkschnittstellen in derselben Ressourcengruppe und demselben VNet.
2. Weisen Sie beiden NetScaler VPX-Instanzen eine verwaltete Identität zu.
3. Weisen Sie den Client- und Server-Netzwerkschnittstellen des primären Knotens sekundäre Azure IP-Konfigurationen zu.
4. Konfigurieren Sie VIP und SNIP auf dem primären Knoten mithilfe der privaten Azure IP-Adresse aus der sekundären IP-Konfiguration.
5. Konfigurieren Sie die primären privaten IP-Adressen der Server-Netzwerkschnittstellen auf beiden NetScaler-Instanzen (primär und sekundär) als VIP auf dem primären Knoten.
6. Konfigurieren Sie HA auf beiden Knoten.

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

**Schritt 1.** Stellen Sie zwei NetScaler VPX-Instanzen (primäre und sekundäre Knoten) in derselben Ressourcengruppe und demselben VNet bereit. Stellen Sie sicher, dass jede NetScaler VPX-Instanz drei NICs hat: Ethernet 0, Ethernet 1 und Ethernet 2.

Detaillierte Schritte finden Sie unter Bereitstellen von zwei VPX-Instanzen in Azure.

**Schritt 2.** Wenden Sie entweder eine systemseitig zugewiesene oder eine benutzerseitig zugewiesene verwaltete Identität auf beide NetScaler VPX-Instanzen an.

**HINWEIS:**

Der Azure-Dienstprinzipal wird für diese Funktion nicht unterstützt.

Weitere Informationen finden Sie unter Verwaltete Identitäten für Azure-Ressourcen.

Anweisungen zum Konfigurieren einer verwalteten Identität auf NetScaler VPX finden Sie unter Konfigurieren einer verwalteten Identität auf einer virtuellen Maschine.

**Schritt 3.** Fügen Sie der verwalteten Identität, die den NetScaler VPX-Instanzen zugeordnet ist, eine der folgenden Azure-Rollenzuweisungen hinzu.

- **Leser und Netzwerkmitwirkender**: Gewährt schreibgeschützten Zugriff auf Azure-Ressourcen und die Berechtigungen, die zur Verwaltung von Netzwerkressourcen erforderlich sind.
- **Mitwirkender**: Bietet vollständigen Zugriff auf Azure-Ressourcen.

**Schritt 4.** Weisen Sie auf dem primären Knoten private IP-Adressen Ethernet 1 (Client-IP oder VIP) und Ethernet 2 (Back-End-Server-IP oder SNIP) zu.

Das Azure-Portal weist den konfigurierten NICs automatisch primäre private IP-Adressen zu. Um weitere private IP-Adressen für die VIP- und SNIP-Netzwerkschnittstellen zuzuweisen, verwenden Sie sekundäre IP-Konfigurationen.

Um einer Netzwerkschnittstelle in Azure eine sekundäre IP-Konfiguration zuzuweisen, führen Sie die folgenden Schritte aus:

1. Melden Sie sich beim **Azure-Portal** an und navigieren Sie zu **Virtuelle Maschinen**.
2. Wählen Sie die virtuelle Maschine aus, die der Netzwerkschnittstelle zugeordnet ist.
3. Gehen Sie in den Einstellungen der virtuellen Maschine zu **Netzwerkeinstellungen** und wählen Sie die NIC aus, der Sie eine sekundäre private IP-Adresse hinzufügen möchten.

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

4. Klicken Sie in den Netzwerkschnittstelleneinstellungen auf die Registerkarte **IP-Konfigurationen**.
5. Klicken Sie auf **Hinzufügen**, um eine IP-Konfiguration vom Typ **Sekundär** zuzuweisen.
   - Wenn Sie eine statische Zuweisungsmethode wählen, geben Sie eine bestimmte IPv4-Adresse innerhalb des Subnetzbereichs für die Instanz ein.
   - Wenn Sie eine dynamische Zuweisungsmethode wählen, weist Azure automatisch eine IP-Adresse zu.
6. Klicken Sie auf **Hinzufügen** oder **Speichern**, um die Änderungen zu übernehmen.

**Schritt 5.** Konfigurieren Sie VIP und SNIP auf dem primären Knoten unter Verwendung der privaten IP-Adressen aus der sekundären IP-Konfiguration.

1. Greifen Sie über SSH auf den primären Knoten zu. Öffnen Sie einen SSH-Client und führen Sie den folgenden Befehl aus:

   ```
   ssh -i <location of your private key> nsroot@<public DNS of the instance>
   ```

2. Konfigurieren Sie die VIP- und SNIP-Adressen.

   Führen Sie zum Konfigurieren der VIP-Adresse den folgenden Befehl aus:

   ```
   add ns ip <IPAddress> <netmask> -type VIP
   ```

   **Beispiel:**

   ```
   add ns ip 192.0.2.11 255.255.255.0 -type VIP
   ```

   Führen Sie zum Konfigurieren der SNIP-Adresse den folgenden Befehl aus:

   ```
   add ns ip <IPAddress> <netmask> -type SNIP
   ```

   **Beispiel:**

   ```
   add ns ip 192.0.3.11 255.255.255.0 -type SNIP
   ```

3. Speichern Sie die Konfiguration, indem Sie den Befehl `save config` ausführen.

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

4. Überprüfen Sie die konfigurierten IP-Adressen mit dem folgenden Befehl:

```
show ns ip
```

**Schritt 6.** Konfigurieren Sie die primären privaten IP-Adressen der Server-Netzwerkschnittstellen auf dem primären Knoten sowohl auf den primären als auch auf den sekundären NetScaler-Instanzen als VIP.

1. Greifen Sie über SSH auf den primären Knoten zu. Öffnen Sie einen SSH-Client und führen Sie den folgenden Befehl aus:

```
ssh -i <location of your private key> nsroot@<public DNS of the
instance>
```

**Beispiel:**

```
ssh -i ~/.ssh/mykey.pem nsroot@primary-
instance.eastus.cloudapp.azure.com
```

2. Konfigurieren Sie auf dem primären Knoten die primäre private IP-Adresse von Ethernet 2 (Back-End-Server-NIC) sowohl der primären als auch der sekundären NetScaler-Instanzen als VIP:

```
add ns ip <private IPaddress of primary instance> <netmask> -type VIP



add ns ip <private IPaddress of secondary instance> <netmask> -type VIP
```

**Beispiel:**

```
add ns ip 192.0.3.10 255.255.255.0 -type VIP



add ns ip 192.0.3.20 255.255.255.0 -type VIP
```

**Schritt 7.** Konfigurieren Sie HA auf beiden Knoten.

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

1. Öffnen Sie auf dem primären Knoten einen Shell-Client und führen Sie den folgenden Befehl aus:

   ```
   add ha node <peer node id> <private IP address of the management NIC of the secondary node>
   ```

   **Beispiel:**

   ```
   add ha node 1 192.0.1.20
   ```

2. Führen Sie auf dem sekundären Knoten den folgenden Befehl aus:

   ```
   add ha node <peer node id> <private IP address of the management NIC of the primary node>
   ```

   **Beispiel:**

   ```
   add ha node 1 192.0.1.10
   ```

3. Speichern Sie die Konfiguration, indem Sie den Befehl `save config` ausführen.
4. Überprüfen Sie die konfigurierten HA-Knoten, indem Sie den Befehl `show ha node` ausführen.

   Während des Failovers werden die sekundären IP-Konfigurationen für die VIP- und SNIP-Netzwerkschnittstellen vom vorherigen primären Knoten auf den neuen primären Knoten verschoben.

## Bereitstellen eines NetScaler VPX HA-Paares in Azure mithilfe von Lösungsvorlagen

Die Azure-Lösungsvorlagen automatisieren die Bereitstellung von NetScaler VPX High Availability (HA), wodurch die Bereitstellungszeit verkürzt und die manuelle Konfiguration sowohl in Azure als auch in NetScaler entfällt. Kunden können mit diesen Lösungsvorlagen eine produktionsreife HA-Lösung mit minimalem Aufwand bereitstellen.

Diese Lösung stellt zwei NetScaler VPX-Instanzen über verschiedene Verfügbarkeitszonen oder Verfügbarkeitssätze für Hochverfügbarkeit und Fehlertoleranz bereit.

Weitere Informationen zu Lösungsvorlagen finden Sie in der Microsoft-Dokumentation.

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

### Hauptmerkmale der NetScaler VPX Azure-Lösungsbereitstellung

- **Hochverfügbarkeit:** Stellt zwei NetScaler VPX-Instanzen über separate Azure-Verfügbarkeitszonen mit automatischer HA-Konfiguration und Peer-Knoten-Erkennung bereit.
- **Netzwerk:**
  - **Bereitstellung mit drei NICs:** Verwendet dedizierte Verwaltungs-, Client- und Server-Subnetze für die Netzwerksegmentierung.
  - **Unterstützung für virtuelle Netzwerke:** Funktioniert mit neuen und bestehenden virtuellen Netzwerken.
  - **Konfiguration der öffentlichen IP-Adresse:** Ermöglicht konfigurierbare öffentliche IP-Adressen sowohl für den Verwaltungs- als auch für den Client-Datenverkehr.
  - **Beschleunigtes Netzwerk:** Option zum Aktivieren oder Deaktivieren des beschleunigten Netzwerks.
- **Sicherheit und Compliance:**
  - **Netzwerksicherheitsgruppen (NSGs):** Enthält anpassbare Eingangsregeln für verbesserte Sicherheit.
  - **RBAC-Integration:** Automatische Rollenzuweisungen über systemseitig zugewiesene verwaltete Identität.

### Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie Folgendes haben:

- Ein aktives Azure-Abonnement mit Administratorberechtigungen.
- Eine Azure-Region mit Unterstützung für Verfügbarkeitszonen.
- NetScaler-Lizenzdateien (Eigene Lizenz mitbringen).

### Marketplace-Angebotsinformationen (Eigene Lizenz mitbringen – BYOL)

Verwenden Sie beim Bereitstellen von NetScaler VPX in Azure mithilfe der Lösungsvorlage das Modell „Eigene Lizenz mitbringen“ (BYOL).

- **Angebots-ID: netscalervpx-141**
- **SKU-/Plan-ID: netscalerbyol**
- **Anbieter: Citrix**

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

### Bereitstellen eines NetScaler VPX HA-Paares in Azure mithilfe von Lösungsvorlagen

Dieser Abschnitt beschreibt, wie NetScaler VPX mithilfe des Azure Marketplace-Portals bereitgestellt wird.

**Schritt 1. Bereitstellung über den Azure Marketplace.**

1. Melden Sie sich beim Azure-Portal an.
2. Suchen Sie im Azure Marketplace nach **NetScaler VPX**, um die Bereitstellungsoptionen zu finden.

**Schritt 2. Wählen Sie einen Bereitstellungsplan aus.**

Wählen Sie einen der folgenden Pläne basierend auf Ihren Verfügbarkeitsanforderungen:

- NetScaler VPX HA (Verfügbarkeitszone) über sekundäre IP – BYOL
- NetScaler VPX HA (Verfügbarkeitsgruppe) über sekundäre IP – BYOL

**Schritt 3. Grundlegende Einstellungen und Administratoranmeldeinformationen konfigurieren.**

- **Abonnement** – Wählen Sie Ihr Azure-Abonnement aus.
- **Ressourcengruppe** – Erstellen Sie eine neue Ressourcengruppe oder wählen Sie eine vorhandene aus.
- **Region** – Wählen Sie eine Azure-Region, die Verfügbarkeitszonen oder Verfügbarkeitsgruppen unterstützt.
- **VM-Namenspräfix** – Geben Sie ein Präfix für die NetScaler VPX-Instanzen der virtuellen Maschine ein.
- **Release-Version** – Geben Sie die gewünschte NetScaler VPX-Version an (z. B. 14.1).
- **Administrator-Benutzername** – Geben Sie einen Administrator-Benutzernamen ein.
- **Authentifizierungstyp** – Wählen Sie **Passwort** oder **Öffentlicher SSH-Schlüssel**.
- **Anmeldeinformationen** – Geben Sie Ihr Passwort oder Ihren SSH-Schlüssel basierend auf dem ausgewählten Authentifizierungstyp ein.

**Schritt 4. Einstellungen der virtuellen Maschine konfigurieren.**

- **VM-Größe** – Wählen Sie eine Größe, die Ihren Leistungsanforderungen entspricht.

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

- **Betriebssystem-Datenträgertyp** – Wählen Sie einen Speichermedientyp (z. B. Standard_LRS oder Premium_LRS).
- **Überwachungsmetriken veröffentlichen** – Aktivieren Sie diese Option, um NetScaler ADC-Leistungsmetriken an Azure Monitor zu senden.

**Schritt 5. Netzwerkeinstellungen konfigurieren.**

- **Virtuelles Netzwerk** – Erstellen Sie ein neues virtuelles Netzwerk oder wählen Sie ein vorhandenes aus.
- **Adressraum** – Geben Sie den CIDR-Block für ein neues virtuelles Netzwerk an.
- **Subnetze** – Konfigurieren Sie Management-, Client- und Server-Subnetze.
- **Beschleunigtes Netzwerk** – Aktivieren Sie dies für eine verbesserte Netzwerkleistung auf wichtigen Schnittstellen.
- **Öffentliche Management-IP-Adressen** – Weisen Sie öffentliche IP-Adressen für VM 1 und VM 2 zu (empfohlen).
- **Öffentliche Client-IP-Adresse** – Weisen Sie optional eine öffentliche IP-Adresse für den Clientzugriff zu.
- **DNS-Bezeichnungen** – Fügen Sie eindeutige DNS-Bezeichnungen hinzu, wenn eine DNS-Auflösung erforderlich ist.
- **Öffentliche eingehende Ports** – Erforderliche Ports zulassen (z. B. SSH-22, HTTP-80, HTTPS-443).

**Schritt 6. Bereitstellung überprüfen und abschließen.**

1. Überprüfen Sie alle ausgewählten Konfigurationsparameter, um sicherzustellen, dass sie Ihren Anforderungen entsprechen.
2. Akzeptieren Sie die Geschäftsbedingungen.
3. Wählen Sie **Erstellen**, um die Bereitstellung zu starten.

**Schritt 7. Überprüfen Sie Ihre Bereitstellung.**

Nach Abschluss der Bereitstellung überprüfen Sie, ob Ihr NetScaler HA-Paar korrekt konfiguriert ist und wie erwartet funktioniert.

1. HA-Knotenstatus überprüfen.

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

a. Verbinden Sie sich über SSH mit einer der NetScaler-Instanzen.
b. Führen Sie den Befehl `show ha node` aus, um den HA-Knotenstatus zu überprüfen.
c. Überprüfen Sie Folgendes:

- Beide Knoten erscheinen in der Ausgabe
- Der Synchronisierungsstatus (Sync) ist fehlerfrei
- Der INC-Modus (Independent Network Configuration) ist korrekt konfiguriert

☐

2. IP-Adresskonfiguration validieren.

   Führen Sie den Befehl `show ns ip` auf der NetScaler-Instanz aus. Überprüfen Sie die Ausgabe, um sicherzustellen, dass alle virtuellen IP-Adressen (VIPs) und Subnetz-IP-Adressen (SNIPs) vorhanden und korrekt konfiguriert sind.

   ☐

3. Führen Sie einen Hochverfügbarkeits-Failover-Test durch.

   Wir empfehlen Ihnen, einen manuellen Failover-Test durchzuführen, um die Ausfallsicherheit Ihrer HA-Einrichtung zu überprüfen.

   a. Führen Sie den Befehl `force ha failover –force` aus, um den Failover zu initiieren.
   b. Überprüfen Sie Folgendes:

   - Das Failover wird erfolgreich abgeschlossen
   - Alle sekundären IP-Konfigurationen werden auf den neuen primären Knoten übertragen

# Installieren einer NetScaler VPX-Instanz in Azure VMware Solution

Azure VMware Solution (AVS) stellt Ihnen private Clouds zur Verfügung, die vSphere-Cluster enthalten, die aus dedizierter Bare-Metal-Azure-Infrastruktur aufgebaut sind. Die minimale Ersteinrichtung umfasst drei Hosts, aber zusätzliche Hosts können einzeln hinzugefügt werden, bis zu einem Maximum von 16 Hosts pro Cluster. Alle bereitgestellten privaten Clouds verfügen über vCenter Server, vSAN, vSphere und NSX-T.

Die VMware Cloud (VMC) auf Azure ermöglicht Ihnen die Erstellung von Cloud-Software-definierten Rechenzentren (SDDC) auf Azure mit der gewünschten Anzahl von ESX-Hosts. Die VMC auf Azure unterstützt NetScaler VPX-Bereitstellungen. VMC bietet eine Benutzeroberfläche,

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

die der lokalen vCenter-Oberfläche gleicht. Sie funktioniert ähnlich wie die ESX-basierten NetScaler VPX-Bereitstellungen.

Das folgende Diagramm zeigt die Azure VMware-Lösung in der öffentlichen Azure Cloud, auf die ein Administrator oder ein Client über das Internet zugreifen kann. Ein Administrator kann Workload- oder Server-VMs mit der Azure VMware-Lösung erstellen, verwalten und konfigurieren. Der Administrator kann über eine Windows Jumpbox auf das webbasierte vCenter und den NSX-T Manager von AVS zugreifen. Sie können die NetScaler VPX-Instanzen (Standalone oder Hochverfügbarkeitspaar) und Server-VMs innerhalb der Azure VMware Solution mit vCenter erstellen und die entsprechende Netzwerkkonfiguration mit dem NSX-T Manager verwalten. Die NetScaler VPX-Instanz auf AVS funktioniert ähnlich wie der lokale VMware-Host-Cluster. AVS wird von einer Windows Jumpbox aus verwaltet, die im selben virtuellen Netzwerk erstellt wird.

Ein Client kann den AVS-Dienst nur durch Verbinden mit der VIP des ADC erreichen. Eine weitere NetScaler VPX-Instanz außerhalb der Azure VMware Solution, aber im selben virtuellen Azure-Netzwerk, hilft dabei, die VIP der NetScaler VPX-Instanz innerhalb der Azure VMware Solution als Dienst hinzuzufügen. Je nach Anforderung können Sie die NetScaler VPX-Instanz so konfigurieren, dass sie Dienste über das Internet bereitstellt.

## Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, führen Sie die folgenden Schritte aus:

- Weitere Informationen zur Azure VMware-Lösung und ihren Voraussetzungen finden Sie in der Azure VMware Solution-Dokumentation.
- Weitere Informationen zur Bereitstellung der Azure VMware-Lösung finden Sie unter Bereitstellen einer privaten Azure VMware Solution-Cloud.
- Weitere Informationen zum Erstellen einer Windows Jumpbox-VM für den Zugriff und die Verwaltung der Azure VMware Solution finden Sie unter Zugreifen auf eine private Azure VMware Solution-Cloud
- Laden Sie in der Windows Jumpbox-VM die Setup-Dateien der NetScaler VPX-Appliance herunter.
- Erstellen Sie entsprechende NSX-T-Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden. Weitere Informationen finden Sie unter Hinzufügen eines Netzwerksegments in Azure VMware Solution
- VPX-Lizenzdateien beschaffen.

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

- Virtuelle Maschinen (VMs), die in der privaten Azure VMware Solution-Cloud erstellt oder dorthin migriert wurden, müssen an ein Netzwerksegment angehängt werden.

## VMware Cloud-Hardwareanforderungen

Die folgende Tabelle listet die virtuellen Computerressourcen auf, die das VMware SDDC für jede virtuelle VPX nCore-Appliance bereitstellen muss.

Tabelle 1. Mindestanforderungen an virtuelle Computerressourcen für den Betrieb einer NetScaler VPX-Instanz

| KOMPONENTE | ANFORDERUNG |
|---|---|
| Arbeitsspeicher | 2 GB |
| Virtuelle CPU (vCPU) | 2 |
| Virtuelle Netzwerkschnittstellen | In VMware SDDC können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird. |
| Festplattenspeicher | 20 GB |

**HINWEIS:**

Dies gilt zusätzlich zu allen Festplattenanforderungen für den Hypervisor.

Für den Produktionseinsatz der virtuellen VPX-Appliance muss die gesamte Speicherzuweisung reserviert werden.

## OVF Tool 1.0 Systemanforderungen

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. Die folgende Tabelle beschreibt die Systemanforderungen für die Installation des OVF Tools.

Tabelle 2. Systemanforderungen für die OVF Tool-Installation

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

| KOMPONENTE | ANFORDERUNG |
| --- | --- |
| Betriebssystem | Detaillierte Anforderungen von VMware finden Sie in der PDF-Datei „OVF Tool User Guide“ unter `<http://kb.vmware.com/>`. |
| CPU | 750 MHz Minimum, 1 GHz oder schneller empfohlen |
| RAM | 1 GB Minimum, 2 GB empfohlen |
| NIC | 100 Mbit/s oder schnellere NIC |

Informationen zur Installation von OVF finden Sie in der PDF-Datei „OVF Tool User Guide“ unter `<http://kb.vmware.com/>`.

## Herunterladen der NetScaler VPX-Setup-Dateien

Das NetScaler VPX-Instanz-Setup-Paket für VMware ESX folgt dem Standard des Open Virtual Machine (OVF)-Formats. Sie können die Dateien von der Citrix-Website herunterladen. Sie benötigen ein Citrix-Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.com auf. Klicken Sie auf den Link **Neue Benutzer** und folgen Sie den Anweisungen, um ein neues Citrix-Konto zu erstellen.

Nach der Anmeldung navigieren Sie auf der Citrix®-Startseite zum folgenden Pfad:

Citrix.com > **Downloads > NetScaler > Virtuelle Appliances**.

Kopieren Sie die folgenden Dateien auf eine Workstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX-\<release number\>-\<build number\>-disk1.vmdk (zum Beispiel NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX-\<release number\>-\<build number\>.ovf (zum Beispiel NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX-\<release number\>-\<build number\>.mf (zum Beispiel NSVPX-ESX-13.0-79.64.mf)

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

## Azure VMware Solution bereitstellen

1. Melden Sie sich bei Ihrem Microsoft Azure-Portal an und navigieren Sie zum **Azure Marketplace**.
2. Suchen Sie im **Azure Marketplace** nach **Azure VMware Solution** und klicken Sie auf **Erstellen**.

3. Geben Sie auf der Seite **Private Cloud erstellen** die folgenden Details ein:

   - Wählen Sie mindestens 3 ESXi-Hosts aus, um den Standardcluster Ihrer privaten Cloud zu erstellen.
   - Verwenden Sie für das Feld **Adressblock** den Adressraum **/22**.
   - Für das **virtuelle Netzwerk** stellen Sie sicher, dass der CIDR-Bereich sich nicht mit Ihren lokalen oder anderen Azure-Subnetzen (virtuellen Netzwerken) oder mit dem Gateway-Subnetz überschneidet.
   - Das Gateway-Subnetz wird verwendet, um die Verbindung per ExpressRoute mit der privaten Cloud herzustellen.

4. Klicken Sie auf **Überprüfen + Erstellen**.
5. Überprüfen Sie die Einstellungen. Wenn Sie Einstellungen ändern müssen, klicken Sie auf **Zurück**.

6. Klicken Sie auf **Erstellen**. Der Bereitstellungsprozess der privaten Cloud beginnt. Es kann bis zu zwei Stunden dauern, bis die private Cloud bereitgestellt ist.

7. Klicken Sie auf **Zu Ressource wechseln**, um die erstellte private Cloud zu überprüfen.

**HINWEIS:**

Um auf diese Ressource zuzugreifen, benötigen Sie eine VM unter Windows, die als Jumpbox fungiert.

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

## Verbinden mit einer virtuellen Azure-Maschine unter Windows

Dieses Verfahren zeigt Ihnen, wie Sie das Azure-Portal verwenden, um eine virtuelle Maschine (VM) in Azure bereitzustellen, die Windows Server 2019 ausführt. Um Ihre VM in Aktion zu sehen, stellen Sie dann eine RDP-Verbindung zur VM her und installieren den IIS-Webserver.

Um auf die von Ihnen erstellte private Cloud zuzugreifen, müssen Sie eine Windows-Jumpbox innerhalb desselben virtuellen Netzwerks erstellen.

1. Gehen Sie zum **Azure-Portal**, und klicken Sie auf **Ressource erstellen**.

2. Suchen Sie nach **Microsoft Windows 10**, und klicken Sie auf **Erstellen**.

3. Erstellen Sie eine virtuelle Maschine (VM), auf der Windows Server 2019 ausgeführt wird. Die Seite **Virtuelle Maschine erstellen** wird angezeigt. Geben Sie alle Details auf der Registerkarte **Grundlagen** ein und aktivieren Sie das Kontrollkästchen **Lizenzierung**. Behalten Sie die restlichen Standardeinstellungen bei und wählen Sie dann die Schaltfläche **Überprüfen + erstellen** am unteren Rand der Seite.

4. Nachdem die Validierung abgeschlossen ist, wählen Sie die Schaltfläche **Erstellen** am unteren Rand der Seite.
5. Nach Abschluss der Bereitstellung wählen Sie **Zu Ressource wechseln**.
6. Gehen Sie zu der von Ihnen erstellten Windows-VM. Verwenden Sie die öffentliche IP-Adresse der Windows-VM und stellen Sie eine Verbindung über RDP her.

   Verwenden Sie die Schaltfläche **Verbinden** im Azure-Portal, um eine Remotedesktop-Sitzung (RDP) von einem Windows-Desktop aus zu starten. Zuerst stellen Sie eine Verbindung zur virtuellen Maschine her und melden sich dann an.

   Um von einem Mac aus eine Verbindung zu einer Windows-VM herzustellen, müssen Sie einen RDP-Client für Mac installieren, z. B. Microsoft Remote Desktop. Weitere Informationen finden Sie unter Herstellen einer Verbindung und Anmelden bei einer Azure-VM mit Windows.

## Zugriff auf Ihr Private Cloud vCenter-Portal

1. Wählen Sie in Ihrer Azure VMware Solution Private Cloud unter **Verwalten** die Option **Identität**. Notieren Sie sich die vCenter-Anmeldeinformationen.

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

2. Starten Sie den vSphere-Client, indem Sie die vCenter-Webclient-URL eingeben.

3. Melden Sie sich bei VMware vSphere mit den vCenter-Anmeldeinformationen Ihrer Azure VMware Solution Private Cloud an.

4. Im vSphere-Client können Sie die ESXi-Hosts überprüfen, die Sie im Azure-Portal erstellt haben.

Weitere Informationen finden Sie unter Zugriff auf Ihr Private Cloud vCenter-Portal.

## Ein NSX-T-Segment im Azure-Portal erstellen

Sie können ein NSX-T-Segment über die Azure VMware Solution-Konsole im Azure-Portal erstellen und konfigurieren. Diese Segmente sind mit dem Standard-Tier-1-Gateway verbunden, und die Workloads auf diesen Segmenten erhalten Ost-West- und Nord-Süd-Konnektivität. Sobald Sie das Segment erstellt haben, wird es im NSX-T Manager und vCenter angezeigt.

1. Wählen Sie in Ihrer Azure VMware Solution Private Cloud unter **Workload-Netzwerk** die Option **Segmente > Hinzufügen** aus. Geben Sie die Details für das neue logische Segment an und wählen Sie **OK** aus. Sie können drei separate Segmente für Client-, Management- und Server-Schnittstellen erstellen.

2. Wählen Sie in Ihrer Azure VMware Solution Private Cloud unter **Verwalten** die Option **Identität** aus. Notieren Sie sich die Anmeldeinformationen des NSX-T Managers.

3. Starten Sie den VMware NSX-T Manager, indem Sie die NSX-T Webclient-URL eingeben.

4. Im NSX-T Manager sehen Sie unter **Netzwerk > Segmente** alle Segmente, die Sie erstellt haben. Sie können auch die Subnetze überprüfen.

Weitere Informationen finden Sie unter Erstellen eines NSX-T-Segments im Azure-Portal.

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

## Installieren einer NetScaler VPX-Instanz in der VMware Cloud

Nachdem Sie das VMware Software-Defined Data Center (SDDC) installiert und konfiguriert haben, können Sie das SDDC verwenden, um virtuelle Appliances in der VMware Cloud zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der im SDDC verfügbaren Speichermenge ab.

Um NetScaler VPX-Instanzen in der VMware Cloud zu installieren, führen Sie die folgenden Schritte in der Windows Jumpbox VM aus:

1. Laden Sie die Setup-Dateien der NetScaler VPX-Instanz für den ESXi-Host von der NetScaler-Downloadseite herunter.
2. Öffnen Sie VMware SDDC in der Windows Jumpbox.
3. Geben Sie in den Feldern **Benutzername** und **Passwort** die Administratoranmeldeinformationen ein und klicken Sie dann auf **Anmelden**.
4. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
5. Navigieren Sie im Dialogfeld **OVF-Vorlage bereitstellen** im Feld **Aus Datei bereitstellen** zu dem Speicherort, an dem Sie die Setup-Dateien der NetScaler VPX-Instanz gespeichert haben, wählen Sie die .ovf-Datei aus und klicken Sie auf **Weiter**.

   **HINWEIS:**

   Standardmäßig verwendet die NetScaler VPX-Instanz E1000-Netzwerkschnittstellen. Um ADC mit der VMXNET3-Schnittstelle bereitzustellen, ändern Sie die OVF so, dass die VMXNET3-Schnittstelle anstelle von E1000 verwendet wird. Die Verfügbarkeit der VMXNET3-Schnittstelle ist durch die Azure-Infrastruktur begrenzt und möglicherweise in der Azure VMware Solution nicht verfügbar.

6. Ordnen Sie die in der OVF-Vorlage der virtuellen Appliance angezeigten Netzwerke den Netzwerken zu, die Sie im VMware SDDC konfiguriert haben. Klicken Sie auf **OK**.

7. Klicken Sie auf **Fertig stellen**, um die Installation einer virtuellen Appliance auf dem VMware SDDC zu starten.

8. Sie können die NetScaler VPX-Instanz nun starten. Wählen Sie im Navigationsbereich die NetScaler VPX-Instanz aus, die Sie installiert haben, und wählen Sie im Kontextmenü die

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

Option **Einschalten**. Klicken Sie auf die Registerkarte **Konsole**, um einen Konsolenport zu emulieren.

9. Sie sind jetzt über den vSphere-Client mit der NetScaler-VM verbunden.

10. Um über die SSH-Schlüssel auf die NetScaler-Appliance zuzugreifen, geben Sie den folgenden Befehl in die CLI ein:

```
ssh nsroot@<management IP address>
```

**Beispiel:**

```
ssh nsroot@192.168.4.5
```

11. Sie können die ADC-Konfiguration mit dem Befehl `show ns ip` überprüfen.

# NetScaler VPX-Standalone-Instanz in Azure VMware Solution konfigurieren

Sie können eine NetScaler VPX-Standalone-Instanz in Azure VMware Solution (AVS) für internetbasierte Anwendungen konfigurieren.

Das folgende Diagramm zeigt die NetScaler VPX-Standalone-Instanz in Azure VMware Solution. Ein Client kann auf den AVS-Dienst zugreifen, indem er sich mit der virtuellen IP-Adresse (VIP) von NetScaler innerhalb der AVS verbindet. Dies kann erreicht werden, indem ein NetScaler Load Balancer oder die Azure Load Balancer-Instanz außerhalb von AVS, aber im selben virtuellen Azure-Netzwerk bereitgestellt wird. Konfigurieren Sie den Load Balancer so, dass er auf die VIP der NetScaler VPX-Instanz innerhalb des AVS-Dienstes zugreift.

## Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, lesen Sie die folgenden Azure-Voraussetzungen:

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

- Weitere Informationen zur Azure VMware Solution und ihren Voraussetzungen finden Sie unter Azure VMware Solution-Dokumentation.
- Weitere Informationen zur Bereitstellung der Azure VMware Solution finden Sie unter Bereitstellen einer privaten Azure VMware Solution-Cloud.
- Weitere Informationen zum Erstellen einer Windows Jump Box-VM für den Zugriff auf und die Verwaltung der Azure VMware Solution finden Sie unter Zugriff auf eine private Azure VMware Solution-Cloud.
- Laden Sie auf der Windows Jump Box-VM die Setup-Dateien der NetScaler VPX-Appliance herunter.
- Erstellen Sie auf VMware SDDC entsprechende NSX-T-Netzwerksegmente, mit denen sich die virtuellen Maschinen verbinden. Weitere Informationen finden Sie unter Hinzufügen eines Netzwerksegments in Azure VMware Solution
- Weitere Informationen zur Installation einer NetScaler VPX-Instanz in der VMware Cloud finden Sie unter Installieren einer NetScaler VPX-Instanz in der VMware Cloud.

## Konfigurieren einer NetScaler VPX-Standalone-Instanz in AVS mithilfe des NetScaler Load Balancers

Führen Sie die folgenden Schritte aus, um die NetScaler VPX-Standalone-Instanz in AVS für internetbasierte Anwendungen mithilfe des NetScaler Load Balancers zu konfigurieren.

1. Stellen Sie eine NetScaler VPX-Instanz in der Azure Cloud bereit. Weitere Informationen finden Sie unter Konfigurieren einer NetScaler VPX-Standalone-Instanz.

   **HINWEIS:**

   Stellen Sie sicher, dass es im selben virtuellen Netzwerk wie die Azure VMware Cloud bereitgestellt wird.

2. Konfigurieren Sie die NetScaler VPX-Instanz so, dass sie auf die VIP-Adresse der auf AVS bereitgestellten NetScaler VPX zugreifen kann.

   a. Fügen Sie einen virtuellen Lastausgleichsserver hinzu.

   ```
   add lb vserver <name> <serviceType> [<vip>] [<port>]
   ```

   **Beispiel:**

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

```
add lb vserver lb1 HTTPS 172.31.0.6 443
```

b. Fügen Sie einen Dienst hinzu, der sich mit der VIP der auf AVS bereitgestellten NetScaler VPX verbindet.

```
add service <name> <ip> <serviceType> <port>
```

**Beispiel:**

```
add service webserver1 192.168.4.10 HTTP 80
```

c. Binden Sie einen Dienst an den virtuellen Lastausgleichsserver.

```
bind lb vserver <name> <serviceName>
```

**Beispiel:**

```
bind lb vserver lb1 webserver1
```

## NetScaler VPX Standalone-Instanz auf AVS mit dem Azure Load Balancer konfigurieren

Führen Sie die folgenden Schritte aus, um die NetScaler VPX Standalone-Instanz auf AVS für internetfähige Anwendungen mithilfe des Azure Load Balancers zu konfigurieren.

1. Konfigurieren Sie eine Azure Load Balancer-Instanz in der Azure Cloud. Weitere Informationen finden Sie in der Azure-Dokumentation zum Erstellen eines Load Balancers.
2. Fügen Sie die VIP-Adresse der auf AVS bereitgestellten NetScaler VPX-Instanz zum Back-End-Pool hinzu.

   Der folgende Azure-Befehl fügt eine Back-End-IP-Adresse zum Back-End-Adresspool des Lastausgleichs hinzu.

```
az network lb address-pool address add

                                  --resource-group <Azure VMC
Resource Group>
```

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

```
                                    --lb-name <LB Name>

                                    --pool-name <Backend pool name>

                                    --vnet <Azure VMC Vnet>

                                    --name <IP Address name>

                                    --ip-address <VIP of ADC in VMC>
```

**HINWEIS:**

Stellen Sie sicher, dass der Azure Load Balancer im selben virtuellen Netzwerk wie die Azure VMware Cloud bereitgestellt wird.

# Konfigurieren einer NetScaler VPX Hochverfügbarkeits-Einrichtung in der Azure VMware Solution

Sie können eine NetScaler VPX HA-Einrichtung in der Azure VMware Solution (AVS) für internetbasierte Anwendungen konfigurieren.

Das folgende Diagramm zeigt das NetScaler VPX HA-Paar auf AVS. Ein Client kann auf den AVS-Dienst zugreifen, indem er sich mit der VIP des primären ADC-Knotens innerhalb der AVS verbindet. Dies erreichen Sie, indem Sie einen NetScaler Load Balancer oder die Azure Load Balancer-Instanz außerhalb von AVS, aber im selben virtuellen Azure-Netzwerk bereitstellen. Konfigurieren Sie den Load Balancer so, dass er auf die VIP des primären ADC-Knotens innerhalb des AVS-Dienstes zugreift.

## Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, lesen Sie die folgenden Azure-Voraussetzungen:

- Weitere Informationen zur Azure VMware Solution und ihren Voraussetzungen finden Sie unter Azure VMware Solution-Dokumentation.
- Weitere Informationen zur Bereitstellung der Azure VMware Solution finden Sie unter Bereitstellen einer privaten Azure VMware Solution-Cloud.

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

- Weitere Informationen zum Erstellen einer Windows Jump Box VM für den Zugriff und die Verwaltung der Azure VMware Solution finden Sie unter Zugriff auf eine private Azure VMware Solution-Cloud.
- Laden Sie in der Windows Jump Box VM die Setup-Dateien der NetScaler VPX Appliance herunter.
- Erstellen Sie entsprechende NSX-T-Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden. Weitere Informationen finden Sie unter Hinzufügen eines Netzwerksegments in Azure VMware Solution.

### Konfigurationsschritte

Führen Sie die folgenden Schritte aus, um die NetScaler VPX Hochverfügbarkeits-Einrichtung in AVS für internetbasierte Anwendungen zu konfigurieren.

1. Erstellen Sie zwei NetScaler VPX-Instanzen in der VMware Cloud. Weitere Informationen finden Sie unter Installieren einer NetScaler VPX-Instanz in der VMware Cloud.
2. Konfigurieren Sie die NetScaler HA-Einrichtung. Weitere Informationen finden Sie unter Konfigurieren der Hochverfügbarkeit.
3. Konfigurieren Sie die NetScaler HA-Einrichtung, damit sie für internetbasierte Anwendungen zugänglich ist.
    - Informationen zum Konfigurieren der NetScaler VPX-Instanz mithilfe des NetScaler Load Balancers finden Sie unter Konfigurieren einer eigenständigen NetScaler VPX-Instanz auf AVS mithilfe des NetScaler Load Balancers.
    - Informationen zum Konfigurieren der NetScaler VPX-Instanz mithilfe des Azure Load Balancers finden Sie unter Konfigurieren einer eigenständigen NetScaler VPX-Instanz auf AVS mithilfe des Azure Load Balancers.

## Azure Route Server mit NetScaler VPX HA-Paar konfigurieren

Sie können den Azure Route Server mit einer NetScaler VPX-Instanz konfigurieren, um die mit dem virtuellen Netzwerk konfigurierten VIP-Routen mithilfe des BGP-Protokolls auszutauschen. Der NetScaler kann im Standalone-Modus oder im HA-INC-Modus bereitgestellt und anschließend mit BGP konfiguriert werden. Diese Bereitstellung erfordert keinen Azure Load Balancer (ALB) vor dem ADC HA-Paar.

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

Das folgende Diagramm zeigt, wie eine VPX HA-Topologie in den Azure Route Server integriert ist. Jede der ADC-Instanzen verfügt über 3 Schnittstellen: eine für die Verwaltung, eine für den Client-Datenverkehr und eine für den Server-Datenverkehr.

VPX HA-Topologie mit dem Azure Route Server(/en-us/vpx/media/ars-ha-topology.jpg)

Das Topologiediagramm verwendet die folgenden IP-Adressen.

**Beispiel-IP-Konfiguration für die primäre ADC-Instanz:**

```
NSIP: 10.0.0.4/24

SNIP on 1/1: 10.0.1.4/24

SNIP on 1/2: 10.0.2.4/24

VIP: 172.168.1.1/32
```

**Beispiel-IP-Konfiguration für die sekundäre ADC-Instanz:**

```
NSIP: 10.0.0.5/24

SNIP on 1/1: 10.0.1.5/24

SNIP on 1/2: 10.0.2.5/24

VIP: 172.168.1.1/32
```

## Voraussetzungen

Sie müssen mit den folgenden Informationen vertraut sein, bevor Sie eine NetScaler VPX-Instanz in Azure bereitstellen.

- Azure-Terminologie und Netzwerkdetails. Weitere Informationen finden Sie unter Azure-Terminologie.
- Übersicht über Azure Route Server. Weitere Informationen finden Sie unter Was ist Azure Route Server?.
- Funktionsweise einer NetScaler Appliance. Weitere Informationen finden Sie unter NetScaler-Dokumentation.
- NetScaler-Netzwerk. Weitere Informationen finden Sie unter ADC-Netzwerk.

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

## So konfigurieren Sie einen Azure Route Server mit einem NetScaler VPX HA-Paar

1. Erstellen Sie einen Route Server im Azure-Portal. Weitere Informationen finden Sie unter Erstellen und Konfigurieren eines Route Servers mithilfe des Azure-Portals.

   Im folgenden Beispiel wird das Subnetz 10.0.3.0/24 für die Bereitstellung des Azure-Servers verwendet. Sobald der Routenserver erstellt wurde, rufen Sie die IP-Adressen des Routenservers ab, zum Beispiel: 10.0.3.4, 10.0.3.5.

   Routenserver erstellen(/en-us/vpx/media/azure-route-server.png)

2. Richten Sie das Peering mit der virtuellen Netzwerk-Appliance (NVA) im Azure-Portal ein. Fügen Sie Ihre NetScaler VPX-Instanz als NVA hinzu. Weitere Informationen finden Sie unter Peering mit NVA einrichten.

   Im folgenden Beispiel werden die ADC-SNIPs auf den 1/1-Schnittstellen: 10.0.1.4 und 10.0.1.5, sowie die ASNs: 400 und 500, beim Hinzufügen des Peers verwendet.

   Peers einrichten(/en-us/vpx/media/ars-peers.png)

3. Fügen Sie zwei NetScaler VPX-Instanzen für die HA-Konfiguration hinzu.

   Führen Sie die folgenden Schritte aus:

   a. Stellen Sie zwei VPX-Instanzen (primäre und sekundäre Instanzen) auf Azure bereit.
   b. Fügen Sie Client- und Server-NICs auf beiden Instanzen hinzu.
   c. Konfigurieren Sie die HA-Einstellungen auf beiden Instanzen mithilfe der NetScaler GUI.

4. Konfigurieren Sie dynamisches Routing in der primären ADC-Instanz.

   **Beispielkonfiguration:**

```
enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD

enable ns feature LB BGP

add ns ip 10.0.1.4 255.255.255.0 -vServer DISABLED -dynamicRouting
ENABLED

VTYSH

configure terminal
```

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

```
router BGP 400

timers bgp 1 3

neighbor 10.0.3.4 remote-as 65515

neighbor 10.0.3.4 advertisement-interval 3

neighbor 10.0.3.4 fall-over  bfd

neighbor 10.0.3.5 remote-as 65515

neighbor 10.0.3.5 advertisement-interval 3

neighbor 10.0.3.5 fall-over  bfd

address-family ipv4

redistribute kernel

redistribute static
```

5. Konfigurieren Sie dynamisches Routing in der sekundären ADC-Instanz.

   **Beispielkonfiguration:**

```
enable ns mode L3 MBF USNIP SRADV DRADV  PMTUD

enable ns feature LB BGP

add ns ip 10.0.1.5 255.255.255.0 -vServer DISABLED -dynamicRouting
ENABLED

VTYSH

configure terminal

router BGP 500

timers bgp 1 3

neighbor 10.0.3.4 remote-as 65515
```

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

```
neighbor 10.0.3.4 advertisement-interval 3

neighbor 10.0.3.4 fall-over  bfd

neighbor 10.0.3.5 remote-as 65515

neighbor 10.0.3.5 advertisement-interval 3

neighbor 10.0.3.5 fall-over  bfd

address-family ipv4

redistribute kernel

redistribute static
```

6. Überprüfen Sie die eingerichteten BGP-Peers mithilfe der BGP-Befehle in der VTY-Shell-Schnittstelle. Weitere Informationen finden Sie unter Überprüfen der BGP-Konfiguration.

   ```
   show ip bgp neighbors
   ```

7. Konfigurieren Sie den virtuellen LB-Server in der primären ADC-Instanz.

   **Beispielkonfiguration:**

   ```
   add ns ip 172.16.1.1 255.255.255.255 -type VIP -hostRoute ENABLED

   add lbvserver v1 HTTP 172.16.1.1 80

   add service s1 10.0.2.6 HTTP 80

   bind lbvserver v1 s1

   enable ns feature lb
   ```

   Ein Client im selben virtuellen Netzwerk wie die NetScaler VPX-Instanz kann nun auf den virtuellen LB-Server zugreifen. In diesem Fall bewirbt die NetScaler VPX-Instanz die VIP-Route beim Azure Route Server.

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

# Back-End Azure Autoscaling-Dienst hinzufügen

Ein effizientes Hosting von Anwendungen in einer Cloud beinhaltet eine einfache und kostengünstige Verwaltung von Ressourcen, abhängig von der Anwendungsnachfrage. Um steigende Anforderungen zu erfüllen, müssen Sie Netzwerkressourcen hochskalieren. Wenn die Nachfrage nachlässt, müssen Sie herunterskalieren, um unnötige Kosten für ungenutzte Ressourcen zu vermeiden. Um die Kosten für den Betrieb der Anwendung zu minimieren, müssen Sie ständig den Datenverkehr, die Speicherauslastung, die CPU-Nutzung usw. überwachen. Die manuelle Überwachung des Datenverkehrs ist jedoch umständlich. Damit die Anwendungsumgebung dynamisch hoch- oder herunterskaliert werden kann, müssen Sie die Prozesse der Verkehrsüberwachung und des Hoch- und Herunterskalierens von Ressourcen bei Bedarf automatisieren.

Sie können Autoscale™ mit Azure Virtual Machine Scale Sets (VMSS) für die VPX Multi-IP Standalone- und Hochverfügbarkeitsbereitstellung in Azure verwenden.

Integriert in die Azure VMSS- und Autoscale-Funktion bietet die NetScaler VPX-Instanz die folgenden Vorteile:

- Lastverteilung und -verwaltung: Konfiguriert Server automatisch zum Hoch- und Herunterskalieren, je nach Bedarf. Die NetScaler VPX-Instanz erkennt automatisch die VMSS Autoscale-Einstellung im selben virtuellen Netzwerk, in dem die VPX-Instanz bereitgestellt wird, oder in den gepeerten virtuellen Netzwerken, die sich in demselben Azure-Abonnement befinden. Sie können die VMSS Autoscale-Einstellung auswählen, um die Last auszugleichen. Dies geschieht durch die automatische Konfiguration der virtuellen NetScaler-IP-Adresse und der Subnetz-IP-Adresse auf der VPX-Instanz.
- Hochverfügbarkeit: Erkennt Autoscale-Gruppen und gleicht die Last der Server aus.
- Bessere Netzwerkverfügbarkeit: Die VPX-Instanz unterstützt Back-End-Server in verschiedenen virtuellen Netzwerken (VNets).

Weitere Informationen finden Sie im folgenden Azure-Thema

- Dokumentation zu Virtual Machine Scale Sets
- Übersicht über Autoscale in Microsoft Azure Virtual Machines, Cloud Services und Web Apps

## Bevor Sie beginnen

- Lesen Sie die Azure-bezogenen Nutzungsrichtlinien. Weitere Informationen finden Sie unter Bereitstellen einer NetScaler VPX-Instanz in Microsoft Azure.

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

- Erstellen Sie eine oder mehrere NetScaler VPX-Instanzen mit drei Netzwerkschnittstellen in Azure, entsprechend Ihren Anforderungen (Standalone- oder Hochverfügbarkeitsbereitstellung).
- Öffnen Sie den TCP-Port 9001 in der Netzwerksicherheitsgruppe der 0/1-Schnittstelle der VPX-Instanz. Die VPX-Instanz verwendet diesen Port, um die Scale-Out- und Scale-In-Benachrichtigung zu empfangen.
- Erstellen Sie eine Azure VMSS im selben virtuellen Netzwerk, in dem die NetScaler VPX-Instanz bereitgestellt wird. Wenn die VMSS und die NetScaler VPX-Instanz in verschiedenen virtuellen Azure-Netzwerken bereitgestellt werden, müssen die folgenden Bedingungen erfüllt sein:
  - Beide virtuellen Netzwerke müssen sich im selben Azure-Abonnement befinden.
  - Die beiden virtuellen Netzwerke müssen über die Funktion für virtuelles Netzwerk-Peering von Azure verbunden sein.

  Wenn Sie keine vorhandene VMSS-Konfiguration haben, führen Sie die folgenden Aufgaben aus:

  a) Erstellen Sie eine VMSS

  b) Aktivieren Sie Autoscale auf der VMSS

  c) Erstellen Sie Skalierungsrichtlinien (Scale-in und Scale-out) in den VMSS Autoscale-Einstellungen

  Weitere Informationen finden Sie unter Übersicht über Autoscale mit Azure-Skalierungsgruppen für virtuelle Maschinen.
- NetScaler VPX unterstützt VMSS nur mit Uniform Orchestration. VMSS mit Flexible Orchestration wird nicht unterstützt. Weitere Informationen finden Sie unter Orchestrierungsmodi für Skalierungsgruppen für virtuelle Maschinen in Azure.
- Ab NetScaler Release 14.1-12.x unterstützt NetScaler VPX verwaltete Identitäten in der Azure Cloud. Verwaltete Identitäten verknüpfen einen Dienstprinzipal mit einer Azure-Ressource wie einer virtuellen Maschine. Mit verwalteten Identitäten müssen Sie die Cloud-Anmeldeinformationen (Anwendungs-ID, Anwendungsgeheimnis und Mandanten-ID) nicht verwalten und vermeiden so Sicherheitsrisiken. Derzeit unterstützt NetScaler VPX nur die systemseitig zugewiesene und eine einzelne benutzerseitig zugewiesene verwaltete Identität. Eine mehreren Benutzern zugewiesene verwaltete Identität wird nicht unterstützt.

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

Für NetScaler-Releases vor 14.1-12.x müssen Sie die Cloud-Anmeldeinformationen in NetScaler VPX manuell über Azure Active Directory (AAD) verwalten. Weisen Sie der neu erstellten AAD-Anwendung eine Mitwirkendenrolle zu. Die Cloud-Anmeldeinformationen müssen nach Ablauf regelmäßig neu erstellt werden. Weitere Informationen finden Sie unter Erstellen einer Azure Active Directory-Anwendung und eines Dienstprinzipals.

Wenn Sie eine verwaltete Identität in der Azure-Konsole und Cloud-Anmeldeinformationen in NetScaler® konfigurieren, hat die verwaltete Identität Vorrang vor den Cloud-Anmeldeinformationen.

## Konfigurieren einer verwalteten Identität auf einer virtuellen Maschine

1. Melden Sie sich beim Azure-Portal an.
2. Navigieren Sie zu Ihrer virtuellen Maschine und wählen Sie **Identität** aus.
3. Wählen Sie je nach Ihren Anforderungen entweder **Systemseitig zugewiesen** oder **Benutzerseitig zugewiesen**.
4. Wählen Sie unter **Status** die Option **Ein** und klicken Sie dann auf **Speichern**.

   Verwaltete Identität aktivieren(/en-us/vpx/media/azure-mi-on.png)

   Sobald der Status gespeichert ist, sehen Sie, dass ein Dienstprinzipalobjekt erstellt und der VM zugewiesen wird.
5. Klicken Sie auf **Azure-Rollenzuweisungen**.

   Azure-Rollenzuweisungen(/en-us/vpx/media/azure-mi-on-service-principal.png)
6. Wählen Sie im Fenster **Rollenzuweisung hinzufügen** einen Bereich aus. Sie können aus den folgenden Optionen wählen:

   - Abonnement

     Wenn sich VMSS und VM in verschiedenen Ressourcengruppen befinden, verwenden Sie **Abonnement** als Bereich.
   - Ressourcengruppe

     Wenn sich die VMSS in derselben Ressourcengruppe wie Ihre VM befindet, verwenden Sie **Ressourcengruppe** als Bereich.
   - Key Vault
   - Speicher

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

- SQL

Basierend auf Ihrer Bereichsauswahl füllen Sie die Details für andere Felder aus. Weisen Sie die Rolle **Mitwirkender** zu und **speichern** Sie die Konfiguration.

Die Seite **Azure-Rollenzuweisungen** zeigt die von Ihnen erstellte verwaltete Identität an.

7. Um eine benutzerseitig zugewiesene verwaltete Identität zu erstellen, wählen Sie ein Abonnement aus, wählen Sie eine benutzerseitig zugewiesene verwaltete Identität und klicken Sie auf **Hinzufügen**.

## VMSS zu einer NetScaler VPX-Instanz hinzufügen

Führen Sie die folgenden Schritte aus, um die Autoscale-Einstellung zur VPX-Instanz hinzuzufügen:

1. Melden Sie sich bei der VPX-Instanz an.
2. Navigieren Sie zu **Konfiguration > Azure > Anmeldeinformationen festlegen**. Fügen Sie die erforderlichen Azure-Anmeldeinformationen hinzu, damit die Autoscale-Funktion funktioniert.

**HINWEIS:**

Wenn Sie eine verwaltete Azure-Identität verwenden, ist es nicht erforderlich, Anmeldeinformationen festzulegen.

3. Gehen Sie zu **System > Azure > Cloud-Profil** und klicken Sie auf **Hinzufügen**, um ein Cloud-Profil zu erstellen.

Die Konfigurationsseite **Cloud-Profil erstellen** wird angezeigt.

Ein Cloud-Profil erstellt einen NetScaler-Lastausgleichs-Virtual-Server und eine Dienstgruppe mit Mitgliedern (Servern) als Server der Auto-Scaling-Gruppe. Ihre Backend-Server müssen über die auf der VPX-Instanz konfigurierte SNIP erreichbar sein.

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

### Hinweise zur Erstellung eines Cloud-Profils

- Die IP-Adresse des virtuellen Servers wird automatisch aus der freien IP-Adresse, die der VPX-Instanz zur Verfügung steht, ausgefüllt. Weitere Informationen finden Sie unter Zuweisen mehrerer IP-Adressen zu virtuellen Maschinen über das Azure-Portal.
- Die Autoscale-Einstellung wird aus der VMSS-Instanz vorab ausgefüllt, die mit der NetScaler VPX-Instanz entweder im selben virtuellen Netzwerk oder in gepeerten virtuellen Netzwerken verbunden ist. Weitere Informationen finden Sie unter Übersicht über Autoscale mit Azure-Skalierungsgruppen für virtuelle Maschinen.
- Beim Auswählen des **Auto Scale Setting Protocol** und des **Auto Scale Setting Port** stellen Sie sicher, dass Ihre Server auf den Protokollen und Ports lauschen und Sie den richtigen Monitor in der Dienstgruppe binden. Standardmäßig wird der TCP-Monitor verwendet.
- Für die Autoskalierung vom Typ SSL-Protokoll ist nach dem Erstellen des Cloud-Profils der Lastausgleichs-Virtual-Server oder die Dienstgruppe aufgrund eines fehlenden Zertifikats ausgefallen. Sie können das Zertifikat manuell an den virtuellen Server oder die Dienstgruppe binden.

**HINWEIS:**

Ab NetScaler Release 13.1-42.x können Sie verschiedene Cloud-Profile für verschiedene Dienste (unter Verwendung unterschiedlicher Ports) mit derselben VMSS in Azure erstellen. Somit unterstützt die NetScaler VPX-Instanz mehrere Dienste mit derselben Autoscaling-Gruppe in der Public Cloud.

Um Autoscale-bezogene Informationen im Azure-Portal anzuzeigen, navigieren Sie zu **Virtual machine scale sets** und wählen Sie **virtual machine scale set** > **Scaling**.

## Migration von nicht verwalteten Datenträgern zu verwalteten Datenträgern in Azure

Wenn Ihre NetScaler VPX-Instanz oder VMSS mit nicht verwalteten Datenträgern bereitgestellt wird, ist eine Migration zu verwalteten Datenträgern erforderlich, um den Änderungen in der Azure Cloud gerecht zu werden. Beachten Sie die folgende Azure-Dokumentation für den Migrationsleitfaden und die zugehörigen FAQs:

- Migrieren einer virtuellen Linux-Maschine von nicht verwalteten Datenträgern zu verwalteten Datenträgern
- FAQs

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

### Referenzen

Weitere Informationen zum Autoscaling von NetScaler VPX in Microsoft Azure mit NetScaler Application Delivery and Management finden Sie unter Azure Autoscale mit NetScaler ADM.

## Azure-Tags für die NetScaler VPX-Bereitstellung

Im Azure Cloud-Portal können Sie Ressourcen mit einem Name-Wert-Paar (z. B. Dept: Finance) taggen, um Ressourcen über Ressourcengruppen und innerhalb des Portals über Abonnements hinweg zu kategorisieren und anzuzeigen. Das Tagging ist hilfreich, wenn Sie Ressourcen für die Abrechnung, Verwaltung oder Automatisierung organisieren müssen.

### Wie Azure-Tags für die VPX-Bereitstellung funktionieren

Für NetScaler VPX-Standalone- und Hochverfügbarkeitsinstanzen, die in der Azure Cloud bereitgestellt werden, können Sie jetzt Lastausgleichsdienstgruppen erstellen, die einem Azure-Tag zugeordnet sind. Die VPX-Instanz überwacht ständig Azure-VMs (Back-End-Server) und Netzwerkschnittstellen (NICs) oder beides mit dem entsprechenden Tag und aktualisiert die Dienstgruppe entsprechend.

Die VPX-Instanz erstellt die Dienstgruppe, die die Back-End-Server mithilfe von Tags lastausgleicht. Die Instanz fragt die Azure-API nach allen Ressourcen ab, die mit einem bestimmten Tag-Namen und Tag-Wert versehen sind. Abhängig von der zugewiesenen Abfrageperiode (standardmäßig 60 Sekunden) fragt die VPX-Instanz die Azure-API regelmäßig ab und ruft die Ressourcen ab, die mit dem in der VPX-GUI zugewiesenen Tag-Namen und Tag-Werten verfügbar sind. Immer wenn eine VM oder NIC mit dem entsprechenden Tag hinzugefügt oder gelöscht wird, erkennt der ADC die jeweilige Änderung und fügt die VM- oder NIC-IP-Adresse automatisch zur Dienstgruppe hinzu oder löscht sie daraus.

### Bevor Sie beginnen

Bevor Sie NetScaler-Lastausgleichsdienstgruppen erstellen, fügen Sie den Servern in Azure ein Tag hinzu. Sie können das Tag entweder der virtuellen Maschine oder der NIC zuweisen.

Weitere Informationen zum Hinzufügen von Azure-Tags finden Sie im Microsoft-Dokument Verwenden von Tags zum Organisieren Ihrer Azure-Ressourcen.

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

**HINWEIS:**

ADC CLI-Befehle zum Hinzufügen von Azure-Tag-Einstellungen unterstützen Tag-Namen und Tag-Werte, die nur mit Ziffern oder Buchstaben beginnen und keine anderen Tastaturzeichen enthalten.

## So fügen Sie Azure-Tag-Einstellungen über die VPX-GUI hinzu

Sie können das Azure-Tag-Cloud-Profil über die VPX-GUI zu einer VPX-Instanz hinzufügen, damit die Instanz die Back-End-Server mithilfe des angegebenen Tags lastausgleichen kann. Gehen Sie wie folgt vor:

1. Gehen Sie in der VPX-GUI zu **Configuration > Azure > Cloud Profile**.
2. Klicken Sie auf Hinzufügen, um ein Cloud-Profil zu erstellen. Das Cloud-Profil-Fenster wird geöffnet.

1. Geben Sie Werte für die folgenden Felder ein:

   - Name: Geben Sie einen Namen für Ihr Profil ein
   - IP-Adresse des virtuellen Servers: Die IP-Adresse des virtuellen Servers wird automatisch aus der freien IP-Adresse, die der VPX-Instanz zur Verfügung steht, ausgefüllt. Weitere Informationen finden Sie unter Zuweisen mehrerer IP-Adressen zu virtuellen Maschinen über das Azure-Portal.
   - Typ: Wählen Sie im Menü AZURETAGS.
   - Azure-Tag-Name: Geben Sie den Namen ein, den Sie den VMs oder NICs im Azure-Portal zugewiesen haben.
   - Azure-Tag-Wert: Geben Sie den Wert ein, den Sie den VMs oder NICs im Azure-Portal zugewiesen haben.
   - Azure-Abfrageintervalle: Standardmäßig beträgt das Abfrageintervall 60 Sekunden, was der Mindestwert ist. Sie können es je nach Bedarf ändern.
   - Load-Balancing-Server-Protokoll: Wählen Sie das Protokoll aus, auf dem Ihr Load Balancer lauscht.
   - Load-Balancing-Server-Port: Wählen Sie den Port aus, auf dem Ihr Load Balancer lauscht.
   - Azure-Tag-Einstellung: Der Name der Dienstgruppe, die für dieses Cloud-Profil erstellt wird.

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

- Azure-Tag-Einstellungs-Protokoll: Wählen Sie das Protokoll aus, auf dem Ihre Back-End-Server lauschen.
- Azure-Tag-Einstellungs-Port: Wählen Sie den Port aus, auf dem Ihre Back-End-Server lauschen.

2. Klicken Sie auf **Erstellen**.

Ein Load-Balancer-virtueller Server und eine Dienstgruppe werden für die getaggten VMs oder NICs erstellt. Um den virtuellen Load-Balancer-Server anzuzeigen, navigieren Sie in der VPX-GUI zu **Traffic Management > Load Balancing > Virtual Servers**.

## So fügen Sie Azure-Tag-Einstellungen mithilfe der VPX-CLI hinzu

Geben Sie den folgenden Befehl in der NetScaler-CLI ein, um ein Cloud-Profil für Azure-Tags zu erstellen.

```
add cloud profile `<profile name>` -type azuretags -vServerName `< vserver
name>` -serviceType HTTP -IPAddress `<vserver IP address>` -port 80
-serviceGroupName `<service group name>` -boundServiceGroupSvcType HTTP
-vsvrbindsvcport 80 -azureTagName `<Azure tag specified on Azure portal>`
-azureTagValue `<Azure value specified on the Azure portal>`
-azurePollPeriod 60
```

**WICHTIG:**

Sie müssen alle Konfigurationen speichern; andernfalls gehen die Konfigurationen nach dem Neustart der Instanz verloren. Geben Sie `save config` ein.

**Beispiel 1**: Hier ist ein Beispielbefehl für ein Cloud-Profil für HTTP-Traffic aller Azure-VMs/NICs, die mit dem Paar „myTagName/myTagValue“ getaggt sind:

```
add cloud profile MyTagCloudProfile -type azuretags -vServerName
MyTagVServer -serviceType HTTP -IPAddress 40.115.116.57 -port 80
-serviceGroupName MyTagsServiceGroup -boundServiceGroupSvcType HTTP
-vsvrbindsvcport 80 -azureTagName myTagName -azureTagValue myTagValue
-azurePollPeriod 60
```

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

```
Done
```

Um das Cloud-Profil anzuzeigen, geben Sie `show cloudprofile` ein.

**Beispiel 2**: Der folgende CLI-Befehl gibt Informationen über das neu hinzugefügte Cloud-Profil in Beispiel 1 aus.

```
show cloudprofile

1)    Name:  MyTagCloudProfile Type:  azuretags         VServerName:
 MyTagVServer ServiceType:  HTTP       IPAddress:  52.178.209.133 Port:
 80               ServiceGroupName:  MyTagsServiceGroup
BoundServiceGroupSvcType:  HTTP

     Vsvrbindsvcport:  80     AzureTagName:  myTagName AzureTagValue:
 myTagValue AzurePollPeriod:  60     GraceFul:  NO            Delay:  60
```

Um ein Cloud-Profil zu entfernen, geben Sie rm cloud profile `<cloud profile name>` ein.

**Beispiel 3**: Der folgende Befehl entfernt das in Beispiel 1 erstellte Cloud-Profil.

```
> rm cloudprofile MyTagCloudProfile

  Done
```

## Fehlerbehebung

**Problem**: In sehr seltenen Fällen kann der CLI-Befehl „rm cloud profile“ die mit dem gelöschten Cloud-Profil verbundenen Dienstgruppen und Server möglicherweise nicht entfernen. Dies geschieht, wenn der Befehl Sekunden vor Ablauf des Abfragezeitraums des zu löschenden Cloud-Profils ausgegeben wird.

**Lösung**: Löschen Sie die verbleibenden Dienstgruppen manuell, indem Sie den folgenden CLI-Befehl für jede der verbleibenden Dienstgruppen eingeben:

```
#> rm servicegroup <serviceGroupName>
```

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

Entfernen Sie außerdem jeden der verbleibenden Server, indem Sie den folgenden CLI-Befehl für jeden der verbleibenden Server eingeben:

```
#> rm server <name>
```

**Problem**: Wenn Sie eine Azure-Tag-Einstellung mithilfe der CLI zu einer VPX-Instanz hinzufügen, läuft der rain_tags-Prozess nach einem Warmstart auf einem HA-Paar-Knoten weiter.

**Lösung**: Beenden Sie den Prozess auf dem sekundären Knoten nach einem Warmstart manuell. Wechseln Sie von der CLI des sekundären HA-Knotens zur Shell-Eingabeaufforderung:

```
#> shell
```

Verwenden Sie den folgenden Befehl, um den rain_tags-Prozess zu beenden:

```
# PID=`ps -aux | grep rain_tags | awk '{print $2}'`; kill -9 $PID
```

**Problem**: Back-End-Server sind möglicherweise nicht erreichbar und werden von der VPX-Instanz als DOWN gemeldet, obwohl sie fehlerfrei sind. **Lösung**: Stellen Sie sicher, dass die VPX-Instanz die getaggte IP-Adresse erreichen kann, die dem Back-End-Server entspricht. Bei einer getaggten NIC ist dies die IP-Adresse der NIC; während bei einer getaggten VM dies die primäre IP-Adresse der VM ist. Wenn die VM/NIC in einem anderen Azure VNet liegt, stellen Sie sicher, dass VNet-Peering aktiviert ist.

## GSLB auf NetScaler VPX-Instanzen konfigurieren

NetScaler-Appliances, die für das globale Server-Lastenausgleich (GSLB) konfiguriert sind, bieten Notfallwiederherstellung und kontinuierliche Verfügbarkeit von Anwendungen, indem sie vor Ausfallpunkten in einem WAN schützen. GSLB kann die Last über Rechenzentren hinweg ausgleichen, indem Client-Anfragen an das nächstgelegene oder leistungsstärkste Rechenzentrum oder im Falle eines Ausfalls an die verbleibenden Rechenzentren weitergeleitet werden.

Dieser Abschnitt beschreibt, wie GSLB auf VPX-Instanzen an zwei Standorten in einer Microsoft Azure-Umgebung mithilfe von Windows PowerShell-Befehlen aktiviert wird.

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

**HINWEIS:**

Weitere Informationen zu GSLB finden Sie unter Globaler Server-Lastenausgleich.

Sie können GSLB auf einer NetScaler VPX-Instanz in Azure in zwei Schritten konfigurieren:

1. Erstellen Sie an jedem Standort eine VPX-Instanz mit mehreren NICs und mehreren IP-Adressen.
2. Aktivieren Sie GSLB auf den VPX-Instanzen.

**HINWEIS:**

Weitere Informationen zum Konfigurieren mehrerer NICs und IP-Adressen finden Sie unter: Konfigurieren mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus mithilfe von PowerShell-Befehlen

## Szenario

Dieses Szenario umfasst zwei Standorte – Standort 1 und Standort 2. Jeder Standort verfügt über eine VM (VM1 und VM2), die mit mehreren NICs, mehreren IP-Adressen und GSLB konfiguriert ist.

**Abbildung.** GSLB-Einrichtung über zwei Standorte – Standort 1 und Standort 2.

In diesem Szenario verfügt jede VM über drei NICs – NIC 0/1, 1/1 und 1/2. Jede NIC kann mehrere private und öffentliche IP-Adressen haben. Die NICs sind für die folgenden Zwecke konfiguriert.

- NIC 0/1: zur Bereitstellung von Management-Traffic
- NIC 1/1: zur Bereitstellung von Client-seitigem Traffic
- NIC 1/2: zur Kommunikation mit Back-End-Servern

Informationen zu den auf jeder NIC in diesem Szenario konfigurierten IP-Adressen finden Sie im Abschnitt IP-Konfigurationsdetails.

## Parameter

Im Folgenden finden Sie Beispielparameter für dieses Szenario in diesem Dokument.

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

```
$location="West Central US"

$vnetName="NSVPX-vnet"

$RGName="multiIP-RG"

$prmStorageAccountName="multiipstorageaccnt"

$avSetName="MultiIP-avset"

$vmSize="Standard\_DS3\_V2"
```

**HINWEIS:**

Die Mindestanforderung für eine VPX-Instanz sind 2 vCPUs und 2 GB RAM.

```
$publisher="citrix"

$offer="netscalervpx111"

$sku="netscalerbyol"

$version="latest"
```

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

```
$vmNamePrefix="MultiIPVPX"

$nicNamePrefix="MultiipVPX"

$osDiskSuffix="osdiskdb"

$numberOfVMs=1

$ipAddressPrefix="10.0.0."

$ipAddressPrefix1="10.0.1."

$ipAddressPrefix2="10.0.2."

$pubIPName1="MultiIP-pip1"

$pubIPName2="MultiIP-pip2"

$IpConfigName1="IPConfig1"

$IPConfigName2="IPConfig-2"
```

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

```
$IPConfigName3="IPConfig-3"

$IPConfigName4="IPConfig-4"

$frontendSubnetName="default"

$backendSubnetName1="subnet\_1"

$backendSubnetName2="subnet\_2"

$suffixNumber=10
```

## Eine VM erstellen

Führen Sie die Schritte 1–10 aus, um VM1 mit mehreren NICs und mehreren IP-Adressen mithilfe von PowerShell-Befehlen zu erstellen:

1. Ressourcengruppe erstellen
2. Speicherkonto erstellen
3. Verfügbarkeitsgruppe erstellen
4. Virtuelles Netzwerk erstellen
5. Öffentliche IP-Adresse erstellen
6. NICs erstellen
7. VM-Konfigurationsobjekt erstellen
8. Anmeldeinformationen abrufen und BS-Eigenschaften für die VM festlegen
9. NICs hinzufügen
10. Betriebssystemdatenträger angeben und VM erstellen

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

Nachdem Sie alle Schritte und Befehle zur Erstellung von VM1 abgeschlossen haben, wiederholen Sie diese Schritte, um VM2 mit den für sie spezifischen Parametern zu erstellen.

### Ressourcengruppe erstellen

```
New-AzureRMResourceGroup -Name $RGName -Location $location
```

### Speicherkonto erstellen

```
$prmStorageAccount=New-AzureRMStorageAccount -Name $prmStorageAccountName
-ResourceGroupName $RGName -Type Standard_LRS -Location $location
```

### Verfügbarkeitsgruppe erstellen

```
$avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
$RGName -Location $location
```

### Virtuelles Netzwerk erstellen

1. Subnetze hinzufügen.

   ```
   $subnet1=New-AzureRmVirtualNetworkSubnetConfig -Name
   $frontendSubnetName -AddressPrefix "10.0.0.0/24"

   $subnet2=New-AzureRmVirtualNetworkSubnetConfig -Name
   $backendSubnetName1 -AddressPrefix "10.0.1.0/24"

   $subnet3=New-AzureRmVirtualNetworkSubnetConfig -Name
   $backendSubnetName2 -AddressPrefix "10.0.2.0/24"
   ```

2. Virtuelles Netzwerkobjekt hinzufügen.

   ```
   $vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
   $RGName -Location $location -AddressPrefix 10.0.0.0/16 -Subnet
   $subnet1, $subnet2, $subnet3
   ```

3. Subnetze abrufen.

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

```
$frontendSubnet=$vnet.Subnets|?{$_.Name -eq $frontendSubnetName}

$backendSubnet1=$vnet.Subnets|?{$_.Name -eq $backendSubnetName1}

$backendSubnet2=$vnet.Subnets|?{$_.Name -eq $backendSubnetName2}
```

### Öffentliche IP-Adresse erstellen

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
$RGName -Location $location -AllocationMethod Dynamic

$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
$RGName -Location $location -AllocationMethod Dynamic
```

### NICs erstellen

NIC 0/1 erstellen

```
$nic1Name=$nicNamePrefix + $suffixNumber + "-Mgmnt"

$ipAddress1=$ipAddressPrefix + $suffixNumber

$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1
-SubnetId $frontendSubnet.Id -PublicIpAddress $pip1 -PrivateIpAddress
$ipAddress1 -Primary

$nic1=New-AzureRMNetworkInterface -Name $nic1Name -ResourceGroupName
$RGName -Location $location -IpConfiguration $IpConfig1
```

NIC 1/1 erstellen

```
$nic2Name $nicNamePrefix + $suffixNumber + "-frontend"

$ipAddress2=$ipAddressPrefix1 + ($suffixNumber)

$ipAddress3=$ipAddressPrefix1 + ($suffixNumber + 1)

$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2
-PublicIpAddress $pip2 -SubnetId $backendSubnet1.Id  -PrivateIpAddress
$ipAddress2  -Primary
```

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

```
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3
-SubnetId $backendSubnet1.Id  -PrivateIpAddress $ipAddress3

nic2=New-AzureRMNetworkInterface -Name $nic2Name -ResourceGroupName
$RGName -Location $location -IpConfiguration $IpConfig2, $IpConfig3
```

NIC 1/2 erstellen

```
$nic3Name=$nicNamePrefix + $suffixNumber + "-backend"

$ipAddress4=$ipAddressPrefix2 + ($suffixNumber)

$IPConfig4=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4
-SubnetId $backendSubnet2.Id -PrivateIpAddress $ipAddress4 -Primary

$nic3=New-AzureRMNetworkInterface -Name $nic3Name -ResourceGroupName
$RGName -Location $location -IpConfiguration $IpConfig4
```

### VM-Konfigurationsobjekt erstellen

```
$vmName=$vmNamePrefix

$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize
-AvailabilitySetId $avSet.Id
```

### Anmeldeinformationen abrufen und Betriebssystemeigenschaften festlegen

```
$cred=Get-Credential -Message "Type the name and password for VPX login."

$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName
$vmName -Credential $cred

$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher
-Offer $offer -Skus $sku -Version $version
```

### NICs hinzufügen

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id
-Primary
```

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

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.Id

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.Id
```

### Betriebssystemdatenträger angeben und VM erstellen

```
$osDiskName=$vmName + "-" + $osDiskSuffix

$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/" +
$osDiskName + ".vhd"

$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
$osVhdUri -CreateOption fromImage

Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer
-Name $sku

New-AzureRMVM -VM $vmConfig -ResourceGroupName $RGName -Location $location
```

**HINWEIS:**

Wiederholen Sie die Schritte 1–10, die unter „Erstellen von Multi-NIC-VMs mithilfe von PowerShell-Befehlen“ aufgeführt sind, um VM2 mit VM2-spezifischen Parametern zu erstellen.

## Details zur IP-Konfiguration

Die folgenden IP-Adressen werden verwendet.

**Tabelle 1**. In VM1 verwendete IP-Adressen

| NIC | PRIVATE IP | ÖFFENTLICHE IP (PIP) | BESCHREIBUNG |
|---|---|---|---|
| 0/1 | 10.0.0.10 | PIP1 | Konfiguriert als NSIP (Verwaltungs-IP) |
| 1/1 | 10.0.1.10 | PIP2 | Konfiguriert als SNIP/GSLB-Site-IP |

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

| NIC | PRIVATE IP | ÖFFENTLICHE IP (PIP) | BESCHREIBUNG |
|---|---|---|---|
| - | 10.0.1.11 | - | Konfiguriert als LB-Server-IP. Eine öffentliche IP ist nicht zwingend erforderlich. |
| 1/2 | 10.0.2.10 | - | Als SNIP zum Senden von Monitor-Probes an Dienste konfiguriert; öffentliche IP ist nicht zwingend erforderlich |

**Tabelle 2.** In VM2 verwendete IP-Adressen

| NIC | INTERNE IP | ÖFFENTLICHE IP (PIP) | BESCHREIBUNG |
|---|---|---|---|
| 0/1 | 20.0.0.10 | PIP4 | Als NSIP (Verwaltungs-IP) konfiguriert |
| 1/1 | 20.0.1.10 | PIP5 | Als SNIP/GSLB-Site-IP konfiguriert |
| - | 20.0.1.11 | - | Konfiguriert als LB-Server-IP. Eine öffentliche IP ist nicht zwingend erforderlich. |
| 1/2 | 20.0.2.10 | - | Konfiguriert als SNIP zum Senden von Monitor-Probes an Dienste; eine öffentliche IP ist nicht zwingend erforderlich. |

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

Hier sind Beispielkonfigurationen für dieses Szenario, die die IP-Adressen und die anfänglichen LB-Konfigurationen zeigen, wie sie über die NetScaler VPX CLI für VM1 und VM2 erstellt wurden.

Hier ist eine Beispielkonfiguration auf VM1.

```
add ns ip 10.0.1.10 255.255.255.0 -mgmtAccess ENABLED

Add nsip 10.0.2.10 255.255.255.0

add service svc1 10.0.1.10 ADNS 53

add lb vserver v1 HTTP 10.0.1.11 80

add service s1 10.0.2.120 http 80

Add service s2 10.0.2.121 http 80

Bind lb vs v1 s[1-2]
```

Hier ist eine Beispielkonfiguration auf VM2.

```
add ns ip 20.0.1.10 255.255.255.0  -mgmtAccess ENABLED

Add nsip 20.0.2.10 255.255.255.0

add service svc1 20.0.1.10 ADNS 53

add lb vserver v1 HTTP 20.0.1.11 80

Add service s1 20.0.2.90 http 80

Add service s2 20.0.2.91 http 80

Bind lb vs v1 s[1-2]
```

## GSLB-Sites und andere Einstellungen konfigurieren

Führen Sie die im folgenden Thema beschriebenen Aufgaben aus, um die beiden GSLB-Sites und andere notwendige Einstellungen zu konfigurieren:

Global Server Load Balancing

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

Hier ist eine Beispiel-GSLB-Konfiguration auf VM1 und VM2.

```
enable ns feature LB GSLB

add gslb site site1 10.0.1.10 -publicIP PIP2

add gslb site site2 20.0.1.10 -publicIP PIP5

add gslb service site1_gslb_http_svc1 10.0.1.11 HTTP 80 -publicIP PIP3
-publicPort 80 -siteName site1

add gslb service site2_gslb_http_svc1 20.0.1.11 HTTP 80 -publicIP PIP6
-publicPort 80 -siteName site2

add gslb vserver gslb_http_vip1 HTTP

bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

Sie haben GSLB auf NetScaler VPX-Instanzen konfiguriert, die auf Azure ausgeführt werden.

## Notfallwiederherstellung

Eine Katastrophe ist eine plötzliche Unterbrechung der Geschäftsfunktionen, die durch Naturkatastrophen oder von Menschen verursachte Ereignisse hervorgerufen wird. Katastrophen beeinträchtigen den Betrieb von Rechenzentren, wonach die am Katastrophenort verlorenen Ressourcen und Daten vollständig wiederhergestellt werden müssen. Der Datenverlust oder die Ausfallzeit im Rechenzentrum ist kritisch und gefährdet die Geschäftskontinuität.

Eine der Herausforderungen, vor denen Kunden heute stehen, ist die Entscheidung, wo sie ihren DR-Standort einrichten sollen. Unternehmen suchen nach Konsistenz und Leistung, unabhängig von zugrunde liegenden Infrastruktur- oder Netzwerkfehlern.

Mögliche Gründe, warum viele Organisationen sich für die Migration in die Cloud entscheiden, sind:

- Ein lokales Rechenzentrum ist sehr teuer. Durch die Nutzung der Cloud können Unternehmen Zeit und Ressourcen sparen, die sie sonst für die Erweiterung ihrer eigenen Systeme aufwenden müssten.

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

- Viele der automatisierten Orchestrierungen ermöglichen eine schnellere Wiederherstellung
- Daten replizieren durch Bereitstellung von kontinuierlichem Datenschutz oder kontinuierlichen Snapshots, um sich vor Ausfällen oder Angriffen zu schützen.
- Unterstützung von Anwendungsfällen, bei denen Kunden viele verschiedene Arten von Compliance- und Sicherheitskontrollen benötigen, die bereits in den öffentlichen Clouds vorhanden sind. Dies erleichtert es, die benötigte Compliance zu erreichen, anstatt eigene zu entwickeln.

Ein für GSLB konfigurierter NetScaler leitet den Datenverkehr an das am wenigsten ausgelastete oder leistungsstärkste Rechenzentrum weiter. Diese Konfiguration, die als Active-Active-Setup bezeichnet wird, verbessert nicht nur die Leistung, sondern bietet auch eine sofortige Notfallwiederherstellung, indem der Datenverkehr an andere Rechenzentren geleitet wird, wenn ein Teil des Setups ausfällt. NetScaler spart Kunden dadurch wertvolle Zeit und Geld.

### Multi-NIC Multi-IP (Drei-NIC)-Bereitstellung für die Notfallwiederherstellung

Kunden würden möglicherweise eine Drei-NIC-Bereitstellung verwenden, wenn sie in einer Produktionsumgebung bereitstellen, in der Sicherheit, Redundanz, Verfügbarkeit, Kapazität und Skalierbarkeit entscheidend sind. Bei dieser Bereitstellungsmethode sind Komplexität und einfache Verwaltung keine kritischen Bedenken für die Benutzer.

### Single-NIC Multi-IP (Ein-NIC)-Bereitstellung für die Notfallwiederherstellung

Kunden würden möglicherweise eine Ein-NIC-Bereitstellung verwenden, wenn sie aus den folgenden Gründen in einer Nicht-Produktionsumgebung bereitstellen:

- Einrichtung der Umgebung zum Testen oder Vorbereitung einer neuen Umgebung vor der Produktionsbereitstellung.
- Schnelles und effizientes Bereitstellen direkt in die Cloud.
- Dabei die Einfachheit einer einzelnen Subnetzkonfiguration anstreben.

## GSLB in einer Aktiv-Standby-Hochverfügbarkeitskonfiguration konfigurieren

Sie können Global Server Load Balancing (GSLB) in einer Aktiv-Standby-HA-Bereitstellung in Azure in drei Schritten konfigurieren:

1. Erstellen Sie ein VPX-HA-Paar an jedem GSLB-Standort. Siehe Konfigurieren einer Hochverfügbarkeitskonfiguration mit mehreren IP-Adressen und NICs für Informationen zur Erstellung eines HA-Paares.

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

2. Konfigurieren Sie den Azure Load Balancer (ALB) mit der Front-End-IP-Adresse und Regeln, um GSLB- und DNS-Verkehr zuzulassen.

   Dieser Schritt umfasst die folgenden Unterschritte. Die PowerShell-Befehle zur Ausführung dieser Unterschritte finden Sie im Szenario in diesem Abschnitt.

   a. Erstellen Sie ein Front-End `IPconfig` für den GSLB-Standort.

   b. Erstellen Sie einen Back-End-Adresspool mit der IP-Adresse von NIC 1/1 der Knoten in HA.

   c. Erstellen Sie Lastenausgleichsregeln für Folgendes:

   ```
   TCP/3009 – gslb communication

   TCP/3008 - gslb communication

   UDP/53 - DNS communication
   ```

   d. Ordnen Sie den Back-End-Adresspool den in Schritt c erstellten LB-Regeln zu.

   e. Aktualisieren Sie die Netzwerksicherheitsgruppe von NIC 1/1 der Knoten in beiden HA-Paaren, um den Datenverkehr für die Ports TCP 3008, TCP 3009 und UDP 53 zuzulassen.

3. Aktivieren Sie GSLB auf jedem HA-Paar.

## Szenario

Dieses Szenario umfasst zwei Standorte – Standort 1 und Standort 2. Jeder Standort verfügt über ein HA-Paar (HA1 und HA2), das mit mehreren NICs, mehreren IP-Adressen und GSLB konfiguriert ist.

**Abbildung:** GSLB in einer Aktiv-Standby-HA-Bereitstellung in Azure

In diesem Szenario hat jede VM drei NICs – NIC 0/1, 1/1 und 1/2. Die NICs sind für die folgenden Zwecke konfiguriert.

NIC 0/1: zur Bereitstellung von Management-Traffic

NIC 1/1: zur Bereitstellung von Client-seitigem Traffic

NIC 1/2: zur Kommunikation mit Backend-Servern

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

## Parametereinstellungen

Im Folgenden finden Sie Beispiel-Parametereinstellungen für den ALB. Sie können bei Bedarf andere Einstellungen verwenden.

```
$locName="South east Asia"


$rgName="MulitIP-MultiNIC-RG"


$pubIPName4="PIPFORGSLB1"


$domName4="vpxgslbdns"


$lbName="MultiIPALB"


$frontEndConfigName2="FrontEndIP2"


$backendPoolName1="BackendPoolHttp"


$lbRuleName2="LBRuleGSLB1"


$lbRuleName3="LBRuleGSLB2"


$lbRuleName4="LBRuleDNS"
```

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

```
$healthProbeName="HealthProbe"
```

## ALB mit der Frontend-IP-Adresse und Regeln konfigurieren, um GSLB- und DNS-Traffic zuzulassen

Schritt 1. **Erstellen Sie eine öffentliche IP für die GSLB-Site-IP**

```
$pip4=New-AzureRmPublicIpAddress -Name $pubIPName4 -ResourceGroupName
$rgName -DomainNameLabel $domName4 -Location $locName -AllocationMethod
Dynamic




Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName | Add-
AzureRmLoadBalancerFrontendIpConfig -Name $frontEndConfigName2
-PublicIpAddress $pip4 | Set-AzureRmLoadBalancer
```

Schritt 2. **Erstellen Sie LB-Regeln und aktualisieren Sie den vorhandenen ALB**.

```
$alb = get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName




$frontendipconfig2=Get-AzureRmLoadBalancerFrontendIpConfig -LoadBalancer
$alb -Name $frontEndConfigName2




$backendPool=Get-AzureRmLoadBalancerBackendAddressPoolConfig -LoadBalancer
$alb -Name $backendPoolName1
```

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

```
$healthprobe=Get-AzureRmLoadBalancerProbeConfig -LoadBalancer $alb -Name
$healthProbeName




$alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName2
-BackendAddressPool $backendPool -FrontendIPConfiguration
 $frontendipconfig2 -Protocol "Tcp" -FrontendPort 3009 -BackendPort 3009
-Probe $healthprobe -EnableFloatingIP  | Set-AzureRmLoadBalancer




$alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName3
-BackendAddressPool $backendPool -FrontendIPConfiguration
 $frontendipconfig2 -Protocol "Tcp" -FrontendPort 3008 -BackendPort 3008
-Probe $healthprobe -EnableFloatingIP  | Set-AzureRmLoadBalancer




$alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName4
-BackendAddressPool $backendPool -FrontendIPConfiguration
 $frontendipconfig2 -Protocol "Udp" -FrontendPort 53 -BackendPort 53
-Probe $healthprobe -EnableFloatingIP  | Set-AzureRmLoadBalancer
```

## GSLB auf jedem Hochverfügbarkeitspaar aktivieren

Jetzt haben Sie zwei Frontend-IP-Adressen für jeden ALB: ALB 1 und ALB 2. Eine IP-Adresse ist für den virtuellen LB-Server und die andere für die GSLB-Site-IP.

HA 1 hat die folgenden Frontend-IP-Adressen:

- FrontEndIPofALB1 (für virtuellen LB-Server)
- PIPFORGSLB1 (GSLB-IP)

HA 2 hat die folgenden Frontend-IP-Adressen:

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

- FrontEndIPofALB2 (für virtuellen LB-Server)
- PIPFORGSLB2 (GSLB-IP)

Die folgenden Befehle werden für dieses Szenario verwendet.

```
enable ns feature LB GSLB


add service dnssvc PIPFORGSLB1 ADNS 53


add gslb site site1 PIPFORGSLB1 -publicIP PIPFORGSLB1


add gslb site site2 PIPFORGSLB2 -publicIP PIPFORGSLB2


add gslb service site1_gslb_http_svc1 FrontEndIPofALB1 HTTP 80 -publicIP
FrontEndIPofALB1 -publicPort 80 -siteName site1


add gslb service site2_gslb_http_svc1 FrontEndIPofALB2 HTTP 80 -publicIP
FrontEndIPofALB2 -publicPort 80 -siteName site2


add gslb vserver gslb_http_vip1 HTTP


bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1


bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
```

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

```
bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

**Verwandte Ressourcen**:

GSLB auf NetScaler VPX-Instanzen konfigurieren

Globaler Server-Lastausgleich

# NetScaler GSLB in Azure bereitstellen

Mit der steigenden Nachfrage möchten Unternehmen, die ein lokales Rechenzentrum betreiben und regionale Kunden bedienen, global skalieren und in der Azure Cloud bereitstellen. Mit NetScaler auf Seiten des Netzwerkadministrators können Sie das GSLB StyleBook verwenden, um Anwendungen sowohl lokal als auch in der Cloud zu konfigurieren. Sie können dieselbe Konfiguration mit NetScaler ADM in die Cloud übertragen. Je nach Nähe mit GSLB können Sie entweder lokale oder Cloud-Ressourcen erreichen. Dies ermöglicht Ihnen ein nahtloses Erlebnis, egal wo auf der Welt Sie sich befinden.

## DBS-Übersicht

NetScaler GSLB unterstützt die Verwendung von Domain-Based Services (DBS) für Cloud-Lastenausgleichsdienste. Dies ermöglicht die automatische Erkennung dynamischer Cloud-Dienste mithilfe einer Cloud-Lastenausgleichslösung. Diese Konfiguration ermöglicht es dem NetScaler, GSLB DBS in einer Active-Active-Umgebung zu implementieren. DBS ermöglicht die Skalierung von Backend-Ressourcen in Microsoft Azure-Umgebungen durch DNS-Erkennung. Dieser Abschnitt behandelt die Integration zwischen NetScalern in der Azure Autoscale-Umgebung.

### Domänennamenbasierte Dienste mit Azure Load Balancer (ALB)

GSLB DBS verwendet den FQDN des Benutzer-ALB, um die GSLB-Dienstgruppen dynamisch zu aktualisieren und die Backend-Server einzuschließen, die in Azure erstellt und gelöscht werden. Um diese Funktion zu konfigurieren, verweist der Benutzer den Citrix® ADC auf seinen ALB, um dynamisch zu verschiedenen Servern in Azure zu routen. Dies kann geschehen, ohne den Citrix ADC jedes Mal manuell aktualisieren zu müssen, wenn eine Instanz in Azure erstellt oder gelöscht wird. Die Citrix ADC DBS-Funktion für GSLB-Dienstgruppen verwendet die DNS-basierte Dienstermittlung, um die Mitgliedsdienstressourcen des im Autoscale™-Gruppe identifizierten DBS-Namespaces zu bestimmen.

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

Die folgende Abbildung zeigt die NetScaler GSLB DBS Autoscale-Komponenten mit Cloud-Lastenausgleichsdiensten:

## Azure GSLB-Voraussetzungen

Die Voraussetzungen für die NetScaler GSLB-Dienstgruppen umfassen eine funktionierende Microsoft Azure-Umgebung sowie das Wissen und die Fähigkeit zur Konfiguration von Linux-Webservern, NetScaler-Appliances in Azure, öffentlichen IP-Adressen und Azure Load Balancern (ALB).

- Die GSLB DBS-Dienstintegration erfordert NetScaler Version 12.0.57 für Microsoft Azure Load Balancer-Instanzen.
- GSLB-Dienstgruppenentität: NetScaler Version 12.0.57.
- Die GSLB-Dienstgruppe wird eingeführt, die Autoscale mittels dynamischer DBS-Erkennung unterstützt.
- DBS-Funktionskomponenten (Domain-Based Service) müssen an die GSLB-Dienstgruppe gebunden werden.

**Beispiel:**

```
add server sydney_server LB-Sydney-
xxxxxxxxxx.australiaeast.cloudapp.azure.com

add gslb serviceGroup sydney_sg HTTP -autoscale DNS -siteName sydney

bind gslb serviceGroup sydney_sg sydney_server 80
```

## Azure-Komponenten konfigurieren

1. Melden Sie sich beim Azure-Benutzerportal an und erstellen Sie eine neue virtuelle Maschine aus einer NetScaler-Vorlage.
2. Erstellen Sie einen Azure Load Balancer.

3. Fügen Sie die erstellten NetScaler-Back-End-Pools hinzu.

4. Erstellen Sie einen Integritätstest für Port 80.

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

Erstellen Sie eine Lastenausgleichsregel unter Verwendung der Front-End-IP, die vom Load Balancer erstellt wurde.

- Protokoll: TCP
- Back-End-Port: 80
- Back-End-Pool: NetScaler, erstellt in Schritt 1
- Integritätstest: Erstellt in Schritt 4
- Sitzungspersistenz: Keine

## NetScaler GSLB-domänenbasierten Dienst konfigurieren

Die folgenden Konfigurationen fassen zusammen, was erforderlich ist, um domänenbasierte Dienste für die automatische Skalierung von ADCs in einer GSLB-fähigen Umgebung zu aktivieren.

- Konfigurationen für die Datenverkehrsverwaltung
- GSLB-Konfigurationen

### Konfigurationen für die Datenverkehrsverwaltung

**HINWEIS:**

Es ist erforderlich, den NetScaler entweder mit einem Nameserver oder einem virtuellen DNS-Server zu konfigurieren, über den die ALB-Domänen für die DBS-Dienstgruppen aufgelöst werden. Weitere Informationen zu Nameservern oder virtuellen DNS-Servern finden Sie unter DNS-Nameserver.

1. Navigieren Sie zu **Traffic Management > Load Balancing > Servers**.
2. Klicken Sie auf **Hinzufügen**, um einen Server zu erstellen, geben Sie einen Namen und den FQDN ein, der dem A-Eintrag (Domänenname) in Azure für den ALB entspricht.

3. Wiederholen Sie Schritt 2, um den zweiten ALB aus der zweiten Ressource in Azure hinzuzufügen.

### GSLB-Konfigurationen

1. Klicken Sie auf **Hinzufügen**, um eine GSLB-Site zu konfigurieren.

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

2. Geben Sie die Details für die Konfiguration der GSLB-Site an.

   Benennen Sie die Site. Der Typ wird als remote oder lokal konfiguriert, je nachdem, auf welchem NetScaler Sie die Site konfigurieren. Die Site-IP-Adresse ist die IP-Adresse für die GSLB-Site. Die GSLB-Site verwendet diese IP-Adresse, um mit den anderen GSLB-Sites zu kommunizieren. Die öffentliche IP-Adresse ist erforderlich, wenn ein Cloud-Dienst verwendet wird, bei dem eine bestimmte IP-Adresse auf einer externen Firewall oder einem NAT-Gerät gehostet wird. Konfigurieren Sie die Site als übergeordnete Site und stellen Sie sicher, dass die **Trigger Monitors** auf **ALWAYS** eingestellt sind. Stellen Sie außerdem sicher, dass die drei Kontrollkästchen unten für **Metric Exchange**, **Network Metric Exchange** und **Persistence Session Entry Exchange** aktiviert sind.

   Wir empfehlen Ihnen, den **Trigger Monitor** auf **MEPDOWN** einzustellen. Weitere Informationen finden Sie unter Konfigurieren einer GSLB-Dienstgruppe.

3. Klicken Sie auf **Erstellen**.
4. Navigieren Sie zu **Traffic Management > GSLB > Dienstgruppen**.
5. Klicken Sie auf **Hinzufügen**, um eine Dienstgruppe hinzuzufügen.
6. Geben Sie die Details zur Konfiguration der Dienstgruppe an.

   Benennen Sie die Dienstgruppe, verwenden Sie das HTTP-Protokoll. Wählen Sie unter **Site Name** die entsprechende Site aus, die Sie erstellt haben. Stellen Sie sicher, dass der Autoskalierungsmodus als DNS konfiguriert ist und aktivieren Sie die Kontrollkästchen für Status und Zustandsüberwachung. Klicken Sie auf **OK**, um die Dienstgruppe zu erstellen.

7. Klicken Sie auf **Dienstgruppenmitglieder** und wählen Sie **Serverbasiert**. Wählen Sie den entsprechenden ALB aus, der zu Beginn des Ausführungsleitfadens konfiguriert wurde. Konfigurieren Sie den Datenverkehr so, dass er über Port 80 läuft. Klicken Sie auf **Erstellen**.

   Die Bindung der Dienstgruppenmitglieder wird mit 2 Instanzen gefüllt, die sie vom ALB empfängt.

8. Wiederholen Sie die Schritte 5 und 6, um die Dienstgruppe für den zweiten Ressourcenstandort in Azure zu konfigurieren. (Dies kann über dieselbe NetScaler-GUI erfolgen).

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

9. Um einen GSLB-virtuellen Server einzurichten. Navigieren Sie zu **Traffic Management > GSLB > Virtuelle Server**.
10. Klicken Sie auf **Hinzufügen**, um den virtuellen Server zu erstellen.
11. Geben Sie die Details zur Konfiguration des GSLB-virtuellen Servers an.

    Benennen Sie den Server, der DNS-Eintragstyp ist auf A festgelegt, der Diensttyp ist auf HTTP festgelegt, und aktivieren Sie die Kontrollkästchen für „Nach Erstellung aktivieren“ und „AppFlow®-Protokollierung“. Klicken Sie auf **OK**, um den GSLB Virtual Server zu erstellen.

12. Sobald der GSLB Virtual Server erstellt wurde, klicken Sie auf **Keine GSLB Virtual Server ServiceGroup-Bindung**.

13. Verwenden Sie unter **ServiceGroup-Bindung** die Option **Dienstgruppenname auswählen**, um die in den vorherigen Schritten erstellten Dienstgruppen auszuwählen und hinzuzufügen.

14. Konfigurieren Sie die GSLB Virtual Server-Domänenbindung, indem Sie auf **Keine GSLB Virtual Server-Domänenbindung** klicken. Konfigurieren Sie den FQDN und binden Sie ihn. Behalten Sie die Standardeinstellung für andere Parameter bei.

15. Konfigurieren Sie den ADNS-Dienst, indem Sie auf **Kein Dienst** klicken.
16. Geben Sie die Details zur Konfiguration des Lastausgleichsdienstes an.

    Fügen Sie einen **Dienstnamen** hinzu, klicken Sie auf **Neuer Server**, und geben Sie die **IP-Adresse** des ADNS-Servers ein. Wenn der Benutzer-ADNS bereits konfiguriert ist, können Benutzer **Vorhandener Server** auswählen und dann den Benutzer-ADNS aus dem Dropdown-Menü auswählen. Stellen Sie sicher, dass das Protokoll ADNS ist und der Datenverkehr über Port 53 geleitet wird.

17. Konfigurieren Sie die **Methode** als **Least Connection** und die Backup-Methode als **Round Robin**.
18. Klicken Sie auf **Fertig** und überprüfen Sie, ob der GSLB Virtual Server des Benutzers als „Up“ angezeigt wird.

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

### Weitere Ressourcen

NetScaler Global Load Balancing für Hybrid- und Multi-Cloud-Bereitstellungen

# Eine NetScaler VPX-Instanz auf Azure Local bereitstellen

NetScaler VPX™ unterstützt die Bereitstellung auf Azure Local (Azure Stack hyperkonvergente Infrastruktur (HCI)) Versionen 22H2, 23H2 und 24H2. Sie können NetScaler VPX-Instanzen auf eigenständigen Azure Local-Hosts bereitstellen oder sie als Hochverfügbarkeitspaar (HA-Paar) in Azure Local-Instanzen (ehemals Azure Stack HCI-Cluster) einrichten. Azure Local ist eine hybride Cloud-Plattform, die es Unternehmen ermöglicht, Azure-Dienste in ihren eigenen Rechenzentren auszuführen. Die Bereitstellung von NetScaler VPX auf Azure Local bietet erweiterte Lastverteilung, Anwendungsbereitstellung und Sicherheitsfunktionen vor Ort, während eine nahtlose Integration mit Azure Cloud-Diensten gewährleistet wird. Diese Lösung ist vorteilhaft für Unternehmen, die geringe Latenz, Datenhoheit oder die Einhaltung gesetzlicher Vorschriften benötigen, da NetScaler Anwendungen lokal optimieren und sichern kann, mit den Vorteilen des Azure-Ökosystems.

## Voraussetzungen für die Bereitstellung einer NetScaler VPX-Instanz auf Azure Local

- Stellen Sie sicher, dass Ihre Umgebung die folgenden Anforderungen an die NetScaler VPX-Version und die Azure Local-Version erfüllt.
  - **Unterstützte NetScaler VPX-Versionen:** 14.1-60.x und höher
  - **Unterstützte Azure Local OS-Builds:** 25398.1965, 26100.7171 und 20349.3692

    Weitere Informationen zu Azure Local Release-Versionen finden Sie in der Microsoft-Dokumentation.
- Stellen Sie sicher, dass Sie Zugriff auf einen dedizierten Azure Local-Knoten haben und dass Windows Admin Center installiert und ordnungsgemäß mit diesem Knoten verbunden ist.
- Laden Sie das NetScaler Virtual Hard Disk (VHD)-Image von der offiziellen Citrix-Website oder Ihrer lizenzierten Quelle herunter. Stellen Sie sicher, dass das Image mit Ihrer Umgebung kompatibel ist.

## Eine NetScaler VPX-Instanz auf Azure Local mithilfe eines VM-Dateipakets aus dem Windows Admin Center bereitstellen

Verwenden Sie diese Methode, um NetScaler VPX auf Azure Local aus einem VM-Dateipaket bereitzustellen.

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

Um NetScaler VPX auf Azure Local mithilfe eines VM-Dateipakets bereitzustellen, befolgen Sie diese fünf Schritte:

1. Laden Sie das NetScaler Hyper-V-Paket herunter und laden Sie das heruntergeladene Paket auf einen Azure Local-Knoten hoch.
2. Erstellen Sie eine neue virtuelle Maschine mithilfe des extrahierten Pakets.
3. Konfigurieren Sie die VM-Einstellungen und starten Sie die virtuelle Maschine.
4. Weisen Sie die NetScaler IP-Adresse über Konsolenzugriff zu.
5. Stellen Sie eine Remote-Verbindung zu NetScaler VPX für die weitere Konfiguration her.

**Schritt 1.** Laden Sie das NetScaler Hyper-V-Paket herunter.

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://www.citrix.com/`.
2. Melden Sie sich mit Ihren zugewiesenen Anmeldeinformationen an.
3. Suchen und klicken Sie auf den Abschnitt **Downloads**.
4. Wählen Sie im Dropdown-Menü **Produkt auswählen** die Option **NetScaler (NetScaler ADC)** aus.
5. Wählen Sie **NetScaler VPX Release X.X** unter dem Abschnitt **NetScaler Release X.X > Virtuelle Appliances** aus.
6. Laden Sie das komprimierte Installationspaket (zum Beispiel `NSVPX-HyperV-14.1-60.57_nc_64.zip`) direkt auf Ihren Server herunter.
7. Laden Sie das heruntergeladene Paket an Ihrem bevorzugten Speicherort auf Ihren Azure Local-Knoten hoch. Extrahieren Sie den Inhalt des Pakets.

**Schritt 2.** Erstellen Sie eine neue virtuelle Maschine mithilfe des extrahierten VM-Pakets.

Führen Sie die folgenden Schritte aus, um die virtuelle Maschine zu erstellen und zu konfigurieren:

1. Öffnen Sie **Windows Admin Center** und navigieren Sie zum Abschnitt **Virtuelle Maschinen**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie dann **Importieren**.

3. Navigieren Sie zu dem Ordner, der das extrahierte NetScaler VM-Image enthält, und wählen Sie ihn aus.
4. Wählen Sie aus dem Dropdown-Menü der verfügbaren virtuellen Maschinen die Option **NetScaler Virtual Appliance**.

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

5. Klicken Sie auf **Importieren**.
6. Fahren Sie mit der Option **Überprüfen + Erstellen** fort, um die neue virtuelle Maschine fertigzustellen und zu erstellen.

**Schritt 3.** VM-Einstellungen konfigurieren und die virtuelle Maschine starten.

Nach dem Import der NetScaler Virtual Appliance konfigurieren Sie die VM für optimale Leistung und Konnektivität.

1. **Ressourcen überprüfen:** Überprüfen Sie den VM-Namen, den Arbeitsspeicher, die CPU und die Speicherzuweisungen und passen Sie diese bei Bedarf an.
2. **Netzwerkadapter zuweisen:** Verbinden Sie den richtigen Netzwerkadapter, um die Konnektivität zu ermöglichen.

3. **VM starten:** Schalten Sie die NetScaler VM ein, um die Initialisierung zu starten.

**Schritt 4.** Weisen Sie die NetScaler IP-Adresse über den Konsolenzugriff zu.

1. Greifen Sie direkt über den **Hyper-V Manager** auf die NetScaler Instanzkonsole zu.
2. Melden Sie sich über die Hyper-V-Konsole des Azure Local-Knotens bei NetScaler an.

3. Weisen Sie die IP-Adresse zu.
4. Speichern Sie die IP-Konfiguration.

**Schritt 5.** Stellen Sie eine Remote-Verbindung zu NetScaler VPX her.

1. Überprüfen Sie die Konnektivität zur NetScaler-Verwaltungsoberfläche.
2. Melden Sie sich an und konfigurieren Sie NetScaler für weitere Einrichtungs- und Verwaltungsaufgaben.

## Bereitstellen einer NetScaler VPX-Instanz auf Azure Local mithilfe von VHD aus dem Windows Admin Center

Um eine NetScaler VPX-Instanz auf Azure Local mithilfe von VHD aus dem Windows Admin Center bereitzustellen, führen Sie die folgenden Schritte aus:

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

1. Laden Sie die NetScaler VHD-Datei mithilfe des Windows Admin Centers auf Ihren Azure Stack HCI-Knoten hoch.
2. Erstellen Sie eine neue virtuelle Maschine (VM) im Windows Admin Center und konfigurieren Sie die VM-Einstellungen wie Name, Generation 1, CPU, Arbeitsspeicher, virtueller Switch und wählen Sie die hochgeladene VHD aus.
3. Starten Sie die neu erstellte NetScaler-VM und überwachen Sie ihren Startstatus.
4. Greifen Sie mithilfe des Hyper-V-Managers auf die Konsole der NetScaler-Instanz zu, melden Sie sich an und weisen Sie die IP-Adresse zu.
5. Stellen Sie eine Remote-Verbindung zur NetScaler VPX-Instanz mithilfe von SSH für weitere Einrichtungs- und Verwaltungsaufgaben her.
6. Überprüfen Sie die Bereitstellung, indem Sie die Konnektivität zur NetScaler-Verwaltungsschnittstelle prüfen und die erforderliche Konfiguration abschließen.

**Schritt 1.** Laden Sie die NetScaler VHD-Datei über das Windows Admin Center auf Ihre Azure Local-Maschine hoch.

1. Öffnen Sie das Windows Admin Center und stellen Sie eine Verbindung zu Ihrer Azure Local-Maschine her.
2. Navigieren Sie zu **Tools > Files and file sharing**.
3. Navigieren Sie zum gewünschten Volume und dann zu dem spezifischen Ordner, in den Sie die VHD-Datei hochladen möchten.
4. Klicken Sie auf **Upload** und wählen Sie die VHD-Datei von Ihrem Computer aus.
5. Warten Sie, bis der Upload-Vorgang abgeschlossen ist. Überprüfen Sie nach Abschluss, ob die VHD-Datei im ausgewählten Ordner angezeigt wird.

**Schritt 2.** Erstellen Sie eine neue virtuelle Maschine und konfigurieren Sie die VM-Einstellungen.

1. Gehen Sie im Windows Admin Center zu **Virtual machines**.
2. Klicken Sie auf **Add** und wählen Sie dann **New**.
3. Geben Sie einen Namen für die VM ein und wählen Sie **Generation 1**.
4. Konfigurieren Sie virtuelle Prozessoren (CPU), Arbeitsspeicher und den virtuellen Switch, um die NetScaler-Anforderungen und Ihre Bereitstellungsbedürfnisse zu erfüllen.
5. Wählen Sie in den **Storage**-Einstellungen **Use an existing virtual hard disk** und wählen Sie das hochgeladene VHD-Image aus.
6. Schließen Sie die Erstellung der VM ab.

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

**Schritt 3.** Starten Sie die NetScaler-VM.

1. Nachdem Sie die Konfiguration abgeschlossen haben, starten Sie die NetScaler-VM, die Sie im vorherigen Schritt erstellt haben.

2. Überwachen Sie den VM-Status im Windows Admin Center, um sicherzustellen, dass sie erfolgreich startet.

**Schritt 4.** Konfigurieren Sie das Netzwerk und richten Sie den Fernzugriff über den Hyper-V-Manager ein.

1. Nachdem die NetScaler-Instanz gestartet ist, öffnen Sie die Konsole im Hyper-V-Manager.

2. Melden Sie sich von der Hyper-V-Konsole auf dem Azure Local-Knoten bei NetScaler an.

3. Weisen Sie die IP-Adresse zu und speichern Sie sie.
4. Verwenden Sie SSH, um sich für weitere Einrichtung und Verwaltung remote mit NetScaler zu verbinden.

**Schritt 5.** Überprüfen Sie die NetScaler VPX-Bereitstellung.

1. Melden Sie sich an der NetScaler GUI oder CLI mithilfe der konfigurierten IP-Adresse an und fahren Sie mit der NetScaler VPX-Konfiguration fort.
2. Überprüfen Sie, ob die NetScaler-Konfiguration abgeschlossen ist und die VPX-Instanz wie erwartet funktioniert.

# Bereitstellen von NetScaler® Web App Firewall in Azure

NetScaler Web App Firewall ist eine Unternehmenslösung, die modernste Schutzfunktionen für moderne Anwendungen bietet. Sie mindert Bedrohungen für öffentlich zugängliche Assets, einschließlich Websites, Webanwendungen und APIs. Die NetScaler Web App Firewall umfasst IP-Reputations-basiertes Filtern, Bot-Minderung, Schutz vor OWASP Top 10 Anwendungsbedrohungen, Layer-7-DDoS-Schutz und mehr. Ebenfalls enthalten sind Optionen zur Erzwingung von Authentifizierung, starken SSL/TLS-Chiffren, TLS 1.3, Ratenbegrenzung und

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

Rewrite-Richtlinien. Durch die Verwendung sowohl grundlegender als auch erweiterter WAF-Schutzfunktionen bietet sie umfassenden Schutz für Ihre Anwendungen mit unübertroffener Benutzerfreundlichkeit. Die Inbetriebnahme dauert nur wenige Minuten. Darüber hinaus spart die NetScaler Web App Firewall den Benutzern durch ein automatisiertes Lernmodell, das als dynamisches Profiling bezeichnet wird, wertvolle Zeit. Indem sie automatisch lernt, wie eine geschützte Anwendung funktioniert, passt sie sich der Anwendung an, selbst wenn Entwickler die Anwendungen bereitstellen und ändern. Die NetScaler Web App Firewall unterstützt die Einhaltung aller wichtigen regulatorischen Standards und Gremien, einschließlich PCI-DSS, HIPAA und mehr. Mit unseren CloudFormation-Vorlagen war es noch nie einfacher, schnell einsatzbereit zu sein. Mit Auto-Scaling können Benutzer sicher sein, dass ihre Anwendungen geschützt bleiben, selbst wenn ihr Datenverkehr zunimmt.

NetScaler Web App Firewall kann entweder als Layer-3-Netzwerkgerät oder als Layer-2-Netzwerkbrücke zwischen Kundenservern und Kundenbenutzern installiert werden, normalerweise hinter dem Router oder der Firewall des Kundenunternehmens. Weitere Informationen finden Sie unter Einführung in NetScaler Web App Firewall.

## NetScaler Web App Firewall Bereitstellungsstrategie

1. Bei der Bereitstellung der Web Application Firewall geht es darum zu bewerten, welche Anwendungen oder spezifischen Daten den maximalen Sicherheitsschutz benötigen, welche weniger anfällig sind und welche Sicherheitsprüfung sicher umgangen werden kann. Dies hilft Benutzern, eine optimale Konfiguration zu erstellen und geeignete Richtlinien und Bindungspunkte zu entwerfen, um den Datenverkehr zu trennen. Benutzer könnten beispielsweise eine Richtlinie konfigurieren, um die Sicherheitsprüfung von Anforderungen für statische Webinhalte wie Bilder, MP3-Dateien und Filme zu umgehen, und eine andere Richtlinie konfigurieren, um erweiterte Sicherheitsprüfungen auf Anforderungen für dynamische Inhalte anzuwenden. Benutzer können mehrere Richtlinien und Profile verwenden, um verschiedene Inhalte derselben Anwendung zu schützen.
2. Um die Bereitstellung zu baselinen, erstellen Sie einen virtuellen Server und leiten Sie Testdatenverkehr darüber, um eine Vorstellung von der Rate und Menge des Datenverkehrs zu erhalten, der durch das Benutzersystem fließt.
3. Stellen Sie die Web Application Firewall bereit. Verwenden Sie NetScaler ADM und das Web Application Firewall StyleBook, um die Web Application Firewall zu konfigurieren. Weitere Informationen finden Sie im Abschnitt StyleBook weiter unten in diesem Handbuch.
4. Implementieren Sie die NetScaler Web App Firewall und OWASP Top Ten.

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

Drei der Schutzfunktionen der Web Application Firewall sind besonders wirksam gegen gängige Arten von Webangriffen und werden daher häufiger eingesetzt als alle anderen. Daher sollten sie bei der Ersteinrichtung implementiert werden. Sie sind:

- **HTML-Cross-Site-Scripting**: Untersucht Anfragen und Antworten auf Skripte, die versuchen, Inhalte auf einer anderen Website als der, auf der sich das Skript befindet, zuzugreifen oder zu ändern. Wenn diese Prüfung ein solches Skript findet, macht sie das Skript entweder harmlos, bevor sie die Anfrage oder Antwort an ihr Ziel weiterleitet, oder sie blockiert die Verbindung.
- **HTML-SQL-Injection**: Untersucht Anfragen, die Formularfelddaten enthalten, auf Versuche, SQL-Befehle in eine SQL-Datenbank einschleusen einzuschleusen. Wenn diese Prüfung eingeschleusten SQL-Code erkennt, blockiert sie entweder die Anfrage oder macht den eingeschleusten SQL-Code harmlos, bevor sie die Anfrage an den Webserver weiterleitet.

  **HINWEIS:**

  Stellen Sie sicher, dass Ihre Web App Firewall für die folgenden Bedingungen in Ihrer Konfiguration korrekt konfiguriert ist:

  ```
  >-  If users enable the HTML Cross-Site Scripting check or the HTML SQL
  Injection check (or both).

  >

  >-  User protected websites accept file uploads or contain Web forms
  that can contain large POST body data.
  ```

Weitere Informationen zum Konfigurieren der Web Application Firewall für diesen Fall finden Sie unter Konfigurieren der Application Firewall: Konfigurieren der Web App Firewall.

- **Pufferüberlauf**: Untersucht Anfragen, um Versuche zu erkennen, einen Pufferüberlauf auf dem Webserver zu verursachen.

## Konfigurieren der Web Application Firewall

Stellen Sie sicher, dass die NetScaler Web App Firewall bereits aktiviert ist und ordnungsgemäß funktioniert. Wir empfehlen Ihnen, die NetScaler Web App Firewall mithilfe des Web Application Firewall StyleBook zu konfigurieren. Die meisten Benutzer empfinden dies als die einfachste Methode zur Konfiguration der Web Application Firewall, und sie wurde entwickelt, um Fehler zu vermeiden. Sowohl die GUI als auch die Befehlszeilenschnittstelle sind für erfahrene Benutzer

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

gedacht, hauptsächlich um eine bestehende Konfiguration zu ändern oder erweiterte Optionen zu nutzen.

### SQL-Injection

Die NetScaler Web App Firewall HTML SQL Injection-Prüfung bietet spezielle Abwehrmaßnahmen gegen die Einschleusung von nicht autorisiertem SQL-Code, der die Sicherheit der Benutzeranwendung beeinträchtigen könnte. Die NetScaler Web App Firewall untersucht die Anforderungsnutzlast auf eingeschleusten SQL-Code an drei Stellen: 1) POST-Body, 2) Header und 3) Cookies. Weitere Informationen finden Sie unter HTML SQL-Injection-Prüfung.

### Cross-Site-Scripting

Die HTML Cross-Site Scripting (Cross-Site-Scripting)-Prüfung untersucht sowohl die Header als auch die POST-Bodies von Benutzeranfragen auf mögliche Cross-Site-Scripting-Angriffe. Wenn sie ein Cross-Site-Skript findet, ändert (transformiert) sie entweder die Anfrage, um den Angriff harmlos zu machen, oder blockiert die Anfrage. Weitere Informationen finden Sie unter HTML Cross-Site-Scripting-Prüfung.

### Pufferüberlaufprüfung

Die Pufferüberlaufprüfung erkennt Versuche, einen Pufferüberlauf auf dem Webserver zu verursachen. Wenn die Web Application Firewall feststellt, dass die URL, Cookies oder der Header länger als die konfigurierte Länge sind, blockiert sie die Anfrage, da dies einen Pufferüberlauf verursachen kann. Weitere Informationen finden Sie unter Pufferüberlaufprüfung.

### Virtuelles Patching/Signaturen

Die Signaturen bieten spezifische, konfigurierbare Regeln, um die Aufgabe des Schutzes von Benutzer-Websites vor bekannten Angriffen zu vereinfachen. Eine Signatur stellt ein Muster dar, das eine Komponente eines bekannten Angriffs auf ein Betriebssystem, einen Webserver, eine Website, einen XML-basierten Webdienst oder eine andere Ressource ist. Ein umfangreicher Satz vorkonfigurierter integrierter oder nativer Regeln bietet eine benutzerfreundliche Sicherheitslösung, die die Leistungsfähigkeit der Mustererkennung nutzt, um Angriffe zu erkennen und vor Anwendungsschwachstellen zu schützen. Weitere Informationen finden Sie unter Signaturen.

NetScaler Web App Firewall unterstützt sowohl die **automatische als auch die manuelle** Aktualisierung von Signaturen. Wir empfehlen außerdem, die **automatische Aktualisierung** für Signaturen zu aktivieren, um auf dem neuesten Stand zu bleiben.

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

Diese Signaturdateien werden in der AWS-Umgebung gehostet, und es ist wichtig, den ausgehenden Zugriff auf die IP-Adressen des NetScaler von Netzwerk-Firewalls aus zuzulassen, um die neuesten Signaturdateien abzurufen. Die Aktualisierung von Signaturen auf dem NetScaler hat keine Auswirkungen auf die Verarbeitung des Echtzeit-Datenverkehrs.

## Anwendungssicherheitsanalyse

Das **Application Security Dashboard** bietet einen ganzheitlichen Überblick über den Sicherheitsstatus von Benutzeranwendungen. Es zeigt beispielsweise wichtige Sicherheitsmetriken wie Sicherheitsverletzungen, Signaturverletzungen und Bedrohungsindizes an. Das Anwendungssicherheits-Dashboard zeigt auch angriffsbezogene Informationen wie SYN-Angriffe, Small-Window-Angriffe und DNS-Flood-Angriffe für den erkannten NetScaler an.

**HINWEIS:**

Um die Metriken des Anwendungssicherheits-Dashboards anzuzeigen, muss AppFlow for Security Insight auf den NetScaler-Instanzen aktiviert sein, die Benutzer überwachen möchten.

So zeigen Sie die Sicherheitsmetriken einer NetScaler-Instanz im Anwendungssicherheits-Dashboard an:

1. Melden Sie sich mit den Administratoranmeldeinformationen bei NetScaler ADM an.
2. Navigieren Sie zu **Applications > App Security Dashboard**, und wählen Sie die IP-Adresse der Instanz aus der Liste Geräte.

Benutzer können die im Application Security Investigator gemeldeten Diskrepanzen weiter untersuchen, indem sie auf die im Diagramm dargestellten Blasen klicken.

## Zentralisiertes Lernen auf ADM

NetScaler Web App Firewall schützt Webanwendungen von Benutzern vor böswilligen Angriffen wie SQL-Injection und Cross-Site-Scripting (XSS). Um Datenschutzverletzungen zu verhindern und den richtigen Sicherheitsschutz zu bieten, müssen Benutzer ihren Datenverkehr auf Bedrohungen und Echtzeit-Aktionsdaten zu Angriffen überwachen. Manchmal können die gemeldeten Angriffe Fehlalarme sein, die als Ausnahme behandelt werden müssen.

Das zentralisierte Lernen auf NetScaler ADM ist ein sich wiederholender Musterfilter, der es WAF ermöglicht, das Verhalten (die normalen Aktivitäten) der Webanwendungen von Benutzern zu

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

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.

Um die Lernfunktion bereitzustellen, müssen Benutzer zunächst ein Web Application Firewall-Profil (eine Reihe von Sicherheitseinstellungen) auf dem Benutzer-NetScaler konfigurieren. Weitere Informationen finden Sie unter Erstellen von Web App Firewall-Profilen.

NetScaler ADM generiert eine Liste von Ausnahmen (Entspannungen) für jede Sicherheitsprüfung. Als Administrator können Sie die Liste der Ausnahmen in NetScaler ADM überprüfen und entscheiden, ob Sie sie bereitstellen oder überspringen möchten.

Mit der WAF-Lernfunktion in NetScaler ADM können Sie:

- Ein Lernprofil mit den folgenden Sicherheitsprüfungen konfigurieren.
  - Pufferüberlauf
  - HTML-Cross-Site-Scripting

    **HINWEIS:**

    Die Cross-Site-Script-Einschränkung des Speicherorts ist nur FormField.

  - HTML-SQL-Injection

    **HINWEIS:**

    Für die HTML-SQL-Injection-Prüfung müssen Benutzer `set -sqlinjectionTransformSpecialChars ON` und `set -sqlinjectiontype sqlspclcharorkeywords` im NetScaler konfigurieren.
- Überprüfen Sie die Entspannungsregeln in NetScaler ADM und entscheiden Sie, die notwendigen Maßnahmen zu ergreifen (Bereitstellen oder Überspringen).
- Erhalten Sie Benachrichtigungen per E-Mail, Slack und ServiceNow.
- Verwenden Sie das Dashboard, um Details zur Entspannung anzuzeigen.

So verwenden Sie das WAF-Lernen in NetScaler ADM:

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

1. Lernprofil konfigurieren: Lernprofil konfigurieren
2. Entspannungsregeln anzeigen: Entspannungsregeln und Leerlaufregeln anzeigen
3. WAF-Lern-Dashboard verwenden: WAF-Lern-Dashboard anzeigen

## StyleBooks

StyleBooks vereinfachen die Verwaltung komplexer NetScaler-Konfigurationen für Benutzeranwendungen. Ein StyleBook ist eine Vorlage, die Benutzer verwenden können, um NetScaler-Konfigurationen zu erstellen und zu verwalten. Hier geht es den Benutzern hauptsächlich um das StyleBook, das zur Bereitstellung der Web Application Firewall verwendet wird. Weitere Informationen zu StyleBooks finden Sie unter StyleBooks.

## Security Insight-Analysen

Web- und Webdienst-Anwendungen, die dem Internet ausgesetzt sind, sind zunehmend anfällig für Angriffe geworden. Um Anwendungen vor Angriffen zu schützen, benötigen Benutzer Einblick in die Art und das Ausmaß vergangener, gegenwärtiger und bevorstehender Bedrohungen, umsetzbare Echtzeitdaten zu Angriffen und Empfehlungen für Gegenmaßnahmen. Security Insight bietet eine Single-Pane-Lösung, die Benutzern hilft, den Sicherheitsstatus ihrer Anwendungen zu bewerten und Korrekturmaßnahmen zur Sicherung der Benutzeranwendungen zu ergreifen. Weitere Informationen finden Sie unter Security Insight.

### Detaillierte Informationen zu Sicherheitsverletzungen abrufen

Benutzer möchten möglicherweise eine Liste der Angriffe auf eine Anwendung anzeigen und Einblicke in die Art und Schwere der Angriffe, die von der ADC-Instanz ergriffenen Maßnahmen, die angeforderten Ressourcen und die Quelle der Angriffe erhalten.

Benutzer möchten beispielsweise ermitteln, wie viele Angriffe auf Microsoft Lync blockiert wurden, welche Ressourcen angefordert wurden und welche IP-Adressen die Quellen hatten.

Klicken Sie im **Security Insight-Dashboard** auf **Lync** > **Total Violations**. Klicken Sie in der Tabelle auf das Filtersymbol in der Spaltenüberschrift **Action Taken** und wählen Sie dann **Blocked** aus.

Informationen zu den angeforderten Ressourcen finden Sie in der Spalte **URL**. Informationen zu den Quellen der Angriffe finden Sie in der Spalte **Client IP**.

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

### Details der Protokollausdrücke anzeigen

NetScaler verwendet Protokollausdrücke, die mit dem Application Firewall-Profil konfiguriert sind, um Maßnahmen gegen Angriffe auf eine Anwendung im Unternehmen des Benutzers zu ergreifen. In **Security Insight** können Benutzer die für die von der ADC-Instanz verwendeten Protokollausdrücke zurückgegebenen Werte anzeigen. Diese Werte umfassen den Anforderungsheader, den Anforderungstext und so weiter. Zusätzlich zu den Werten der Protokollausdrücke können Benutzer auch den Namen des Protokollausdrucks und den Kommentar für den im Application Firewall-Profil definierten Protokollausdruck anzeigen, den die ADC-Instanz zur Abwehr des Angriffs verwendet hat.

**Voraussetzungen**:

Stellen Sie sicher, dass Benutzer:

- Konfigurieren Sie Protokollausdrücke im Application Firewall-Profil. Weitere Informationen finden Sie unter Application Firewall.
- Aktivieren Sie die auf Protokollausdrücken basierenden Security Insights-Einstellungen in NetScaler ADM. Gehen Sie wie folgt vor:
  - Navigieren Sie zu **Analytics** > **Settings**, und klicken Sie auf **Enable Features for Analytics**.
  - Wählen Sie auf der Seite „Funktionen für Analysen aktivieren“ unter dem Abschnitt **Einstellung für Log-Ausdruck-basiertes Security Insight** die Option **Security Insight aktivieren** und klicken Sie auf **OK**.

Beispielsweise möchten Sie möglicherweise die Werte des Log-Ausdrucks anzeigen, die von der ADC-Instanz für die Aktion zurückgegeben wurden, die sie bei einem Angriff auf Microsoft Lync im Benutzerunternehmen durchgeführt hat.

Navigieren Sie auf dem **Security Insight-Dashboard** zu **Lync** > **Gesamtzahl der Verstöße**. Klicken Sie in der Tabelle „Anwendungsübersicht“ auf die URL, um die vollständigen Details des Verstoßes auf der Seite **Verstoßinformationen** anzuzeigen, einschließlich des Namens des Log-Ausdrucks, des Kommentars und der von der ADC-Instanz für die Aktion zurückgegebenen Werte.

Bestimmen Sie den Sicherheitsindex, bevor Sie die Konfiguration bereitstellen. Sicherheitsverletzungen treten auf, nachdem Benutzer die Sicherheitskonfiguration auf einer ADC-Instanz bereitgestellt haben, aber Benutzer möchten möglicherweise die Wirksamkeit der Sicherheitskonfiguration bewerten, bevor sie diese bereitstellen.

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

Beispielsweise möchten Benutzer möglicherweise den Sicherheitsindex der Konfiguration für die SAP-Anwendung auf der ADC-Instanz mit der IP-Adresse 10.102.60.27 bewerten.

Klicken Sie auf dem **Security Insight-Dashboard** unter **Geräte** auf die IP-Adresse der ADC-Instanz, die Benutzer konfiguriert haben. Benutzer können sehen, dass sowohl der Bedrohungsindex als auch die Gesamtzahl der Angriffe 0 sind. Der Bedrohungsindex ist ein direktes Abbild der Anzahl und Art der Angriffe auf die Anwendung. Null Angriffe bedeuten, dass die Anwendung keiner Bedrohung ausgesetzt ist.

Klicken Sie auf **Sap** > **Sicherheitsindex** > **SAP_Profile** und bewerten Sie die angezeigten Sicherheitsindexinformationen.

In der Zusammenfassung der Anwendungs-Firewall können Benutzer den Konfigurationsstatus verschiedener Schutzeinstellungen anzeigen. Wenn eine Einstellung auf Protokollierung gesetzt ist oder wenn eine Einstellung nicht konfiguriert ist, wird der Anwendung ein niedrigerer Sicherheitsindex zugewiesen.

## Sicherheitsverletzungen

Webanwendungen, die dem Internet ausgesetzt sind, sind drastisch anfälliger für Angriffe geworden. NetScaler ADM ermöglicht es Ihnen, umsetzbare Verstoßdetails zu visualisieren, um Anwendungen vor Angriffen zu schützen.

### Details zu Anwendungssicherheitsverletzungen anzeigen

Webanwendungen, die dem Internet ausgesetzt sind, sind drastisch anfälliger für Angriffe geworden. NetScaler ADM ermöglicht Benutzern, umsetzbare Verletzungsdetails zu visualisieren, um Anwendungen vor Angriffen zu schützen. Navigieren Sie zu **Sicherheit** > **Sicherheitsverletzungen** für eine Single-Pane-Lösung, um:

- Auf Anwendungssicherheitsverletzungen basierend auf ihren Kategorien wie **Netzwerk**, **Bot** und **WAF** zugreifen
- Korrekturmaßnahmen zur Sicherung der Anwendungen ergreifen

Um die Sicherheitsverletzungen in NetScaler ADM anzuzeigen, stellen Sie sicher:

- Benutzer haben eine Premium-Lizenz für den NetScaler (für WAF- und BOT-Verletzungen).

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

- Benutzer haben eine Lizenz auf den virtuellen Servern für Lastenausgleich oder Inhaltswechsel beantragt (für WAF und BOT). Weitere Informationen finden Sie unter Lizenzierung auf virtuellen Servern verwalten.
- Benutzer können weitere Einstellungen aktivieren. Weitere Informationen finden Sie in der Prozedur im Abschnitt „Einrichtung“ in der NetScaler-Produktdokumentation: Einrichtung.

### Verletzungskategorien

NetScaler ADM ermöglicht Benutzern, die in Alle Verletzungen verfügbaren Verletzungen anzuzeigen:

### Einrichtung

Stellen Sie bei Verletzungen sicher, dass **Metrics Collector** aktiviert ist. Standardmäßig ist **Metrics Collector** auf dem NetScaler aktiviert. Weitere Informationen finden Sie unter Intelligent App Analytics konfigurieren.

### Erweiterte Sicherheitsanalysen aktivieren

- Navigieren Sie zu **Netzwerke** > **Instanzen** > **NetScaler**, und wählen Sie den Instanztyp aus. Zum Beispiel MPX.
- Wählen Sie die NetScaler-Instanz aus und wählen Sie aus der Liste **Aktion auswählen** die Option **Analysen konfigurieren**.
- Wählen Sie den virtuellen Server aus und klicken Sie auf **Analytics aktivieren**.
- Im Fenster **Analytics aktivieren**:
  - Wählen Sie **Web Insight** aus. Nachdem Benutzer Web Insight ausgewählt haben, wird die schreibgeschützte Option **Advanced Security Analytics** automatisch aktiviert.

**HINWEIS:**

Die Option **Advanced Security Analytics** wird nur für ADC-Instanzen mit Premium-Lizenz angezeigt.

  - Wählen Sie **Logstream** als Transportmodus aus
  - Der Ausdruck ist standardmäßig wahr
  - Klicken Sie auf **OK**

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

### Webtransaktionseinstellungen aktivieren

- Navigieren Sie zu **Analytics** > **Einstellungen**.

Die Seite **Einstellungen** wird angezeigt.

- Klicken Sie auf **Funktionen für Analytics aktivieren**.
- Wählen Sie unter **Webtransaktionseinstellungen** die Option **Alle** aus.

- Klicken Sie auf **Ok**.

## Dashboard für Sicherheitsverletzungen

Im Dashboard für Sicherheitsverletzungen können Benutzer Folgendes anzeigen:

- Gesamtzahl der auf allen NetScaler-Instanzen und Anwendungen aufgetretenen Verstöße. Die Gesamtverstöße werden basierend auf der ausgewählten Zeitdauer angezeigt.

- Gesamtzahl der Verstöße in jeder Kategorie.

- Gesamtzahl der betroffenen ADCs, Gesamtzahl der betroffenen Anwendungen und Top-Verstöße basierend auf der Gesamtzahl der Vorkommen und der betroffenen Anwendungen.

Weitere Informationen zu den Details der Verstöße finden Sie unter Alle Verstöße.

## Bot-Einblicke

Konfigurieren Sie BOT-Einblicke in NetScaler. Weitere Informationen finden Sie unter Bot.

### Bots anzeigen

Klicken Sie auf den virtuellen Server, um die **Anwendungsübersicht** anzuzeigen.

1. Bietet die Details der Anwendungszusammenfassung, wie zum Beispiel:
    - **Durchschnittliche RPS** – Zeigt die durchschnittlichen Bot-Transaktionsanfragen pro Sekunde (RPS) an, die auf virtuellen Servern empfangen wurden.

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

- **Bots nach Schweregrad** – Zeigt an, dass die höchsten Bot-Transaktionen basierend auf dem Schweregrad aufgetreten sind. Der Schweregrad wird nach **Kritisch**, **Hoch**, **Mittel** und **Niedrig** kategorisiert.

Wenn die virtuellen Server beispielsweise 11770 Bots mit hohem Schweregrad und 1550 Bots mit kritischem Schweregrad aufweisen, zeigt NetScaler ADM unter **Bots nach Schweregrad** den Wert **Kritisch 1,55 K** an.

- **Größte Bot-Kategorie** – Zeigt an, dass die höchsten Bot-Angriffe basierend auf der Bot-Kategorie aufgetreten sind.

Wenn die virtuellen Server beispielsweise 8000 blockierte Bots, 5000 zugelassene Bots und 10000 Bots mit überschrittener Ratenbegrenzung aufweisen, zeigt NetScaler ADM unter **Größte Bot-Kategorie** den Wert **Ratenbegrenzung überschritten 10 K** an.

- **Größte Geo-Quelle** – Zeigt an, dass die höchsten Bot-Angriffe basierend auf einer Region aufgetreten sind.

Wenn die virtuellen Server beispielsweise 5000 Bot-Angriffe in Santa Clara, 7000 Bot-Angriffe in London und 9000 Bot-Angriffe in Bangalore aufweisen, zeigt NetScaler ADM unter **Größte Geo-Quelle** den Wert **Bangalore 9 K** an.

- **Durchschnittlicher % Bot-Traffic** – Zeigt das Verhältnis von menschlichem zu Bot-Traffic an.

2. Zeigt den Schweregrad der Bot-Angriffe basierend auf Standorten in der Kartenansicht an
3. Zeigt die Arten von Bot-Angriffen an (Gut, Schlecht und alle)
4. Zeigt die gesamten Bot-Angriffe zusammen mit den entsprechenden konfigurierten Aktionen an. Wenn Sie beispielsweise Folgendes konfiguriert haben:

   - IP-Adressbereich (192.140.14.9 bis 192.140.14.254) als Blockierlisten-Bots und „Verwerfen“ als Aktion für diese IP-Adressbereiche ausgewählt
   - IP-Bereich (192.140.15.4 bis 192.140.15.254) als Blockierlisten-Bots und die Erstellung einer Protokollnachricht als Aktion für diese IP-Bereiche ausgewählt

     In diesem Szenario zeigt NetScaler ADM Folgendes an:

     - Gesamtanzahl der blockierten Bots
     - Gesamtanzahl der Bots unter **Verworfen**
     - Gesamtanzahl der Bots unter Protokoll

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

### CAPTCHA-Bots anzeigen

Auf Webseiten sind CAPTCHAs dazu konzipiert, zu identifizieren, ob der eingehende Traffic von einem Menschen oder einem automatisierten Bot stammt. Um die CAPTCHA-Aktivitäten in NetScaler ADM anzuzeigen, müssen Benutzer CAPTCHA als Bot-Aktion für IP-Reputations- und Geräte-Fingerprint-Erkennungstechniken in einer NetScaler ADM-Instanz konfigurieren. Weitere Informationen finden Sie unter: Bot-Management konfigurieren.

Im Folgenden sind die CAPTCHA-Aktivitäten aufgeführt, die NetScaler ADM in Bot Insight anzeigt:

- **CAPTCHA-Versuche überschritten** – Bezeichnet die maximale Anzahl von CAPTCHA-Versuchen, die nach Anmeldefehlern unternommen wurden
- **CAPTCHA-Client stummgeschaltet** – Bezeichnet die Anzahl der Client-Anfragen, die verworfen oder umgeleitet werden, weil diese Anfragen zuvor mit der CAPTCHA-Herausforderung als schlechte Bots erkannt wurden
- **Mensch** – Bezeichnet die CAPTCHA-Eingaben, die von menschlichen Benutzern vorgenommen wurden
- **Ungültige CAPTCHA-Antwort** – Bezeichnet die Anzahl der falschen CAPTCHA-Antworten, die vom Bot oder Menschen empfangen wurden, wenn NetScaler eine CAPTCHA-Herausforderung sendet

### Bot-Fallen anzeigen

Um Bot-Fallen in NetScaler ADM anzuzeigen, müssen Sie die Bot-Falle in NetScaler konfigurieren. Weitere Informationen finden Sie unter: Bot-Management konfigurieren.

Um die Bot-Falle zu identifizieren, wird ein Skript auf der Webseite aktiviert, das vor Menschen verborgen ist, aber nicht vor Bots. NetScaler ADM identifiziert und meldet die Bot-Fallen, wenn dieses Skript von den Bots aufgerufen wird.

Klicken Sie auf den virtuellen Server und wählen Sie **Zero Pixel Request**

### Bot-Details anzeigen

Für weitere Details klicken Sie unter **Bot Category** auf den Bot-Angriffstyp.

Die Details wie Angriffszeit und Gesamtzahl der Bot-Angriffe für die ausgewählte Captcha-Kategorie werden angezeigt.

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

Benutzer können auch das Balkendiagramm ziehen, um den spezifischen Zeitraum auszuwählen, der mit Bot-Angriffen angezeigt werden soll.

Um zusätzliche Informationen zum Bot-Angriff zu erhalten, klicken Sie auf erweitern.

- **Instance IP** – Gibt die IP-Adresse der NetScaler-Instanz an.
- **Total Bots** – Gibt an, dass die gesamten Bot-Angriffe zu diesem bestimmten Zeitpunkt aufgetreten sind.
- **HTTP Request URL** – Gibt die URL an, die für die Captcha-Berichterstattung konfiguriert ist.
- **Country Code** – Gibt das Land an, in dem der Bot-Angriff aufgetreten ist.
- **Region** – Gibt die Region an, in der der Bot-Angriff aufgetreten ist.
- **Profilname** – Gibt den Profilnamen an, den Benutzer während der Konfiguration eingegeben haben.

### Erweiterte Suche

Benutzer können auch das Suchtextfeld und die Liste der Zeitdauern verwenden, in denen sie Bot-Details gemäß den Benutzeranforderungen anzeigen können. Wenn Benutzer auf das Suchfeld klicken, bietet das Suchfeld die folgende Liste von Suchvorschlägen.

- **Instanz-IP** – IP-Adresse der NetScaler-Instanz.
- **Client-IP** – Client-IP-Adresse.
- **Bot-Typ** – Bot-Typ wie Gut oder Schlecht.
- **Schweregrad** – Schweregrad des Bot-Angriffs.
- **Durchgeführte Aktion** – Nach dem Bot-Angriff durchgeführte Aktion, z. B. Verwerfen, Keine Aktion, Umleiten.
- **Bot-Kategorie** – Kategorie des Bot-Angriffs, z. B. Blockierliste, Zulassungsliste, Fingerabdruck. Basierend auf einer Kategorie können Benutzer eine Bot-Aktion damit verknüpfen.
- **Bot-Erkennung** – Bot-Erkennungstypen (Blockierliste, Zulassungsliste usw.), die Benutzer auf NetScaler konfiguriert haben.
- **Standort** – Region/Land, in dem der Bot-Angriff stattgefunden hat
- **Anforderungs-URL** – URL, die die möglichen Bot-Angriffe enthält

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

Benutzer können auch Operatoren in den Benutzersuchanfragen verwenden, um den Fokus der Benutzersuche einzugrenzen. Wenn Benutzer beispielsweise alle schlechten Bots anzeigen möchten:

- Klicken Sie auf das Suchfeld und wählen Sie **Bot-Typ** aus.
- Klicken Sie erneut auf das Suchfeld und wählen Sie den Operator **=** aus.
- Klicken Sie erneut auf das Suchfeld und wählen Sie **Bad** aus.
- Klicken Sie auf **Search**, um die Ergebnisse anzuzeigen.

### Ungewöhnlich hohe Anfragerate

Benutzer können den eingehenden und ausgehenden Datenverkehr von oder zu einer Anwendung steuern. Ein Bot-Angriff kann eine ungewöhnlich hohe Anfragerate verursachen. Wenn Benutzer beispielsweise eine Anwendung so konfigurieren, dass 100 Anfragen/Minute zugelassen werden, und 350 Anfragen beobachten, könnte es sich um einen Bot-Angriff handeln.

Mithilfe des Indikators **Unusually High Request Rate** können Benutzer die ungewöhnliche Anfragerate analysieren, die bei der Anwendung eingeht.

Unter **Event Details** können Benutzer Folgendes anzeigen:

- Die betroffene Anwendung. Benutzer 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 für den Verstoß, die die insgesamt empfangenen Anfragen und den Prozentsatz der übermäßigen Anfragen im Vergleich zu den erwarteten Anfragen angibt
- Der akzeptierte Bereich der erwarteten Anfrageraten von der Anwendung

### Bot-Erkennung

Das NetScaler Bot-Managementsystem verwendet verschiedene Techniken, um den eingehenden Bot-Verkehr zu erkennen. Die Techniken werden als Erkennungsregeln verwendet, um den Bot-Typ zu identifizieren.

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

#### Bot-Management mit der NetScaler GUI konfigurieren

Benutzer können das NetScaler Bot-Management konfigurieren, indem sie die Funktion zunächst auf dem Gerät aktivieren. Weitere Informationen finden Sie unter Bot-Erkennung.

### IP-Reputation

Die IP-Reputation ist ein Tool, das IP-Adressen identifiziert, die unerwünschte Anfragen senden. Mithilfe der IP-Reputationsliste können Sie Anfragen ablehnen, die von einer IP-Adresse mit schlechter Reputation stammen.

#### IP-Reputation mit der NetScaler GUI konfigurieren

Diese Konfiguration ist eine Voraussetzung für die Bot-IP-Reputationsfunktion. Weitere Informationen finden Sie unter IP-Reputation.

#### Automatische Aktualisierung für Bot-Signaturen

Die statische Bot-Signaturtechnik verwendet eine Signatur-Nachschlagetabelle mit einer Liste guter und schlechter Bots. Weitere Informationen finden Sie unter Automatische Signaturaktualisierung.

## NetScaler Web App Firewall und OWASP Top Ten–2021

Das Open Web Application Security Project (OWASP) hat die OWASP Top 10 für 2021 für die Webanwendungssicherheit veröffentlicht. Diese Liste dokumentiert die häufigsten Schwachstellen von Webanwendungen und ist ein hervorragender Ausgangspunkt für die Bewertung der Websicherheit. Dieser Abschnitt erläutert, wie die NetScaler Web App Firewall konfiguriert wird, um diese Schwachstellen zu mindern. WAF ist als integriertes Modul in NetScaler (Premium Edition) und einer vollständigen Palette von Appliances verfügbar.

Das vollständige OWASP Top 10-Dokument ist unter OWASP Top Ten verfügbar.

| OWASP TOP-10 2021 | NETSCALER WEB APP FIREWALL-FUNKTIONEN |
|---|---|
| A1:2021 Fehlerhafte Zugriffskontrolle | AAA, Sicherheitsfunktionen für die Autorisierung innerhalb des AAA-Moduls von NetScaler, Formularschutz und Schutz vor Cookie-Manipulation, StartURL und ClosureURL |
| A2:2021 – Kryptographische Fehler | Kreditkartenschutz, sicherer Handel, Cookie-Proxying und Cookie-Verschlüsselung |

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

| OWASP TOP-10 2021 | NETSCALER WEB APP FIREWALL-FUNKTIONEN |
|---|---|
| A3:2021 – Injection | Verhinderung von Injection-Angriffen (SQL oder andere benutzerdefinierte Injections wie OS-Befehlsinjection, XPath-Injection und LDAP-Injection), Funktion zur automatischen Signaturaktualisierung |
| A5:2021 Fehlkonfiguration der Sicherheit | Dieser Schutz umfasst WSI-Prüfungen, XML-Nachrichtenvalidierung und XML-SOAP-Fehlerfilterprüfung |
| A6:2021 – Schwachstellen und veraltete Komponenten | Schwachstellen-Scanberichte, Application Firewall-Vorlagen und benutzerdefinierte Signaturen |
| A7:2021 – Fehler bei Identifizierung und Authentifizierung | AAA, Schutz vor Cookie-Manipulation, Cookie-Proxying, Cookie-Verschlüsselung, CSRF-Tagging, Verwendung von SSL |
| A8:2021 – Fehler bei der Software- und Datenintegrität | XML-Sicherheitsprüfungen, GWT-Inhaltstyp, benutzerdefinierte Signaturen, XPath für JSON und XML |
| A9:2021 – Fehler bei der Sicherheits-Protokollierung und -Überwachung | Benutzerkonfigurierbare benutzerdefinierte Protokollierung, NetScaler Management and Analytics System |

## A1:2021 Fehlerhafte Zugriffskontrolle

Einschränkungen dessen, was authentifizierte Benutzer tun dürfen, werden oft nicht richtig durchgesetzt. Angreifer können diese Schwachstellen ausnutzen, um auf unbefugte Funktionen und Daten zuzugreifen, z. B. auf Konten anderer Benutzer zuzugreifen, vertrauliche Dateien anzuzeigen, Daten anderer Benutzer zu ändern oder Zugriffsrechte zu ändern.

### NetScaler Web App Firewall-Schutzfunktionen

- Die AAA-Funktion, die Authentifizierung, Autorisierung und Auditierung für den gesamten Anwendungsverkehr unterstützt, ermöglicht es einem Site-Administrator, Zugriffssteuerungen mit der ADC-Appliance zu verwalten.

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

- Die Sicherheitsfunktion „Autorisierung“ innerhalb des AAA-Moduls der ADC-Appliance ermöglicht es der Appliance zu überprüfen, auf welche Inhalte eines geschützten Servers jeder Benutzer zugreifen darf.
- Formularfeldkonsistenz: Wenn Objektreferenzen als ausgeblendete Felder in Formularen gespeichert werden, können Sie mithilfe der Formularfeldkonsistenz überprüfen, ob diese Felder bei nachfolgenden Anfragen nicht manipuliert wurden.
- Cookie-Proxying und Cookie-Konsistenz: Objektreferenzen, die in Cookie-Werten gespeichert sind, können mit diesen Schutzmaßnahmen validiert werden.
- Start-URL-Prüfung mit URL-Abschluss: Ermöglicht Benutzern den Zugriff auf eine vordefinierte Positivliste von URLs. Der URL-Abschluss erstellt eine Liste aller URLs, die in gültigen Antworten während der Benutzersitzung gesehen wurden, und ermöglicht automatisch den Zugriff darauf während dieser Sitzung.

## A2:2021 – Kryptografische Fehler

Viele Webanwendungen und APIs schützen sensible Daten wie Finanz-, Gesundheits- und PII-Daten nicht ordnungsgemäß. Angreifer können solche schlecht geschützten Daten stehlen oder ändern, um Kreditkartenbetrug, Identitätsdiebstahl oder andere Verbrechen zu begehen. Sensible Daten können ohne zusätzlichen Schutz, wie Verschlüsselung im Ruhezustand oder während der Übertragung, kompromittiert werden und erfordern besondere Vorsichtsmaßnahmen beim Austausch mit dem Browser.

### NetScaler Web App Firewall-Schutzfunktionen

- Die Web Application Firewall schützt Anwendungen vor dem Verlust sensibler Daten wie Kreditkartendaten.
- Sensible Daten können als sichere Objekte im Safe Commerce-Schutz konfiguriert werden, um eine Offenlegung zu vermeiden.
- Alle sensiblen Daten in Cookies können durch Cookie-Proxying und Cookie-Verschlüsselung geschützt werden.

## A3:2021 – Injection

Injection-Schwachstellen, wie SQL-, NoSQL-, OS- und LDAP-Injection, treten auf, wenn nicht vertrauenswürdige Daten als Teil eines Befehls oder einer Abfrage an einen Interpreter gesendet werden. Die feindseligen Daten des Angreifers können den Interpreter dazu verleiten, unbeabsichtigte Befehle auszuführen oder ohne entsprechende Autorisierung auf Daten zuzugreifen.

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

XSS-Schwachstellen treten immer dann auf, wenn eine Anwendung nicht vertrauenswürdige Daten ohne ordnungsgemäße Validierung oder Maskierung in eine neue Webseite einfügt oder eine bestehende Webseite mit vom Benutzer bereitgestellten Daten über eine Browser-API aktualisiert, die HTML oder JavaScript erstellen kann. XSS ermöglicht es Angreifern, Skripte im Browser des Opfers auszuführen, die Benutzersitzungen kapern, Webseiten verunstalten oder den Benutzer auf bösartige Websites umleiten können.

### NetScaler Web App Firewall-Schutzfunktionen

- Die Funktion zur Verhinderung von SQL-Injection schützt vor gängigen Injection-Angriffen. Benutzerdefinierte Injection-Muster können hochgeladen werden, um vor jeder Art von Injection-Angriff zu schützen, einschließlich XPath und LDAP. Dies gilt sowohl für HTML- als auch für XML-Payloads.
- Die Funktion zur automatischen Signaturaktualisierung hält die Injection-Signaturen auf dem neuesten Stand.
- Die Felddatenformat-Schutzfunktion ermöglicht es dem Administrator, jeden Benutzerparameter auf einen regulären Ausdruck zu beschränken. Sie können beispielsweise erzwingen, dass ein Postleitzahlenfeld nur ganze Zahlen oder sogar 5-stellige ganze Zahlen enthält.
- Die Formularfeldkonsistenz validiert jedes übermittelte Benutzerformular anhand der Formularsignatur der Benutzersitzung, um die Gültigkeit aller Formularelemente sicherzustellen.
- Pufferüberlaufprüfungen stellen sicher, dass URL, Header und Cookies innerhalb der richtigen Grenzen liegen, und blockieren alle Versuche, große Skripte oder Code zu einschleusen.
- Der XSS-Schutz schützt vor gängigen XSS-Angriffen. Benutzerdefinierte XSS-Muster können hochgeladen werden, um die Standardliste der erlaubten Tags und Attribute zu ändern. Die ADC WAF verwendet eine Whitelist von erlaubten HTML-Attributen und Tags, um XSS-Angriffe zu erkennen. Dies gilt sowohl für HTML- als auch für XML-Payloads.
- ADC WAF blockiert alle Angriffe, die im OWASP XSS Filter Evaluation Cheat Sheet aufgeführt sind.
- Die Felddatenformatprüfung verhindert, dass ein Angreifer unangemessene Webformulardaten sendet, die einen potenziellen XSS-Angriff darstellen könnten.
- Formularfeldkonsistenz.

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

## A5:2021 – Sicherheitsfehlkonfiguration

Sicherheitsfehlkonfiguration ist das am häufigsten auftretende Problem. Dies ist häufig das Ergebnis unsicherer Standardkonfigurationen, unvollständiger oder improvisierter Konfigurationen, offener Cloud-Speicher, falsch konfigurierter HTTP-Header und ausführlicher Fehlermeldungen, die sensible Informationen enthalten. Nicht nur alle Betriebssysteme, Frameworks, Bibliotheken und Anwendungen müssen sicher konfiguriert sein, sondern sie müssen auch zeitnah gepatcht und aktualisiert werden.

Viele ältere oder schlecht konfigurierte XML-Prozessoren werten externe Entitätsreferenzen in XML-Dokumenten aus. Externe Entitäten können verwendet werden, um interne Dateien mithilfe des Datei-URI-Handlers, interne Dateifreigaben, internes Port-Scanning, Remote-Code-Ausführung und Denial-of-Service-Angriffe offenzulegen.

### NetScaler Web App Firewall-Schutzfunktionen

- Der vom Application Firewall generierte PCI-DSS-Bericht dokumentiert die Sicherheitseinstellungen auf dem Firewall-Gerät.
- Berichte der Scan-Tools werden in ADC WAF-Signaturen umgewandelt, um Sicherheitsfehlkonfigurationen zu beheben.
- NetScaler Web App Firewall Web Application Firewall unterstützt Cenzic, IBM AppScan (Enterprise und Standard), Qualys, TrendMicro, WhiteHat und benutzerdefinierte Schwachstellenscan-Berichte.
- Zusätzlich zur Erkennung und Blockierung gängiger Anwendungsbedrohungen, die für Angriffe auf XML-basierte Anwendungen angepasst werden können (d. h. Cross-Site-Scripting, Befehlsinjektion usw.).
- NetScaler Web App Firewall Web Application Firewall umfasst eine Vielzahl von XML-spezifischen Sicherheitsschutzmaßnahmen. Dazu gehören die Schema-Validierung zur gründlichen Überprüfung von SOAP-Nachrichten und XML-Nutzdaten sowie eine leistungsstarke XML-Anhangsprüfung, um Anhänge mit bösartigen ausführbaren Dateien oder Viren zu blockieren.
- Automatische Verkehrsinspektionsmethoden blockieren XPath-Injektionsangriffe auf URLs und Formulare, die darauf abzielen, Zugriff zu erlangen.
- NetScaler Web App Firewall Web Application Firewall vereitelt auch verschiedene DoS-Angriffe, einschließlich externer Entitätsreferenzen, rekursiver Erweiterung, übermäßiger Verschachtelung und bösartiger Nachrichten, die entweder lange oder viele Attribute und Elemente enthalten.

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

## A6:2021 – Anfällige und veraltete Komponenten

Komponenten wie Bibliotheken, Frameworks und andere Softwaremodule werden mit denselben Berechtigungen wie die Anwendung ausgeführt. Wird eine anfällige Komponente ausgenutzt, kann ein solcher Angriff zu schwerwiegendem Datenverlust oder zur Übernahme des Servers führen. Anwendungen und APIs, die Komponenten mit bekannten Schwachstellen verwenden, können die Anwendungsverteidigung untergraben und verschiedene Angriffe und Auswirkungen ermöglichen.

### NetScaler Web App Firewall Schutzmaßnahmen

- Wir empfehlen, die Komponenten von Drittanbietern auf dem neuesten Stand zu halten.
- Schwachstellenscan-Berichte, die in ADC-Signaturen umgewandelt werden, können verwendet werden, um diese Komponenten virtuell zu patchen.
- Anwendungs-Firewall-Vorlagen, die für diese anfälligen Komponenten verfügbar sind, können verwendet werden.
- Benutzerdefinierte Signaturen können an die Firewall gebunden werden, um diese Komponenten zu schützen.

## A7:2021 – Fehlerhafte Authentifizierung

Anwendungsfunktionen im Zusammenhang mit Authentifizierung und Sitzungsverwaltung werden oft falsch implementiert, wodurch Angreifer Passwörter, Schlüssel oder Sitzungstoken kompromittieren oder andere Implementierungsfehler ausnutzen können, um vorübergehend oder dauerhaft die Identitäten anderer Benutzer anzunehmen.

### NetScaler Web App Firewall-Schutzmaßnahmen

- Das NetScaler AAA-Modul führt die Benutzerauthentifizierung durch und bietet Single-Sign-On-Funktionalität für Back-End-Anwendungen. Dies ist in die NetScaler AppExpert Policy Engine integriert, um benutzerdefinierte Richtlinien basierend auf Benutzer- und Gruppeninformationen zu ermöglichen.
- Mithilfe von SSL-Offloading- und URL-Transformationsfunktionen kann die Firewall Websites auch dabei unterstützen, sichere Transportschichtprotokolle zu verwenden, um das Stehlen von Sitzungstoken durch Netzwerk-Sniffing zu verhindern.
- Cookie-Proxying und Cookie-Verschlüsselung können eingesetzt werden, um Cookie-Diebstahl vollständig zu verhindern.

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

## A8:2021 – Fehler bei der Software- und Datenintegrität

Unsichere Deserialisierung führt oft zu Remote Code Execution. Auch wenn Deserialisierungsfehler nicht zu Remote Code Execution führen, können sie für Angriffe verwendet werden, einschließlich Replay-Angriffe, Injection-Angriffe und Privilege-Escalation-Angriffe.

### NetScaler Web App Firewall-Schutzmaßnahmen

- JSON-Payload-Inspektion mit benutzerdefinierten Signaturen.
- XML-Sicherheit: schützt vor XML Denial of Service (xDoS), XML SQL- und Xpath-Injection und Cross-Site-Scripting, Formatprüfungen, WS-I Basic Profile-Konformität, XML-Anhangsprüfung.
- Feldformatprüfungen sowie Cookie-Konsistenz und Feldkonsistenz können verwendet werden.

## A9:2021 – Fehler bei der Sicherheits-Protokollierung und -Überwachung

Unzureichende Protokollierung und Überwachung, verbunden mit fehlender oder ineffektiver Integration in die Incident Response, ermöglicht es Angreifern, Systeme weiter anzugreifen, Persistenz aufrechtzuerhalten, auf weitere Systeme überzugreifen und Daten zu manipulieren, zu extrahieren oder zu zerstören. Die meisten Studien zu Sicherheitsverletzungen zeigen, dass die Zeit bis zur Erkennung einer Verletzung über 200 Tage beträgt, wobei diese typischerweise von externen Parteien und nicht durch interne Prozesse oder Überwachung erkannt wird.

### NetScaler Web App Firewall-Schutzmaßnahmen

- Wenn die Protokollierungsaktion für Sicherheitsprüfungen oder Signaturen aktiviert ist, liefern die resultierenden Protokollmeldungen Informationen über die Anfragen und Antworten, die die Anwendungs-Firewall beim Schutz Ihrer Websites und Anwendungen beobachtet hat.
- Die Anwendungs-Firewall bietet den Komfort, die integrierte ADC-Datenbank zur Identifizierung der Standorte zu verwenden, die den IP-Adressen entsprechen, von denen bösartige Anfragen stammen.
- Standardformat-(PI)-Ausdrücke bieten die Flexibilität, die in den Protokollen enthaltenen Informationen anzupassen, mit der Option, die spezifischen Daten hinzuzufügen, die in den von der Anwendungs-Firewall generierten Protokollmeldungen erfasst werden sollen.
- Die Anwendungs-Firewall unterstützt CEF-Protokolle.

## Referenzen

- HTML SQL-Injection-Prüfung(/de-de/citrix-adc/current-release/application-firewall/top-level-protections/html-sql-injection-check.html#sql-fine-grained-relaxations)

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

- XML SQL-Injection-Prüfung(/de-de/citrix-adc/current-release/application-firewall/xml-protections/xml-sql-injection-check.html)
- Konfigurieren der HTML-Cross-Site-Scripting-Prüfung über die Befehlszeile(/de-de/citrix-adc/current-release/application-firewall/top-level-protections/html-cross-site-scripting-check.html#using-the-command-line-to-configure-the-html-cross-site-scripting-check)
- XML Cross-Site-Scripting-Prüfung(/de-de/citrix-adc/current-release/application-firewall/xml-protections/xml-cross-site-scripting-check.html)
- Konfigurieren der Sicherheitsprüfung für Pufferüberlauf über die Befehlszeile(/de-de/citrix-adc/current-release/application-firewall/top-level-protections/buffer-over-flow-check.html#using-the-command-line-to-configure-the-buffer-overflow-security-check)
- Hinzufügen oder Entfernen eines Signaturobjekts(/de-de/citrix-adc/current-release/application-firewall/signatures/add-remove-signatures.html)
- Konfigurieren oder Ändern eines Signaturobjekts(/de-de/citrix-adc/current-release/application-firewall/signatures/modifying-signatures.html)
- Aktualisieren eines Signaturobjekts(/de-de/citrix-adc/current-release/application-firewall/signatures/updating-signatures.html)
- Snort-Regelintegration(/de-de/citrix-adc/current-release/application-firewall/signatures/snort-rule-integration.html)
- Bot-Erkennung(/de-de/citrix-adc/current-release/bot-management/bot-detection.html#configure-bot-management)
- Bereitstellen einer NetScaler VPX-Instanz auf Microsoft Azure(/de-de/vpx/current-release/deploy-vpx-on-azure.html)

# Intranet-IP-Adresspools für eine NetScaler Gateway Appliance konfigurieren

In einigen Situationen benötigen Benutzer, die sich mit dem NetScaler Gateway Plug-in verbinden, eine eindeutige IP-Adresse für eine NetScaler Gateway Appliance. Wenn Sie Adresspools (auch als IP-Pooling bezeichnet) für eine Gruppe aktivieren, kann die NetScaler Gateway Appliance jedem Benutzer einen eindeutigen IP-Adressalias zuweisen. Sie konfigurieren Adresspools mithilfe von Intranet-IP-Adressen (IIP).

Sie können Adresspools auf einer in Azure bereitgestellten NetScaler Gateway Appliance mit diesem zweistufigen Verfahren konfigurieren:

- Registrieren der privaten IP-Adressen, die im Adresspool verwendet werden, in Azure

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

- Konfigurieren von Adresspools in der NetScaler Gateway Appliance

## Eine private IP-Adresse im Azure-Portal registrieren

In Azure können Sie eine NetScaler VPX-Instanz mit mehreren IP-Adressen bereitstellen. Sie können einer VPX-Instanz auf zwei Arten IP-Adressen hinzufügen:

a. Beim Bereitstellen einer VPX-Instanz

Weitere Informationen zum Hinzufügen mehrerer IP-Adressen beim Bereitstellen einer VPX-Instanz finden Sie unter Konfigurieren mehrerer IP-Adressen für eine eigenständige NetScaler-Instanz. Informationen zum Hinzufügen von IP-Adressen mithilfe von PowerShell-Befehlen beim Bereitstellen einer VPX-Instanz finden Sie unter Konfigurieren mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus mithilfe von PowerShell-Befehlen.

b. Nach dem Bereitstellen einer VPX-Instanz

Nachdem Sie eine VPX-Instanz bereitgestellt haben, führen Sie die folgenden Schritte aus, um eine private IP-Adresse im Azure-Portal zu registrieren, die Sie als Adresspool in der NetScaler Gateway Appliance konfigurieren.

1. Gehen Sie im Azure Resource Manager (ARM) zur bereits erstellten NetScaler VPX-Instanz > **Netzwerkschnittstellen**. Wählen Sie die Netzwerkschnittstelle aus, die an ein Subnetz gebunden ist, zu dem die IIP gehört, die Sie registrieren möchten.

2. Klicken Sie auf **IP-Konfigurationen** und dann auf **Hinzufügen**.

3. Geben Sie die erforderlichen Details wie im folgenden Beispiel gezeigt an und klicken Sie auf **OK**.

## Adresspools in der NetScaler Gateway Appliance konfigurieren

Weitere Informationen zum Konfigurieren von Adresspools auf dem NetScaler Gateway finden Sie unter Adresspools konfigurieren.

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

**EINSCHRÄNKUNG:**

Sie können keinen Bereich von IIP-Adressen an Benutzer binden. Jede IIP-Adresse, die in einem Adresspool verwendet wird, muss registriert werden.

# Konfigurieren Sie mehrere IP-Adressen für eine eigenständige NetScaler VPX-Instanz mithilfe von PowerShell-Befehlen

In einer Azure-Umgebung kann eine virtuelle NetScaler VPX-Appliance mit mehreren NICs bereitgestellt werden. Jede NIC kann mehrere IP-Adressen haben. Dieser Abschnitt beschreibt, wie eine NetScaler VPX-Instanz mit einer einzelnen NIC und mehreren IP-Adressen mithilfe von PowerShell-Befehlen bereitgestellt wird. Sie können dasselbe Skript für die Bereitstellung mit mehreren NICs und mehreren IP-Adressen verwenden.

**HINWEIS:**

In diesem Dokument bezieht sich IP-Config auf ein Paar von IP-Adressen, öffentliche IP und private IP, das einer einzelnen NIC zugeordnet ist. Weitere Informationen finden Sie im Abschnitt Azure-Terminologie.

## Anwendungsfall

In diesem Anwendungsfall ist eine einzelne NIC mit einem virtuellen Netzwerk (VNET) verbunden. Die NIC ist drei IP-Konfigurationen zugeordnet, wie in der folgenden Tabelle dargestellt.

| IP-KONFIGURATION | ZUGEORDNET ZU |
|---|---|
| IPConfig-1 | Statische öffentliche IP-Adresse; statische private IP-Adresse |
| IPConfig-2 | Statische öffentliche IP-Adresse; statische private Adresse |
| IPConfig-3 | Statische private IP-Adresse |

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

**HINWEIS:**

IPConfig-3 ist keiner öffentlichen IP-Adresse zugeordnet.

**Diagramm**: Topologie

Hier ist die visuelle Darstellung des Anwendungsfalls.

**HINWEIS:**

Bei einer Azure NetScaler VPX-Bereitstellung mit mehreren NICs und mehreren IPs wird die private IP-Adresse, die der primären (ersten) `IPConfig` der primären (ersten) NIC zugeordnet ist, automatisch als Management-NSIP-Adresse der Appliance hinzugefügt. Die verbleibenden privaten IP-Adressen, die `IPConfigs` zugeordnet sind, müssen in der VPX-Instanz als VIPs oder SNIPs mithilfe des `add ns ip`-Befehls hinzugefügt werden, je nach Ihren Anforderungen.

Hier ist eine Zusammenfassung der Schritte, die zum Konfigurieren mehrerer IP-Adressen für eine virtuelle NetScaler VPX-Appliance im Standalone-Modus erforderlich sind:

1. Ressourcengruppe erstellen
2. Speicherkonto erstellen
3. Verfügbarkeitsgruppe erstellen
4. Netzwerkdienstgruppe erstellen
5. Virtuelles Netzwerk erstellen
6. Öffentliche IP-Adresse erstellen
7. IP-Konfiguration zuweisen
8. NIC erstellen
9. NetScaler VPX-Instanz erstellen
10. NIC-Konfigurationen prüfen
11. VPX-seitige Konfigurationen prüfen

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

## Skript

### Parameter

Im Folgenden sind Beispielparameter für den Anwendungsfall in diesem Dokument aufgeführt.

```
$locName="westcentralus"

$rgName="Azure-MultiIP"

$nicName1="VM1-NIC1"

$vNetName="Azure-MultiIP-vnet"

$vNetAddressRange="11.6.0.0/16"

$frontEndSubnetName="frontEndSubnet"

$frontEndSubnetRange="11.6.1.0/24"

$prmStorageAccountName="multiipstorage"

$avSetName="multiip-avSet"
```

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

```
$vmSize="Standard\_DS4\_V2" (This parameter creates a VM with up to four
NICs.)
```

**HINWEIS:**

Die Mindestanforderung für eine VPX-Instanz sind 2 vCPUs und 2 GB RAM.

```
$publisher="Citrix"

$offer="netscalervpx110-6531" (You can use different offers.)

$sku="netscalerbyol" (According to your offer, the SKU can be different.)

$version="latest"

$pubIPName1="PIP1"

$pubIPName2="PIP2"

$domName1="multiipvpx1"

$domName2="multiipvpx2"
```

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

```
$vmNamePrefix="VPXMultiIP"

$osDiskSuffix="osmultiipalbdiskdb1"

**Network Security Group (NSG)-related information**:

$nsgName="NSG-MultiIP"

$rule1Name="Inbound-HTTP"

$rule2Name="Inbound-HTTPS"

$rule3Name="Inbound-SSH"

$IpConfigName1="IPConfig1"

$IPConfigName2="IPConfig-2"

$IPConfigName3="IPConfig-3"
```

### 1. Ressourcengruppe erstellen

`New-AzureRmResourceGroup -Name $rgName -Location $locName`

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

### 2. Speicherkonto erstellen

```
$prmStorageAccount = New-AzureRMStorageAccount -Name $prmStorageAccountName
-ResourceGroupName $rgName -Type Standard_LRS -Location $locName
```

### 3. Verfügbarkeitsgruppe erstellen

```
$avSet = New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName $rgName
-Location $locName
```

### 4. Netzwerksicherheitsgruppe erstellen

1. Regeln hinzufügen. Sie müssen eine Regel zur Netzwerksicherheitsgruppe für jeden Port hinzufügen, der Datenverkehr bedient.

   ```
   $rule1=New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -Description
   "Allow HTTP" -Access Allow -Protocol Tcp -Direction Inbound -Priority 101
   -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix *
   -DestinationPortRange 80 $rule2=New-AzureRmNetworkSecurityRuleConfig -Name
   $rule2Name -Description "Allow HTTPS" -Access Allow -Protocol Tcp -Direction
   Inbound -Priority 110 -SourceAddressPrefix Internet -SourcePortRange *
   -DestinationAddressPrefix * -DestinationPortRange 443 $rule3=New-
   AzureRmNetworkSecurityRuleConfig -Name $rule3Name -Description "Allow SSH"
   -Access Allow -Protocol Tcp -Direction Inbound -Priority 120
   -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix *
   -DestinationPortRange 22
   ```

2. Netzwerksicherheitsgruppenobjekt erstellen.

   ```
   $nsg=New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -Location
   $locName -Name $nsgName -SecurityRules $rule1,$rule2,$rule3
   ```

### 5. Virtuelles Netzwerk erstellen

1. Subnetze hinzufügen.

   ```
   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
   $frontEndSubnetName -AddressPrefix $frontEndSubnetRange
   ```

2. Objekt für virtuelles Netzwerk hinzufügen.

   ```
   $vnet=New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName $rgName
   -Location $locName -AddressPrefix $vNetAddressRange -Subnet $frontendSubnet
   ```

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

3. Subnetze abrufen.

   `$subnetName="frontEndSubnet"` `$subnet1=$vnet.Subnets|?{$_.Name -eq $subnetName}`

### 6. Öffentliche IP-Adresse erstellen

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName $rgName -DomainNameLabel $domName1 -Location $locName -AllocationMethod Static
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName $rgName -DomainNameLabel $domName2 -Location $locName -AllocationMethod Static
```

**HINWEIS:**

Überprüfen Sie die Verfügbarkeit von Domänennamen vor der Verwendung.

Die Zuweisungsmethode für IP-Adressen kann dynamisch oder statisch sein.

### 7. IP-Konfiguration zuweisen

Beachten Sie in diesem Anwendungsfall die folgenden Punkte, bevor Sie IP-Adressen zuweisen:

- IPConfig-1 gehört zu Subnetz1 von VPX1.
- IPConfig-2 gehört zu Subnetz 1 von VPX1.
- IPConfig-3 gehört zu Subnetz 1 von VPX1.

**HINWEIS:**

Wenn Sie einer NIC mehrere IP-Konfigurationen zuweisen, muss eine Konfiguration als primär zugewiesen werden.

```
$IPAddress1="11.6.1.27"

$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -Subnet $subnet1 -PrivateIpAddress $IPAddress1 -PublicIpAddress $pip1 –Primary

$IPAddress2="11.6.1.28"

$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -Subnet $subnet1 -PrivateIpAddress $IPAddress2 -PublicIpAddress $pip2
```

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

```
$IPAddress3="11.6.1.29"

$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3
-Subnet $subnet1 -PrivateIpAddress $IPAddress3 -Primary
```

Verwenden Sie eine gültige IP-Adresse, die Ihren Subnetzanforderungen entspricht, und prüfen Sie deren Verfügbarkeit.

### 8. NIC erstellen

`$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName $rgName -Location $locName -IpConfiguration $IpConfig1,$IpConfig2,$IPConfig3 -NetworkSecurityGroupId $nsg.Id`

### 9. NetScaler VPX-Instanz erstellen

1. Variablen initialisieren.

   `$suffixNumber = 1` `$vmName = $vmNamePrefix + $suffixNumber`

2. VM-Konfigurationsobjekt erstellen.

   `$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId $avSet.Id`

3. Anmeldeinformationen, Betriebssystem und Image festlegen.

   `$cred=Get-Credential -Message "Type the name and password for VPX login."` `$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName $vmName -Credential $cred` `$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher -Offer $offer -Skus $sku -Version $version`

4. NIC hinzufügen.

   `$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -Primary`

   **HINWEIS:**

   In einer NetScaler VPX-Bereitstellung mit mehreren NICs muss eine NIC primär sein. Daher muss beim Hinzufügen dieser NIC zur NetScaler VPX-Instanz „-Primary“ angehängt werden.

5. Betriebssystem-Datenträger angeben und VM erstellen.

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

`$osDiskName=$vmName + "-" + $osDiskSuffix1` `$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/" + $osDiskName + ".vhd"` `$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri $osVhdUri -CreateOption fromImage` `Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -Name $sku` `New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location $locName`

### 10. NIC-Konfigurationen überprüfen

Nach dem Start der NetScaler VPX-Instanz können Sie die `IPConfigs` zugewiesenen IP-Adressen der NetScaler VPX-NIC mit dem folgenden Befehl überprüfen.

```
$nic.IPConfig
```

### 11. VPX-seitige Konfigurationen überprüfen

Wenn die NetScaler VPX-Instanz startet, wird eine private IP-Adresse, die mit der primären `IPconfig` der primären NIC verknüpft ist, als NSIP-Adresse hinzugefügt. Die verbleibenden privaten IP-Adressen müssen je nach Ihren Anforderungen als VIP- oder SNIP-Adressen hinzugefügt werden. Verwenden Sie den folgenden Befehl.

```
add nsip <Private IPAddress><netmask> -type VIP/SNIP
```

Sie haben nun mehrere IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus konfiguriert.

## Zusätzliche PowerShell-Skripte für die Azure-Bereitstellung

Dieser Abschnitt enthält die PowerShell-Cmdlets, mit denen Sie die folgenden Konfigurationen in Azure PowerShell durchführen können:

- Bereitstellen einer NetScaler VPX Standalone-Instanz
- Bereitstellen eines NetScaler VPX-Paares in einer Hochverfügbarkeitskonfiguration mit einem externen Azure-Lastenausgleich
- Bereitstellen eines NetScaler VPX-Paares in einer Hochverfügbarkeitskonfiguration mit einem internen Azure-Lastenausgleich

Siehe auch die folgenden Themen für Konfigurationen, die Sie mithilfe von PowerShell-Befehlen durchführen können:

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

- Konfigurieren einer Hochverfügbarkeitskonfiguration mit mehreren IP-Adressen und NICs mithilfe von PowerShell-Befehlen
- GSLB auf NetScaler VPX-Instanzen konfigurieren
- GSLB in einer NetScaler Active-Standby-Hochverfügbarkeitskonfiguration konfigurieren
- Konfigurieren mehrerer IP-Adressen für eine NetScaler VPX-Instanz im Standalone-Modus mithilfe von PowerShell-Befehlen

## Bereitstellen einer NetScaler VPX Standalone-Instanz

1. **Ressourcengruppe erstellen**

   Die Ressourcengruppe kann alle Ressourcen für die Lösung oder nur die Ressourcen enthalten, die Sie als Gruppe verwalten möchten. Der hier angegebene Speicherort ist der Standardspeicherort für Ressourcen in dieser Ressourcengruppe. Stellen Sie sicher, dass alle Befehle zum Erstellen eines Lastenausgleichs dieselbe Ressourcengruppe verwenden.

   `$rgName="<resource group name>"` `$locName="<location name, such as West US>` `New-AzureRmResourceGroup -Name $rgName -Location $locName`

   *Beispiel*:

   ```
   $rgName = "ARM-VPX"

   $locName = "West US"

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

2. **Speicherkonto erstellen**

   Wählen Sie einen eindeutigen Namen für Ihr Speicherkonto, der nur Kleinbuchstaben und Zahlen enthält.

   `$saName="<storage account name>"` `$saType="<storage account type>"`, geben Sie eines an: `Standard_LRS`, `Standard_GRS`, `Standard_RAGRS` oder `Premium_LRS` `New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -Type $saType -Location $locName`

   *Zum Beispiel*:

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

```
$saName="vpxstorage"

$saType="Standard\_LRS"

New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
-Type $saType -Location $locName
```

3. **Verfügbarkeitsgruppe erstellen**

   Eine Verfügbarkeitsgruppe trägt dazu bei, dass Ihre virtuellen Maschinen während Ausfallzeiten, z. B. bei Wartungsarbeiten, verfügbar bleiben. Ein mit einer Verfügbarkeitsgruppe konfigurierter Lastenausgleich stellt sicher, dass Ihre Anwendung immer verfügbar ist.

   `$avName="<availability set name>"`

   `New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -Location $locName`

4. **Virtuelles Netzwerk erstellen**

   Fügen Sie ein neues virtuelles Netzwerk mit mindestens einem Subnetz hinzu, falls das Subnetz zuvor nicht erstellt wurde.

   `$FrontendAddressPrefix="10.0.1.0/24"` `$BackendAddressPrefix="10.0.2.0/24"` `$vnetAddressPrefix="10.0.0.0/16"` `$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name frontendSubnet -AddressPrefix $FrontendAddressPrefix` `$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name backendSubnet -AddressPrefix $BackendAddressPrefix` `New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -Subnet $frontendSubnet, $backendSubnet`

   *Zum Beispiel*:

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
frontendSubnet -AddressPrefix $FrontendAddressPrefix



$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
backendSubnet -AddressPrefix $BackendAddressPrefix
```

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

```
New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName
-Location $locName -AddressPrefix $vnetAddressPrefix -Subnet
$frontendSubnet,$backendSubnet
```

5. **NIC erstellen**

   Erstellen Sie eine NIC und ordnen Sie die NIC der NetScaler VPX-Instanz zu. Das im obigen Verfahren erstellte Frontend-Subnetz ist bei 0 indiziert und das Backend-Subnetz bei 1. Erstellen Sie nun die NIC auf eine der drei folgenden Arten:

   a) *NIC mit öffentlicher IP-Adresse*

   ```
   $nicName="<name of the NIC of the VM>"
   ```

   ```
   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName $rgName
   -Location $locName -AllocationMethod Dynamic
   ```

   ```
   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName $rgName
   -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -PublicIpAddressId
   $pip.Id
   ```

   b) *NIC mit öffentlicher IP und DNS-Bezeichnung*

   ```
   $nicName="<name of the NIC of the VM>"
   ```

   ```
   $domName="<domain name label>"
   ```

   ```
   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName $rgName
   -DomainNameLabel $domName -Location $locName -AllocationMethod Dynamic
   ```

   Bevor Sie $domName zuweisen, prüfen Sie mit dem Befehl, ob es verfügbar ist oder nicht:

   ```
   Test-AzureRmDnsAvailability -DomainQualifiedName $domName -Location $locName
   ```

   ```
   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName $rgName
   -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -PublicIpAddressId
   $pip.Id
   ```

   *Zum Beispiel*:

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

```
$nicName="frontendNIC"



$domName="vpxazure"



$pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
$rgName -DomainNameLabel $domName -Location $locName -AllocationMethod
Dynamic



$nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
$rgName -Location $locName -SubnetId $vnet.Subnets\[0\].Id
-PublicIpAddressId $pip.Id
```

c) *NIC mit dynamischer öffentlicher Adresse und statischer privater IP-Adresse*

Stellen Sie sicher, dass die private (statische) IP-Adresse, die Sie der VM hinzufügen, im selben Bereich liegt wie das angegebene Subnetz.

```
$nicName="<name of the NIC of the VM>"
```

```
$staticIP="<available static IP address on the subnet>"
```

```
$pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName $rgName
-Location $locName -AllocationMethod Dynamic
```

```
$nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName $rgName
-Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -PublicIpAddressId
$pip.Id -PrivateIpAddress $staticIP
```

6. **Virtuelles Objekt erstellen**

```
$vmName="<VM name>"
```

```
$vmSize="<VM size string>"
```

```
$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName
```

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

```
$vm=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId $avset.Id
```

7. **NetScaler VPX-Image abrufen**

   ```
   $pubName="<Image publisher name>"
   ```

   ```
   $offerName="<Image offer name>"
   ```

   ```
   $skuName="<Image SKU name>"
   ```

   ```
   $cred=Get-Credential -Message "Type the name and password of the local administrator account."
   ```

   Geben Sie Ihre Anmeldeinformationen ein, die für die Anmeldung bei VPX verwendet werden

   ```
   $vm=Set-AzureRmVMOperatingSystem -VM $vm -Linux -ComputerName $vmName -Credential $cred -Verbose
   ```

   ```
   $vm=Set-AzureRmVMSourceImage -VM $vm -PublisherName $pubName -Offer $offerName -Skus $skuName -Version "latest"
   ```

   ```
   $vm=Add-AzureRmVMNetworkInterface -VM $vm -Id $nic.Id
   ```

   *Zum Beispiel*:

   ```
   $pubName="citrix"
   ```

   Der folgende Befehl wird verwendet, um alle Angebote von Citrix® anzuzeigen:

   ```
   Get-AzureRMVMImageOffer -Location $locName -Publisher $pubName | Select Offer



   $offerName="netscalervpx110-6531"
   ```

   Der folgende Befehl wird verwendet, um die vom Herausgeber für einen bestimmten Angebotsnamen angebotene SKU zu ermitteln:

   ```
   Get-AzureRMVMImageSku -Location $locName -Publisher $pubName -Offer $offerName | Select Skus
   ```

8. **Eine virtuelle Maschine erstellen**

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

`$diskName="<name identifier for the disk in Azure storage, such as OSDisk>"`

*Zum Beispiel*:

```
$diskName="dynamic"



$pubName="citrix"



$offerName="netscalervpx110-6531"



$skuName="netscalerbyol"



$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -Name
$saName



$osDiskUri=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds/" +
$diskName  + ".vhd"



$vm=Set-AzureRmVMOSDisk -VM $vm -Name $diskName -VhdUri $osDiskUri
-CreateOption fromImage
```

Wenn Sie eine VM aus im Marketplace vorhandenen Images erstellen, verwenden Sie den folgenden Befehl, um den VM-Plan anzugeben:

`Set-AzureRmVMPlan -VM $vm -Publisher $pubName -Product $offerName -Name $skuName`

`New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM $vm`

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

# Bereitstellen eines NetScaler VPX-Paares in einer Hochverfügbarkeitskonfiguration mit einem externen Azure Load Balancer

Melden Sie sich mit Ihren Azure-Benutzeranmeldeinformationen bei AzureRmAccount an.

1. **Eine Ressourcengruppe erstellen**

   Der hier angegebene Speicherort ist der Standardspeicherort für Ressourcen in dieser Ressourcengruppe. Stellen Sie sicher, dass alle Befehle, die zum Erstellen eines Lastenausgleichs verwendet werden, dieselbe Ressourcengruppe verwenden.

   `$rgName="<resource group name>"`

   `$locName="<location name, such as West US>"`

   `New-AzureRmResourceGroup -Name $rgName -Location $locName`

   *Zum Beispiel*:

   ```
   $rgName = "ARM-LB-NS"



   $locName = "West US"



   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

2. **Speicherkonto erstellen**

   Wählen Sie einen eindeutigen Namen für Ihr Speicherkonto, der nur Kleinbuchstaben und Zahlen enthält.

   `$saName="<storage account name>"`

   `$saType="<storage account type>"`, geben Sie einen an: `Standard_LRS`, `Standard_GRS`, `Standard_RAGRS` oder `Premium_LRS`

   `New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -Type $saType -Location $locName`

   *Zum Beispiel*:

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

```
$saName="vpxstorage"



$saType="Standard_LRS"



New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
-Type $saType -Location $locName
```

3. **Verfügbarkeitsgruppe erstellen**

   Ein Lastenausgleich, der mit einer Verfügbarkeitsgruppe konfiguriert ist, stellt sicher, dass Ihre Anwendung immer verfügbar ist.

   `$avName="<availability set name>"`

   `New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -Location $locName`

4. **Ein virtuelles Netzwerk erstellen**

   Fügen Sie ein neues virtuelles Netzwerk mit mindestens einem Subnetz hinzu, falls das Subnetz zuvor nicht erstellt wurde.

```
$vnetName = "LBVnet"



$FrontendAddressPrefix="10.0.1.0/24"



$BackendAddressPrefix="10.0.2.0/24"



$vnetAddressPrefix="10.0.0.0/16"



$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
```

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

```
frontendSubnet -AddressPrefix $FrontendAddressPrefix



$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
backendSubnet -AddressPrefix $BackendAddressPrefix



$vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
$rgName -Location $locName -AddressPrefix $vnetAddressPrefix -Subnet
$frontendSubnet,$backendSubnet
```

**HINWEIS:**

Wählen Sie den Wert des Parameters AddressPrefix gemäß Ihren Anforderungen.

Weisen Sie dem virtuellen Netzwerk, das Sie zuvor in diesem Schritt erstellt haben, ein Frontend- und Backend-Subnetz zu.

Wenn das Frontend-Subnetz das erste Element des Arrays VNet ist, muss subnetId $vnet.Subnets\[0\].Id sein.

Wenn das Frontend-Subnetz das zweite Element im Array ist, muss subnetId $vnet.Subnets\[1\].Id sein, und so weiter.

5. **Frontend-IP-Adresse konfigurieren und Backend-Adresspool erstellen**

   Konfigurieren Sie eine Frontend-IP-Adresse für den eingehenden Load Balancer-Netzwerkverkehr und erstellen Sie einen Backend-Adresspool, um den Lastenausgleichsverkehr zu empfangen.

```
$pubName="PublicIp1"



$publicIP1 = New-AzureRmPublicIpAddress -Name $pubName
-ResourceGroupName $rgName -Location $locName -AllocationMethod Static
-DomainNameLabel nsvpx
```

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

**HINWEIS:**

Überprüfen Sie die Verfügbarkeit des Werts für DomainNameLabel.

```
$FIPName = "ELBFIP"



$frontendIP1 = New-AzureRmLoadBalancerFrontendIpConfig -Name $FIPName
-PublicIpAddress $publicIP1



$BEPool = "LB-backend-Pool"



$beaddresspool1= New-AzureRmLoadBalancerBackendAddressPoolConfig -Name
$BEPool
```

6. **Eine Integritätstest-Sonde erstellen**

   Erstellen Sie eine TCP-Integritätstest-Sonde mit Port 9000 und einem Intervall von 5 Sekunden.

```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name HealthProbe
-Protocol Tcp -Port 9000 -IntervalInSeconds 5 -ProbeCount 2
```

7. **Eine Lastenausgleichsregel erstellen**

   Erstellen Sie eine LB-Regel für jeden Dienst, für den Sie den Lastenausgleich durchführen.

   *Zum Beispiel*:

   Sie können das folgende Beispiel verwenden, um den HTTP-Dienst per Lastenausgleich zu verteilen.

```
$lbrule1 = New-AzureRmLoadBalancerRuleConfig -Name "HTTP-LB"
-FrontendIpConfiguration $frontendIP1 -BackendAddressPool
```

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

```
 $beAddressPool1 -Probe $healthProbe -Protocol Tcp -FrontendPort 80
-BackendPort 80
```

8. **Eingehende NAT-Regeln erstellen**

   Erstellen Sie NAT-Regeln für Dienste, die Sie nicht per Lastenausgleich verteilen.

   Zum Beispiel beim Erstellen eines SSH-Zugriffs auf eine NetScaler VPX-Instanz.

   **HINWEIS:**

   Das Triplett Protokoll-FrontEndPort-BackendPort darf für zwei NAT-Regeln nicht dasselbe sein.

   ```
   $inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -Name
   SSH1     -FrontendIpConfiguration $frontendIP1 -Protocol TCP
   -FrontendPort 22 -BackendPort 22



   $inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -Name
   SSH2 -FrontendIpConfiguration $frontendIP1 -Protocol TCP -FrontendPort
   10022 -BackendPort 22
   ```

9. **Eine Lastenausgleichs-Entität erstellen**

   Erstellen Sie den Lastenausgleich, indem Sie alle Objekte (NAT-Regeln, Lastenausgleichsregeln, Sondierungskonfigurationen) zusammenfügen.

   ```
   $lbName="ELB"



   $NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name
   $lbName -Location $locName -InboundNatRule $inboundNATRule1,
   $inboundNATRule2 -FrontendIpConfiguration $frontendIP1
   -LoadBalancingRule $lbrule1 -BackendAddressPool $beAddressPool1 -Probe
   $healthProbe
   ```

10. **Eine NIC erstellen**

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

Erstellen Sie zwei NICs und ordnen Sie jede NIC jeder VPX-Instanz zu.

a) NIC1 mit VPX1

*Zum Beispiel*:

```
$nicName="NIC1"


$lbName="ELB"


$bePoolIndex=0


\* Rule indexes starts from 0.


$natRuleIndex=0


$subnetIndex=0


\* Frontend subnet index


$lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName


$nic1=New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
$rgName -Location $locName -Subnet $vnet.Subnets\[$subnetIndex\]
-LoadBalancerBackendAddressPool $lb.BackendAddressPools\[$bePoolIndex\]
-LoadBalancerInboundNatRule $lb.InboundNatRules\[$natRuleIndex\]
```

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

b) NIC2 mit VPX2

*Zum Beispiel*:

```
$nicName="NIC2"


$lbName="ELB"


$bePoolIndex=0


$natRuleIndex=1


\* Second Inbound NAT (SSH) rule we need to use


`$subnetIndex=0


\* Frontend subnet index


$lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName


$nic2=New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
$rgName -Location $locName -Subnet $vnet.Subnets\[$subnetIndex\]
-LoadBalancerBackendAddressPool $lb.BackendAddressPools\[$bePoolIndex\]
-LoadBalancerInboundNatRule  $lb.InboundNatRules\[$natRuleIndex\]
```

11. **NetScaler VPX-Instanzen erstellen**

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

Erstellen Sie zwei NetScaler VPX-Instanzen als Teil derselben Ressourcengruppe und Verfügbarkeitsgruppe und hängen Sie sie an den externen Lastenausgleich an.

a) NetScaler VPX-Instanz 1

*Zum Beispiel*:

```
$vmName="VPX1"



$vmSize="Standard\_A3"



$pubName="citrix"



$offerName="netscalervpx110-6531"



$skuName="netscalerbyol"



$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName



$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize
-AvailabilitySetId $avset.Id



$cred=Get-Credential -Message "Type Credentials which will be used to
login to VPX instance"



$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName $vmName
```

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

```
-Credential $cred -Verbose



$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -Offer
$offerName -Skus $skuName -Version "latest"



$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $nic1.Id



$diskName="dynamic"



$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -Name
$saName



$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/" +
$diskName  + ".vhd"



$vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri $osDiskUri1
-CreateOption fromImage



Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
-Name $skuName



New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM $vm1
```

b) NetScaler VPX-Instanz 2

*Zum Beispiel*:

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

```
$vmName="VPX2"



$vmSize="Standard\_A3"



$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName



$vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize
-AvailabilitySetId $avset.Id



$cred=Get-Credential -Message " Type Credentials which will be used to
login to VPX instance "



$vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName $vmName
-Credential $cred -Verbose



$vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -Offer
$offerName -Skus $skuName -Version "latest"



$vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id



$diskName="dynamic"



$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -Name
$saName
```

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

```
$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds2/" +
$diskName  + ".vhd"



$vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri $osDiskUri1
-CreateOption fromImage



Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product $offerName
-Name $skuName



New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM $vm2
```

12. **Die virtuellen Maschinen konfigurieren**

    Wenn beide NetScaler VPX-Instanzen gestartet sind, stellen Sie über das SSH-Protokoll eine Verbindung zu beiden NetScaler VPX-Instanzen her, um die virtuellen Maschinen zu konfigurieren.

    a) Aktiv-Aktiv: Führen Sie dieselben Konfigurationsbefehle in der Befehlszeile beider NetScaler VPX-Instanzen aus.

    b) Aktiv-Passiv: Führen Sie diesen Befehl in der Befehlszeile beider NetScaler VPX-Instanzen aus.

    `add ha node #nodeID <nsip of other NetScaler VPX>`

    Im Aktiv-Passiv-Modus führen Sie Konfigurationsbefehle nur auf dem primären Knoten aus.

## Bereitstellen eines NetScaler VPX-Paares in einer Hochverfügbarkeitskonfiguration mit Azure Internal Load Balancer

Melden Sie sich mit Ihren Azure-Benutzeranmeldeinformationen bei AzureRmAccount an.

1. **Eine Ressourcengruppe erstellen**

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

Der hier angegebene Speicherort ist der Standardspeicherort für Ressourcen in dieser Ressourcengruppe. Stellen Sie sicher, dass alle Befehle zum Erstellen eines Lastenausgleichs die gleiche Ressourcengruppe verwenden.

`$rgName="\<resource group name\>"`

`$locName="\<location name, such as West US\>"`

`New-AzureRmResourceGroup -Name $rgName -Location $locName`

*Zum Beispiel*:

```
$rgName = "ARM-LB-NS"



$locName = "West US"



New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. **Speicherkonto erstellen**

   Wählen Sie einen eindeutigen Namen für Ihr Speicherkonto, der nur Kleinbuchstaben und Zahlen enthält.

   `$saName="<storage account name>"`

   `$saType="<storage account type>"`, geben Sie einen an: `Standard_LRS`, `Standard_GRS`, `Standard_RAGRS` oder `Premium_LRS`

   `New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -Type $saType -Location $locName`

   *Zum Beispiel*:

```
$saName="vpxstorage"



$saType="Standard_LRS"
```

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

```
New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
-Type $saType -Location $locName
```

3. **Verfügbarkeitsgruppe erstellen**

   Ein Lastenausgleich, der mit einer Verfügbarkeitsgruppe konfiguriert ist, stellt sicher, dass Ihre Anwendung immer verfügbar ist.

   `$avName="<availability set name>"`

   `New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -Location $locName`

4. **Ein virtuelles Netzwerk erstellen**

   Fügen Sie ein neues virtuelles Netzwerk mit mindestens einem Subnetz hinzu, falls das Subnetz zuvor nicht erstellt wurde.

```
$vnetName = "LBVnet"


$vnetAddressPrefix="10.0.0.0/16"


$FrontendAddressPrefix="10.0.1.0/24"


$BackendAddressPrefix="10.0.2.0/24"


$vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
$rgName -Location $locName -AddressPrefix $vnetAddressPrefix -Subnet
$frontendSubnet,$backendSubnet\`


$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
```

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

```
frontendSubnet -AddressPrefix $FrontendAddressPrefix



$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
backendSubnet -AddressPrefix $BackendAddressPrefix
```

**HINWEIS:**

Wählen Sie den Parameterwert für AddressPrefix gemäß Ihren Anforderungen.

Weisen Sie dem virtuellen Netzwerk, das Sie zuvor in diesem Schritt erstellt haben, ein Frontend- und Backend-Subnetz zu.

Wenn das Frontend-Subnetz das erste Element des Arrays VNet ist, muss subnetId $vnet.Subnets\[0\].Id sein.

Wenn das Frontend-Subnetz das zweite Element im Array ist, muss subnetId $vnet.Subnets\[1\].Id sein, und so weiter.

5. **Einen Backend-Adresspool erstellen**

   `$beaddresspool= New-AzureRmLoadBalancerBackendAddressPoolConfig -Name "LB-backend"`

6. **NAT-Regeln erstellen**

   Erstellen Sie NAT-Regeln für Dienste, die Sie nicht per Lastenausgleich verteilen.

   ```
   $inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -Name
   "Inboundnatrule1" -FrontendIpConfiguration $frontendIP -Protocol TCP
   -FrontendPort 3441 -BackendPort 3389



   $inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -Name
   "RDP2" -FrontendIpConfiguration $frontendIP -Protocol TCP -FrontendPort
   3442 -BackendPort 3389
   ```

   Verwenden Sie Frontend- und Backend-Ports gemäß Ihren Anforderungen.

7. **Eine Integritätsprüfung erstellen**

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

Erstellen Sie eine TCP-Integritätsprüfung mit Port 9000 und einem Intervall von 5 Sekunden.

```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name "HealthProbe"
 " -Protocol tcp -Port 9000 -IntervalInSeconds 5 -ProbeCount 2
```

8. **Eine Lastenausgleichsregel erstellen**

   Erstellen Sie eine LB-Regel für jeden Dienst, für den Sie einen Lastenausgleich durchführen.

   Zum Beispiel:

   Sie können das folgende Beispiel verwenden, um den HTTP-Dienst per Lastenausgleich zu verteilen.

   ```
   $lbrule = New-AzureRmLoadBalancerRuleConfig -Name "lbrule1"
   -FrontendIpConfiguration $frontendIP -BackendAddressPool $beAddressPool
   -Probe $healthProbe -Protocol Tcp -FrontendPort 80 -BackendPort 80
   ```

   Verwenden Sie Front-End- und Back-End-Ports gemäß Ihren Anforderungen.

9. **Lastenausgleichs-Entität erstellen**

   Erstellen Sie den Lastenausgleich, indem Sie alle Objekte (NAT-Regeln, Lastenausgleichsregeln, Sondierungskonfigurationen) zusammenfügen.

   ```
   $NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgname -Name
   "InternalLB" -Location $locName -FrontendIpConfiguration $frontendIP
   -InboundNatRule $inboundNATRule1,$inboundNatRule2 -LoadBalancingRule
   $lbrule -BackendAddressPool $beAddressPool -Probe $healthProbe
   ```

10. **NIC erstellen**

    Erstellen Sie zwei NICs und ordnen Sie jede NIC jeder NetScaler VPX-Instanz zu

    ```
    $backendnic1= New-AzureRmNetworkInterface -ResourceGroupName $rgName
    -Name lb-nic1-be -Location $locName -PrivateIpAddress 10.0.2.6 -Subnet
    $backendSubnet -LoadBalancerBackendAddressPool
    $nrplb.BackendAddressPools\[0\] -LoadBalancerInboundNatRule
    $nrplb.InboundNatRules\[0\]
    ```

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

Diese NIC ist für NetScaler VPX 1. Die private IP muss sich im selben Subnetz befinden wie das hinzugefügte Subnetz.

```
$backendnic2= New-AzureRmNetworkInterface -ResourceGroupName $rgName
-Name lb-nic2-be -Location $locName -PrivateIpAddress 10.0.2.7 -Subnet
$backendSubnet -LoadBalancerBackendAddressPool
$nrplb.BackendAddressPools\[0\] -LoadBalancerInboundNatRule
$nrplb.InboundNatRules\[1\].
```

Diese NIC ist für NetScaler VPX 2. Der Parameter `Private IPAddress` kann jede private IP-Adresse gemäß Ihren Anforderungen haben.

11. **NetScaler VPX-Instanzen erstellen**

    Erstellen Sie zwei VPX-Instanzen, die Teil derselben Ressourcengruppe und Verfügbarkeitsgruppe sind, und verbinden Sie sie mit dem internen Lastenausgleich.

    a) NetScaler VPX-Instanz 1

    *Zum Beispiel*:

```
$vmName="VPX1"



$vmSize="Standard\_A3"



$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName



$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize
-AvailabilitySetId $avset.Id



$cred=Get-Credential -Message "Type Credentials which will be used to
login to VPX instance"
```

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

```
$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName $vmName
-Credential $cred -Verbose



$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -Offer
$offerName -Skus $skuName -Version "latest"



$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $backendnic1.Id



$diskName="dynamic"



$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -Name
$saName



$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/" +
$diskName  + ".vhd"



$vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri $osDiskUri1
-CreateOption fromImage



Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
-Name $skuName



New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM $vm1
```

b) NetScaler VPX-Instanz 2

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

*Zum Beispiel*:

```
$vmName="VPX2"



$vmSize="Standard\_A3"



$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName



$vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize
-AvailabilitySetId $avset.Id



$cred=Get-Credential -Message " Type Credentials which will be used to
login to VPX instance "



$vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName $vmName
-Credential $cred -Verbose



$vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -Offer
$offerName -Skus $skuName -Version "latest"



$vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $backendnic2.Id



$diskName="dynamic"
```

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

```
$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -Name
$saName



$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds2/" +
$diskName  + ".vhd"



$vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri $osDiskUri1
-CreateOption fromImage



Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product $offerName
-Name $skuName



New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM $vm2
```

12. **Konfigurieren Sie die virtuellen Maschinen**

    Wenn beide NetScaler VPX-Instanzen starten, verbinden Sie sich dann über das SSH-Protokoll mit beiden NetScaler VPX-Instanzen, um die virtuellen Maschinen zu konfigurieren.

    a) Aktiv-Aktiv: Führen Sie dieselben Konfigurationsbefehle auf der Befehlszeile beider NetScaler VPX-Instanzen aus.

    b) Aktiv-Passiv: Führen Sie diesen Befehl auf der Befehlszeile beider NetScaler VPX-Instanzen aus.

    `add ha node #nodeID <nsip of other NetScaler VPX>`

    Im Aktiv-Passiv-Modus führen Sie Konfigurationsbefehle nur auf dem primären Knoten aus.

# Ein Support-Ticket für die VPX-Instanz in Azure erstellen

Wenn Sie Probleme mit Ihrer NetScaler VPX-Instanz in Azure haben, können Sie zur Fehlerbehebung ein Support-Ticket im NetScaler Support-Portal erstellen.

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

Um ein Support-Ticket einzureichen, stellen Sie Folgendes sicher:

- Ihr Netzwerk ist verbunden.
- Sie haben Ihre Azure-Kontonummer, den Support-PIN-Code des abonnementbasierten NetScaler®-Angebots, das Sie in Azure bereitgestellt haben, und das Azure-Serienprotokoll griffbereit.
  - Den Support-PIN-Code finden Sie auf der Seite **Systeme** in der VPX-GUI.

  - Das Serienprotokoll finden Sie im Azure-Portal (Abschnitt **Startdiagnose** Ihrer VM).

Sobald Sie alle Informationen bereit haben, rufen Sie den NetScaler-Support an. Sie werden gebeten, Ihren Namen und Ihre E-Mail-Adresse anzugeben.

## Azure-FAQs

- **Unterscheidet sich das Upgrade-Verfahren der aus dem Azure Marketplace installierten NetScaler VPX-Instanz von dem lokalen Upgrade-Verfahren?**

  Nein. Sie können Ihre NetScaler VPX-Instanz in der Microsoft Azure Cloud auf NetScaler VPX Release 11.1 oder höher aktualisieren, indem Sie die standardmäßigen NetScaler VPX-Upgrade-Verfahren verwenden. Sie können entweder über GUI- oder CLI-Verfahren aktualisieren. Für neue Installationen verwenden Sie das NetScaler VPX-Image für die Microsoft Azure Cloud.

  Um die NetScaler VPX-Upgrade-Builds herunterzuladen, gehen Sie zu **NetScaler-Downloads** > **NetScaler-Firmware**.

- **Wie korrigiert man MAC-Verschiebungen und Schnittstellenstummschaltungen, die bei auf Azure gehosteten NetScaler VPX-Instanzen beobachtet werden?**

  In einer Azure Multi-NIC-Umgebung können standardmäßig alle Datenschnittstellen MAC-Verschiebungen und Schnittstellenstummschaltungen anzeigen. Um MAC-Verschiebungen und Schnittstellenstummschaltungen in Azure-Umgebungen zu vermeiden, empfiehlt Citrix, ein VLAN pro Datenschnittstelle (ohne Tag) der NetScaler VPX-Instanz zu erstellen und die primäre IP der NIC in Azure zu binden.

  Weitere Informationen finden Sie im Artikel CTX224626.

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

# Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform

Sie können eine NetScaler VPX-Instanz auf der Google Cloud Platform (GCP) bereitstellen. Eine VPX-Instanz in GCP ermöglicht es Ihnen, die Cloud-Computing-Funktionen von GCP zu nutzen und die Lastenausgleichs- und Datenverkehrsmanagementfunktionen von Citrix für Ihre Geschäftsanforderungen einzusetzen. Sie können VPX-Instanzen in GCP als eigenständige Instanzen bereitstellen. Sowohl Einzel-NIC- als auch Multi-NIC-Konfigurationen werden unterstützt.

## Unterstützte GCP-Maschinentypfamilien

| MASCHINENTYPFAMILIE | MINDESTMASCHINENTYP |
|---|---|
| Allzweckmaschinen | e2-medium, e2-standard-2, e2-highmem-2, n1-standard-2, n1-highmem-2, n2-standard-2, n2-highmem-2, n2d-standard-2, n2d-highmem-2, c3-standard-4, n4-standard-2, c4-standard-2, c4d-standard-2 |
| Rechenoptimierte Maschinen | c2-standard-4, c2d-standard-2, c2d-highmem-2 |

**HINWEIS:**

- Die Unterstützung für N4- und C3-Instanztypen beginnt mit NetScaler Release 14.1-56.x.
- Die Unterstützung für C4- und C4D-Instanztypen beginnt mit NetScaler Release 14.1-73.x.

## Unterstützte Funktionen

Alle Premium-, Advanced- und Standardfunktionen werden auf der GCP basierend auf dem verwendeten Lizenz- oder Versionstyp unterstützt.

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

## Einschränkung

- IPv6 wird nicht unterstützt.

## Hardware-Anforderungen

Eine VPX-Instanz in GCP muss mindestens 2 vCPUs und 4 GB RAM haben.

## Hinweise

Beachten Sie die folgenden GCP-spezifischen Punkte, bevor Sie mit der Bereitstellung beginnen.

- Nach dem Erstellen der Instanz können Sie keine Netzwerkschnittstellen hinzufügen oder entfernen.
- Für eine Multi-NIC-Bereitstellung erstellen Sie separate VPC-Netzwerke für jede NIC. Eine NIC kann nur einem Netzwerk zugeordnet werden.
- Für eine Single-NIC-Instanz erstellt die GCP-Konsole standardmäßig ein Netzwerk.
- Für eine Instanz mit mehr als zwei Netzwerkschnittstellen sind mindestens 4 vCPUs erforderlich.
- Wenn IP-Weiterleitung erforderlich ist, müssen Sie die IP-Weiterleitung beim Erstellen der Instanz und beim Konfigurieren der NIC aktivieren.

## Szenario: Bereitstellen einer Multi-NIC-, Multi-IP-Standalone-NetScaler-VPX-Instanz

Dieses Szenario veranschaulicht, wie eine NetScaler VPX Standalone-Instanz in GCP bereitgestellt wird. In diesem Szenario erstellen Sie eine Standalone-VPX-Instanz mit mehreren NICs. Die Instanz kommuniziert mit Back-End-Servern (der Serverfarm).

Erstellen Sie drei NICs für die folgenden Zwecke.

| NIC | ZWECK | ZUGEORDNET ZUM VPC-NETZWERK |
|---|---|---|
| NIC 0 | Dient dem Management-Traffic (NetScaler IP) | Management-Netzwerk |

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

| NIC | ZWECK | ZUGEORDNET ZUM VPC-NETZWERK |
|---|---|---|
| NIC 1 | Dient dem clientseitigen Traffic (VIP) | Client-Netzwerk |
| NIC 2 | Kommuniziert mit Back-End-Servern (SNIP) | Back-End-Server-Netzwerk |

Richten Sie die erforderlichen Kommunikationsrouten zwischen den folgenden Elementen ein:

- NetScaler VPX-Instanz und den Back-End-Servern.
- NetScaler VPX-Instanz und den externen Hosts im öffentlichen Internet.

## Zusammenfassung der Bereitstellungsschritte

1. Erstellen Sie drei VPC-Netzwerke für drei verschiedene NICs.
2. Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443.
3. Erstellen Sie eine Instanz mit drei NICs.

Wählen Sie die NetScaler VPX-Instanz aus dem GCP Marketplace.

**HINWEIS:**

Erstellen Sie eine Instanz in derselben Region, in der Sie die VPC-Netzwerke erstellt haben.

**Schritt 1. VPC-Netzwerke erstellen.**

Erstellen Sie drei VPC-Netzwerke, die mit der Management-NIC, der Client-NIC und der Server-NIC verknüpft sind. Um ein VPC-Netzwerk zu erstellen, melden Sie sich bei **Google Console > Networking > VPC network > Create VPC Network** an. Füllen Sie die erforderlichen Felder aus, wie im Screenshot gezeigt, und klicken Sie auf **Erstellen**.

Erstellen Sie auf ähnliche Weise VPC-Netzwerke für Client- und serverseitige NICs.

**HINWEIS:**

Alle drei VPC-Netzwerke müssen sich in derselben Region befinden, die in diesem Szenario asia-east1 ist.

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

**Schritt 2. Firewall-Regeln für die Ports 22, 80 und 443 erstellen.**

Erstellen Sie Regeln für SSH (Port 22), HTTP (Port 80) und HTTPS (Port 443) für jedes VPC-Netzwerk. Weitere Informationen zu Firewall-Regeln finden Sie unter Firewall Rules Overview.

**Schritt 3. Erstellen Sie die VPX-Instanz.**

1. Melden Sie sich bei der GCP-Konsole an.
2. Navigieren Sie zum GCP Marketplace.
3. Wählen Sie ein Abonnement basierend auf Ihren Anforderungen aus.

4. Klicken Sie bei dem ausgewählten Abonnement auf **Launch**.

5. Füllen Sie das Bereitstellungsformular aus und klicken Sie auf **Deploy**.

   **HINWEIS:**

   Verwenden Sie die in **Schritt 1** erstellten VPC-Netzwerke.

6. Die bereitgestellte Instanz wird unter **Compute Engine > VM-Instanzen** angezeigt.

   Verwenden Sie GCP SSH oder die serielle Konsole, um die VPX-Instanz zu konfigurieren und zu verwalten.

## Szenario: Bereitstellen einer eigenständigen VPX-Instanz mit einer einzelnen NIC

Dieses Szenario veranschaulicht, wie eine eigenständige NetScaler VPX-Instanz mit einer einzelnen NIC in GCP bereitgestellt wird. Die Alias-IP-Adressen werden verwendet, um diese Bereitstellung zu erreichen.

Erstellen Sie eine einzelne NIC (NIC0) für die folgenden Zwecke:

- Verwaltungsdatenverkehr (NetScaler IP) im Verwaltungsnetzwerk verwalten.
- Client-seitigen Datenverkehr (VIP) im Client-Netzwerk verwalten.
- Mit Backend-Servern (SNIP) im Backend-Server-Netzwerk kommunizieren.

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

Richten Sie die erforderlichen Kommunikationsrouten zwischen den folgenden ein:

- Instanz und den Backend-Servern.
- Instanz und den externen Hosts im öffentlichen Internet.

## Zusammenfassung der Bereitstellungsschritte

1. Erstellen Sie ein VPC-Netzwerk für NIC0.
2. Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443.
3. Erstellen Sie eine Instanz mit einer einzelnen NIC.
4. Alias-IP-Adressen zu VPX hinzufügen.
5. VIP und SNIP auf VPX hinzufügen.
6. Fügen Sie einen virtuellen Lastausgleichsserver hinzu.
7. Fügen Sie einen Dienst oder eine Dienstgruppe auf der Instanz hinzu.
8. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf der Instanz.

**HINWEIS:**

Erstellen Sie eine Instanz in derselben Region, in der Sie die VPC-Netzwerke erstellt haben.

**Schritt 1. Erstellen Sie ein VPC-Netzwerk.**

Erstellen Sie ein VPC-Netzwerk, das mit NIC0 verknüpft werden soll.

Führen Sie die folgenden Schritte aus, um ein VPC-Netzwerk zu erstellen:

1. Melden Sie sich bei der **GCP console > Networking > VPC network > Create VPC Network** an.
2. Füllen Sie die erforderlichen Felder aus und klicken Sie auf **Create**.

**Schritt 2. Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443.**

Erstellen Sie Regeln für SSH (Port 22), HTTP (Port 80) und HTTPS (Port 443) für das VPC-Netzwerk. Weitere Informationen zu Firewall-Regeln finden Sie unter Firewall Rules Overview.

**Schritt 3. Erstellen Sie eine Instanz mit einer einzelnen NIC.**

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

Führen Sie die folgenden Schritte aus, um eine Instanz mit einer einzelnen NIC zu erstellen:

1. Melden Sie sich bei der **GCP console** an.
2. Fahren Sie unter **Compute** über **Compute Engine** und wählen Sie **Images** aus.
3. Wählen Sie das Image aus und klicken Sie auf **Create Instance**.

4. Wählen Sie einen Instanztyp mit zwei vCPUs (Mindestanforderung für ADC) aus.

5. Klicken Sie im Fenster **Management, security, disks, networking** auf die Registerkarte **Networking**.
6. Klicken Sie unter **Network interfaces** auf das Symbol **Edit**, um die Standard-NIC zu bearbeiten.
7. Wählen Sie im Fenster **Network interfaces** unter **Network** das von Ihnen erstellte VPC-Netzwerk aus.
8. Sie können eine statische externe IP-Adresse erstellen. Klicken Sie unter **External IP addresses** auf **Create IP address**.
9. Geben Sie im Fenster **Reserve a static address** einen Namen und eine Beschreibung ein und klicken Sie auf **Reserve**.
10. Klicken Sie auf **Create**, um die VPX-Instanz zu erstellen. Die neue Instanz wird unter VM-Instanzen angezeigt.

**Schritt 4. Alias-IP-Adressen zur VPX-Instanz hinzufügen.**

Weisen Sie der VPX-Instanz zwei Alias-IP-Adressen zu, die als VIP- und SNIP-Adressen verwendet werden sollen.

**HINWEIS:**

Verwenden Sie die primäre interne IP-Adresse der VPX-Instanz nicht, um die VIP oder SNIP zu konfigurieren.

Um eine Alias-IP-Adresse zu erstellen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Bearbeiten**.
2. Im Fenster **Netzwerkschnittstelle** bearbeiten Sie die NIC0-Schnittstelle.
3. Geben Sie im Feld **Alias-IP-Bereich** die Alias-IP-Adressen ein.

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

4. Klicken Sie auf **Fertig** und dann auf **Speichern**.
5. Überprüfen Sie die Alias-IP-Adressen auf der Seite **VM-Instanzdetails**.

**Schritt 5. Fügen Sie VIP und SNIP zur VPX-Instanz hinzu.**

Fügen Sie auf der VPX-Instanz eine Client-Alias-IP-Adresse und eine Server-Alias-IP-Adresse hinzu.

1. Navigieren Sie in der NetScaler-GUI zu **System > Netzwerk > IPs > IPv4s** und klicken Sie auf **Hinzufügen**.

2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):
   - Geben Sie die Client-Alias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz in der VM-Instanz konfiguriert sind.
   - Wählen Sie im Feld **IP-Typ Virtuelle IP** aus dem Dropdown-Menü aus.
   - Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine Server-Alias-IP-Adresse (SNIP):
   - Geben Sie die Server-Alias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz in der VM-Instanz konfiguriert sind.
   - Wählen Sie im Feld **IP-Typ** im Dropdown-Menü **Subnetz-IP** aus.
   - Klicken Sie auf **Erstellen**.

**Schritt 6. Virtuellen Lastausgleichsserver hinzufügen.**

1. Navigieren Sie in der NetScaler-GUI zu **Configuration > Traffic Management > Load Balancing > Virtual Servers**, und klicken Sie auf **Add**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (Client-Alias-IP) und Port hinzu.
3. Klicken Sie auf **OK**, um den virtuellen Lastausgleichsserver zu erstellen.

**Schritt 7. Dienst oder Dienstgruppe zur VPX-Instanz hinzufügen.**

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

1. Navigieren Sie in der NetScaler-GUI zu **Configuration > Traffic Management > Load Balancing > Services**, und klicken Sie auf **Add**.
2. Fügen Sie die erforderlichen Werte für Dienstname, IP-Adresse, Protokoll und Port hinzu, und klicken Sie auf **OK**.

**Schritt 8. Binden Sie den Dienst/die Dienstgruppe an den virtuellen Lastausgleichsserver auf der Instanz.**

1. Navigieren Sie in der GUI zu **Configuration > Traffic Management > Load Balancing > Virtual Servers**.
2. Wählen Sie den in **Schritt 6** konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Fenster **Dienst- und Dienstgruppen** auf **Keine Bindung des virtuellen Lastausgleichsserverdienstes**.
4. Wählen Sie den in **Schritt 7** konfigurierten Dienst aus und klicken Sie auf **Binden**.

# Hinweise nach der Bereitstellung der VPX-Instanz auf GCP

- Melden Sie sich bei der VPX mit dem Benutzernamen `nsroot` und der Instanz-ID als Kennwort an. Ändern Sie an der Eingabeaufforderung das Kennwort und speichern Sie die Konfiguration.
- Um ein technisches Support-Bundle zu sammeln, führen Sie den Befehl `shell /netscaler/showtech_cloud.pl` anstelle des üblichen `show techsupport` aus.
- Nach dem Löschen einer NetScaler-VM aus der GCP-Konsole löschen Sie auch die zugehörige interne NetScaler-Zielinstanz. Gehen Sie dazu zur gcloud CLI und geben Sie den folgenden Befehl ein:

```
gcloud compute -q  target-instances delete <instance-name>-adcinternal
--zone <zone>
```

**HINWEIS:**

`<instance-name>-adcinternal` ist der Name der Zielinstanz, die gelöscht werden muss.

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

# NetScaler VPX-Lizenzierung

Eine NetScaler VPX-Instanz auf GCP erfordert eine gültige Lizenz. Die für NetScaler VPX-Instanzen, die auf GCP ausgeführt werden, verfügbare Lizenzierungsoption lautet wie folgt:

**Bring Your Own License (BYOL)**: Um die BYOL-Option zu verwenden, führen Sie die folgenden Schritte aus:

- Verwenden Sie das Lizenzierungsportal auf der NetScaler®-Website, um eine gültige Lizenz zu generieren.
- Laden Sie die generierte Lizenz auf die Instanz hoch.
- **NetScaler VPX Check-in- und Check-out-Lizenz**: Dieses Lizenzierungsmodell ermöglicht es Ihnen, eine Lizenz aus einem Pool verfügbarer Lizenzen auszuchecken und wieder einzuchecken, wenn sie nicht mehr benötigt wird. Weitere Informationen und detaillierte Anweisungen finden Sie unter NetScaler VPX Check-in- und Check-out-Lizenz.

**HINWEIS:**

Abonnementbasierte Lizenzierung wird für NetScaler VPX-Instanzen auf GCP nicht mehr unterstützt.

# Unterstützte NetScaler VPX-Angebote auf GCP

Die folgende Tabelle listet die unterstützten NetScaler VPX-Angebote auf GCP auf.

| UNTERSTÜTZTE VPX-ANGEBOTE |
| --- |
| NetScaler VPX – vom Kunden lizenziert |
| NetScaler VPX FIPS – vom Kunden lizenziert |

# GDM-Vorlagen zur Bereitstellung einer NetScaler VPX-Instanz

Sie können eine NetScaler VPX Google Deployment Manager (GDM)-Vorlage verwenden, um eine VPX-Instanz auf GCP bereitzustellen. Weitere Informationen finden Sie unter NetScaler GDM-Vorlagen.

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

### Ressourcen

- Erstellen von Instanzen mit mehreren Netzwerkschnittstellen
- Erstellen und Starten einer VM-Instanz

### Zugehörige Informationen

- Bereitstellen eines VPX-Hochverfügbarkeitspaares auf der Google Cloud Platform

## Bereitstellen eines VPX-Hochverfügbarkeitspaares auf der Google Cloud Platform

Sie können zwei NetScaler VPX-Instanzen auf der Google Cloud Platform (GCP) als Hochverfügbarkeits- (HA) Aktiv-Passiv-Paar konfigurieren. Wenn Sie eine Instanz als primären Knoten und die andere als sekundären Knoten konfigurieren, akzeptiert der primäre Knoten Verbindungen und verwaltet Server. Der sekundäre Knoten überwacht den primären Knoten. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen akzeptieren kann, übernimmt der sekundäre Knoten.

Weitere Informationen zu HA finden Sie unter Hochverfügbarkeit.

Die Knoten müssen sich in derselben Region befinden; sie können jedoch entweder in derselben Zone oder in verschiedenen Zonen sein. Weitere Informationen finden Sie unter Regionen und Zonen.

Jede VPX-Instanz erfordert mindestens drei IP-Subnetze (Google VPC-Netzwerke):

- Ein Verwaltungs-Subnetz
- Ein clientseitiges Subnetz (VIP)
- Ein Back-End-Subnetz (SNIP, MIP usw.)

Citrix® empfiehlt drei Netzwerkschnittstellen für eine Standard-VPX-Instanz.

Sie können ein VPX-Hochverfügbarkeitspaar mit den folgenden Methoden bereitstellen:

- Verwenden einer externen statischen IP-Adresse
- Verwenden einer privaten IP-Adresse
- Verwenden von VMs mit einer einzelnen NIC und privater IP-Adresse

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

## GDM-Vorlagen zur Bereitstellung eines VPX-Hochverfügbarkeitspaares auf GCP

Sie können eine NetScaler Google Deployment Manager (GDM)-Vorlage verwenden, um ein VPX-Hochverfügbarkeitspaar auf GCP bereitzustellen. Details finden Sie unter NetScaler GDM-Vorlagen.

## Unterstützung von Weiterleitungsregeln für ein VPX-Hochverfügbarkeitspaar auf GCP

Sie können ein VPX-Hochverfügbarkeitspaar auf der GCP mithilfe von Weiterleitungsregeln bereitstellen.

Weitere Informationen zu Weiterleitungsregeln finden Sie unter Übersicht über Weiterleitungsregeln.

### Voraussetzungen

- Weiterleitungsregeln müssen sich in derselben Region wie die VPX-Instanzen befinden.
- Zielinstanzen müssen sich in derselben Zone wie die VPX-Instanz befinden.
- Die Anzahl der Zielinstanzen für primäre und sekundäre Knoten muss übereinstimmen.

**Beispiel:**

Sie haben ein Hochverfügbarkeitspaar in der Region `us-east1` mit primärem VPX in Zone `us-east1-b` und sekundärem VPX in Zone `us-east1-c`. Eine Weiterleitungsregel ist für das primäre VPX mit der Zielinstanz in Zone `us-east1-b` konfiguriert. Konfigurieren Sie eine Zielinstanz für das sekundäre VPX in Zone `us-east1-c`, um die Weiterleitungsregel bei einem Failover zu aktualisieren.

### Einschränkungen

Nur Weiterleitungsregeln, die mit Zielinstanzen im Backend konfiguriert sind, werden in der VPX-Hochverfügbarkeitsbereitstellung unterstützt.

# Bereitstellen eines VPX-Hochverfügbarkeitspaares mit externer statischer IP-Adresse auf der Google Cloud Platform

Sie können ein VPX-Hochverfügbarkeitspaar auf GCP mithilfe einer externen statischen IP-Adresse bereitstellen. Die Client-IP-Adresse des primären Knotens muss an eine externe statische

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

IP-Adresse gebunden sein. Beim Failover wird die externe statische IP-Adresse auf den sekundären Knoten verschoben, damit der Datenverkehr wieder aufgenommen werden kann.

Eine statische externe IP-Adresse ist eine externe IP-Adresse, die für Ihr Projekt reserviert ist, bis Sie sich entscheiden, sie freizugeben. Wenn Sie eine IP-Adresse verwenden, um auf einen Dienst zuzugreifen, können Sie diese IP-Adresse reservieren, sodass nur Ihr Projekt sie verwenden kann. Weitere Informationen finden Sie unter Reservieren einer statischen externen IP-Adresse.

Weitere Informationen zu HA finden Sie unter Hochverfügbarkeit.

## Bevor Sie beginnen

- Lesen Sie die Einschränkungen, Hardwareanforderungen und Hinweise, die unter Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform erwähnt werden. Diese Informationen gelten auch für HA-Bereitstellungen.
- Aktivieren Sie die **Cloud Resource Manager API** für Ihr GCP-Projekt.
- Ermöglichen Sie vollen Zugriff auf alle Cloud APIs beim Erstellen der Instanzen.
- Stellen Sie sicher, dass die IAM-Rolle, die Ihrem GCP-Dienstkonto zugeordnet ist, die folgenden IAM-Berechtigungen besitzt:

```
REQUIRED_INSTANCE_IAM_PERMS = [



"compute.addresses.use",

"compute.forwardingRules.list",

"compute.forwardingRules.setTarget",

"compute.instances.setMetadata"

"compute.instances.addAccessConfig",

"compute.instances.deleteAccessConfig",

"compute.instances.get",

"Compute.instances.list",
```

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

```
"compute.networks.useExternalIp",

"compute.subnetworks.useExternalIp",

"compute.targetInstances.list",

"compute.targetInstances.use",

"compute.targetInstances.create",

"compute.zones.list",

"compute.zoneOperations.get",

]
```

- Wenn Sie Alias-IP-Adressen auf einer anderen Schnittstelle als der Verwaltungsschnittstelle konfiguriert haben, stellen Sie sicher, dass Ihr GCP-Dienstkonto die folgenden zusätzlichen IAM-Berechtigungen besitzt:

  ```
  "compute.instances.updateNetworkInterface"
  ```

- Wenn Sie GCP-Weiterleitungsregeln auf dem primären Knoten konfiguriert haben, lesen Sie die Einschränkungen und Anforderungen, die unter Unterstützung von Weiterleitungsregeln für VPX-Hochverfügbarkeitspaare auf GCP erwähnt werden, um diese beim Failover auf den neuen primären Knoten zu aktualisieren.

## So stellen Sie ein VPX-HA-Paar auf der Google Cloud Platform bereit

Hier ist eine Zusammenfassung der HA-Bereitstellungsschritte:

1. Erstellen Sie VPC-Netzwerke in derselben Region. Zum Beispiel Asien-Ost.
2. Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) in derselben Region. Sie können sich in derselben Zone oder in verschiedenen Zonen befinden. Zum Beispiel Asien-Ost-1a und Asien-Ost-1b.
3. Konfigurieren Sie die HA-Einstellungen auf beiden Instanzen mithilfe der NetScaler-GUI oder der ADC-CLI-Befehle.

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

### Schritt 1. VPC-Netzwerke erstellen

Erstellen Sie VPC-Netzwerke basierend auf Ihren Anforderungen. Citrix® empfiehlt Ihnen, drei VPC-Netzwerke für die Zuordnung mit der Management-NIC, Client-NIC und Server-NIC zu erstellen.

Führen Sie die folgenden Schritte aus, um ein VPC-Netzwerk zu erstellen:

1. Melden Sie sich bei der **Google Console > Networking > VPC network > Create VPC Network** an.
2. Füllen Sie die erforderlichen Felder aus und klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie im Abschnitt **VPC-Netzwerke erstellen** unter Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform.

### Schritt 2. Zwei VPX-Instanzen erstellen

Erstellen Sie zwei VPX-Instanzen, indem Sie die Schritte unter Szenario: Bereitstellen einer eigenständigen VPX-Instanz mit mehreren NICs und mehreren IPs befolgen.

**WICHTIG:**

Weisen Sie dem Client-IP-Adresse (VIP) des primären Knotens eine statische externe IP-Adresse zu. Sie können eine vorhandene reservierte IP-Adresse verwenden oder eine neue erstellen. Um eine statische externe IP-Adresse zu erstellen, navigieren Sie zu **Network interface > External IP** und klicken Sie auf **Create IP address**.

Nach dem Failover, wenn der alte primäre Knoten zum neuen sekundären Knoten wird, wird die statische externe IP-Adresse vom alten primären Knoten verschoben und dem neuen primären Knoten zugewiesen. Weitere Informationen finden Sie im Google Cloud-Dokument Reservieren einer statischen externen IP-Adresse.

Nachdem Sie die VPX-Instanzen konfiguriert haben, können Sie die VIP- und SNIP-Adressen konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von NetScaler-eigenen IP-Adressen.

### Schritt 3. Hochverfügbarkeit konfigurieren

Nachdem Sie die Instanzen auf der Google Cloud Platform erstellt haben, können Sie HA über die NetScaler GUI für CLI konfigurieren.

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

### HA über die GUI konfigurieren

**Schritt 1**. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

Führen Sie auf dem **primären Knoten** die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens aus der GCP-Konsole als Passwort an.
2. Navigieren Sie zu **Configuration > System > High Availability > Nodes** und klicken Sie auf **Add**.
3. Geben Sie im Feld **Remote Node IP address** die private IP-Adresse der Management-NIC des sekundären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Turn on INC (Independent Network Configuration) mode on self node**.
5. Klicken Sie auf **Create**.

Führen Sie auf dem **sekundären Knoten** die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens aus der GCP-Konsole als Passwort an.
2. Navigieren Sie zu **Configuration > System > High Availability > Nodes** und klicken Sie auf **Add**.
3. Geben Sie im Feld **Remote Node IP address** die private IP-Adresse der Management-NIC des primären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Turn on INC (Independent Network Configuration) mode on self node**.
5. Klicken Sie auf **Create**.

Bevor Sie fortfahren, stellen Sie sicher, dass der Synchronisierungsstatus des sekundären Knotens auf der Seite **Knoten** als **ERFOLG** angezeigt wird.

**HINWEIS:**

Nun hat der sekundäre Knoten die gleichen Anmeldeinformationen wie der primäre Knoten.

**Schritt 2**. Fügen Sie die virtuelle IP-Adresse und die Subnetz-IP-Adresse auf beiden Knoten hinzu.

Führen Sie auf dem **primären Knoten** die folgenden Schritte aus:

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

1. Navigieren Sie zu **System > Network > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie eine primäre VIP-Adresse hinzu, indem Sie diese Schritte ausführen:
    a. Geben Sie die interne IP-Adresse der clientseitigen Schnittstelle der primären Instanz und die für das Client-Subnetz in der VM-Instanz konfigurierte Netzmaske ein.
    b. Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdown-Menü aus.
    c. Klicken Sie auf **Erstellen**.
3. Fügen Sie eine primäre SNIP-Adresse hinzu, indem Sie diese Schritte ausführen:
    a. Geben Sie die interne IP-Adresse der serverseitigen Schnittstelle der primären Instanz und die für das Server-Subnetz in der primären Instanz konfigurierte Netzmaske ein.
    b. Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdown-Menü aus.
    c. Klicken Sie auf **Erstellen**.
4. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
    a. Geben Sie die interne IP-Adresse der clientseitigen Schnittstelle der sekundären Instanz und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert ist.
    b. Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdown-Menü aus.
    c. Klicken Sie auf **Erstellen**.

VIP und SNIP auf primären Knoten erstellen(/en-us/vpx/media/primary-vip-snip.png)

Führen Sie auf dem **sekundären Knoten** die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
    a. Geben Sie die interne IP-Adresse der clientseitigen Schnittstelle der sekundären Instanz und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert ist.
    b. Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdown-Menü aus.
3. Fügen Sie eine sekundäre SNIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
    a. Geben Sie die interne IP-Adresse der serverseitigen Schnittstelle der sekundären Instanz und die Netzmaske ein, die für das Server-Subnetz in der sekundären Instanz konfiguriert ist.
    b. Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdown-Menü aus.

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

c. Klicken Sie auf **Erstellen**.

VIP und SNIP auf sekundären Knoten erstellen(/en-us/vpx/media/secondary-vip-snip.png)

**Schritt 3**. Fügen Sie einen IP-Satz hinzu und binden Sie den IP-Satz an die sekundäre VIP auf beiden Instanzen.

Führen Sie auf dem **primären Knoten** die folgenden Schritte aus:

1. Navigieren Sie zu **System > Network > IP Sets > Add**.
2. Fügen Sie einen IP-Satznamen hinzu und klicken Sie auf **Insert**.
3. Wählen Sie auf der Seite **IPV4s** die virtuelle IP (sekundäre VIP) aus und klicken Sie auf **Insert**.
4. Klicken Sie auf **Create**, um den IP-Satz zu erstellen.

Führen Sie auf dem **sekundären Knoten** die folgenden Schritte aus:

1. Navigieren Sie zu **System > Network > IP Sets > Add**.
2. Fügen Sie einen IP-Satznamen hinzu und klicken Sie auf **Insert**.
3. Wählen Sie auf der Seite **IPV4s** die virtuelle IP (sekundäre VIP) aus und klicken Sie auf **Insert**.
4. Klicken Sie auf **Create**, um den IP-Satz zu erstellen.

**HINWEIS:**

Der IP-Satzname muss auf beiden Instanzen identisch sein.

**Schritt 4**. Fügen Sie einen virtuellen Lastausgleichsserver auf der primären Instanz hinzu.

1. Navigieren Sie zu **Configuration > Traffic Management > Load Balancing > Virtual Servers > Add**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäre VIP) und Port hinzu.
3. Klicken Sie auf **More**. Navigieren Sie zu **IP Range IP Set Settings**, wählen Sie **IPset** aus dem Dropdown-Menü und geben Sie das in **Schritt 3** erstellte IPset an.
4. Klicken Sie auf **OK**, um den virtuellen Lastausgleichsserver zu erstellen.

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

**Schritt 5**. Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Configuration > Traffic Management > Load Balancing > Services > Add**.
2. Fügen Sie die erforderlichen Werte für Dienstname, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

**Schritt 6**. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

1. Navigieren Sie zu **Configuration > Traffic Management > Load Balancing > Virtual Servers**.
2. Wählen Sie den in **Schritt 4** konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Edit**.
3. Klicken Sie auf der Registerkarte **Service and Service Groups** auf **No Load Balancing Virtual Server Service Binding**.
4. Wählen Sie den in **Schritt 5** konfigurierten Dienst aus und klicken Sie auf **Bind**.

Speichern Sie die Konfiguration. Nach einem erzwungenen Failover wird der sekundäre Knoten zum neuen primären Knoten. Die externe statische IP der alten primären VIP wird auf die neue sekundäre VIP verschoben.

### Hochverfügbarkeit mithilfe der CLI konfigurieren

**Schritt 1**. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

```
add ha node 1 <sec_ip> -inc ENABLED
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
add ha node 1 <prim_ip> -inc ENABLED
```

`sec_ip` bezieht sich auf die interne IP-Adresse der Management-NIC des sekundären Knotens.

`prim_ip` bezieht sich auf die interne IP-Adresse der Management-NIC des primären Knotens.

**Schritt 2**. Fügen Sie virtuelle und Subnetz-IPs auf beiden Knoten hinzu.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

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

```
add ns ip <primary_vip> <subnet> -type VIP


add ns ip <secondary_vip> <subnet> -type VIP


add ns ip <primary_snip> <subnet> -type SNIP
```

`primary_vip` bezieht sich auf die interne IP-Adresse der clientseitigen Schnittstelle der primären Instanz.

`secondary_vip` bezieht sich auf die interne IP-Adresse der clientseitigen Schnittstelle der sekundären Instanz.

`primary_snip` bezieht sich auf die interne IP-Adresse der serverseitigen Schnittstelle der primären Instanz.

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
add ns ip <secondary_vip> <subnet> -type VIP


add ns ip <secondary_snip> <subnet> -type SNIP
```

`secondary_vip` bezieht sich auf die interne IP-Adresse der clientseitigen Schnittstelle der sekundären Instanz.

`secondary_snip` bezieht sich auf die interne IP-Adresse der serverseitigen Schnittstelle der sekundären Instanz.

**Schritt 3**. Fügen Sie einen IP-Satz hinzu und binden Sie den IP-Satz an die sekundäre VIP auf beiden Instanzen.

Geben Sie auf dem primären Knoten den folgenden Befehl ein:

```
add ipset <ipsetname>

bind ipset <ipsetname> <secondary VIP>
```

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

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein:

```
add ipset <ipsetname>

bind ipset <ipsetname> <secondary VIP>
```

**HINWEIS:**

Der IP-Set-Name muss auf beiden Instanzen gleich sein.

**Schritt 4**. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

Geben Sie den folgenden Befehl ein:

```
add <server_type> vserver <vserver_name> <protocol> <primary_vip> <port>
-ipset <ipset_name>
```

**Schritt 5**. Fügen Sie einen Dienst oder eine Dienstgruppe auf der primären Instanz hinzu.

Geben Sie den folgenden Befehl ein:

```
add service <service_name> <service_ip_address> <protocol> <port>
```

**Schritt 6**. Binden Sie den Dienst/die Dienstgruppe an den virtuellen Lastausgleichsserver auf der primären Instanz.

Geben Sie den folgenden Befehl ein:

```
bind <server_type> vserver <vserver_name> <service_name>
```

**HINWEIS:**

Um Ihre Konfiguration zu speichern, geben Sie den Befehl `save config` ein. Andernfalls gehen die Konfigurationen nach dem Neustart der Instanzen verloren.

**Schritt 7**. Überprüfen Sie die Konfiguration.

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

Stellen Sie sicher, dass die externe IP-Adresse, die an die primäre Client-NIC angehängt ist, bei einem Failover auf die sekundäre verschoben wird.

1. Stellen Sie eine cURL-Anfrage an die externe IP-Adresse und stellen Sie sicher, dass diese erreichbar ist.
2. Auf der primären Instanz Failover durchführen:

   Über die GUI navigieren Sie zu **Configuration > System > High Availability > Action > Force Failover**.

   Über die CLI geben Sie den folgenden Befehl ein:

   ```
   force ha failover -f
   ```

   Wechseln Sie in der GCP-Konsole zur sekundären Instanz. Die externe IP-Adresse muss nach dem Failover auf die Client-NIC der sekundären Instanz verschoben worden sein.
3. Senden Sie eine cURL-Anfrage an die externe IP-Adresse und stellen Sie sicher, dass sie wieder erreichbar ist.

# Bereitstellen eines VPX-Hochverfügbarkeitspaares mit einer einzelnen NIC und privater IP-Adresse auf der Google Cloud Platform

Sie können ein VPX-Hochverfügbarkeitspaar mit einer einzelnen NIC auf GCP unter Verwendung einer privaten IP-Adresse bereitstellen. Die Client-IP-Adresse (VIP) muss als Alias-IP-Adresse auf dem primären Knoten konfiguriert werden. Nach einem Failover wird die Client-IP-Adresse auf den sekundären Knoten verschoben, damit der Datenverkehr wieder aufgenommen werden kann. Die Subnetz-IP-Adressen (SNIPs) für jeden Knoten müssen ebenfalls als Alias-IP-Bereich konfiguriert werden.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit.

## Bevor Sie beginnen

- Lesen Sie die Einschränkungen, Hardwareanforderungen und Hinweise, die unter Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform erwähnt werden. Diese Informationen gelten auch für Hochverfügbarkeitsbereitstellungen.
- Aktivieren Sie die **Cloud Resource Manager API** für Ihr GCP-Projekt.
- Ermöglichen Sie vollen Zugriff auf alle Cloud-APIs während der Erstellung der Instanzen.

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

- Stellen Sie sicher, dass Ihr GCP-Dienstkonto die folgenden IAM-Berechtigungen besitzt:

```
REQUIRED_INSTANCE_IAM_PERMS = [

"compute.forwardingRules.list",

"compute.forwardingRules.setTarget",

"compute.instances.setMetadata",

"compute.instances.get",

"compute.instances.list",

"compute.instances.updateNetworkInterface",

"compute.targetInstances.list",

"compute.targetInstances.use",

"compute.targetInstances.create",

"compute.zones.list",

"compute.zoneOperations.get",

]
```

- Wenn Ihre VMs keinen Internetzugang haben, müssen Sie **Privaten Google-Zugriff** im VPC-Subnetz aktivieren.

- Wenn Sie GCP-Weiterleitungsregeln auf dem primären Knoten konfiguriert haben, lesen Sie die Einschränkungen und Anforderungen, die unter Unterstützung von Weiterleitungsregeln für VPX-Hochverfügbarkeitspaare auf GCP erwähnt werden, um diese bei einem Failover auf den neuen primären Knoten zu aktualisieren.

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

## So stellen Sie ein VPX-Hochverfügbarkeitspaar auf der Google Cloud Platform bereit

Hier ist eine Zusammenfassung der Schritte zur Bereitstellung eines HA-Paares mit einer einzelnen NIC:

1. Erstellen Sie ein VPC-Netzwerk.
2. Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) in derselben Region. Sie können sich in derselben Zone oder in verschiedenen Zonen befinden. Zum Beispiel Asien Ost-1a und Asien Ost-1b.
3. Konfigurieren Sie die HA-Einstellungen auf beiden Instanzen mithilfe der NetScaler GUI oder der ADC CLI-Befehle.

### Schritt 1. Ein VPC-Netzwerk erstellen

Führen Sie die folgenden Schritte aus, um ein VPC-Netzwerk zu erstellen:

1. Melden Sie sich bei der **Google Console > Networking > VPC network > Create VPC Network** an.
2. Füllen Sie die erforderlichen Felder aus und klicken Sie auf **Create**.

Weitere Informationen finden Sie im Abschnitt **Create VPC Networks** unter Bereitstellen einer NetScaler VPX-Instanz auf Google Cloud Platform.

### Schritt 2. Zwei VPX-Instanzen erstellen

Erstellen Sie zwei VPX-Instanzen, indem Sie die Schritte 1 bis 3 unter Szenario: Bereitstellen einer eigenständigen VPX-Instanz mit einer einzelnen NIC befolgen.

**WICHTIG:**

Weisen Sie nur dem primären Knoten eine Client-Alias-IP-Adresse und dem primären und sekundären Knoten Server-Alias-IP-Adressen zu. Verwenden Sie nicht die interne IP-Adresse der VPX-Instanz, um die VIP oder SNIP zu konfigurieren.

Führen Sie die folgenden Schritte auf dem primären Knoten aus, um Client- und Server-Alias-IP-Adressen zu erstellen:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Edit**.
2. Bearbeiten Sie im Fenster **Network Interface** die Client-Schnittstelle (NIC0).
3. Geben Sie im Feld **Alias IP range** die Client-Alias-IP-Adresse ein.

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

4. Klicken Sie auf **Add IP Range** und geben Sie die Server-Alias-IP-Adresse ein.

Führen Sie die folgenden Schritte auf dem sekundären Knoten aus, um eine Server-Alias-IP-Adresse zu erstellen:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Fenster **Netzwerkschnittstelle** die Client-Schnittstelle (NIC0).
3. Geben Sie im Feld **Alias-IP-Bereich** die Server-Alias-IP-Adresse ein.

Nach dem Failover, wenn der alte primäre Knoten zum neuen sekundären Knoten wird, wird die Client-Alias-IP-Adresse vom alten primären Knoten verschoben und dem neuen primären Knoten zugewiesen.

Nachdem Sie die VPX-Instanzen konfiguriert haben, können Sie die virtuellen (VIP) und Subnetz-IP-Adressen (SNIP) konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von NetScaler-eigenen IP-Adressen.

### Schritt 3. Hochverfügbarkeit konfigurieren

Nachdem Sie die Instanzen auf der Google Cloud Platform erstellt haben, können Sie die Hochverfügbarkeit über die NetScaler-GUI oder CLI konfigurieren.

### Hochverfügbarkeit über die GUI konfigurieren

**Schritt 1**. Richten Sie die Hochverfügbarkeit im INC-Enabled-Modus auf beiden Knoten ein.

Führen Sie auf dem **primären Knoten** die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP-Konsole als Kennwort an.
2. Navigieren Sie zu **Configuration > System > High Availability > Nodes** und klicken Sie auf **Add**.
3. Geben Sie im Feld **Remote Node IP address** die private IP-Adresse der Management-NIC des sekundären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **INC (Independent Network Configuration) Modus auf dem eigenen Knoten aktivieren**.
5. Klicken Sie auf **Erstellen**.

Führen Sie auf dem **sekundären Knoten** die folgenden Schritte aus:

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

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens aus der GCP-Konsole als Kennwort an.
2. Navigieren Sie zu **Configuration > System > High Availability > Nodes**, und klicken Sie auf **Add**.
3. Geben Sie im Feld **Remote Node IP address** die private IP-Adresse der Management-NIC des primären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **INC (Independent Network Configuration) Modus auf dem eigenen Knoten aktivieren**.
5. Klicken Sie auf **Erstellen**.

Bevor Sie fortfahren, stellen Sie sicher, dass der Synchronisierungsstatus des sekundären Knotens auf der Seite **Nodes** als **SUCCESS** angezeigt wird.

**HINWEIS:**

Nachdem der sekundäre Knoten mit dem primären Knoten synchronisiert wurde, verfügt der sekundäre Knoten über dieselben Anmeldeinformationen wie der primäre Knoten.

**Schritt 2**. Fügen Sie die virtuelle IP-Adresse und die Subnetz-IP-Adresse auf beiden Knoten hinzu.

Führen Sie auf dem primären Knoten die folgenden Schritte aus:

1. Navigieren Sie zu **System > Network > IPs > IPv4s**, und klicken Sie auf **Add**.
2. So erstellen Sie eine Client-Alias-IP (VIP)-Adresse:
    a. Geben Sie die Client-Alias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz in der primären VM-Instanz konfiguriert sind.
    b. Wählen Sie im Feld **IP-Typ** im Dropdown-Menü **Virtuelle IP** aus.
    c. Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine Server-Alias-IP (SNIP)-Adresse:
    a. Geben Sie die Server-Alias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz in der primären VM-Instanz konfiguriert sind.
    b. Wählen Sie im Feld **IP-Typ** im Dropdown-Menü **Subnetz-IP** aus.
    c. Klicken Sie auf **Erstellen**.

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

Führen Sie auf dem sekundären Knoten die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. So erstellen Sie eine Client-Alias-IP (VIP)-Adresse:
   a. Geben Sie die Client-Alias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz der primären VM-Instanz konfiguriert sind.
   b. Wählen Sie im Feld **IP-Typ** im Dropdown-Menü **Virtuelle IP** aus.
   c. Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine Server-Alias-IP-Adresse (SNIP):
   a. Geben Sie die Server-Alias-IP-Adresse und die Netzmaske ein, die für das VPC-Subnetz der sekundären VM-Instanz konfiguriert sind.
   b. Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdown-Menü.
   c. Klicken Sie auf **Erstellen**.

**Schritt 3**. Fügen Sie einen virtuellen Lastausgleichsserver auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastausgleich > Virtuelle Server > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäre Client-Alias-IP-Adresse) und Port hinzu, und klicken Sie auf **OK**.

**Schritt 4**. Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastausgleich > Dienste > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Dienstname, IP-Adresse, Protokoll und Port hinzu, und klicken Sie auf **OK**.

**Schritt 5**. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastausgleich > Virtuelle Server**.

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

2. Wählen Sie den virtuellen Lastausgleichsserver aus, der in **Schritt 3** konfiguriert wurde, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **Service and Service Groups** auf **No Load Balancing Virtual Server Service Binding**.
4. Wählen Sie den in **Schritt 4** konfigurierten Dienst aus und klicken Sie auf **Bind**.

**Schritt 6**. Speichern Sie die Konfiguration.

Nach einem erzwungenen Failover wird der sekundäre Knoten zum neuen primären Knoten. Die Client-Alias-IP (VIP) vom alten primären Knoten wird auf den neuen primären Knoten verschoben.

### Hochverfügbarkeit mit der CLI konfigurieren

**Schritt 1**. Richten Sie Hochverfügbarkeit im Modus **INC Enabled** auf beiden Instanzen mithilfe der NetScaler CLI ein.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

```
add ha node 1 <sec_ip> -inc ENABLED
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
add ha node 1 <prim_ip> -inc ENABLED
```

Die `sec_ip` bezieht sich auf die interne IP-Adresse der Management-NIC des sekundären Knotens.

Die `prim_ip` bezieht sich auf die interne IP-Adresse der Management-NIC des primären Knotens.

**Schritt 2**. Fügen Sie VIP und SNIP auf primären und sekundären Knoten hinzu.

Geben Sie die folgenden Befehle auf dem primären Knoten ein:

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

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

**HINWEIS:**

Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.

```
add ns ip <primary_server_alias_ip> <subnet> -type SNIP
```

Geben Sie die folgenden Befehle auf dem sekundären Knoten ein:

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

**HINWEIS:**

Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.

```
add ns ip <secondary_server_alias_ip> <subnet> -type SNIP
```

**HINWEIS:**

Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Server-Subnetz in der VM-Instanz konfiguriert sind.

**Schritt 3**. Fügen Sie einen virtuellen Server auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
add <server_type> vserver <vserver_name> <protocol>
<primary_client_alias_ip> <port>
```

**Schritt 4**. Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
add service <service_name> <service_ip_address> <protocol> <port>
```

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

**Schritt 5**. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

Geben Sie den folgenden Befehl ein:

```
bind <server_type> vserver <vserver_name> <service_name>
```

**HINWEIS:**

Um Ihre Konfiguration zu speichern, geben Sie den Befehl `save config` ein. Andernfalls gehen die Konfigurationen nach dem Neustart der Instanzen verloren.

# Bereitstellen eines VPX-Hochverfügbarkeitspaares mit privater IP-Adresse auf Google Cloud Platform

Sie können ein VPX-Hochverfügbarkeitspaar auf GCP mithilfe einer privaten IP-Adresse bereitstellen. Die Client-IP (VIP) muss als Alias-IP-Adresse auf dem primären Knoten konfiguriert werden. Beim Failover wird die Client-IP-Adresse auf den sekundären Knoten verschoben, damit der Datenverkehr wieder aufgenommen werden kann.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit.

## Bevor Sie beginnen

- Lesen Sie die Einschränkungen, Hardwareanforderungen und Hinweise, die unter Bereitstellen einer NetScaler VPX-Instanz auf Google Cloud Platform erwähnt werden. Diese Informationen gelten auch für Hochverfügbarkeitsbereitstellungen.
- Aktivieren Sie die **Cloud Resource Manager API** für Ihr GCP-Projekt.
- Ermöglichen Sie vollen Zugriff auf alle Cloud-APIs beim Erstellen der Instanzen.
- Stellen Sie sicher, dass Ihr GCP-Dienstkonto die folgenden IAM-Berechtigungen besitzt:

```
REQUIRED_INSTANCE_IAM_PERMS = [

"compute.forwardingRules.list",

"compute.forwardingRules.setTarget",

"compute.instances.setMetadata",
```

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

```
"compute.instances.get",

"compute.instances.list",

"compute.instances.updateNetworkInterface",

"compute.targetInstances.list",

"compute.targetInstances.use",

"compute.targetInstances.create",

"compute.zones.list",

"compute.zoneOperations.get",

]
```

- Wenn Sie externe IP-Adressen auf einer anderen Schnittstelle als der Verwaltungsschnittstelle konfiguriert haben, stellen Sie sicher, dass Ihr GCP-Dienstkonto die folgenden zusätzlichen IAM-Berechtigungen besitzt:

```
REQUIRED_INSTANCE_IAM_PERMS = [

"compute.addresses.use"

"compute.instances.addAccessConfig",

"compute.instances.deleteAccessConfig",

"compute.networks.useExternalIp",

"compute.subnetworks.useExternalIp",

]
```

- Wenn Ihre VMs keinen Internetzugang haben, müssen Sie den **privaten Google-Zugriff** im Verwaltungs-Subnetz aktivieren.

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

- Wenn Sie GCP-Weiterleitungsregeln auf dem primären Knoten konfiguriert haben, lesen Sie die Einschränkungen und Anforderungen, die unter Unterstützung von Weiterleitungsregeln für VPX-Hochverfügbarkeitspaar auf GCP erwähnt sind, um sie beim Failover auf den neuen primären Knoten zu aktualisieren.

## So stellen Sie ein VPX-Hochverfügbarkeitspaar auf Google Cloud Platform bereit

Hier ist eine Zusammenfassung der Schritte zur Bereitstellung der Hochverfügbarkeit:

1. Erstellen Sie VPC-Netzwerke in derselben Region. Zum Beispiel Asien-Ost.
2. Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) in derselben Region. Sie können sich in derselben Zone oder in verschiedenen Zonen befinden. Zum Beispiel Asien-Ost-1a und Asien-Ost-1b.
3. Konfigurieren Sie Hochverfügbarkeitseinstellungen auf beiden Instanzen mithilfe der NetScaler-GUI oder der ADC-CLI-Befehle.

### Schritt 1. VPC-Netzwerke erstellen

Erstellen Sie VPC-Netzwerke basierend auf Ihren Anforderungen. Citrix® empfiehlt Ihnen, drei VPC-Netzwerke für die Zuordnung mit der Management-NIC, der Client-NIC und der Server-NIC zu erstellen.

Führen Sie die folgenden Schritte aus, um ein VPC-Netzwerk zu erstellen:

1. Melden Sie sich bei der **Google Console > Networking > VPC network > Create VPC Network** an.
2. Füllen Sie die erforderlichen Felder aus und klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie im Abschnitt **VPC-Netzwerke erstellen** unter Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform.

### Schritt 2. Zwei VPX-Instanzen erstellen

Erstellen Sie zwei VPX-Instanzen, indem Sie die Schritte unter Szenario: Bereitstellen einer eigenständigen VPX-Instanz mit mehreren NICs und mehreren IPs befolgen.

**WICHTIG:**

Weisen Sie dem primären Knoten eine Client-Alias-IP-Adresse zu. Verwenden Sie nicht die interne IP-Adresse der VPX-Instanz, um die VIP zu konfigurieren.

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

Führen Sie die folgenden Schritte aus, um eine Client-Alias-IP-Adresse zu erstellen:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Fenster **Netzwerkschnittstelle** die Client-Schnittstelle.
3. Geben Sie im Feld **Alias-IP-Bereich** die Client-Alias-IP-Adresse ein.

Nach dem Failover, wenn der alte primäre Knoten zum neuen sekundären Knoten wird, werden die Alias-IP-Adressen vom alten primären Knoten verschoben und dem neuen primären Knoten zugewiesen.

Nachdem Sie die VPX-Instanzen konfiguriert haben, können Sie die virtuellen (VIP) und Subnetz-IP-Adressen (SNIP) konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von NetScaler-eigenen IP-Adressen.

### Schritt 3. Hochverfügbarkeit konfigurieren

Nachdem Sie die Instanzen auf der Google Cloud Platform erstellt haben, können Sie die Hochverfügbarkeit über die NetScaler GUI oder CLI konfigurieren.

### Hochverfügbarkeit über die GUI konfigurieren

**Schritt 1**. Richten Sie Hochverfügbarkeit im INC-aktivierten Modus auf beiden Knoten ein.

Führen Sie auf dem **primären Knoten** die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens aus der GCP-Konsole als Kennwort an.
2. Navigieren Sie zu **Configuration > System > High Availability > Nodes** und klicken Sie auf **Add**.
3. Geben Sie im Feld **Remote Node IP address** die private IP-Adresse der Management-NIC des sekundären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Turn on INC (Independent Network Configuration) mode on self node**.
5. Klicken Sie auf **Create**.

Führen Sie auf dem **sekundären Knoten** die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens aus der GCP-Konsole als Kennwort an.

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

2. Navigieren Sie zu **Configuration > System > High Availability > Nodes**, und klicken Sie auf **Add**.
3. Geben Sie im Feld **Remote Node IP address** die private IP-Adresse der Management-NIC des primären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Turn on INC (Independent Network Configuration) mode on self node**.
5. Klicken Sie auf **Create**.

Bevor Sie fortfahren, stellen Sie sicher, dass der Synchronisierungsstatus des sekundären Knotens auf der Seite **Nodes** als **SUCCESS** angezeigt wird.

**HINWEIS:**

Nachdem der sekundäre Knoten mit dem primären Knoten synchronisiert wurde, verfügt der sekundäre Knoten über dieselben Anmeldeinformationen wie der primäre Knoten.

**Schritt 2**. Fügen Sie auf beiden Knoten eine virtuelle IP-Adresse und eine Subnetz-IP-Adresse hinzu.

Führen Sie auf dem primären Knoten die folgenden Schritte aus:

1. Navigieren Sie zu **System > Network > IPs > IPv4s**, und klicken Sie auf **Add**.
2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):
    a. Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.
    b. Wählen Sie im Feld **IP Type** aus dem Dropdown-Menü **Virtual IP** aus.
    c. Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine Server-IP-Adresse (SNIP):
    a. Geben Sie die interne IP-Adresse der serverseitigen Schnittstelle der primären Instanz und die für das Server-Subnetz konfigurierte Netzmaske ein.
    b. Wählen Sie im Feld **IP-Typ** im Dropdown-Menü die Option **Subnetz-IP** aus.
    c. Klicken Sie auf **Erstellen**.

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

Führen Sie auf dem sekundären Knoten die folgenden Schritte aus:

1. Navigieren Sie zu **System > Network > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):
   a. Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz auf der primären VM-Instanz konfiguriert sind.
   b. Wählen Sie im Feld **IP-Typ** im Dropdown-Menü die Option **Subnetz-IP** aus.
   c. Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine Server-IP-Adresse (SNIP):
   a. Geben Sie die interne IP-Adresse der serverseitigen Schnittstelle der sekundären Instanz und die für das Server-Subnetz konfigurierte Netzmaske ein.
   b. Wählen Sie im Feld **IP-Typ** im Dropdown-Menü die Option **Subnetz-IP** aus.
   c. Klicken Sie auf **Erstellen**.

**Schritt 3**. Fügen Sie einen virtuellen Lastausgleichsserver auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäre Client-Alias-IP-Adresse) und Port hinzu, und klicken Sie auf **OK**.

**Schritt 4**. Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Dienste > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Dienstname, IP-Adresse, Protokoll und Port hinzu, und klicken Sie auf **OK**.

**Schritt 5**. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.

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

2. Wählen Sie den in **Schritt 3** konfigurierten virtuellen Lastausgleichsserver aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **Dienst- und Dienstgruppen** auf **Keine Bindung des virtuellen Lastausgleichsserverdienstes**.
4. Wählen Sie den in **Schritt 4** konfigurierten Dienst aus, und klicken Sie auf **Binden**.

**Schritt 5**. Speichern Sie die Konfiguration.

Nach einem erzwungenen Failover wird der sekundäre Knoten zum neuen primären Knoten. Die Client-Alias-IP (VIP) und die Server-Alias-IP (SNIP) vom alten primären Knoten werden auf den neuen primären Knoten verschoben.

### Hochverfügbarkeit mithilfe der CLI konfigurieren

**Schritt 1**. Richten Sie Hochverfügbarkeit im Modus **INC Enabled** in beiden Instanzen mithilfe der NetScaler-CLI ein.

Auf dem primären Knoten geben Sie den folgenden Befehl ein.

```
add ha node 1 <sec_ip> -inc ENABLED
```

Auf dem sekundären Knoten geben Sie den folgenden Befehl ein.

```
add ha node 1 <prim_ip> -inc ENABLED
```

`sec_ip` bezieht sich auf die interne IP-Adresse der Management-NIC des sekundären Knotens.

`prim_ip` bezieht sich auf die interne IP-Adresse der Management-NIC des primären Knotens.

**Schritt 2**. Fügen Sie VIP und SNIP auf beiden Knoten hinzu.

Geben Sie die folgenden Befehle auf dem primären Knoten ein:

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

**HINWEIS:**

Geben Sie die Alias-IP-Adresse und Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.

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

```
add ns ip <primary_snip> <subnet> -type SNIP
```

`primary_snip` bezieht sich auf die interne IP-Adresse der serverseitigen Schnittstelle der primären Instanz.

Geben Sie die folgenden Befehle auf dem sekundären Knoten ein:

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
```

**HINWEIS:**

Geben Sie die Alias-IP-Adresse und Netzmaske ein, die für das Client-Subnetz auf der primären VM-Instanz konfiguriert sind.

```
add ns ip <secondary_snip> <subnet> -type SNIP
```

Der `secondary_snip` bezieht sich auf die interne IP-Adresse der serverorientierten Schnittstelle der sekundären Instanz.

**HINWEIS:**

Geben Sie die IP-Adresse und Netzmaske ein, die für das Server-Subnetz in der VM-Instanz konfiguriert sind.

**Schritt 3**. Fügen Sie einen virtuellen Server auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
add <server_type> vserver <vserver_name> <protocol>
<primary_client_alias_ip> <port>
```

**Schritt 4**. Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
add service <service_name> <service_ip_address> <protocol> <port>
```

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

**Schritt 5**. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

Geben Sie den folgenden Befehl ein:

```
bind <server_type> vserver <vserver_name> <service_name>
```

**HINWEIS:**

Um Ihre Konfiguration zu speichern, geben Sie den Befehl `save config` ein. Andernfalls gehen die Konfigurationen nach dem Neustart der Instanzen verloren.

# Installieren einer NetScaler VPX-Instanz auf Google Cloud VMware Engine

Google Cloud VMware Engine (GCVE) stellt Ihnen private Clouds zur Verfügung, die vSphere-Cluster enthalten, die auf dedizierter Bare-Metal-Infrastruktur der Google Cloud Platform basieren. Die minimale Ersteinrichtung umfasst drei Hosts, aber zusätzliche Hosts können einzeln hinzugefügt werden. Alle bereitgestellten privaten Clouds verfügen über vCenter Server, vSAN, vSphere und NSX-T.

GCVE ermöglicht Ihnen die Erstellung von Cloud-Software-Defined Data Centern (SDDC) auf der Google Cloud Platform mit der gewünschten Anzahl von ESX-Hosts. GCVE unterstützt NetScaler VPX-Bereitstellungen. GCVE bietet eine Benutzeroberfläche, die der von On-Prem-vCenter gleicht. Es funktioniert identisch mit den ESX-basierten NetScaler VPX-Bereitstellungen.

Das folgende Diagramm zeigt die GCVE auf der Google Cloud Platform, auf die ein Administrator oder ein Client über das Internet zugreifen kann. Ein Administrator kann Workload- oder Server-VMs mit GCVE erstellen, verwalten und konfigurieren. Der Administrator kann über eine OpenVPN-Verbindung auf das webbasierte vCenter und den NSX-T Manager von GCVE zugreifen. Sie können die NetScaler VPX-Instanzen (Standalone oder HA-Paar) und Server-VMs innerhalb von GCVE mit vCenter erstellen und die entsprechende Netzwerkkonfiguration mit dem NSX-T Manager verwalten. Die NetScaler VPX-Instanz auf GCVE funktioniert ähnlich wie der lokale VMware-Host-Cluster. GCVE kann über eine OpenVPN-Verbindung zur Management-Infrastruktur verwaltet werden.

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

## Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, führen Sie die folgenden Schritte aus:

- Weitere Informationen zu Google Cloud VMware Engine und seinen Voraussetzungen finden Sie in der Google Cloud VMware Engine-Dokumentation.
- Weitere Informationen zur Bereitstellung von Google Cloud VMware Engine finden Sie unter Bereitstellen einer privaten Google Cloud VMware Engine-Cloud.
- Weitere Informationen zum Herstellen einer Verbindung zu Ihrer privaten Cloud über ein Point-to-Site-VPN-Gateway, um auf Google Cloud VMware Engine zuzugreifen und diese zu verwalten, finden Sie unter Zugriff auf eine private Google Cloud VMware Engine-Cloud.
- Laden Sie auf dem VPN-Client-Computer die Setup-Dateien der NetScaler VPX-Appliance herunter.
- Erstellen Sie entsprechende NSX-T-Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden. Weitere Informationen finden Sie unter Hinzufügen eines Netzwerksegments in Google Cloud VMware Engine.
- Beschaffen Sie VPX-Lizenzdateien. Weitere Informationen zu NetScaler VPX-Instanzlizenzen finden Sie unter Lizenzübersicht.
- Virtuelle Maschinen (VMs), die in der privaten GCVE-Cloud erstellt oder dorthin migriert wurden, müssen an ein Netzwerksegment angehängt werden.

## Hardwareanforderungen für VMware Cloud

Die folgende Tabelle listet die virtuellen Computerressourcen auf, die das VMware SDDC für jede virtuelle VPX nCore Appliance bereitstellen muss.

Tabelle 1. Mindestressourcen für virtuelle Computer, die zum Ausführen einer NetScaler VPX-Instanz erforderlich sind

| KOMPONENTE | ANFORDERUNG |
|---|---|
| Arbeitsspeicher | 2 GB |
| Virtuelle CPU (vCPU) | 2 |
| Virtuelle Netzwerkschnittstellen | Im VMware SDDC können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, |

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

| KOMPONENTE | ANFORDERUNG |
| --- | --- |
| | wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird. |
| Festplattenspeicher | 20 GB |

**HINWEIS:**

Dies gilt zusätzlich zu allen Festplattenanforderungen für den Hypervisor.

Für den Produktionseinsatz der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden.

## OVF Tool 1.0 Systemanforderungen

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. Die folgende Tabelle beschreibt die Mindestsystemanforderungen für die Installation des OVF Tools.

Tabelle 2. Mindestsystemanforderungen für die OVF Tool-Installation

| KOMPONENTE | ANFORDERUNG |
| --- | --- |
| Betriebssystem | Detaillierte Anforderungen von VMware finden Sie in der PDF-Datei „OVF Tool User Guide“ unter `<http://kb.vmware.com/>`. |
| CPU | Mindestens 750 MHz, 1 GHz oder schneller empfohlen |
| RAM | Mindestens 1 GB, 2 GB empfohlen |
| NIC | 100 Mbit/s oder schnellere NIC |

Informationen zur Installation von OVF finden Sie in der PDF-Datei „OVF Tool User Guide“ unter `<http://kb.vmware.com/>`.

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

## Herunterladen der NetScaler VPX-Setup-Dateien

Das NetScaler VPX-Instanz-Setup-Paket für VMware ESX folgt dem Open Virtual Machine (OVF)-Formatstandard. Sie können die Dateien von der Citrix-Website herunterladen. Sie benötigen ein Citrix-Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.com auf. Klicken Sie auf den Link **New Users** und folgen Sie den Anweisungen, um ein neues Citrix-Konto zu erstellen.

Nach der Anmeldung navigieren Sie auf der Citrix®-Startseite zum folgenden Pfad:

Citrix.com > **Downloads > NetScaler > Virtual Appliances**.

Kopieren Sie die folgenden Dateien auf eine Workstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX-\<release number\>-\<build number\>-disk1.vmdk (zum Beispiel NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX-\<release number\>-\<build number\>.ovf (zum Beispiel NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX-\<release number\>-\<build number\>.mf (zum Beispiel NSVPX-ESX-13.0-79.64.mf)

## Google Cloud VMware Engine bereitstellen

1. Melden Sie sich bei Ihrem GCVE-Portal an und navigieren Sie zu **Home**.

2. Geben Sie auf der Seite **New Private Cloud** die folgenden Details ein:

   - Wählen Sie mindestens 3 ESXi-Hosts aus, um den Standardcluster Ihrer privaten Cloud zu erstellen.
   - Verwenden Sie für das Feld **vSphere/vSan subnet CIDR range** einen /22-Adressbereich.
   - Verwenden Sie für das Feld **HCX Deployment Network CIDR range** einen /26-Adressbereich.
   - Stellen Sie für das virtuelle Netzwerk sicher, dass der CIDR-Bereich keine Überschneidungen mit Ihren lokalen oder anderen GCP-Subnetzen (virtuellen Netzwerken) aufweist.

3. Klicken Sie auf **Überprüfen und erstellen**.

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

4. Überprüfen Sie die Einstellungen. Wenn Sie Einstellungen ändern müssen, klicken Sie auf **Zurück**.

5. Klicken Sie auf **Erstellen**. Der Bereitstellungsprozess der privaten Cloud beginnt. Es kann bis zu zwei Stunden dauern, bis die private Cloud bereitgestellt ist.
6. Gehen Sie zu **Ressourcen**, um die erstellte private Cloud zu überprüfen.

7. Um auf diese Ressource zuzugreifen, müssen Sie über ein Point-to-Site-VPN eine Verbindung zu GCVE herstellen. Weitere Informationen finden Sie in der folgenden Dokumentation:

   - VPN-Gateways
   - Verbindung über VPN herstellen

## Zugriff auf Ihr Private Cloud vCenter-Portal

1. Navigieren Sie zu Ihrer Google Cloud VMware Engine Private Cloud. Klicken Sie auf der Registerkarte **ZUSAMMENFASSUNG** unter **vCenter-Anmeldeinformationen** auf **Anzeigen**.

2. Notieren Sie sich die vCenter-Anmeldeinformationen.

3. Starten Sie den vSphere-Client, indem Sie auf **LAUNCH VSPHERE CLIENT** klicken oder zu **VSPHERE MANAGEMENT NETWORK** navigieren und auf den FQDN der **vCenter Server Appliance** klicken.

4. Melden Sie sich bei VMware vSphere mit den vCenter-Anmeldeinformationen an, die in Schritt 2 dieses Verfahrens vermerkt sind.

5. Im vSphere-Client können Sie die ESXi-Hosts überprüfen, die Sie im GCVE-Portal erstellt haben.

## Ein NSX-T-Segment im GCVE NSX-T-Portal erstellen

Sie können ein NSX-T-Segment über den NSX Manager in der Google Cloud VMware Engine-Konsole erstellen und konfigurieren. Diese Segmente sind mit dem Standard-Tier-1-Gateway

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

verbunden, und die Workloads auf diesen Segmenten erhalten Ost-West- und Nord-Süd-Konnektivität. Sobald Sie das Segment erstellt haben, wird es in vCenter angezeigt.

1. Wählen Sie in Ihrer privaten GCVE-Cloud unter **Summary -> NSX-T login info** die Option **View**.

2. Notieren Sie sich die NSX-T-Anmeldeinformationen.

3. Starten Sie den NSX Manager, indem Sie zu **VSPHERE MANAGEMENT NETWORK** navigieren und auf den FQDN des **NSX Manager** klicken.

4. Melden Sie sich beim NSX Manager mit den Anmeldeinformationen an, die in Schritt 2 dieses Verfahrens vermerkt sind.

5. Richten Sie den DHCP-Dienst für die neuen Segmente oder Subnetze ein.
6. Bevor Sie ein Subnetz erstellen können, richten Sie einen DHCP-Dienst ein.
7. Gehen Sie in NSX-T zu **Networking > DHCP**. Das Netzwerk-Dashboard zeigt an, dass der Dienst ein Tier-0- und ein Tier-1-Gateway erstellt.
8. Um mit der Bereitstellung eines DHCP-Servers zu beginnen, klicken Sie auf **Add DHCP Profile**.
9. Geben Sie im Feld DHCP-Name einen Namen für das **Client-Management**-Profil ein.
10. Wählen Sie **DHCP server** als Profiltyp aus.
11. Geben Sie in der Spalte **Server IP address** einen IP-Adressbereich für den DHCP-Dienst an.
12. Wählen Sie Ihren **Edge Cluster** aus.
13. Klicken Sie auf **Save**, um den DHCP-Dienst zu erstellen.

14. Wiederholen Sie die Schritte 6 bis 13 für den Server-DHCP-Bereich.

15. Erstellen Sie zwei separate Segmente: eines für Client- und Management-Schnittstellen und ein weiteres für Server-Schnittstellen.
16. Gehen Sie in NSX-T zu **Networking > Segments**.
17. Klicken Sie auf **Segment hinzufügen**.

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

18. Geben Sie im Feld **Segmentname** einen Namen für Ihr **Client-Management**-Segment ein.
19. Wählen Sie in der Liste **Verbundenes Gateway** die Option **Tier1** aus, um eine Verbindung zum Tier-1-Gateway herzustellen.
20. Wählen Sie in der Liste **Transportzone** die Option **TZ-OVERLAY | Overlay** aus.
21. Geben Sie in der Spalte **Subnetze** den Subnetzbereich ein. Geben Sie den Subnetzbereich mit `.1` als letztem Oktett an. Zum Beispiel 10.12.2.1/24.
22. Klicken Sie auf **DHCP-Konfiguration festlegen** und geben Sie Werte für das Feld **DHCP-Bereiche** an.
23. Klicken Sie auf **Übernehmen**, um Ihre DHCP-Konfiguration zu speichern.
24. Klicken Sie auf **Speichern**.
25. Wiederholen Sie die Schritte 17 bis 24 auch für das Server-Segment.
26. Sie können diese Netzwerksegmente nun in vCenter auswählen, wenn Sie eine VM erstellen.

Weitere Informationen finden Sie unter Ihr erstes Subnetz erstellen.

## Installieren einer NetScaler VPX-Instanz in der VMware Cloud

Nachdem Sie Private Cloud auf GCVE installiert und konfiguriert haben, können Sie vCenter verwenden, um virtuelle Appliances auf der VMware Engine zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge der auf der Private Cloud verfügbaren Ressourcen ab.

Um NetScaler VPX-Instanzen in der Private Cloud zu installieren, führen Sie diese Schritte auf einem Desktop aus, der mit einem Private Cloud Point-to-Site-VPN verbunden ist:

1. Laden Sie die NetScaler VPX-Instanz-Setup-Dateien für den ESXi-Host von der NetScaler-Download-Website herunter.
2. Öffnen Sie VMware vCenter in einem Browser, der mit Ihrem Private Cloud Point-to-Site-VPN verbunden ist.
3. Geben Sie in den Feldern **Benutzername** und **Passwort** die Administratoranmeldeinformationen ein und klicken Sie dann auf **Anmelden**.

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

4. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
5. Navigieren Sie im Dialogfeld **OVF-Vorlage bereitstellen** im Feld **Aus Datei bereitstellen** zu dem Speicherort, an dem Sie die NetScaler VPX-Instanz-Setup-Dateien gespeichert haben, wählen Sie die .ovf-Datei aus und klicken Sie auf **Weiter**.

   **HINWEIS:**

   Standardmäßig verwendet die NetScaler VPX-Instanz E1000-Netzwerkschnittstellen. Um ADC mit der VMXNET3-Schnittstelle bereitzustellen, ändern Sie die OVF so, dass sie die VMXNET3-Schnittstelle anstelle von E1000 verwendet. Die Verfügbarkeit der VMXNET3-Schnittstelle ist durch die GCP-Infrastruktur begrenzt und möglicherweise in Google Cloud VMware Engine nicht verfügbar.

6. Ordnen Sie die in der OVF-Vorlage der virtuellen Appliance angezeigten Netzwerke den Netzwerken zu, die Sie im NSX-T Manager konfiguriert haben. Klicken Sie auf **OK**.

7. Klicken Sie auf **Fertig stellen**, um die Installation einer virtuellen Appliance in der VMware Cloud zu starten.

8. Sie können die NetScaler VPX-Instanz nun starten. Wählen Sie im Navigationsbereich die installierte NetScaler VPX-Instanz aus und wählen Sie im Kontextmenü **Power On**. Klicken Sie auf die Registerkarte **Launch Web Console**, um einen Konsolenport zu emulieren.

9. Sie sind jetzt über den vSphere-Client mit der NetScaler VM verbunden.

10. Beim ersten Start legen Sie die Verwaltungs-IP und das Gateway für die ADC-Instanz fest.

11. Um auf die NetScaler Appliance mithilfe der SSH-Schlüssel zuzugreifen, geben Sie den folgenden Befehl in der CLI ein:

    ```
    ssh nsroot@<management IP address>
    ```

    **Beispiel:**

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

```
ssh nsroot@10.230.1.10
```

12. Sie können die ADC-Konfiguration mit dem Befehl `show ns ip` überprüfen.

## Einer NetScaler VPX-Instanz in der VMware Cloud eine öffentliche IP-Adresse zuweisen

Nachdem Sie die NetScaler VPX-Instanz auf GCVE installiert und konfiguriert haben, müssen Sie der Client-Schnittstelle eine öffentliche IP-Adresse zuweisen. Bevor Sie Ihren VMs öffentliche IP-Adressen zuweisen, stellen Sie sicher, dass der Public IP-Dienst für Ihre Google Cloud-Region aktiviert ist.

Um den Public IP-Dienst für eine neue Region zu aktivieren, führen Sie die folgenden Schritte aus:

1. Wechseln Sie in der GCVE-Konsole zu **Network > REGIONAL SETTINGS > Add Region**.

2. Wählen Sie Ihre Region aus und aktivieren Sie **Internetzugang** und **Öffentlicher IP-Dienst**.
3. Weisen Sie eine Edge Services CIDR zu und stellen Sie sicher, dass der CIDR-Bereich sich nicht mit Ihren lokalen oder anderen GCP/GCVE-Subnetzen (virtuellen Netzwerken) überschneidet.

4. Der öffentliche IP-Dienst wird für die ausgewählte Region in wenigen Minuten aktiviert.

Um der Client-Schnittstelle auf der NetScaler VPX-Instanz in GCVE eine öffentliche IP zuzuweisen, führen Sie diese Schritte im GCVE-Portal aus:

1. Navigieren Sie in der GCVE-Konsole zu **Netzwerk > ÖFFENTLICHE IPS > Zuweisen**.

2. Geben Sie einen Namen für die öffentliche IP ein. Wählen Sie Ihre Region und die private Cloud aus, in der die IP verwendet werden soll.
3. Geben Sie die private IP für die Schnittstelle an, der Sie die öffentliche IP zuordnen möchten. Dies ist die **private IP** für Ihre **Client**-Schnittstelle.
4. Klicken Sie auf **Senden**.

5. Die öffentliche IP ist in wenigen Minuten einsatzbereit.

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

6. Sie müssen Firewallregeln hinzufügen, um den Zugriff auf die öffentliche IP zu ermöglichen, bevor Sie sie verwenden können. Weitere Informationen finden Sie unter Firewallregeln.

# Backend-GCP-Autoscaling-Dienst hinzufügen

Ein effizientes Hosting von Anwendungen in einer Cloud erfordert eine einfache und kostengünstige Verwaltung von Ressourcen, je nach Anwendungsbedarf. Um der steigenden Nachfrage gerecht zu werden, müssen Sie Netzwerkressourcen nach oben skalieren. Wenn die Nachfrage nachlässt, müssen Sie die Skalierung reduzieren, um unnötige Kosten für nicht ausgelastete Ressourcen zu vermeiden. Um die Kosten für den Betrieb der Anwendung zu minimieren, müssen Sie ständig den Datenverkehr, die Speicher- und CPU-Auslastung usw. überwachen. Die manuelle Überwachung des Datenverkehrs ist jedoch umständlich. Damit die Anwendungsumgebung dynamisch hoch- oder herunterskaliert werden kann, müssen Sie die Prozesse der Datenverkehrsüberwachung und der bedarfsweisen Skalierung von Ressourcen automatisieren.

Integriert in den GCP Autoscaling-Dienst bietet die NetScaler VPX-Instanz die folgenden Vorteile:

- **Lastverteilung und -verwaltung**: Konfiguriert Server automatisch für die Skalierung nach oben und unten, je nach Bedarf. Die VPX-Instanz erkennt automatisch verwaltete Instanzgruppen im Backend-Subnetz und ermöglicht Ihnen die Auswahl der verwalteten Instanzgruppen zur Lastverteilung. Die virtuellen IP-Adressen und Subnetz-IP-Adressen werden automatisch auf der VPX-Instanz konfiguriert.
- **Hohe Verfügbarkeit**: Erkennt verwaltete Instanzgruppen, die sich über mehrere Zonen erstrecken, und verteilt die Last auf Server.
- **Bessere Netzwerkverfügbarkeit**: Die VPX-Instanz unterstützt:
  - Backend-Server in denselben Platzierungsgruppen
  - Backend-Server in verschiedenen Zonen

Dieses Diagramm veranschaulicht, wie der GCP Autoscaling-Dienst in einer NetScaler VPX-Instanz funktioniert, die als virtueller Lastverteilungsserver fungiert.

## Bevor Sie beginnen

Bevor Sie Autoscaling mit Ihrer NetScaler VPX-Instanz verwenden, müssen Sie die folgenden Aufgaben erledigen.

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

- Erstellen Sie eine NetScaler VPX-Instanz in GCP entsprechend Ihren Anforderungen.
  - Weitere Informationen zum Erstellen einer NetScaler VPX-Instanz finden Sie unter Bereitstellen einer NetScaler VPX-Instanz auf der Google Cloud Platform.
  - Weitere Informationen zur Bereitstellung von VPX-Instanzen im HA-Modus finden Sie unter Bereitstellen eines VPX-Hochverfügbarkeitspaares auf der Google Cloud Platform.
- Aktivieren Sie die **Cloud Resource Manager API** für Ihr GCP-Projekt.
- Ermöglichen Sie vollen Zugriff auf alle Cloud-APIs während der Erstellung der Instanzen.
- Stellen Sie sicher, dass Ihr GCP-Dienstkonto die folgenden IAM-Berechtigungen besitzt:

```
REQUIRED_INSTANCE_IAM_PERMS = [

"compute.instances.get",

"compute.instanceGroupManagers.get",

"compute.instanceGroupManagers.list",

"compute.zones.list",

"logging.sinks.create",

"logging.sinks.delete",

"logging.sinks.get",

"logging.sinks.list",

"logging.sinks.update",

"pubsub.subscriptions.consume",

"pubsub.subscriptions.create",

"pubsub.subscriptions.delete",

"pubsub.subscriptions.get",

"pubsub.topics.attachSubscription",
```

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

```
"pubsub.topics.create",

"pubsub.topics.delete",

"pubsub.topics.get",

"pubsub.topics.getIamPolicy",

"pubsub.topics.setIamPolicy",

]
```

- Um die Autoskalierung einzurichten, stellen Sie sicher, dass Folgendes konfiguriert ist:
  - Instanzvorlage
  - Verwaltete Instanzgruppe
  - Autoskalierungsrichtlinie

## Hinzufügen des GCP-Autoskalierungsdienstes zu einer NetScaler VPX-Instanz

Sie können den Autoskalierungsdienst mit einem einzigen Klick über die GUI zu einer VPX-Instanz hinzufügen. Führen Sie die folgenden Schritte aus, um den Autoskalierungsdienst zur VPX-Instanz hinzuzufügen:

1. Melden Sie sich mit Ihren Anmeldeinformationen für `nsroot` bei der VPX-Instanz an.
2. Wenn Sie sich zum ersten Mal bei der NetScaler VPX-Instanz anmelden, wird die Standardseite für das Cloud-Profil angezeigt. Wählen Sie die verwaltete GCP-Instanzgruppe aus dem Dropdown-Menü aus und klicken Sie auf **Erstellen**, um ein Cloud-Profil zu erstellen.

   - Das Feld **IP-Adresse des virtuellen Servers** wird automatisch mit allen IP-Adressen ausgefüllt, die den Instanzen zugeordnet sind.
   - Die **Autoscale™-Gruppe** wird vorab aus der verwalteten Instanzgruppe ausgefüllt, die in Ihrem GCP-Konto konfiguriert ist.
   - Bei der Auswahl des **Autoscale-Gruppenprotokolls** und des **Autoscale-Gruppenports** stellen Sie sicher, dass Ihre Server auf dem konfigurierten Protokoll und den Ports lauschen. Binden Sie den richtigen Monitor in der Dienstgruppe. Standardmäßig wird der TCP-Monitor verwendet.

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

- Deaktivieren Sie das Kontrollkästchen **Graceful**, da es nicht unterstützt wird.

**HINWEIS:**

Bei der Autoskalierung des SSL-Protokolltyps ist der virtuelle Lastausgleichsserver oder die Dienstgruppe nach dem Erstellen des Cloud-Profils aufgrund eines fehlenden Zertifikats ausgefallen. Sie können das Zertifikat manuell an den virtuellen Server oder die Dienstgruppe binden.

3. Wenn Sie nach der ersten Anmeldung ein Cloud-Profil erstellen möchten, gehen Sie in der GUI zu **System > Google Cloud Platform > Cloud Profile** und klicken Sie auf **Add**.

   Die Konfigurationsseite **Create Cloud Profile** wird angezeigt.

   Cloud Profile erstellt einen virtuellen NetScaler-Lastausgleichsserver und eine Dienstgruppe mit den Servern der verwalteten Instanzgruppe als Mitglieder. Ihre Back-End-Server müssen über die auf der VPX-Instanz konfigurierte SNIP erreichbar sein.

   **HINWEIS:**

   Ab NetScaler Release 13.1-42.x können Sie verschiedene Cloud-Profile für verschiedene Dienste (unter Verwendung unterschiedlicher Ports) mit derselben verwalteten Instanzgruppe in GCP erstellen. Somit unterstützt die NetScaler VPX-Instanz mehrere Dienste mit derselben Autoscaling-Gruppe in der Public Cloud.

## VIP-Skalierungsunterstützung für NetScaler VPX-Instanz auf GCP

Eine NetScaler-Appliance befindet sich zwischen den Clients und den Servern, sodass Client-Anfragen und Server-Antworten diese passieren. In einer typischen Installation stellen auf der Appliance konfigurierte virtuelle Server Verbindungspunkte bereit, die Clients verwenden, um auf die Anwendungen hinter der Appliance zuzugreifen. Die Anzahl der für eine Bereitstellung benötigten öffentlichen virtuellen IP (VIP)-Adressen variiert von Fall zu Fall.

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

Die GCP-Architektur beschränkt jede Schnittstelle der Instanz darauf, mit einer anderen VPC verbunden zu sein. Eine VPC auf GCP ist eine Sammlung von Subnetzen, und jedes Subnetz kann sich über Zonen einer Region erstrecken. Darüber hinaus legt GCP die folgende Einschränkung auf:

- Es gibt eine 1:1-Zuordnung der Anzahl öffentlicher IP-Adressen zur Anzahl der NICs. Einer NIC kann nur eine öffentliche IP-Adresse zugewiesen werden.
- Auf einem Instanztyp mit höherer Kapazität können maximal nur 8 NICs angeschlossen werden.

Zum Beispiel kann eine n1-standard-2-Instanz nur 2 NICs haben, und die Anzahl der hinzufügbaren öffentlichen VIPs ist auf 2 begrenzt. Weitere Informationen finden Sie unter VPC-Ressourcenkontingente.

Um höhere Skalierungen öffentlicher virtueller IP-Adressen auf einer NetScaler VPX-Instanz zu erreichen, können Sie die VIP-Adressen als Teil der Metadaten der Instanz konfigurieren. Die NetScaler VPX-Instanz verwendet intern von GCP bereitgestellte Weiterleitungsregeln, um die VIP-Skalierung zu erreichen. Die NetScaler VPX-Instanz bietet auch Hochverfügbarkeit für die konfigurierten VIPs. Nachdem Sie VIP-Adressen als Teil der Metadaten konfiguriert haben, können Sie einen virtuellen LB-Server mit derselben IP konfigurieren, die zum Erstellen der Weiterleitungsregeln verwendet wird. Somit können wir Weiterleitungsregeln verwenden, um die Einschränkungen hinsichtlich der Skalierung bei der Verwendung öffentlicher VIP-Adressen auf einer NetScaler VPX-Instanz auf GCP zu mindern.

Weitere Informationen zu Weiterleitungsregeln finden Sie unter Übersicht über Weiterleitungsregeln.

Weitere Informationen zu HA finden Sie unter Hochverfügbarkeit.

## Hinweise

- Google berechnet zusätzliche Kosten für jede virtuelle IP-Weiterleitungsregel. Die tatsächlichen Kosten hängen von der Anzahl der erstellten Einträge ab. Die damit verbundenen Kosten können den Google-Preisdokumenten entnommen werden.
- Weiterleitungsregeln gelten nur für öffentliche VIPs. Sie können Alias-IP-Adressen verwenden, wenn die Bereitstellung private IP-Adressen als VIPs benötigt.
- Sie können Weiterleitungsregeln nur für die Protokolle erstellen, die den virtuellen LB-Server benötigen. VIPs können spontan erstellt, aktualisiert oder gelöscht werden. Sie können auch einen neuen virtuellen Lastausgleichsserver mit derselben VIP-Adresse, aber mit einem anderen Protokoll hinzufügen.

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

## Bevor Sie beginnen

- Die NetScaler VPX-Instanz muss auf GCP bereitgestellt werden.
- Die externe IP-Adresse muss reserviert werden. Weitere Informationen finden Sie unter Reservieren einer statischen externen IP-Adresse.
- Stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_IAM_PERMS = [

"compute.addresses.list",

"compute.addresses.get",

"compute.addresses.use",

"compute.forwardingRules.create",

"compute.forwardingRules.delete",

"compute.forwardingRules.get",

"compute.forwardingRules.list",

"compute.instances.use",

"compute.subnetworks.use",

"compute.targetInstances.create"

"compute.targetInstances.get"

"compute.targetInstances.use",

]
```

- Aktivieren Sie die **Cloud Resource Manager API** für Ihr GCP-Projekt.
- Wenn Sie die VIP-Skalierung auf einer eigenständigen VPX-Instanz verwenden, stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

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

```
REQUIRED_IAM_PERMS = [

"compute.addresses.list",

"compute.addresses.get",

"compute.addresses.use",

"compute.forwardingRules.create",

"compute.forwardingRules.delete",

"compute.forwardingRules.get",

"compute.forwardingRules.list",

"compute.instances.use",

"compute.subnetworks.use",

"compute.targetInstances.create",

"compute.targetInstances.list",

"compute.targetInstances.use",

]
```

- Wenn Sie die VIP-Skalierung im Hochverfügbarkeitsmodus verwenden, stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_IAM_PERMS = [

"compute.addresses.get",

"compute.addresses.list",

"compute.addresses.use",

"compute.forwardingRules.create",

"compute.forwardingRules.delete",
```

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

```
"compute.forwardingRules.get",

"compute.forwardingRules.list",

"compute.forwardingRules.setTarget",

"compute.instances.use",

"compute.instances.get",

"compute.instances.list",

"compute.instances.setMetadata",

"compute.subnetworks.use",

"compute.targetInstances.create",

"compute.targetInstances.list",

"compute.targetInstances.use",

"compute.zones.list",

]
```

**HINWEIS:**

Wenn Ihr Dienstkonto im Hochverfügbarkeitsmodus keine Eigentümer- oder Bearbeiterrollen hat, müssen Sie Ihrem Dienstkonto die **Dienstkontobenutzerrolle** hinzufügen.

## Konfigurieren externer IP-Adressen für die VIP-Skalierung auf der NetScaler VPX-Instanz

1. Navigieren Sie in der Google Cloud Console zur Seite **VM-Instanzen**.
2. Erstellen Sie eine neue VM-Instanz oder verwenden Sie eine vorhandene Instanz.
3. Klicken Sie auf den Instanznamen. Klicken Sie auf der Seite **Details zur VM-Instanz** auf **Bearbeiten**.

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

4. Aktualisieren Sie die **Benutzerdefinierten Metadaten**, indem Sie Folgendes eingeben:

   - Schlüssel = vips
   - Wert = Geben Sie einen Wert im folgenden JSON-Format an:

     { "Name der externen reservierten IP": , }

   GCP unterstützt die folgenden Protokolle:

   - AH
   - ESP
   - ICMP
   - SCT
   - TCP
   - UDP

   Weitere Informationen finden Sie unter Benutzerdefinierte Metadaten.

   Beispiel für benutzerdefinierte Metadaten:

   { "external-ip1-name":, "external-ip2-name": }

   In diesem Beispiel erstellt die NetScaler VPX-Instanz intern eine Weiterleitungsregel für jedes IP-Protokollpaar. Die Metadateneinträge werden den Weiterleitungsregeln zugeordnet. Dieses Beispiel hilft Ihnen zu verstehen, wie viele Weiterleitungsregeln für einen Metadateneintrag erstellt werden.

   Vier Weiterleitungsregeln werden wie folgt erstellt:

   a. external-ip1-name und TCP
   b. external-ip1-name und UDP
   c. external-ip2-name und ICMP
   d. external-ip2-name und AH

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

**HINWEIS:**

Im HA-Modus müssen Sie benutzerdefinierte Metadaten nur auf der primären Instanz hinzufügen. Beim Failover werden die benutzerdefinierten Metadaten mit der neuen primären Instanz synchronisiert.

5. Klicken Sie auf **Speichern**.

## Einrichten eines virtuellen Lastausgleichsservers mit externer IP-Adresse auf einer NetScaler VPX-Instanz

**Schritt 1**. Fügen Sie einen virtuellen Lastausgleichsserver hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastausgleich > Virtuelle Server > Hinzufügen**.

2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (Externe IP-Adresse der Weiterleitungsregel, die als VIP auf dem ADC hinzugefügt wird) und Port hinzu, und klicken Sie auf **OK**.

**Schritt 2**. Fügen Sie einen Dienst oder eine Dienstgruppe hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastausgleich > Dienste > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Dienstname, IP-Adresse, Protokoll und Port hinzu, und klicken Sie auf **OK**.

**Schritt 3**. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastausgleich > Virtuelle Server**.
2. Wählen Sie den virtuellen Lastausgleichsserver aus, der in **Schritt 1** konfiguriert wurde, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Dienst- und Dienstgruppen** auf **Keine Dienstbindung für virtuellen Lastausgleichsserver**.

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

4. Wählen Sie den Dienst aus, der in **Schritt 3** konfiguriert wurde, und klicken Sie auf **Binden**.

5. Speichern Sie die Konfiguration.

# Fehlerbehebung bei einer VPX-Instanz auf GCP

Die Google Cloud Platform (GCP) bietet Konsolenzugriff auf eine NetScaler VPX-Instanz. Sie können nur debuggen, wenn das Netzwerk verbunden ist. Um das Systemprotokoll einer Instanz anzuzeigen, greifen Sie auf die Konsole zu und überprüfen Sie die **Systemprotokolldateien**.

Um einen Supportfall zu eröffnen, suchen Sie Ihre GCP-Kontonummer und Ihren Support-PIN-Code und rufen Sie den NetScaler®-Support an. Sie werden gebeten, Ihren Namen und Ihre E-Mail-Adresse anzugeben. Um den Support-PIN zu finden, melden Sie sich bei der VPX-GUI an und navigieren Sie zur Seite **System**.

Hier ist ein Beispiel für eine Systemseite, die den Support-PIN anzeigt.

Technischer GCP-PIN(/en-us/vpx/media/gcp-technical-pin.png)

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

# Jumbo-Frames auf NetScaler VPX-Instanzen

NetScaler VPX-Appliances unterstützen den Empfang und die Übertragung von Jumbo-Frames, die bis zu 9216 Byte IP-Daten enthalten. Jumbo-Frames können große Dateien effizienter übertragen, als dies mit der Standard-IP-MTU-Größe von 1500 Byte möglich ist.

Eine NetScaler Appliance kann Jumbo-Frames in den folgenden Bereitstellungsszenarien verwenden:

- Jumbo zu Jumbo. Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als Jumbo-Frames.
- Nicht-Jumbo zu Jumbo. Die Appliance empfängt Daten als reguläre Frames und sendet sie als Jumbo-Frames.
- Jumbo zu Nicht-Jumbo. Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als reguläre Frames.

Weitere Informationen finden Sie unter Konfigurieren der Jumbo-Frame-Unterstützung auf einer NetScaler Appliance.

Die Unterstützung von Jumbo-Frames ist auf NetScaler VPX-Appliances verfügbar, die auf den folgenden Virtualisierungsplattformen ausgeführt werden:

- VMware ESX
- Linux-KVM-Plattform
- Citrix® XenServer®
- Amazon Web Services (AWS)

Jumbo-Frames auf VPX-Appliances funktionieren ähnlich wie Jumbo-Frames auf MPX-Appliances. Weitere Informationen zu Jumbo-Frames und ihren Anwendungsfällen finden Sie unter Konfigurieren von Jumbo-Frames auf MPX-Appliances. Die Anwendungsfälle von Jumbo-Frames auf MPX-Appliances gelten auch für VPX-Appliances.

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

## Jumbo-Frames für eine VPX-Instanz konfigurieren, die auf VMware ESX ausgeführt wird

Führen Sie die folgenden Aufgaben aus, um Jumbo-Frames auf einer NetScaler VPX-Appliance zu konfigurieren, die auf dem VMware ESX-Server ausgeführt wird:

1. Legen Sie die MTU der Schnittstelle oder des Kanals der VPX-Appliance auf einen Wert im Bereich von 1501–9000 fest. Verwenden Sie die CLI oder GUI, um die MTU-Größe festzulegen. Die auf VMware ESX ausgeführten NetScaler VPX-Appliances unterstützen das Empfangen und Senden von Jumbo-Frames, die bis zu 9000 Byte IP-Daten enthalten.
2. Legen Sie dieselbe MTU-Größe auf den entsprechenden physischen Schnittstellen des VMware ESX-Servers mithilfe seiner Verwaltungsanwendungen fest. Weitere Informationen zum Festlegen der MTU-Größe auf den physischen Schnittstellen von VMware ESX finden Sie unter http://vmware.com/.

## Jumbo-Frames für eine auf einem Linux-KVM-Server ausgeführte VPX-Instanz konfigurieren

Führen Sie die folgenden Aufgaben aus, um Jumbo-Frames auf einer NetScaler VPX-Appliance zu konfigurieren, die auf einem Linux-KVM-Server ausgeführt wird:

1. Legen Sie die MTU der Schnittstelle oder des Kanals der VPX-Appliance auf einen Wert im Bereich von 1501–9216 fest. Verwenden Sie die NetScaler VPX CLI oder GUI, um die MTU-Größe festzulegen.
2. Legen Sie dieselbe MTU-Größe auf den entsprechenden physischen Schnittstellen eines Linux-KVM-Servers mithilfe seiner Verwaltungsanwendungen fest. Weitere Informationen zum Festlegen der MTU-Größe auf den physischen Schnittstellen von Linux-KVM finden Sie unter `<http://www.linux-kvm.org/>`.

## Jumbo-Frames für eine auf Citrix XenServer ausgeführte VPX-Instanz konfigurieren

Führen Sie die folgenden Aufgaben aus, um Jumbo-Frames auf einer NetScaler VPX-Appliance zu konfigurieren, die auf Citrix XenServer ausgeführt wird:

1. Stellen Sie mithilfe von XenCenter eine Verbindung zum XenServer her.
2. Fahren Sie alle VPX-Instanzen herunter, die die Netzwerke verwenden, für die die MTU geändert werden muss.

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

3. Wählen Sie auf der Registerkarte **Networking** das Netzwerk – Netzwerk 0/1/2 aus.
4. Wählen Sie **Eigenschaften** aus und bearbeiten Sie die MTU.

Nachdem Sie die Jumbo-Frames auf dem XenServer konfiguriert haben, können Sie die Jumbo-Frames auf der ADC-Appliance konfigurieren. Weitere Informationen finden Sie unter Unterstützung von Jumbo-Frames auf einer NetScaler-Appliance konfigurieren.

## Jumbo-Frames für eine auf AWS ausgeführte VPX-Instanz konfigurieren

Eine Host-Level-Konfiguration ist für VPX unter Azure nicht erforderlich. Um Jumbo-Frames auf VPX zu konfigurieren, befolgen Sie die Schritte unter Unterstützung von Jumbo-Frames auf einer NetScaler-Appliance konfigurieren.

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

# FAQs

Der folgende Abschnitt hilft Ihnen, die FAQs basierend auf Citrix® Application Delivery Controller™ (ADC) VPX zu kategorisieren.


- Funktionen und Funktionalität
- Verschlüsselung
- Preise und Pakete
- NetScaler VPX™ Express und 90-tägige kostenlose Testversion
- Hypervisor
- Kapazitätsplanung oder Dimensionierung
- Systemanforderungen
- Weitere technische FAQs


## Funktionen und Funktionalität

### Was ist NetScaler VPX?

NetScaler VPX ist eine virtuelle ADC-Appliance, die auf einem Hypervisor gehostet werden kann, der auf Industriestandardservern installiert ist.

### Umfasst NetScaler VPX alle Funktionen zur Webanwendungsoptimierung wie ADC-Appliances?

Ja. NetScaler VPX umfasst alle Funktionen für Lastausgleich, Datenverkehrsmanagement, Anwendungsbeschleunigung, Anwendungssicherheit (einschließlich NetScaler Gateway und Citrix Application Firewall) und Offload. Eine vollständige Übersicht über die Funktionen und Merkmale von NetScaler finden Sie unter Anwendungsbereitstellung nach Ihren Wünschen.

### Gibt es Einschränkungen bei der Citrix Application Firewall, wenn sie auf NetScaler VPX verwendet wird?

Die Citrix Application Firewall auf NetScaler VPX bietet die gleichen Sicherheitsfunktionen wie auf NetScaler Appliances. Die Leistung oder der Durchsatz der Citrix Application Firewall variiert je nach Plattform.

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

## Gibt es Unterschiede zwischen NetScaler Gateway auf NetScaler VPX und NetScaler Gateway auf NetScaler Appliances?

Funktionell sind sie identisch. NetScaler Gateway auf NetScaler VPX unterstützt alle NetScaler Gateway-Funktionen, die in NetScaler Software Release 14.1 verfügbar sind. Da NetScaler Appliances jedoch dedizierte SSL-Beschleunigungshardware bieten, bieten sie eine größere SSL-VPN-Skalierbarkeit als eine NetScaler VPX-Instanz.

## Abgesehen vom offensichtlichen Unterschied, dass NetScaler VPX auf einem Hypervisor laufen kann, wie unterscheidet es sich von physischen NetScaler Appliances?

Es gibt zwei Hauptbereiche, in denen Kunden Verhaltensunterschiede feststellen. Der erste ist, dass NetScaler VPX nicht die gleiche Leistung wie viele NetScaler Appliances bieten kann. Der zweite ist, dass NetScaler Appliances zwar eine eigene L2-Netzwerkfunktionalität integrieren, NetScaler VPX sich jedoch für seine L2-Netzwerkdienste auf den Hypervisor verlässt. Im Allgemeinen schränkt dies die Bereitstellung von NetScaler VPX nicht ein. Es kann bestimmte L2-Funktionen geben, die auf einer physischen NetScaler Appliance konfiguriert werden müssen und auf dem zugrunde liegenden Hypervisor konfiguriert werden müssen.

## Welche Rolle spielt NetScaler VPX auf dem Markt für Anwendungsbereitstellung?

NetScaler VPX verändert das Spiel auf dem Markt für Anwendungsbereitstellung auf folgende Weisen:

- Indem NetScaler VPX eine NetScaler Appliance noch erschwinglicher macht, ermöglicht es jeder IT-Organisation, eine NetScaler Appliance bereitzustellen. Dies gilt nicht nur für ihre geschäftskritischsten Webanwendungen, sondern für alle ihre Webanwendungen.
- NetScaler VPX ermöglicht es Kunden, Netzwerke und Virtualisierung in ihren Rechenzentren weiter zusammenzuführen. NetScaler VPX kann nicht nur zur Optimierung von Webanwendungen verwendet werden, die auf virtualisierten Servern gehostet werden. Es ermöglicht auch, dass die Webanwendungsbereitstellung selbst zu einem virtualisierten Dienst wird, der einfach und schnell überall bereitgestellt werden kann. IT-Organisationen nutzen die Standard-Rechenzentrumsprozesse für Aufgaben wie Bereitstellung, Automatisierung und Kostenverrechnung für die Webanwendungsbereitstellungsinfrastruktur.
- NetScaler VPX eröffnet neue Bereitstellungsarchitekturen, die bei ausschließlicher Verwendung physischer Appliances nicht praktikabel wären. NetScaler VPX und NetScaler MPX Appliances können je nach Bedarf eingesetzt werden, zugeschnitten auf die individuellen

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

Anforderungen jeder jeweiligen Anwendung, um prozessorintensive Aktionen wie Komprimierung und Application Firewall-Inspektion zu bewältigen. Am Rechenzentrumsrand übernehmen NetScaler MPX Appliances hochvolumige netzwerkweite Aufgaben wie die anfängliche Verkehrsverteilung, SSL-Verschlüsselung oder -Entschlüsselung, die Verhinderung von Denial-of-Service (DoS)-Angriffen und das globale Lastverteilung. Die Kombination von leistungsstarken NetScaler MPX Appliances mit einfach zu implementierenden virtuellen NetScaler VPX Appliances bietet beispiellose Flexibilität und Anpassungsmöglichkeiten für moderne, große Rechenzentrumsumgebungen und reduziert gleichzeitig die Gesamtkosten des Rechenzentrums.

### Wie passt NetScaler VPX in unsere Citrix Delivery Center-Strategie?

Mit der Verfügbarkeit von NetScaler VPX ist das gesamte Citrix Delivery Center-Angebot als virtualisiertes Angebot verfügbar. Das gesamte Citrix Delivery Center profitiert von den leistungsstarken Verwaltungs-, Bereitstellungs-, Überwachungs- und Berichtsfunktionen, die in Citrix XenCenter verfügbar sind. Dies kann schnell in nahezu jede Umgebung bereitgestellt und zentral von überall aus verwaltet werden. Mit einer integrierten, virtualisierten Anwendungsbereitstellungsinfrastruktur können Unternehmen Desktops, Client-Server-Anwendungen und Webanwendungen bereitstellen.

## Verschlüsselung

### Unterstützt NetScaler VPX SSL-Offload?

Ja. NetScaler VPX führt jedoch die gesamte SSL-Verarbeitung in Software durch, sodass NetScaler VPX nicht die gleiche SSL-Leistung wie NetScaler Appliances bietet. NetScaler VPX kann bis zu 750 neue SSL-Transaktionen pro Sekunde unterstützen.

### Beschleunigen SSL-Karten von Drittanbietern, die auf dem Server installiert sind, der NetScaler VPX hostet, die SSL-Verschlüsselung oder -Entschlüsselung?

Nein. Die Unterstützung von SSL-Karten von Drittanbietern kann die NetScaler VPX nicht an spezifische Hardwareimplementierungen binden. Dies beeinträchtigt die Fähigkeit eines Unternehmens erheblich, NetScaler VPX flexibel überall im Rechenzentrum zu hosten. NetScaler MPX Appliances müssen verwendet werden, wenn ein höherer SSL-Durchsatz als von NetScaler VPX bereitgestellt erforderlich ist.

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

### Unterstützt NetScaler VPX die gleichen Verschlüsselungs-Ciphers wie physische NetScaler Appliances?

VPX unterstützt alle Verschlüsselungs-Ciphers wie physische NetScaler Appliances, mit Ausnahme von ECDSA.

### Wie hoch ist der SSL-Transaktionsdurchsatz von NetScaler VPX?

Informationen zum SSL-Transaktionsdurchsatz finden Sie im NetScaler VPX-Datenblatt.

## Preise und Pakete

### Wie wird NetScaler VPX verpackt?

Die Auswahl von NetScaler VPX ähnelt der Auswahl von NetScaler Appliances. Zuerst wählt der Kunde die NetScaler Edition basierend auf seinen Funktionsanforderungen aus. Anschließend wählt der Kunde die spezifische NetScaler VPX Bandbreitenstufe basierend auf seinen Durchsatzanforderungen aus. NetScaler VPX ist in den Editionen Standard, Advanced und Premium erhältlich. NetScaler VPX bietet von 10 Mbit/s (VPX 10) bis 100 Gbit/s (VPX 100G). Weitere Details finden Sie im NetScaler VPX-Datenblatt.

### Ist NetScaler VPX für alle Hypervisoren gleich bepreist?

Ja.

### Werden dieselben NetScaler SKUs für VPX auf allen Hypervisoren verwendet?

Ja.

### Kann eine NetScaler VPX-Lizenz von einem Hypervisor auf einen anderen verschoben werden (z. B. von VMware zu Hyper-V)?

Ja. NetScaler VPX-Lizenzen sind unabhängig vom zugrunde liegenden Hypervisor. Wenn Sie die virtuelle NetScaler VPX-Maschine von einem Hypervisor zu einem anderen verschieben, müssen Sie keine neue Lizenz erwerben. Es kann jedoch erforderlich sein, die vorhandene NetScaler VPX-Lizenz neu zu hosten.

### Können NetScaler VPX-Instanzen aktualisiert werden?

Ja. Sowohl die Durchsatzgrenzen als auch die NetScaler Family Edition können aktualisiert werden. Upgrade-SKUs für beide Arten von Upgrades sind verfügbar.

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

### Wenn ich NetScaler VPX in einem Hochverfügbarkeitspaar bereitstellen möchte, wie viele Lizenzen benötige ich?

Wie bei physischen NetScaler-Appliances erfordert eine NetScaler-Hochverfügbarkeitskonfiguration zwei aktive Instanzen. Daher muss der Kunde zwei Lizenzen erwerben.

## NetScaler® VPX Express und 90-Tage-Testversion

### Umfasst NetScaler VPX Express alle NetScaler-Standardfunktionen? Umfasst es NetScaler Gateway und Lastausgleich für Citrix Virtual Apps (ehemals XenApp) Web Interface und XML-Broker?

Ja. NetScaler VPX Express umfasst die vollständige NetScaler Premium-Funktionalität. Ab NetScaler Release 14.1–29.65 hat NetScaler das Verhalten von VPX Express geändert.

### Benötigt NetScaler VPX Express eine Lizenz?

Mit dem neuesten NetScaler VPX Express Release (14.1–29.65 und höher) ist VPX Express kostenlos nutzbar und erfordert keine Lizenzdatei für die Installation oder Nutzung. Es ist keine Verpflichtung erforderlich. Wenn Sie bereits eine VPX Express-Lizenz besitzen, bleibt das bisherige Lizenzierungsverhalten in Kraft. Wenn Sie jedoch die vorhandene VPX Express-Lizenzdatei entfernen und Version 14.1–29.65 oder höher verwenden, gilt das aktualisierte VPX Express-Verhalten.

### Läuft die NetScaler VPX Express-Lizenz ab?

Mit dem neuen VPX Express gibt es keine Lizenz und kein Ablaufdatum. Wenn Sie bereits eine VPX Express-Lizenz besitzen, läuft diese ein Jahr nach dem Download ab.

### Unterstützt NetScaler VPX Express dieselben Verschlüsselungs-Ciphers wie NetScaler MPX-Appliances?

Für die allgemeine Verfügbarkeit sind alle starken Verschlüsselungs-Ciphers, die auf NetScaler-Appliances unterstützt werden, auch auf NetScaler VPX und NetScaler VPX Express verfügbar. Es unterliegt denselben Import- oder Exportbestimmungen.

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

### Kann ich technische Supportfälle für NetScaler VPX Express einreichen?

Nein. Benutzer von NetScaler VPX Express können sowohl das NetScaler VPX Knowledge Center nutzen als auch über die Diskussionsforen Hilfe von der Community anfordern.

### Kann NetScaler VPX Express auf eine Einzelhandelsversion aktualisiert werden?

Ja. Kaufen Sie einfach die benötigte Einzelhandelslizenz für NetScaler VPX und wenden Sie dann die entsprechende Lizenz auf die NetScaler VPX Express-Instanz an.

## Hypervisor

### Welche VMware-Versionen unterstützt NetScaler VPX?

NetScaler VPX unterstützt sowohl VMware ESX als auch ESXi für Versionen 3.5 oder höher. Weitere Informationen finden Sie unter Support-Matrix und Nutzungsrichtlinien

### Wie viele virtuelle Netzwerkschnittstellen können Sie einem VPX in VMware zuweisen?

Sie können einem NetScaler VPX bis zu 10 virtuelle Netzwerkschnittstellen zuweisen.

### Wie können wir über vSphere auf die NetScaler VPX-Befehlszeile zugreifen?

Der VMware vSphere-Client bietet über eine Konsolenregisterkarte integrierten Zugriff auf die NetScaler VPX-Befehlszeile. Sie können auch jeden SSH- oder Telnet-Client verwenden, um auf die Befehlszeile zuzugreifen. Sie können die NSIP-Adresse des NetScaler VPX im SSH- oder Telnet-Client verwenden.

### Wie können Sie auf die NetScaler VPX-GUI zugreifen?

Um auf die NetScaler VPX-GUI zuzugreifen, geben Sie die NSIP des NetScaler VPX, z. B. `http://NSIP address`, in das Adressfeld eines beliebigen Browsers ein.

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

### Können zwei NetScaler VPX-Instanzen, die auf demselben VMware ESX installiert sind, in einer Hochverfügbarkeitskonfiguration eingerichtet werden?

Ja, aber es wird nicht empfohlen. Ein Hardwarefehler würde beide NetScaler VPX-Instanzen betreffen.

### Können zwei NetScaler VPX-Instanzen, die auf zwei verschiedenen VMware ESX-Systemen ausgeführt werden, in einer Hochverfügbarkeitskonfiguration eingerichtet werden?

Ja. Es wird in einer Hochverfügbarkeitskonfiguration empfohlen.

### Werden für VMware schnittstellenbezogene Ereignisse auf NetScaler VPX unterstützt?

Nein. Schnittstellenbezogene Ereignisse werden nicht unterstützt.

### Werden für VMware getaggte VLANs auf NetScaler VPX unterstützt?

Ja. NetScaler getaggte VLANs werden auf NetScaler VPX ab Version 11.0 und höher unterstützt. Weitere Informationen finden Sie in der NetScaler-Dokumentation.

### Werden für VMware Link-Aggregation und LACP auf NetScaler VPX unterstützt?

Nein. Link-Aggregation und LACP werden für NetScaler VPX nicht unterstützt. Die Link-Aggregation muss auf VMware-Ebene konfiguriert werden.

### Wie greifen wir auf die NetScaler VPX-Dokumentation zu?

Die Dokumentation ist über die NetScaler VPX GUI verfügbar. Wählen Sie nach der Anmeldung die Registerkarte **Dokumentation** aus.

## Kapazitätsplanung oder Dimensionierung

### Welche Leistung kann ich von NetScaler VPX erwarten?

NetScaler VPX bietet eine gute Leistung. Ein spezifisches Leistungsniveau, das mit NetScaler VPX erreicht werden kann, finden Sie im NetScaler VPX-Datenblatt.

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

## Angesichts der Tatsache, dass die CPU-Leistung des Servers variiert, wie können wir die maximale Leistung einer NetScaler-Instanz abschätzen?

Die Verwendung einer schnelleren CPU kann zu einer höheren Leistung führen (bis zum durch die Lizenz erlaubten Maximum), während die Verwendung einer langsameren CPU die Leistung sicherlich einschränken kann.

## Gelten die Bandbreiten- oder Durchsatzgrenzen von NetScaler VPX nur für eingehenden Datenverkehr oder für eingehenden und ausgehenden Datenverkehr?

Die Bandbreitenbeschränkungen von NetScaler VPX werden nur für den eingehenden Datenverkehr zum NetScaler erzwungen, unabhängig davon, ob es sich um Anforderungs- oder Antwortdatenverkehr handelt. Dies bedeutet, dass ein NetScaler VPX-1000 (zum Beispiel) gleichzeitig 1 Gbit/s eingehenden und 1 Gbit/s ausgehenden Datenverkehr verarbeiten kann. Eingehender und ausgehender Datenverkehr ist nicht dasselbe wie Anforderungs- und Antwortdatenverkehr. Für den NetScaler ist sowohl der von Endpunkten kommende Datenverkehr (Anforderungsdatenverkehr) als auch der von Ursprungsservern kommende Datenverkehr (Antwortdatenverkehr) „eingehend“ (d. h. er kommt in den NetScaler hinein).

## Können mehrere Instanzen von NetScaler VPX auf demselben Server ausgeführt werden?

Ja. Stellen Sie jedoch sicher, dass der physische Server über genügend CPU- und E/A-Kapazität verfügt, um die gesamte auf dem Host ausgeführte Arbeitslast zu unterstützen, da sonst die Leistung von NetScaler VPX beeinträchtigt werden kann.

## Wenn mehr als eine Instanz von NetScaler VPX auf einem physischen Server ausgeführt wird, wie lauten die Mindestanforderungen an die Hardware pro NetScaler VPX-Instanz?

Jeder NetScaler VPX-Instanz müssen 2 GB physischer RAM, 20 GB Festplattenspeicher und 2 vCPUs zugewiesen werden. Für kritische Bereitstellungen empfehlen wir 2 GB RAM für VPX nicht, da das System in einer speicherbeschränkten Umgebung arbeitet. Dies könnte zu Problemen in Bezug auf Skalierung, Leistung oder Stabilität führen. Empfohlen werden 4 GB RAM oder 8 GB RAM.

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

**HINWEIS:**

Der NetScaler VPX ist eine latenzempfindliche, hochleistungsfähige virtuelle Appliance. Um die erwartete Leistung zu erbringen, erfordert die Appliance vCPU-Reservierung, Speicherreservierung und vCPU-Pinning auf dem Host. Außerdem muss Hyper-Threading auf dem Host deaktiviert sein. Wenn der Host diese Anforderungen nicht erfüllt, treten Probleme wie High-Availability-Failover, CPU-Spitzen innerhalb der VPX-Instanz, Trägheit beim Zugriff auf die VPX-CLI, Absturz des Pit-Boss-Daemons, Paketverluste und geringer Durchsatz auf.

Stellen Sie sicher, dass jede VPX-Instanz die vordefinierten Bedingungen erfüllt.

## Kann ich NetScaler VPX und andere Anwendungen auf demselben Server hosten?

Ja. Zum Beispiel können NetScaler VPX, Citrix Virtual Apps Web Interface und Citrix Virtual Apps XML Broker alle virtualisiert und auf demselben Server ausgeführt werden. Für die beste Leistung stellen Sie sicher, dass der physische Host über genügend CPU- und E/A-Kapazität verfügt, um alle laufenden Workloads zu unterstützen.

## Erhöht das Hinzufügen von CPU-Kernen zu einer einzelnen NetScaler VPX-Instanz die Leistung dieser Instanz?

Ja, das Hinzufügen von CPU-Kernen kann die Leistung von NetScaler VPX verbessern, vorausgesetzt, die NetScaler VPX-Instanz ist für die zusätzlichen vCPUs lizenziert. NetScaler VPX kann je nach Konfiguration und Leistungsstufe bis zu 20 vCPUs (für 41 Gbit/s - 100 Gbit/s Leistung) unterstützen. Mehr vCPUs können dazu beitragen, den Durchsatz zu erhöhen, insbesondere in Hochleistungsszenarien. Der Einfluss auf die Leistung hängt jedoch auch von Faktoren wie den Netzwerktreibern (z. B. PCI-Passthrough oder SR-IOV) und der spezifischen Arbeitslast ab. Informationen zur Anzahl der vCPUs, die für verschiedene VPX-Leistungsstufen unterstützt werden, finden Sie im NetScaler VPX-Datenblatt.

## Warum scheint NetScaler VPX mehr als 90 % der CPU zu verbrauchen, obwohl es im Leerlauf ist?

Dies ist ein normales Verhalten, und NetScaler-Appliances zeigen dasselbe Verhalten. Um das wahre Ausmaß der NetScaler VPX-CPU-Auslastung zu sehen, verwenden Sie den Befehl „stat CPU“ in der NetScaler CLI oder zeigen Sie die NetScaler VPX-CPU-Auslastung über die NetScaler GUI an. Die NetScaler-Paketverarbeitungs-Engine ist immer „auf der Suche nach Arbeit“, auch

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

wenn keine Arbeit zu erledigen ist. Daher tut sie alles, um die Kontrolle über die CPU zu übernehmen und sie nicht freizugeben. Auf einem Server, auf dem NetScaler VPX und nichts anderes installiert ist, sieht es (aus Sicht des Hypervisors) so aus, als würde NetScaler VPX die gesamte CPU verbrauchen. Ein Blick auf die CPU-Auslastung von „innerhalb des NetScaler“ (mithilfe der CLI oder der GUI) liefert ein Bild der genutzten NetScaler VPX-CPU-Kapazität.

# Systemanforderungen

## Was sind die Mindestanforderungen an die Hardware für NetScaler VPX?

Die folgende Tabelle erläutert die Mindestanforderungen an die Hardware für NetScaler VPX.

| TYP | ANFORDERUNGEN |
|---|---|
| Prozessor | Die Prozessoranforderungen für Ihre VPX-Plattform finden Sie in der Tabelle Unterstützte Prozessoren für NetScaler VPX. |
| Arbeitsspeicher | Mindestens 2 GB. Es werden jedoch 4 GB empfohlen. |
| Festplatte | Mindestens 20 GB Festplatte. |
| Hypervisor | Citrix Hypervisor 5.6 oder höher, VMware ESX/ESXi 3.5 oder höher oder Windows Server 2008 R2 mit Hyper-V |
| Netzwerkkonnektivität | Mindestens 100 Mbit/s, es werden jedoch 1 Gbit/s empfohlen. |
| NIC | Verwenden Sie eine NIC, die mit Ihrem Hypervisor kompatibel ist. Weitere Informationen finden Sie unter Unterstützte NICs für NetScaler VPX. |

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

**HINWEIS:**

- Für kritische Bereitstellungen werden 4 GB Arbeitsspeicher für NetScaler VPX bevorzugt. Mit 2 GB Arbeitsspeicher arbeitet NetScaler VPX in einer speicherbeschränkten Umgebung. Dies kann zu Problemen bei Skalierung, Leistung oder Stabilität führen.
- Ab NetScaler Version 13.1 unterstützt die NetScaler VPX-Instanz auf dem VMware ESXi-Hypervisor AMD EPYC-Prozessoren.

Weitere Informationen zu den Systemanforderungen finden Sie im NetScaler VPX-Datenblatt.

## Was ist Intel VT-x?

Diese Funktionen, manchmal als „Hardware-Unterstützung“ oder „Virtualisierungs-Unterstützung“ bezeichnet, leiten sensible oder privilegierte CPU-Anweisungen, die vom Gast-Betriebssystem ausgeführt werden, an den Hypervisor weiter. Dies vereinfacht das Hosten von Gast-Betriebssystemen (BSD für einen NetScaler VPX) auf dem Hypervisor.

## Wie verbreitet ist VT-x?

Bei vielen Servern sind Virtualisierungsunterstützungsfunktionen (wie VT-x oder AMD-V) in den BIOS-Einstellungen standardmäßig deaktiviert. Bevor Sie zu dem Schluss kommen, dass Sie NetScaler VPX nicht ausführen können, überprüfen Sie die BIOS-Konfiguration. Wenn die Virtualisierungsunterstützung deaktiviert ist, müssen Sie sie möglicherweise im BIOS aktivieren, um sicherzustellen, dass Ihr Server virtualisierte Anwendungen wie NetScaler VPX ordnungsgemäß ausführen kann.

## Gibt es eine Hardware-Kompatibilitätsliste (HCL) für NetScaler VPX?

Solange der Server Intel VT-x unterstützt, muss NetScaler VPX auf jedem Server ausgeführt werden, der mit dem zugrunde liegenden Hypervisor kompatibel ist. Eine umfassende Liste der unterstützten Plattformen finden Sie in der Hypervisor-HCL.

## Auf welcher Version von NetScaler OS basiert NetScaler VPX?

NetScaler VPX basiert auf NetScaler 9.1 oder späteren Versionen.

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

### Da NetScaler VPX auf BSD läuft, kann es nativ auf einem Server mit installiertem BSD Unix ausgeführt werden?

Nein. NetScaler VPX benötigt den Hypervisor, um ausgeführt zu werden. Detaillierte Hypervisor-Unterstützung finden Sie im NetScaler VPX-Datenblatt.

## Weitere technische FAQs

### Funktioniert Link-Aggregation auf einem physischen Server mit mehreren NICs?

LACP wird nicht unterstützt. Für den Citrix Hypervisor wird statische Link-Aggregation unterstützt und hat Beschränkungen von vier Kanälen und sieben virtuellen Schnittstellen. Für VMware wird statische Link-Aggregation innerhalb von NetScaler VPX nicht unterstützt, kann aber auf VMware-Ebene konfiguriert werden.

### Wird MAC-basiertes Forwarding (MBF) auf VPX unterstützt? Gibt es Änderungen gegenüber der Implementierung der NetScaler Appliance?

MBF wird unterstützt und verhält sich genauso wie bei der NetScaler Appliance. Der Hypervisor leitet im Grunde alle von NetScaler VPX empfangenen Pakete nach außen und umgekehrt weiter.

### Wie wird der NetScaler VPX Upgrade-Prozess durchgeführt?

Upgrades werden auf die gleiche Weise wie bei NetScaler Appliances durchgeführt: Laden Sie eine Kernel-Datei herunter und verwenden Sie install ns oder das Upgrade-Dienstprogramm in der GUI.

### Wie werden Flash- und Festplattenspeicher zugewiesen? Können wir das ändern?

Jedem NetScaler VPX-Instanz müssen mindestens 2 GB Arbeitsspeicher zugewiesen werden. Das NetScaler VPX-Festplatten-Image hat eine Größe von 20 GB, um Wartungsanforderungen zu erfüllen, einschließlich Speicherplatz für bis zu 4 GB Core-Dumps sowie Protokoll- und Trace-Dateien. Obwohl es möglich wäre, ein kleineres Festplatten-Image zu generieren, gibt es derzeit keine Pläne dafür. `/flash` und `/var` befinden sich beide im selben Festplatten-Image. Sie werden aus Kompatibilitätsgründen als separate Dateisysteme beibehalten.

Die folgenden Werte stellen den zugewiesenen Festplattenspeicher für bestimmte Verzeichnisse auf der NetScaler VPX-Instanz dar:

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

- /flash ist 965M
- /var ist 14G

Für detaillierte Empfehlungen zur Speicherzuweisung siehe NetScaler VPX-Datenblatt.

## Können wir eine neue Festplatte hinzufügen, um den Speicherplatz auf der NetScaler VPX-Instanz zu erhöhen?

Ja. Ab NetScaler Release 13.1 Build 21.x haben Sie die Möglichkeit, den Festplattenspeicher auf der NetScaler VPX-Instanz durch Hinzufügen einer zweiten Festplatte zu erhöhen. Wenn Sie die zweite Festplatte anschließen, wird das Verzeichnis „/var/crash“ automatisch auf dieser Festplatte gemountet. Die zweite Festplatte wird zum Speichern von Core-Dateien und zur Protokollierung verwendet. Bestehende Verzeichnisse, die zum Speichern von Core-Dateien und Protokolldateien verwendet werden, funktionieren weiterhin wie zuvor.

**HINWEIS:**

Erstellen Sie ein externes Backup beim Downgrade der NetScaler Appliance, um Datenverlust zu vermeiden.

Informationen zum Anschließen eines neuen Festplattenlaufwerks (HDD) an eine NetScaler VPX-Instanz in einer Cloud finden Sie unter den folgenden Links:

- Azure-Dokumentation

  **HINWEIS:**

  Um eine sekundäre Festplatte an NetScaler VPX-Instanzen anzuschließen, die in Azure bereitgestellt werden, stellen Sie sicher, dass die Azure VM-Größen über eine lokale temporäre Festplatte verfügen. Weitere Informationen finden Sie unter Azure VM-Größen ohne lokale temporäre Festplatte.

- AWS-Dokumentation
- GCP-Dokumentation

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

**WARNUNG:**

Nachdem Sie eine neue HDD zu NetScaler VPX hinzugefügt haben, können einige der Skripte, die mit Dateien arbeiten, die auf die neue HDD verschoben wurden, unter den folgenden Bedingungen fehlschlagen:

Wenn Sie den Shell-Befehl „link“ verwenden, um Hardlinks zu den Dateien zu erstellen, die auf eine neue HDD verschoben wurden.
Ersetzen Sie alle derartigen Befehle durch „ln -s“, um einen symbolischen Link zu verwenden. Passen Sie auch die fehlerhaften Skripte entsprechend an.

## Kann ich die Größe der primären Festplatte auf NetScaler VPX erhöhen?

Ab NetScaler Release 14.1 Build 21.x können Administratoren die Größe der primären Festplatte auf NetScaler VPX dynamisch von 20 GB auf bis zu 1 TB auf einmal erhöhen. Und beim nächsten Mal können Sie erneut auf bis zu 1 TB erhöhen. Um den Speicherplatz zu erhöhen, erweitern Sie die Größe der primären Festplatte in der jeweiligen Cloud- oder Hypervisor-Benutzeroberfläche auf mindestens 1 GB.

**HINWEIS:**

Sie können die Größe der Festplatten nur erhöhen. Sobald die neue Größe zugewiesen ist, können Sie sie später nicht mehr verringern. Erhöhen Sie die Festplattengröße daher nur, wenn dies unbedingt erforderlich ist.

## Wie erhöhe ich manuell die Größe der primären Festplatte auf NetScaler VPX?

Führen Sie die folgenden Schritte aus, um die Größe der primären VPX-Festplatte manuell von einem Hypervisor oder einer Cloud aus zu erhöhen:

1. Fahren Sie die VM herunter.
2. Erweitern Sie die Standardfestplattengröße von 20 GB auf einen höheren Wert. Zum Beispiel von 20 GB auf 30 GB oder 40 GB. Erweitern Sie für Azure die Standardfestplattengröße von 32 GB auf 64 GB.
3. Schalten Sie die VM ein und geben Sie die Boot-Eingabeaufforderung ein.
4. Melden Sie sich im Einzelbenutzermodus mit dem Befehl „boot -s“ an.

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

5. Überprüfen Sie den Speicherplatz. Sie können den neu zugewiesenen Speicherplatz mit dem Befehl „gpart show“ überprüfen.
6. Notieren Sie den Partitionsnamen. Zum Beispiel ist die VM-Partition da0.
7. Ändern Sie die Größe der Festplattenpartition mit dem Befehl „gpart resize“.

   **Beispiel:** Lassen Sie uns die da0 MBR-Partition so anpassen, dass sie 10 GB freien Speicherplatz enthält, indem Sie den folgenden Befehl ausführen.

   ```
   gpart resize -i 1 da0
   ```
8. Führen Sie den freien Speicherplatz mit der letzten Partition zusammen.

   **Beispiel:**

   ```
   gpart resize -i 5 da0s1
   ```
9. Erweitern Sie das Dateisystem, um neu zugewiesenen freien Speicherplatz mithilfe des Befehls „growfs“ einzuschließen.

   **Beispiel:**

   ```
   growfs /dev/ada0s1e
   ```
10. Starten Sie die VM neu und überprüfen Sie den erhöhten Speicherplatz mithilfe des Befehls „df -h“ an der Shell-Eingabeaufforderung.

## Was ist hinsichtlich der NetScaler VPX Build-Nummerierung und der Interoperabilität mit anderen Builds zu erwarten?

NetScaler VPX hat eine ähnliche Build-Nummerierung wie die 9.1. Cl (Classic) und 9.1. Nc (nCore) Releases, zum Beispiel 9.1_97.3.vpx, 9.1_97.3.nc und 9.1_97.3.cl.

## Kann der NetScaler VPX Teil eines Hochverfügbarkeits-Setups mit einer NetScaler Appliance sein?

Keine unterstützte Konfiguration.

## Sind alle in NetScaler VPX sichtbaren Schnittstellen direkt mit der Anzahl der Schnittstellen auf dem Hypervisor verbunden?

Nein. Sie können bis zu sieben Schnittstellen (10 für VMware) über das NetScaler VPX Konfigurationsdienstprogramm mit nur einer physischen NIC auf dem Hypervisor hinzufügen.

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

## Warum wird eine paravirtuelle (PV) Schnittstelle auf NetScaler VPX als 1G-Schnittstelle (`1/x`) angezeigt, obwohl die zugrunde liegende physische Schnittstelle 10G ist? Bedeutet dies, dass der maximale Durchsatz auf 1 Gbit/s begrenzt ist?

Auf NetScaler VPX werden alle paravirtualisierten NICs (wie VMXNET3) als `1/x` angezeigt, unabhängig von der Geschwindigkeit der dahinterliegenden physischen NIC. Dies ist ein erwartetes Verhalten und bedeutet nicht, dass der Durchsatz auf 1 Gbit/s begrenzt ist. Der tatsächliche Durchsatz wird durch die Kapazität der zugrunde liegenden physischen NIC bestimmt, sodass eine PV-Schnittstelle, die von einer 10G-NIC unterstützt wird, weit über 1 Gbit/s liefern kann.

## Können Citrix Hypervisor XenMotion oder VMware vMotion oder Hyper-V Live-Migration verwendet werden, um aktive Instanzen von NetScaler VPX zu verschieben?

NetScaler VPX unterstützt keine Hyper-V Live-Migration. vMotion wird ab NetScaler Release 13.0 unterstützt. Live Migration (ehemals XenMotion) wird ab NetScaler Release 14.1 Build 17.38 unterstützt.

© 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.