NetScaler Console 14.1

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

Contents

发行说明 65

将 NetScaler Console 本地部署迁移到 Citrix Cloud 67

配置 NetScaler 代理 68

从 Citrix Cloud 获取客户端和密钥 CSV 文件 68

验证 NetScaler Console 服务许可证 68

使用脚本进行迁移 69

回滚到本地部署的 NetScaler Console 73

先决条件 73

使用回滚脚本 73

常见问题 75

NetScaler Console 服务 75

NetScaler 代理是否像本地 NetScaler 代理一样是可选? 75

为什么选择 NetScaler Console 服务? 75

如果本地 NetScaler Console 是高可用性对，迁移后会发生什么? 75

如果代理因任何原因宕机，会发生什么? 75

实例备份也会迁移? 75

历史数据也会迁移? 76

本地许可证也会迁移吗? 76

哪些内容不会从本地 NetScaler Console 迁移? 76

本地 NetScaler Console 与 Citrix Director 集成后会发生什么? 76

迁移后，是否需要再次许可实例或启用分析? 76

迁移工具 76

运行迁移脚本后，显示错误消息。可能是什么问题? 76

NetScaler 实例的版本低于池化许可的限制。如果选择选项“Y”来更改许可证服务器，会发生什么? 77

如果迁移脚本在 NetScaler 实例配置方面失败，会发生什么? 77

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

如果部分 NetScaler 实例未能迁移到 NetScaler Console 服务，会发生什么？重新运行迁移脚本会有帮助吗? 77

是否有日志文件可以检查迁移状态? 77

如果在运行迁移脚本时会话终止，会发生什么? 77

如果 NetScaler Console 服务许可证少于本地 NetScaler Console 且已启动迁移脚本，会发生什么情况? 77

将本地 NetScaler Console 迁移到 NetScaler Console 服务 Express Account 时会发生什么情况? 77

如果 Citrix Cloud 邀请用户（非创建 Citrix Cloud 帐户的管理员用户）尝试迁移本地 NetScaler Console 设置，会发生什么情况? 78

回滚脚本 78

如果在 NetScaler Console 本地 HA 对中使用回滚脚本，会发生什么情况? 78

使用回滚脚本后，灾难恢复节点会发生什么? 78

故障排除 78

手动配置文件已添加到 NetScaler Console 服务 79

NetScaler 设备已添加到 NetScaler Console 服务 79

StyleBook 自定义模板导入到 NetScaler Console 服务 79

添加到 NetScaler Console 服务的配置作业 80

添加到 NetScaler Console 服务的 IP 块 80

网络控制板报告添加状态 80

所有操作指南文章 81

实例管理 81

配置管理 82

证书管理 83

StyleBook 83

分析 84

事件管理 84

身份验证 85

NetScaler Console 系统 85

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

网络功能 86

概述 87

功能和解决方案 87

应用程序分析和管理 87

网络 88

编排 89

架构 89

NetScaler Console 如何发现实例 90

轮询概述 92

NetScaler Console 如何轮询托管实例和实体 93

轮询实例的不同方式 96

实例的全局轮询 96

实例的手动轮询 97

实体的手动轮询 98

NetScaler® 遥测程序 99

遥测数据收集模式 103

自动化遥测数据收集模式 103

手动遥测收集模式 104

用于排查遥测数据收集和上传问题的诊断 106

从版本 14.1 build 56.x 开始的诊断行为 106

工作原理 107

收集器级别（控制台）诊断 107

设备级 (NetScaler) 诊断 108

14.1 build 56.x 版本之前的诊断行为 113

遥测上传通知 116

数据治理 118

IoC 信息使用条件 120

NetScaler Console 许可 121

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

许可 121
高可用性 124
NetScaler Console 高可用性节点之间如何同步许可证? 125
编排 125
升级虚拟服务器许可证 125
验证 126
管理虚拟服务器 126
禁用虚拟服务器的自动授权 127
选择第三方虚拟服务器进行授权 127
手动应用虚拟服务器许可证 127
配置基于策略的虚拟服务器许可 128
查看已获得许可的虚拟服务器 128
为不可寻址的虚拟服务器配置自动许可证支持 129
许可 129
高可用性 131
系统要求 132
NetScaler Console 的要求 132
NetScaler Console 本地代理的要求 132
NetScaler Console 功能所需的最低 NetScaler 版本 133
NetScaler Console 分析的要求 134
NetScaler Console 功能所需的最低 Citrix Virtual Apps and Desktops 版本 134
HDX™ Insight 支持的瘦客户端 135
HDX Insight 所需的 NetScaler 实例许可证 135
支持的虚拟机管理程序 135
支持的操作系统和 Workspace 版本 136
支持的浏览器 136
支持的端口 137
NetScaler Console 服务器的端口 138

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

代理端口 140

NetScaler 实例的端口 141

NetScaler 内置代理的端口 142

外部服务器端口 142

限制 143

开始使用 145

步骤 1 - 查看系统要求 145

步骤 2 - 部署 NetScaler Console 145

步骤 3 - 将实例添加到 NetScaler Console 146

步骤 4 - 在虚拟服务器上启用分析 146

步骤 5 - 在 NetScaler Console 上配置 NTP 服务器 147

步骤 6 - 配置系统设置以优化 NetScaler Console 性能 147

接下来 148

增强型图形用户界面 149

悬停显示菜单 149

精简的菜单层级结构 149

更新的子菜单标签 150

基础架构 > 配置 150

NetScaler 许可 > 许可池 151

网关 > HDX Insight 151

设置 152

可折叠菜单 152

展开的菜单 152

折叠的菜单 152

侧边栏切换 153

显示侧边栏 153

隐藏侧边栏 153

设置为主屏幕 154

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

固定收藏项 154
迁移到服务 155
部署 157
安装 NetScaler Console 的先决条件 158
NetScaler Console 的一般要求 158
仅适用于池化或弹性许可的轻量级 NetScaler® Console 159
思杰虚拟化管理程序上的 NetScaler Console 159
先决条件 159
XenCenter® 系统要求 160
安装 NetScaler® 应用交付管理 160
验证 161
在 Microsoft Hyper-V 虚拟化平台上的 NetScaler Console 162
先决条件 162
Microsoft Hyper-V 系统要求 162
安装 NetScaler® 应用交付管理 162
验证 167
NetScaler 控制台 在 VMware ESXi 上 168
先决条件 168
安装 NetScaler Console 168
验证 172
在 VMware ESXi 上自动部署 NetScaler® 代理 173
配置 NetScaler 代理 173
注册 NetScaler 代理并更改默认密码 173
先决条件 174
如何配置和注册 NetScaler 代理 174
步骤 1：下载并编辑 .OVF 文件 174
步骤 2：在 VMware ESXi 上安装 NetScaler Console 虚拟设备 178
步骤 3: 验证 186

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

Kubernetes 集群上的 NetScaler Console 187
先决条件 187
Kubernetes 集群 187
NFS 共享 187
NetScaler 设备 188
在 Kubernetes 集群上安装 NetScaler Console 188
Linux KVM 服务器上的 NetScaler Console 190
先决条件 190
硬件要求 190
软件要求 191
下载 NetScaler Console 安装文件 191
在 Linux-KVM 上安装 NetScaler 应用交付管理 192
配置 NetScaler 应用交付管理 194
NetScaler Console 在 Nutanix 虚拟机监控程序 (Acropolis) 上 196
硬件要求 196
下载 NetScaler Console 安装文件 197
在 Nutanix 管理程序上配置 NetScaler Console 197
网络配置 201
NetScaler Console 在 红帽 OpenShift 虚拟化 上 203
硬件要求 203
先决条件 203
平台要求 203
部署架构 204
在 红帽 OpenShift 虚拟化 上安装 NetScaler Console 204
步骤 1 - 准备环境 204
步骤 2 - 下载 NetScaler Console 安装文件 204
步骤 3 - 将映像上传到 RHOCPV 可引导卷 204
步骤 4 - 创建虚拟机 206

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

步骤 5. 启动虚拟机 207

步骤 6. 访问 NetScaler Console 207

Azure 云上的 NetScaler Console 207

先决条件 207

配置 NetScaler Console 208

Azure 云上的 NetScaler Console HA 对 209

先决条件 209

配置 NetScaler Console HA 对 209

亚马逊网络服务 (AWS) 上的 NetScaler 控制台 213

先决条件 213

配置 NetScaler Console 213

配置高可用性部署 214

部署场景 215

高可用性架构的组件 217

监控工具 217

主节点 217

辅助节点 217

物理流复制 217

心跳消息 217

浮动 IP 地址 217

关键注意事项 218

先决条件 219

在高可用性模式下设置 NetScaler Console 220

注册第一个服务器（主节点） 220

注册第二个服务器（辅助节点） 221

从主节点 GUI 部署高可用性设置 221

禁用高可用性 223

重新部署高可用性 223

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

高可用性故障转移场景 223

查看数据库同步日志消息 223

脑裂场景 225

许可 225

配置跨不同第 3 层子网的高可用性 (L3 上的 HA) 225

高级架构 226

部署和配置 227

在 NetScaler Console 中配置 HA 228

将 NetScaler 配置为外部负载均衡器 230

NetScaler 负载均衡配置脚本示例 231

优势 236

为高可用性配置灾难恢复 236

启用基本身份验证 237

配置基本身份验证 237

灾难恢复工作流 238

灾难发生前的初始设置 238

先决条件 238

首次灾难恢复设置 239

以高可用性模式部署 NetScaler Console 239

使用 DR 控制台部署并注册 NetScaler Console 灾难恢复节点 240

使用 NetScaler Console GUI 部署灾难恢复节点 242

灾难后的工作流 243

灾难恢复后 244

将配置恢复到原始主站点 244

为独立节点配置灾难恢复 245

灾难恢复工作流 246

先决条件 246

首次灾难恢复设置 247

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

灾难发生后的工作流 250

灾难恢复后 251

将配置还原到原始主站点 251

配置用于多站点部署的本地代理 253

架构 254

启用基本身份验证 254

配置基本身份验证 254

入门 255

在数据中心安装代理 255

端口 256

注册代理 257

将代理附加到站点 258

代理操作 258

添加 NetScaler 实例 259

将现有实例附加到代理 259

访问实例的 GUI 以验证事件 259

NetScaler 代理故障转移 260

配置代理不可达阈值和通知 261

NetScaler® Console 代理与 NetScaler Console 之间的安全通信 261

在 Kubernetes 集群上将 NetScaler® 代理安装为微服务 262

入门 262

在 Kubernetes 集群中安装 NetScaler 代理 263

为 NetScaler Console 本地部署安装 NetScaler Console 代理 OpenShift 操作器 264

先决条件 264

安装代理操作员 265

删除代理实例 269

卸载代理操作员 269

升级代理 269

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

升级工作流 270
将 NetScaler Console 单服务器部署迁移到高可用性部署 272
从 NetScaler Insight Center 迁移到 NetScaler Console 273
先决条件 273
硬件要求 274
安装步骤 274
将 NetScaler Console 与 Citrix Director 集成 275
先决条件 276
HDX Insight 到 NetScaler Console 迁移的硬件要求 276
最低要求 276
软件要求 276
限制 276
将额外磁盘附加到 NetScaler Console 277
在独立 NetScaler Console 中附加额外磁盘 278
启动磁盘分区工具 278
在新的附加磁盘中创建分区 279
调整现有附加磁盘中的分区大小 281
移除附加磁盘中的分区 282
重新启动虚拟机 283
创建磁盘数据备份文件 284
附加命令 285
将附加磁盘连接到高可用性部署中的 NetScaler Console 287
通过 NetScaler Console 进行 NetScaler MPX™ 磁盘加密 289
先决条件 290
在 HSM (Thales CipherTrust Manager) 服务器中添加实例序列号 290
通过 NetScaler Console 进行实例磁盘加密 292
加密后验证 296
加密后恢复 NetScaler MPX 实例 297

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

加密后 NetScaler MPX™ HA 对的行为 297
NetScaler MPX™ 群集加密后的行为 299
NetScaler Console 云连接 301
先决条件 301
配置云连接 304
工作流 1 – 新用户（无 Citrix Cloud 帐户且无 NetScaler Console 服务租户） 304
工作流 2 – Citrix Cloud 帐户存在但 NetScaler Console 服务租户不存在 305
工作流 3 - Citrix Cloud 帐户和 NetScaler Console 服务租户已存在 306
Cloud Connect 的代理配置支持 307
Cloud Connect 状态和刷新行为 308
云连接状态 308
刷新 Cloud Connect 状态 309
云连接诊断 309
错误处理和消息传递 311
Cloud Connect 状态通知 311
通知频率 313
通知渠道 313
管理通知 313
通过 Cloud Connect 收集的数据 314
Cloud Connect 连接问题故障排除 314
其他选项 314
特定版本的功能行为 318
常见问题 318
配置 320
将实例添加到 NetScaler Console 321
如何创建 NetScaler 配置文件 321
将 NetScaler 实例添加到 NetScaler Console 325
将 NetScaler CPX 实例添加到 NetScaler Console 326

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

在 NetScaler Console 中添加独立 NetScaler BLX 实例 327
在 NetScaler Console 中添加高可用性 NetScaler BLX 实例 328
从 NetScaler Console 访问实例 GUI 329
将部署在云中的 NetScaler VPX 实例添加到 NetScaler Console 329
配置分析 331
管理许可并在虚拟服务器上启用分析 331
管理虚拟服务器上的许可 332
全局配置分析功能 337
先决条件 338
启用分析 338
在虚拟服务器上配置分析 340
在现有虚拟服务器上配置分析 341
配置全局分析 344
迁移分析 347
为托管的 NetScaler 实例分配网络配置文件 348
先决条件 349
配置 NTP 服务器 349
配置系统设置 350
配置系统警报 350
配置系统通知 351
配置系统备份设置 351
配置实例备份设置 351
启用基本身份验证 352
配置基本身份验证 352
启用或禁用 NetScaler Console 功能 352
将 NetScaler Console 与 ServiceNow 实例集成 353
先决条件 354
如何将 NetScaler Console 与 ServiceNow 集成? 354

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

步骤 1 - 在 Citrix Cloud 中订阅 ITSM Adapter 服务 354
步骤 2 - 在 ServiceNow 实例中创建端点访问 355
步骤 3 - 添加 ServiceNow 实例 356
步骤 4 - 在 NetScaler Console 中测试 ServiceNow 票证的自动生成 356
在 NetScaler Console 中设置 ServiceNow 通知 357
导出或计划导出报告 358
导出报告 358
计划导出报告 358
查看和编辑计划导出的报告 359
升级 360
升级前 360
升级到 14.1-xx.xx 及更高版本之前需要注意的重要事项 361
将单个 NetScaler Console 服务器升级到 14.1-xx.xx 361
将高可用性对升级到 14.1 版本 362
升级 NetScaler Console 灾难恢复部署 362
升级 NetScaler Console 灾难恢复节点 363
升级多站点部署的本地代理 363
升级本地代理 363
向 NetScaler Console 服务器添加额外磁盘 364
认证 365
外部认证服务器 365
在 NetScaler Console 中认证用户 366
添加 LDAP 身份验证服务器 366
添加 RADIUS 身份验证服务器 368
添加 TACACS 身份验证服务器 371
NetScaler Console 中的用户 374
NetScaler Console 中的用户组 374
提取身份验证服务器组 375

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

启用外部身份验证服务器和回退选项 375
配置回退和级联外部服务器 376
LDAP、RADIUS 和 TACACS 支持双因素认证 (2FA) 377
配置双因素认证 377
使用双因素身份验证访问 NetScaler® Console 380
访问控制 382
基于角色的访问控制 382
限制 383
配置访问策略 384
授予用户 StyleBook 权限 387
配置组 387
创建用户组 387
用户访问权限如何根据授权范围而变化 397
将 NetScaler Console 从 12.0 升级到更高版本时 RBAC 的映射 397
配置角色 398
配置用户 399
可操作任务和建议 401
任务 404
建议 409
如何使用“引导我”工作流并完成建议? 411
配置通知 411
常见问题 412
统一仪表板，用于查看实例关键指标详细信息 413
应用程序 413
NetScaler 基础架构 414
应用程序安全性 415
网关 416
自定义仪表板 417

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

查看代理详细信息 419
创建并应用筛选器 420
编辑筛选器 422
创建自定义仪表板以查看实例关键指标详细信息 423
仪表板中的更多选项 425
将仪表板共享给其他用户 426
应用程序 427
先决条件 427
应用程序概述 427
离散应用程序 427
自定义应用程序 428
注意事项 428
微服务应用程序 428
应用程序管理和应用程序仪表板 428
管理应用程序 428
应用程序仪表板 429
新仪表板行为与旧仪表板相比的更新 429
管理应用程序 430
查看应用程序详细信息 430
添加应用程序 431
使用 StyleBook 创建应用程序 433
编辑或删除应用程序 434
导出应用程序仪表板和安全仪表板报告 434
查看应用程序 434
配置并将一个应用程序关联到多个自定义应用程序 435
应用程序仪表板概述 437
使用搜索栏搜索和筛选结果 440
创建标签并将其应用于应用程序 440

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

应用程序详细信息 442
选择应用评分组件并设置阈值 447
微服务应用程序的应用程序详细信息 450
智能应用分析 455
配置智能应用分析 455
应用程序分析的性能指标 457
响应时间 458
活动服务 459
平均 CPU 使用率 459
内存使用情况 460
服务抖动 461
不稳定服务器 462
会话堆积 463
低会话重用 464
突发队列积压 465
异常大的 HTTP 数据包 465
不当的持久性类型 466
TCP 重组队列达到限制 467
SSL 实时流量 468
应用程序仪表板故障排除 469
故障排除场景 470
应用程序已获得许可 470
指标收集器已启用 471
NetScaler® 实例早期版本 471
NetScaler 实例后续版本 473
应用程序使用情况和异常 477
峰值和低谷使用情况分析 478
评估应用程序扩展限制 478

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

识别前 5 个应用程序维护窗口 479

应用程序使用情况分析 481

以图形格式查看指标详细信息 488

排查 Web Insight 问题 490

A+ SSL 评级分析 491

升级到 A+ SSL 评级 492

回滚 SSL 评级 493

确定 SSL 评级对应用程序流量的影响 495

Web Insight 仪表板 496

集成缓存请求 499

排查 Web Insight 问题 500

查看应用程序延迟的根本原因 500

应用程序深入分析 501

响应时间 502

服务图 504

所有 NetScaler 实例中应用程序的服务图 504

Kubernetes 应用程序的服务图 505

三层 Web 应用程序的服务图 505

适用于 Kubernetes 应用程序的服务图 506

设置服务图 507

软件要求 507

开始之前 508

单层或统一入口拓扑 508

双层或 Service Mesh Lite 拓扑 508

服务网格拓扑 509

在服务图中查看详细信息 510

服务图仪表板 511

使用表格视图查看关键指标趋势 514

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

查看客户端指标 515

查看 TCP 和 SSL 指标 519

查看服务详情 520

应用筛选器 520

使用设置选项 522

分析错误 523

查看 HTTP 事务详情 524

在服务图中配置阈值 526

单阈值 527

双阈值 527

查看服务详情 528

指标详情 529

查看后端 Pod 详细信息 529

查看入口详细信息以排查问题 530

分布式追踪 533

先决条件 534

查看服务跟踪详细信息 539

查看事务详细信息 540

查看服务图中部分数据或无数据的诊断详细信息 542

无数据诊断 542

部分数据的诊断 543

故障排除 544

应用程序的服务图 544

应用程序视图 545

网络功能视图 545

无活动事务的服务图视图 546

分析指标 547

客户端指标 547

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

网络功能指标 548

服务指标 548

NetScaler 指标（仅适用于 GSLB 应用程序） 549

服务图中所有应用程序的全局视图 549

查看客户端指标 550

查看 NetScaler 详细信息 551

查看离散应用程序 552

查看微服务应用程序 555

搜索栏以筛选结果 557

StyleBooks 559

StyleBook 类别 560

默认 StyleBook 和自定义 StyleBook 561

公共 StyleBook 和私有 StyleBook 561

标记为私有的 StyleBook 示例 561

查看 StyleBook 562

下载自定义 StyleBook 563

更新自定义 StyleBook 564

删除自定义 StyleBook 565

查看 StyleBook 依赖项 566

查看 StyleBook 依赖项 566

正向依赖项 566

反向依赖项 566

根据配置包审核 NetScaler 配置 567

下载配置包的支持包 568

为 StyleBook 创建标签 569

使用 CLI 命令配置 StyleBook 570

克隆 StyleBook 570

从外部存储库导入和同步 StyleBook 571

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

添加存储库并从外部存储库导入 StyleBook 572

从 GitHub/GitLab 导入 StyleBook 和配置包的步骤 576

使用默认样式簿 576

从默认样式簿创建配置 576

Web 应用防火墙 StyleBook 582

部署应用程序防火墙配置 583

隐藏所有默认 StyleBook 587

Prometheus 分析 StyleBook 588

先决条件 588

使用 StyleBooks 配置构建器迁移 NetScaler® 应用程序配置 589

在迁移的配置之间共享配置实体 590

支持的 NetScaler 功能 590

创建 StyleBook 以迁移 NetScaler 应用程序配置 591

限制 595

业务应用程序样式书 595

SSO Google 应用样式簿 596

部署 SSO Google 应用 StyleBook 596

SSO Office 365 样式簿 599

部署 SSO Microsoft Office 365 样式簿 600

微软商务版 Skype 样式簿 609

主要组件 610

在企业中配置 NetScaler 实例 611

Microsoft Exchange 样式簿 616

使用 Microsoft Exchange StyleBook 配置的 NetScaler 功能 616

先决条件 617

配置 Microsoft Exchange 样式簿 617

Microsoft SharePoint 样式簿 619

先决条件 619

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

由 Microsoft SharePoint 2016 样式簿配置的 NetScaler 功能 619

部署 SharePoint StyleBook 配置 621

查看 NetScaler 实例上定义的对象 627

Microsoft ADFS 代理 StyleBook 629

使用 NetScaler 作为 ADFS 代理的优势 629

Oracle 电子商务 StyleBook 649

为 Oracle E-Business Suite 12.2 创建配置 649

Citrix StoreFront™ 样式簿 650

为 Citrix StoreFront 应用程序创建配置 651

创建和使用自定义 StyleBook 652

开始之前 652

StyleBook 的结构 653

用于创建负载均衡虚拟服务器的样式簿 654

标头 654

组件 659

构建您的 StyleBook 660

用于创建基本负载均衡配置的 StyleBook 663

标头 663

组件 666

输出 670

构建您的 StyleBook 671

创建复合 StyleBook 675

构建您的 StyleBook 676

在自定义 StyleBook 中使用 GUI 属性 680

导入自定义 StyleBook 681

导入您的 StyleBook 681

搜索自定义 StyleBook 687

创建和编辑配置包 687

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

创建配置包 687
重用在 StyleBooks 外部创建的配置并在 ConfigPacks 之间共享配置 688
更改配置包的 StyleBook 689
导出或导入配置包 691
将配置包另存为草稿 694
为配置包创建计划 696
从配置包中分离目标实例 697
构建您的 StyleBook 698
创建 StyleBook 以将文件上传到 NetScaler Console 702
StyleBook 配置 702
构建您的 StyleBook -1 702
构建您的 StyleBook - 2 704
创建用于上传文件的配置 706
创建 StyleBook 以将 SSL 证书和证书密钥文件上传到 NetScaler Console 707
StyleBook 配置 707
创建用于上传 SSL 文件的配置 710
构建您的 StyleBook 711
使用 StyleBooks 从证书存储管理 SSL 证书 715
参数 716
组件 717
构建您的 StyleBook 717
在 StyleBook 中定义的虚拟服务器上启用分析并配置警报 722
实例角色 724
目标角色部分 724
角色“默认” 725
具有角色的组件 725
构建您的 StyleBook 729
使用 API 734

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

创建 StyleBook 以执行非 CRUD 操作 735
支持非 CRUD 操作 736
将 StyleBook 的配置包迁移到另一个 StyleBook 737
迁移配置包 737
构建您的 StyleBook 740
管理数据源 744
将 NetScaler 实例用作数据源 745
不带集合使用内置数据源 745
使用带集合的内置数据源 748
将目标 NetScaler 实例用作数据源 755
将目标 NetScaler 实例用作数据源的示例 StyleBook 756
使用自定义数据源 757
添加数据源类型 758
在数据源类型下添加集合架构 759
添加数据源 759
添加集合数据 760
使用不带集合的自定义数据源 761
将自定义数据源与集合一起使用 763
使用 API 从 StyleBook 创建配置 766
示例 1 767
示例 2 770
示例 3 772
示例 4 774
更新配置 776
删除配置 778
使用 API 创建配置以上传证书和密钥文件 779
使用 API 创建配置以上传任何文件类型 781
使用 API 导入自定义 StyleBook 782

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

使用 API 下载自定义 StyleBook 784
使用 API 删除自定义 StyleBook 785
StyleBooks 语法 786
标头 787
导入 StyleBooks 789
参数 790
'名称' 791
'标签' 791
'描述' 791
'类型' 791
'网络' 794
'动态分配' 794
'键' 795
'必需' 795
'允许值' 795
'默认值' 797
'模式' 798
'最小值' 799
'最大值' 799
'最小长度' 800
'最大长度' 800
“最小项数” 800
“最大项数” 801
“GUI” 801
“列” 801
“可更新” 802
'collapse_pane' 802
“布局” 808

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

'依赖参数' 808
参数-默认源构造 810
参数源构造 815
参数条件 816
'增加允许值' 816
'显示' 或 '隐藏' 817
'设置默认值' 817
'设置必需' 818
'设置允许值' 819
'设置标签' 819
'设置描述' 820
'折叠窗格' 或 '展开窗格' 820
'设置模式' 821
嵌套参数条件 821
替换 822
替换映射 829
遍历替换列表 830
组件 833
辅助组件 835
可选属性 837
属性默认源 构造体 839
组件属性的计算 841
嵌套组件 841
条件构造 843
重复构造 845
重复条件构造 848
嵌套重复 849
输出 851

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

参数参考 853
父级引用 854
组件参考 856
替换引用 858
变量引用 858
操作 859
分析 864
目标虚拟服务器和洞察类型 867
告警 867
表达式 871
算术表达式 871
字符串表达式 871
列表表达式 871
关系表达式 872
逻辑表达式 - 布尔型 872
逐字字符串表达式 873
目标表达式 874
表达式类型验证 874
就地插值 877
插值中允许的类型 878
简单插值 878
自动类型转换 878
顺序插值 879
嵌套插值 879
带引号包装的插值 879
内置函数 880
字符串() 880
整数() 881

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

布尔() 881
len() 函数 881
min() 函数 882
max() (最大值) 882
二进制() 882
八进制() 883
十六进制() 883
小写() 883
大写() 883
求和() 883
pow() (幂函数) 884
ip() 884
base64.encode() 884
base64.decode() 885
存在() 885
过滤() 885
如果-那么-否则() 885
连接() 886
分割() 887
映射() 887
引用包装() 888
替换() 888
修剪() 889
截断() 889
去重() 890
url.encode() 890
url.decode() 890
是-IPv4() 890

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

是-ipv6() 890

以开头() 890

以结尾() 891

包含() 891

子串() 891

多重() 892

反转() 892

依赖检测 893

循环依赖 895

安全 897

应用程序安全仪表板 897

威胁指数详细信息 898

安全指数详情 899

统一安全仪表板 900

已保护的应用程序 901

配置未受保护应用程序的保护 901

查看应用程序安全违规详情 911

先决条件 911

API 安全 912

查看 API 分析 912

API 端点分布 912

API 实例 913

API 端点 914

身份验证失败 914

查看不同的 API 洞察 915

发现 API 端点 921

查看 API 端点 921

网关 923

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

网关洞察 923
注意事项 923
限制 924
启用 网关洞察 924
对于 NetScaler Console 版本 **13.0 Build 41.x 或更高版本** 925
使用 GUI 在 NetScaler Gateway 设备上启用 AppFlow 身份验证、授权和审计用户名日志记录 925
查看 Gateway Insight 报告 926
查看 EPA、SSO、身份验证、授权和应用程序启动失败 926
查看会话模式、客户端和用户数量的摘要 926
查看用户的 Gateway Insight 报告 926
查看用户详细信息 927
查看应用程序的 Gateway Insight 报告 929
查看应用程序详细信息 929
查看网关的 Gateway Insight 报告 930
要查看网关详细信息 930
导出报告 931
导出报告 932
网关洞察用例 932
用户无法登录到 NetScaler Gateway 设备或内部 Web 服务器 932
身份验证失败 933
EPA 失败 934
SSO 故障 935
用户成功登录 NetScaler Gateway 后无法启动任何虚拟应用程序 936
成功启动新应用程序后，用户想要查看该应用程序消耗的总字节数和带宽 937
用户已成功登录 NetScaler Gateway，但无法访问内部网络中的某些网络资源 938
不同的用户可能使用不同的 NetScaler Gateway 部署，或者可能通过不同的访问模式登录到 NetScaler Gateway。管理员必须能够查看有关部署类型和访问模式的详细信息 938

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

排查 Gateway Insight 问题 939
Gateway Insight 配置清单 939
NetScaler 与 NetScaler Console 之间的连接清单 940
NetScaler 中的记录生成清单 940
NetScaler Console 中记录的验证 940
NetScaler Console 中 Logstream 日志的验证 941
Gateway Insight 计数器 941
NetScaler 日志中的 AppFlow 记录 942
联系 Citrix 技术支持 943
已知问题 943
HDX™ 洞察 943
识别性能缓慢问题的根本原因 945
场景 1 945
场景 2 947
HDX Insight 的地理地图 948
用例 948
限制 949
启用 HDX™ Insight 数据收集 949
为以 LAN 用户模式部署的 NetScaler 启用数据收集 949
为以单跳模式部署的 NetScaler Gateway 设备启用数据收集 953
为以双跳模式部署的 NetScaler Gateway 设备启用数据收集 955
在用于 Optimal Gateway 的虚拟服务器上配置 HDX Insight 956
启用数据收集以监控以透明模式部署的 NetScaler 961
为以单跳模式部署的 NetScaler Gateway 设备启用数据收集 964
启用数据收集以监控以透明模式部署的 NetScaler 965
为双跳模式下部署的 NetScaler Gateway 设备启用数据收集 968
启用数据收集以监控以 LAN 用户模式部署的 NetScaler 973
为 HDX™ Insight 创建阈值并配置警报 977

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

示例用例 978

查看 HDX™ Insight 报告和指标 980

用户视图报告和指标 980

应用程序视图报告和指标 995

桌面视图报告和指标 1002

实例视图报告和指标 1013

许可证视图报告和指标 1018

应用程序视图报告和指标 1019

桌面视图报告和指标 1026

用户视图报告和指标 1038

实例视图报告和指标 1051

许可证视图报告和指标 1057

排查 HDX™ Insight 问题 1058

HDX Insight 配置清单 1058

NetScaler 与 NetScaler Console 之间的连接清单 1059

NetScaler 中 HDX/ICA 流量的记录生成清单 1059

错误计数器 1067

nstrace 验证 1070

NetScaler Console 清单中的记录填充 1070

联系 Citrix 技术支持之前 1071

已知问题 1071

基础架构 1072

基础架构分析 1072

基础架构分析 1073

实例分数 1073

运行状况指示器 1073

查看 NetScaler 容量问题 1075

运行状况指示器值 1075

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

基础架构分析仪表板 1076
圆形打包视图 1077
实例圆圈 1077
分组实例圆圈 1078
集群实例圆圈 1079
如何使用环形图包 1079
表格视图 1080
如何使用摘要面板 1082
实例信息 1085
流量配置文件 1085
如何使用设置面板 1086
视图 1086
分数阈值 1087
如何在仪表板上可视化数据 1088
在基础设施分析中查看实例详细信息 1089
查看 NetScaler 实例中的容量问题 1096
查看解决容量问题的建议操作 1097
增强型基础架构分析，带新指标 1098
表格视图 1100
查看异常详情 1101
实例管理 1101
添加实例 1102
如何使用实例仪表板 1102
监控全球分布式站点 1104
用例 1104
配置地理地图 1105
如何创建标签并将其分配给实例 1109
如何使用标签和属性值搜索实例 1112

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

搜索 NetScaler VPX 实例 1112
通过 NetScaler® Console 集中式 GeoIP 数据库更新 1114
限制 1114
通过 NetScaler Console 配置集中式 GeoIP 数据库更新 1114
管理 NetScaler 实例的管理员分区 1115
创建 NetScaler 高可用性对 1119
备份和恢复 NetScaler 实例 1123
配置实例备份设置 1124
使用 NetScaler Console 还原 NetScaler 实例 1128
强制故障转移到辅助 NetScaler 实例 1130
强制辅助 NetScaler 实例保持辅助状态 1131
创建实例组 1132
使用 NetScaler Console 创建实例组 1132
识别未映射的实例并将其添加到组中 1132
使用 NetScaler Console 在 SDX 上预配 NetScaler VPX 实例 1133
步骤 1 - 添加 VPX 实例 1133
步骤 2 - 分配许可证 1134
步骤 3 - 分配资源 1135
步骤 4 - 添加实例管理 1138
步骤 5 - 指定网络设置 1139
步骤 6 - 指定管理 VLAN 设置 1140
查看已预置的 VPX 实例 1141
在 VMware ESX 上预配 NetScaler VPX 实例 1142
先决条件 1142
将 NetScaler VPX 文件转换为模板 1142
为 NetScaler Console 访问 VMware vCenter 创建权限 1143
在 NetScaler Console 中创建站点 1144
在 VMware ESX 上预置实例 1145

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

重新发现多个 NetScaler VPX 实例 1149
取消管理实例 1149
跟踪到实例的路由 1150
查看 NetScaler 拥有的 IP 地址 1151
导出 NetScaler 拥有的 IP 地址 1152
安排导出 NetScaler 拥有的 IP 地址 1152
将配置从一个 NetScaler 实例复制到另一个实例 1155
将配置从一个实例复制到其他 NetScaler 实例 1155
SSL 证书管理 1156
企业 SSL 策略设置 1156
NetScaler Console 证书的工作原理 1157
SSL 证书管理用例 1158
安装 SSL 证书 1158
证书过期通知设置 1158
证书续订 1159
链接和取消链接 SSL 证书 1162
审计日志 1162
使用 ACME 协议进行自动化证书续订 1163
NetScaler® Console 中的 ACME 支持 1163
ACME 集成配置步骤 1165
颁发和续订 1173
颁发证书 1175
第三方集成 1179
限制 1181
排查与自动证书续订相关的问题 1181
零接触证书管理 1182
上传证书 1183
启用零接触证书管理 1184

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

SSL 过滤模式支持 1185
配置筛选模式设置 1186
使用 SSL 仪表板 1186
监控 SSL 证书 1187
查看 SSL 证书的审计跟踪 1188
在 SSL 控制面板上删除 SSL 证书 1189
在 SSL 控制板上排除默认 NetScaler 证书 1190
查看、上传和下载 SSL 文件 1191
查看 SSL 证书链 1191
设置 SSL 证书过期通知 1192
更新已安装的证书 1194
在 NetScaler 实例上安装 SSL 证书 1195
创建证书签名请求 (CSR) 1197
链接和取消链接 SSL 证书 1200
配置企业策略 1200
从 NetScaler 实例轮询 SSL 证书 1201
使用 NetScaler Console 证书存储来管理 SSL 证书 1202
将 SSL 证书添加到证书存储 1202
更新证书存储中的 SSL 证书 1202
从证书存储中删除 SSL 证书 1203
在 NetScaler® 实例上安装 SSL 证书 1203
从 NetScaler 实例导入证书 1203
更新服务器证书无需中间上传 1204
在高可用性部署中管理数据库自定义证书和密码 1205
在 NetScaler Console 上安装数据库证书 1205
管理您已安装的数据库证书 1206
配置数据库密码套件 1206
事件 1207

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

使用事件仪表板 1208
为事件设置事件时效 1209
计划事件过滤器 1211
设置事件的重复电子邮件通知 1212
抑制事件 1214
创建事件规则 1214
步骤 1 - 定义事件规则 1216
步骤 2 - 选择事件的严重性 1216
步骤 3 - 指定事件类别 1217
步骤 4 - 指定 NetScaler 实例 1217
步骤 5 - 选择故障对象 1217
步骤 6 - 指定高级筛选器 1218
步骤 7 - 添加事件规则操作 1219
修改 NetScaler 实例上发生的事件的报告严重性 1227
查看事件摘要 1228
查看事件消息 1229
显示事件严重性和 SNMP 陷阱详细信息 1229
查看和导出 NetScaler syslog 消息 1231
将 NetScaler Console 配置为 syslog 服务器 1231
查看和搜索 syslog 消息 1232
导出和计划 syslog 消息 1233
抑制 syslog 消息 1236
通过创建过滤器抑制 syslog 消息 1236
禁用筛选器 1238
配置实例事件的清除设置 1238
网络功能 1239
为负载均衡实体生成报告 1239
生成组合负载平衡报告 1240

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

生成单个负载均衡实体报告 1241

导出或计划导出网络功能报告 1242

网络报告 1244

网络报告仪表板 1244

导出网络报告 1247

通过应用聚合查看网络报告数据 1248

如何在 NetScaler Console 上管理网络报告的阈值 1250

设置网络报告的性能轮询间隔 1252

配置网络报告清除设置 1252

配置作业 1252

配置模板 1253

实例 1253

文件 1253

录制和播放 1254

相关文章 1254

创建配置作业 1254

使用录制和回放创建配置作业 1258

使用配置作业将配置从一个实例复制到多个实例 1260

在配置作业中使用变量 1262

从纠正命令创建配置作业 1265

将运行中和已保存的配置从一个 NetScaler 实例复制到另一个实例 1267

重用已运行的配置作业 1268

在配置作业中使用 SCP (put) 命令 1269

使用配置模板 1271

使用主配置模板 1272

使用内置模板创建的计划作业 1279

安排一个作业，用于配置将指标从 NetScaler 导出到 Prometheus 1281

使用配置模板创建审计模板 1284

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

重新安排使用内置模板配置的作业 1286

在配置作业中重用配置审计模板 1286

导入和导出配置模板 1289

配置审计 1290

查看审计报告 1290

审计实例间的配置更改 1296

获取网络配置建议 1303

轮询 NetScaler® 实例的配置审计 1304

为 ConfigChange SNMP 陷阱生成配置审计差异 1305

升级作业 1306

升级前验证 1307

NetScaler Console 执行的预升级检查 1308

NetScaler 执行的预升级检查 1308

安排 NetScaler 实例升级 1308

安排升级 NetScaler SDX 实例 1313

计划升级 NetScaler BLX 实例 1314

计划升级 Autoscale™ 组 1317

计划配置 NetScaler 实例的 HA 对 1318

计划将 HA 实例对转换为群集 1319

使用作业升级 NetScaler® 实例 1320

预验证检查 1320

NetScaler 高可用性对 1321

NetScaler 群集 1321

创建升级维护作业以升级 NetScaler 实例 1321

暂停或恢复计划的升级作业 1329

重试失败的升级作业 1330

清理 NetScaler 磁盘空间 1331

为 NetScaler 高可用性对安排升级作业 1333

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

下载 NetScaler 升级作业的组合差异报告 1333
安全咨询 1334
安全咨询登录页面 1334
安全配置建议 1336
CVE 检测 1336
文件完整性监控 1336
立即扫描 1336
扫描历史记录 1337
受影响的 NetScaler 1338
设置 1338
安全配置建议 1339
基于严重性的优先级划分 1339
详细实例级视图的优势 1340
修复配置建议 1341
CVE 检测 1344
实例视图 1345
CVE 视图 1347
CVE 存储库 1348
注意事项 1348
文件完整性监控 1350
控制台检测 1350
设备报告 1352
NetScaler Console 中的入侵指标检测 1353
先决条件 1353
优势 1353
通过安全通告支持的 CVE 1355
最新支持的 CVE 1355
支持的 CVE 1356

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

识别并修复 CVE-2026-88771 漏洞 1359
修复 CVE-2026-88771 1360
识别并修复 CVE-2026-88772 漏洞 1360
修复 CVE-2026-88772 1360
识别并修复 CVE-2026-88773 漏洞 1361
修复 CVE-2026-88773 1361
识别并修复 CVE-2026-88774 的漏洞 1362
修复 CVE-2026-88774 1362
识别并修复 CVE-2026-88775 的漏洞 1362
修复 CVE-2026-88775 1363
识别并修复 CVE-2026-88776 的漏洞 1363
修复 CVE-2026-88776 1364
识别并修复 CVE-2026-88777 的漏洞 1364
修复 CVE-2026-88777 1365
修复 CVE-2026-88778 的漏洞 1365
修复 CVE-2026-88778 1365
识别并修复 CVE-2026-19490 的漏洞 1367
修复 CVE-2026-19490 1367
识别并修复 CVE-2026-19489 的漏洞 1368
修复 CVE-2026-19489 1368
修复 CVE-2026-13474 的漏洞 1368
修复 CVE-2026-13474 1369
识别并修复 CVE-2026-10817 的漏洞 1371
修复 CVE-2026-10817 1372
识别并修复 CVE-2026-10816 的漏洞 1372
修复 CVE-2026-10816 1373
识别并修复 CVE-2026-8655 漏洞 1373
修复 CVE-2026-8655 1374

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

识别并修复 CVE-2026-8452 的漏洞 1374
修复 CVE-2026-8452 1375
识别并修复 CVE-2026-8451 漏洞 1375
修复 CVE-2026-8451 1376
识别并修复 CVE-2026-4368 漏洞 1376
修复 CVE-2026-4368 1376
识别并修复 CVE-2026-3055 漏洞 1377
修复 CVE-2026-3055 1378
识别并修复 CVE-2025-12101 的漏洞 1378
修复 CVE-2025-12101 1379
识别并修复 CVE-2025-8424 漏洞 1379
修复 CVE-2025-8424 1381
识别并修复 CVE-2025-7776 的漏洞 1381
修复 CVE-2025-7776 1383
识别并修复 CVE-2025-7775 的漏洞 1383
修复 CVE-2025-7775 1385
识别并修复 CVE-2025-6543 漏洞 1385
修复 CVE-2025-6543 1386
识别并修复 CVE-2025-5349 漏洞 1387
修复 CVE-2025-5349 1388
修复 CVE-2025-5777 的漏洞 1389
修复 CVE-2025-5777 1390
修复 CVE-2024-8535 的漏洞 1393
修复 CVE-2024-8535 1393
修复 CVE-2020-8300 的漏洞 1396
修复 CVE-2020-8300 1397
场景 1402
修复 CVE-2021-22927 和 CVE-2021-22920 的漏洞 1404

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

修复 CVE-2021-22927 和 CVE-2021-22920 1406

场景 1413

识别并修复 CVE-2021-22956 漏洞 1416

识别受 CVE-2021-22956 影响的实例 1417

修复 CVE-2021-22956 1417

识别并修复 CVE-2022-27509 漏洞 1420

识别受 CVE-2022-27509 影响的实例 1422

修复 CVE-2022-27509 1422

安全通报中不支持的 CVE 1423

升级建议 1423

查看升级建议 1424

设置首选版本 1426

升级 NetScaler 实例 1426

编排 1430

VMware NSX 管理器 1431

OpenStack: 集成 NetScaler 实例 1432

适用于 OpenStack Neutron LBaaS 的 NetScaler 驱动程序 1432

NetScaler Console 和 OpenStack 相互注册 1432

OpenStack 中的租户 1432

放置策略 1432

服务包 1432

LBaaS V1 和 LBaaS V2 支持的功能 1433

用例场景 1433

NetScaler Console 与 OpenStack 工作流集成 1434

OpenStack: 集成 NetScaler 实例 1435

先决条件 1438

NetScaler Console 和 OpenStack 中的预配置任务 1439

使用 Horizon 配置 LBaaS V1 1449

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

使用命令行配置 LBaaS V2 1449
配置七层内容切换 1454
在 OpenStack 上手动预配 NetScaler VPX 实例 1460
使用 StyleBook 在 OpenStack 上预置 NetScaler VPX 实例 1462
OpenStack 环境的 VPX 签入和签出许可证以及池化许可证支持 1463
管理员分区共享 VLAN 支持 1464
试用许可工作流程 1467
与 OpenStack Heat 服务集成 1467
服务包隔离策略 1473
灵活的基于策略的设备分配 1476
NSX Manager: NetScaler 实例的手动预配 1482
先决条件 1482
VMware ESXi 硬件要求 1482
配置 VMware NSX 1483
在 NetScaler Console 中添加 NetScaler VPX 实例 1485
将 VMware NSX Manager 注册到 NetScaler Console 1487
在 NetScaler Console 中创建服务包 1488
为边缘执行负载平衡器服务插入 1490
在 NSX Manager 上查看 L2 网关 1495
查看已分配的 NetScaler 1495
使用 StyleBook 配置 NetScaler VPX 实例 1496
查看负载均衡器配置 1497
删除负载均衡器服务 1497
NSX Manager：NetScaler 实例的自动预配 1498
概述 1498
先决条件 1498
NetScaler Console 和 NetScaler 实例的高可用性部署 1499
设置 NetScaler Console HA 端点详细信息 1499

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

将 VMware NSX Manager 注册到 NetScaler Console 1499

在 NetScaler Console 中上传许可证 1500

在 NetScaler Console 中上传 NetScaler VPX 映像 1501

在 NetScaler Console 中创建服务包 1501

为 Edge 执行负载均衡器服务插入 1503

在 VMware NSX Manager GUI 中配置 NetScaler VPX 上的负载平衡服务 1505

在 NetScaler Console GUI 中配置 NetScaler VPX 上的负载均衡服务 1507

验证 NetScaler VPX 实例中虚拟服务器和服务组的创建 1507

删除负载平衡服务 1507

在 NetScaler Console 中管理 Kubernetes Ingress 配置 1508

开始之前 1509

使用秘密令牌配置 NetScaler Console 以管理 Kubernetes 集群 1509

在 NetScaler Console 中添加 Kubernetes 集群 1509

设置 1512

配置 IP 地址管理 (IPAM) 1512

添加外部 IP 地址提供程序 1512

将 Infoblox DDI 作为外部提供程序 1513

添加网络 1514

查看已分配的 IP 地址 1515

配置操作策略以接收应用程序事件通知 1516

配置操作策略 1517

使用搜索栏 1525

使用审计日志选项 1525

可观测性集成 1525

与 Splunk 集成 1526

配置 Splunk 以从本地 NetScaler Console 接收数据 1526

配置本地 NetScaler Console 以将数据导出到 Splunk 1533

在 Splunk 中查看仪表板 1535

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

与 New Relic 集成 1539

先决条件 1539

New Relic 控制板 1541

与 Microsoft Sentinel 集成 1543

配置 Log Analytics 工作区 1543

创建 Microsoft Entra 应用程序 1547

配置数据收集终结点 1549

创建表以导出数据 1550

在 NetScaler Console 中创建订阅 1564

在 Microsoft Azure 中查看日志 1565

配置 NetScaler® 实例以使用默认架构将洞察数据导出到 Prometheus 1566

查看失败配置的日志 1567

配置将 NetScaler® 指标和审计日志导出到 Splunk 1568

查看失败配置的日志 1568

访问控制列表 1569

使用指南 1569

如何配置 ACL 1569

启用 ACL 功能 1570

创建 ACL 规则 1570

启用 ACL 规则 1573

ACL 规则的其他操作 1573

禁用 ACL 规则 1573

编辑 ACL 规则 1573

删除 ACL 规则 1574

重新编号 ACL 规则的优先级 1574

故障排除 1575

使用 NetScaler Console 审计日志管理和监控您的基础架构 1576

NetScaler 实例相关的审计日志 1576

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

将 NetScaler Console 服务配置为 syslog 服务器 1576
NetScaler Console 相关的审核日志 1577
配置 syslog 服务器以监控审核日志和 shell 日志 1577
应用程序相关审计日志 1578
NetScaler 许可证 1579
许可证激活服务 1579
NetScaler 与 LAS 的版本兼容性 1581
过渡到 LAS 1582
通过 Cloud Connect 激活 LAS 1582
许可或将 NetScaler 实例迁移到 LAS 1584
许可证激活 Blob 行为 1589
许可证宽限期警报 1589
当本地 Console 与 Console 服务之间的连接中断时，NetScaler 行为更新 1589
LAS 许可工作流期间发送到 LAS 的信息 1590
监控已转换为 LAS 的 NetScaler Console 本地部署云连接环境的最佳实践 1591
先决条件 1591
监控本地 Console LAS 激活 Blob 到期 1592
使用 GUI 监控上次续订日期 1592
监控 NetScaler 实例 LAS 激活 blob 过期（通过本地部署云连接的 Console 授权的 NetScaler） 1596
使用 CLI 查看 NetScaler 实例状态 1596
通知 1597
监控许可证权利到期 1599
通知 1599
基于电子邮件的通知 1599
许可证管理 1600
基于 LAS 的许可证 1601
许可证服务器端口 1601

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

许可证到期信息 1602

通知设置 1602

LAS 的 RBAC 支持 1604

手动管理的权利（基于文件的许可证） 1605

许可证文件 1605

重要注意事项 1606

许可证服务器端口设置 1607

许可证到期信息 1608

通知设置 1608

弹性许可和池许可的最小和最大容量 1611

表 1. MPX 支持的弹性容量 1612

表 2A. 适用于低于版本 13.0-47.x 的 NetScaler SDX 支持的弹性容量 1613

表 2B. 适用于 NetScaler SDX 13 版（内部版本 13.0-47.x 及更高版本）、13.1 版（内部版本早于 51.x）和 14.1 版（内部版本早于 12.x）的支持弹性容量 1614

表 2C. 适用于 NetScaler SDX 13.1 版（内部版本 51.x 及更高版本）和 14.1 版（内部版本 12.x 及更高版本）的支持弹性容量 1615

表 3. NetScaler CPX 实例支持的最小/最大带宽和最小/最大实例数 1617

表 4. Hypervisor 和云服务上 NetScaler VPX 实例支持的最小/最大带宽和最小/最大实例数 1617

表 5. NetScaler BLX 实例支持的最小/最大带宽和最小/最大实例数 1618

表 6. 不同外形规格的零容量许可证要求 1618

弹性容量许可证 1619

零容量硬件 1620

管理和安装 Z-cap 许可证 1620

独立 NetScaler VPX 实例 1621

独立 NetScaler CPX 实例 1622

独立 NetScaler BLX 实例 1622

带宽池 1622

实例池 1622

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

配置许可证 1623
基于 LAS 的许可 1624
步骤 1：激活 LAS 并获取权利 1624
步骤 2：将 NetScaler 实例添加到 NetScaler Console On-prem 1625
步骤 3：许可或迁移 NetScaler 实例 1625
步骤 4：编辑弹性吞吐量容量 1625
未授权 MPX 设备专用许可 1625
许可证激活 Blob 行为 1626
许可证宽限期警报 1626
手动管理的权利（基于文件的许可） 1627
开始之前 1627
步骤 1 - 在 NetScaler Console 中应用许可证 1627
步骤 2 - 将 NetScaler Console 注册为许可证服务器并分配许可证 1627
步骤 3 - 编辑 NetScaler 实例的弹性吞吐量容量 1630
NetScaler MPX-Z 1630
NetScaler SDX-Z 1630
NetScaler 高可用性对的许可证要求（LAS 和基于文件的许可通用） 1631
NetScaler 弹性许可状态（LAS 和基于文件的许可通用） 1631
弹性许可证仪表板 1632
编辑 NetScaler 实例上已分配的吞吐量容量 1634
在 NetScaler 实例上释放许可证 1634
弹性许可证报告 1634
过渡到 Flexed 许可 1638
基于 LAS 的许可 1638
手动管理的权利（基于文件的许可证） 1639
池化带宽许可证到弹性许可证 1639
池化 vCPU 到 Flexed 带宽容量 1640
从固定订阅或永久许可证到 Flexed 许可证 1640

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

CICO 到 Flexed 带宽容量 1641
弹性或池化许可证到期和连接问题行为的场景 1642
基于 LAS 的许可证 1642
在期限到期之前 1642
有效期届满后 1643
连接问题行为场景 1643
手动管理的许可证（基于文件的许可证） 1643
Flexed 许可证类型 1644
场景：MPX 外形规格 1644
场景：SDX 外形规格 1644
场景：VPX/BLX/CPX 外形规格 1644
连接问题行为场景 1645
将 NetScaler Console 服务器配置为弹性或池化许可证服务器 1645
如何将 NetScaler Console 服务器配置为仅用作弹性或池化许可证服务器 1646
旧版许可证 1648
NetScaler 池化容量 1649
NetScaler 池化容量许可的工作原理 1650
零容量硬件 1650
独立 NetScaler VPX 实例 1650
独立 NetScaler CPX 实例 1651
独立 NetScaler BLX 实例 1652
带宽池 1652
实例池 1652
NetScaler Console 许可证服务器 1652
配置 NetScaler 池化容量 1658
支持的硬件和软件版本 1659
NetScaler 池容量状态 1659
步骤 1 - 在 NetScaler Console 中应用许可证 1659

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

步骤 2 - 将 NetScaler Console 注册为许可证服务器 1660
步骤 3 - 将池化许可证分配给 NetScaler 实例 1664
在 NetScaler 实例上配置池容量 1666
将 NetScaler VPX 中的永久许可证升级到 NetScaler 池容量 1668
先决条件 1668
将 NetScaler VPX 高可用性对中的永久许可证升级到 NetScaler 池容量 1671
将 NetScaler MPX 中的永久许可证升级到 NetScaler Pooled Capacity 1675
将 NetScaler MPX 高可用性对中的永久许可证升级到 NetScaler 池化容量 1679
将 NetScaler SDX 中的永久许可证升级到 NetScaler Pooled 容量 1683
群集模式下 NetScaler 实例上的 NetScaler 池化容量 1686
将 NetScaler 池化容量分配给 NetScaler 群集 1687
使用 CLI 将 NetScaler 池容量分配给 NetScaler 群集 1689
签入和签出 NetScaler VPX 和 NetScaler BLX 许可证 1690
先决条件 1691
在 NetScaler Console 中安装许可证 1691
验证 1692
使用 NetScaler GUI 将 NetScaler VPX 和 NetScaler BLX 许可证分配给 NetScaler 实例 1692
使用 NetScaler CLI 将 NetScaler VPX 和 NetScaler BLX 许可证分配给 NetScaler 实例 1694
使用 API 将 NetScaler VPX 和 NetScaler BLX 许可证分配给 NetScaler 实例 1695
更新许可服务器 IP 地址 1698
配置 NetScaler VPX 和 NetScaler BLX 签入和签出许可证的到期检查 1698
NetScaler 虚拟 CPU 许可 1699
NetScaler VPX 的虚拟 CPU 许可 1700
使用 CLI 在 NetScaler VPX 许可证中配置许可服务器 1702
在 NetScaler Console 上管理虚拟 CPU 许可证 1703
NetScaler CPX 的虚拟 CPU 许可 1703
出现问题时的预期行为 1705
许可服务器停止响应 1705

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

NetScaler 池化实例停止响应 1706
许可证服务器和 NetScaler 池化实例都停止响应 1706
NetScaler 池化实例正常关机 1707
网络连接问题 1707
宽限期 1707
管理系统设置 1708
网络配置 1708
系统配置 1709
系统维护 1710
数据清理 1710
备份 1711
事件通知 1711
SSL 设置 1712
配置功能 1712
配置系统备份设置 1712
配置代理服务器设置 1713
注意事项 1713
代理服务器配置 1713
管理 CA 证书 1715
代理配置支持 1716
无代理（直接互联网访问） 1716
显式正向代理（非拦截） 1717
显式 SSL 拦截代理 1717
透明 SSL 拦截代理 1717
配置 NTP 服务器 1717
升级 NetScaler Console 1719
升级前检查 1719
当 LAS 预升级检查失败时解除 NetScaler Console 升级阻止 1721

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

如何重置 NetScaler Console 的密码 1722
配置辅助网卡以访问 NetScaler Console 1729
先决条件 1730
在 NetScaler Console 中配置第二个网卡 1730
配置辅助网卡以访问 NetScaler® 代理 1731
使用 CLI 修改 IPV4 网卡网络地址 1732
配置 syslog 清除间隔 1734
配置系统修剪和事件修剪设置 1734
使用 NetScaler Console 配置事件清除设置 1736
为非默认用户启用 shell 访问 1736
恢复无法访问的 NetScaler Console 服务器 1737
如何在 NetScaler Console 独立部署中使用 NetScaler Console 数据库恢复脚本 1737
如何将 NetScaler Console 数据库恢复脚本用于 NetScaler Console 高可用性部署 1741
为 NetScaler Console 服务器分配主机名 1742
备份和恢复您的 NetScaler Console 服务器 1742
备份 NetScaler Console 配置 1744
将 NetScaler Console 备份文件传输到外部系统 1744
从备份文件还原 NetScaler Console 配置 1747
高可用性部署中 NetScaler Console 的 VM 快照 1748
对 NetScaler Console 服务器进行快照 1748
恢复 NetScaler Console 服务器的快照 1748
查看审计信息 1749
配置 SSL 设置 1750
监控 CPU、内存和磁盘使用情况 1750
配置通知设置 1752
创建电子邮件分发列表 1752
创建短信分发列表 1753
创建 Slack 配置文件 1754

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

创建 PagerDuty 配置文件 1755
查看 ServiceNow 配置文件 1756
生成技术支持文件 1756
配置密码组 1758
创建 SNMP trap 目标、管理器社区和用户 1759
配置和查看系统警报 1760
为磁盘利用率警报添加阈值限制 1762
为 NetScaler 代理创建 SNMP 管理器和用户 1762
添加 SNMP v2 管理器 1762
添加 SNMP v3 管理器 1763
添加 SNMP 用户 1764
管理 SNMP 视图 1766
配置代理设置 1767
设置代理的保持活动间隔 1767
在没有当前密码的情况下更改代理密码 1767
使用数据存储管理仪表板 1768
了解您的数据存储 1769
数据摄取活动状态 1769
总存储消耗 1770
存储消耗趋势 1771
按功能划分的存储消耗 1773
管理您的存储空间 1774
执行数据修剪 1774
查看数据保留策略 1776
超出存储限制时通知 1776
数据保留策略 1777
配置系统清除设置 1777
配置实例事件清除设置 1777

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

配置实例 syslog 修剪设置 1778
配置网络报告修剪设置 1778
NetScaler Console 作为 API 代理服务器 1779
NetScaler Console 如何作为 API 代理服务器工作 1779
如何将 NetScaler Console 用作 API 代理服务器 1781
示例 1：检索负载均衡虚拟服务器统计信息 1784
示例 2：创建负载均衡虚拟服务器 1784
示例 3：修改负载均衡虚拟服务器 1785
示例 4：删除负载均衡虚拟服务器 1786
示例 5：下载 NetScaler 上的 CLI 运行配置 1786
常见问题 1787
分析 1787
是否需要在以单跳模式部署的 NetScaler Gateway 实例上启用 EUEM 虚拟通道? 1787
如何启用 NetScaler Console 来监控 Web 应用程序和虚拟桌面流量? 1787
添加 NetScaler 实例后，NetScaler Console 会自动开始收集分析信息? 1788
是否需要访问单个 NetScaler 设备才能启用分析? 1788
可以在 NetScaler 实例上列出哪些类型的虚拟服务器以启用分析? 1788
如何将额外磁盘附加到 NetScaler Console? 1788
NetScaler 实例上未配置收集器是什么意思? 1789
启用客户端测量有什么作用? 1789
身份验证 1789
什么是身份验证请求的负载均衡? 1789
为什么需要级联外部身份验证服务器? 1789
我可以级联多少个外部身份验证服务器? 1789
当外部身份验证失败时，我是否有替代方案? 1789
什么是回退本地身份验证? 1790
什么是外部用户组的提取? 1790
为什么需要分配组权限? 1790

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

配置管理 1790

我可以使用 NetScaler Console 同时在多个 NetScaler 实例上执行配置吗? 1790

NetScaler Console 上的配置作业是什么? 1790

我可以使用 NetScaler Console 中的内置模板来安排作业吗? 1791

证书管理 1791

从 NetScaler Console 中删除 SSL 证书会导致从 NetScaler 实例中删除证书吗? 1791

部署 1791

默认用户名和密码是什么? 1791

如何更改默认密码? 1791

如何重置密码? 1792

在 HA 对中，如果主节点中的密码已更改，并且稍后选择了“中断 HA 对”选项，行为会是怎样? 1792

如果两台独立服务器的密码不同，将这两台服务器部署到 HA 对中会有什么影响? 1792

HA 配置已完成，但主节点 GUI 无法访问。原因可能是什么? 1792

HA 配置已完成，但浮动 IP 地址 GUI 无法访问。原因可能是什么? 1793

NetScaler Console 独立版和 NetScaler Console HA 支持哪些数据库? 1793

辅助节点可能存在哪些数据丢失? 1793

如果主节点宕机，会发生什么? 1793

如何重新安装故障节点? 1793

NetScaler Console 是否支持 SAN 存储? 1793

NetScaler Console 是否支持额外磁盘? 1794

禁用 HA 对后，配置的浮动 IP 地址会发生什么? 1794

重新部署时可以提供不同的浮动 IP 地址吗? 1794

为什么辅助节点 GUI 无法访问? 1794

如果主节点长时间宕机，是否仍可以使用浮动 IP 地址 GUI 进行配置? 1794

如果将来需要更改主节点 IP 地址、辅助节点 IP 地址或浮动 IP 地址（例如，更改为 IPv6），建议遵循哪些解决方案? 1794

NetScaler Console 是否支持 AMD 处理器? 1795

部署（灾难恢复） 1795

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

主站点和灾难恢复站点之间的复制频率如何? 1795

在灾难恢复站点启动备份脚本后，灾难恢复站点是否会成为临时主站点，直到主站点恢复并完全运行? 1795

如果选择了“中断 HA 对”选项，则两个节点都将作为独立服务器运行。由于灾难恢复不支持独立服务器，如果选择了“中断 HA 对”，灾难恢复站点会发生什么? 1795

事件管理 1795

如何使用 NetScaler Console 跟踪我的托管 NetScaler 实例上生成的所有事件? 1795

什么是事件规则? 1796

实例管理 1796

当您使用 NetScaler 池容量许可时，如果在分配带宽后 NetScaler 实例无法连接到 NetScaler Console，会发生什么? 1796

NetScaler Console 中的数据中心是什么? 1796

NetScaler Console 支持哪些不同的 NetScaler 设备? 1796

什么是实例配置文件? 1797

我可以在 NetScaler Console 中重新发现多个 NetScaler VPX 实例吗? 1797

NetScaler Console 可以安装在 NetScaler SDX 上吗? 1797

我可以使用公共 IP 地址在 NetScaler Console 软件上添加 NetScaler 实例吗? 1797

如果 DR 节点凭据已更改，如何注册灾难恢复节点? 1797

StyleBooks 1798

StyleBook 能否用于配置运行不同版本 NetScaler 软件的不同 NetScaler 实例? 1798

当 StyleBook 同时用于配置多个 NetScaler 实例时，如果其中一个 NetScaler 实例的配置失败，会发生什么? 1798

通过 NetScaler 进行的备份是否包含通过 StyleBook 应用的配置? 1798

系统管理 1798

我可以为我的 NetScaler Console 服务器分配主机名? 1798

我可以备份和恢复我的 NetScaler Console 配置? 1798

NetScaler Console 中的阈值和警报是什么? 1799

我可以为 NetScaler Console 生成技术支持文件吗? 1799

syslog 清除是什么? 1799

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

我可以在 NetScaler Console 上配置 NTP 服务器吗? 1799

NetScaler Console 主动-被动 HA 部署从哪个版本开始支持? 1799

我有一个 NetScaler Console 主动-主动 HA 设置，并且在其上配置了带有负载平衡虚拟服务器的 NetScaler 设备，用于统一 GUI 访问。如何更新此配置? 1800

我可以在 NetScaler 实例上使用端口 443 配置 NetScaler Console HA 对的负载平衡吗? 1800

NetScaler Console 服务器备份文件可用于恢复另一个 NetScaler Console 服务器的配置吗? 1800

NetScaler Console 备份 NetScaler 实例后，该备份文件是否可以通过 NetScaler Console 用于恢复另一个 NetScaler 实例的配置? 1800

我们可以强制 NetScaler Console 使用 SNIP 地址与 NetScaler 实例通信，而不是使用 NetScaler Console 服务器的 NSIP 地址吗? 1800

当我在 NetScaler Console 中备份 NetScaler 实例时，结果是完全备份还是基本备份? 1800

NetScaler Console 是否有故障排除指南? 1801

NetScaler Console HA 故障转移发生时 NetScaler 实例的管理? 1801

NetScaler Console HA 节点故障后恢复时的处理? 1801

NetScaler 实例如何在 NetScaler Console HA 节点之间分布? 1801

如果发生 NetScaler Console HA 故障转移，如何管理虚拟服务器许可证? 1801

NetScaler Console HA 设置是否强制要求负载均衡器? 1801

NetScaler Console 是否支持外部数据库? 1801

由 NetScaler Console 管理的 NetScaler 实例能否用作 NetScaler Console HA 的负载均衡器? 1802

NetScaler Console HA 节点之间同步哪些数据? 1802

index 1803

配置自适应阈值 1804

使用 NetScaler Console 创建自适应阈值 1804

配置数据库汇总 1804

配置数据库汇总 1804

配置 SLA 管理 1805

配置 NetScaler 实例的 SLA 违规 1806

创建阈值和警报 1806

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

使用 NetScaler Console 创建阈值和警报 1807
禁用 URL 数据收集 1807
从 NetScaler Console 禁用 URL 数据收集 1807
Logstream 概述 1808
启用 Logstream 作为传输模式 1808
仪表板 1811
出站流量仪表板 1812
查看网络中的出站流量 1812
用户仪表板 1813
用户活动调查器 1814
用户事务 1815
风险评分 1816
所有违规 1817
违规类别 1817
安全违规仪表板 1819
违规详情 1819
应用程序概览 1820
违规类别 1821
查看 WAF 违规详情 1822
查看机器人违规详情 1825
查看事件历史记录 1827
网络违规详情 1827
HTTP 慢速洛里斯 1827
DNS 慢速洛里斯 1828
HTTP 慢速 POST 1829
NXDOMAIN 洪水攻击 1829
HTTP 解同步攻击 1830
布莱兴巴赫攻击 1832

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

分段粉碎攻击 1832

SYN 洪水攻击 1834

小窗口攻击 1835

SSL 洞察 1836

先决条件 1837

配置 SSL Insight 1837

启用 AppFlow 功能 1838

启用 SSL Insight 参数 1842

查看 SSL Insight 指标 1842

用例：获取 SSL 事务概述 1843

用例：客户端的 SSL 指标 1844

排查 Web Insight 问题 1845

无数据诊断 1845

与 Web Insight 控制板报告相关的问题 1846

配置问题 1846

NetScaler 与 NetScaler Console 之间的连接问题 1846

未从 NetScaler® 接收到 AppFlow 数据 1847

许可证问题 1847

观察点 ID 问题 1847

AppFlow 参数缺失问题 1848

使用计数器进行故障排除 1848

查看 Web 事务分析 1849

详细的 Web 事务 1850

查看事件 1852

在事件列表中添加列 1855

高级搜索 1856

保存搜索 1858

导出数据 1859

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

设置双层或服务网格精简拓扑的详细步骤 1860
软件要求 1860
开始之前 1860
软件要求 1861
开始之前 1861
在 NetScaler Console 中配置静态路由 1861
从 GitHub 下载示例部署文件 1863
在 CPX YAML 文件中添加参数 1863
在 NetScaler Console 中添加 VPX、SDX、MPX 或 BLX 实例 1865
在 NetScaler Console 中添加 Kubernetes 集群 1865
部署示例微服务应用程序 1867
部署 CPX 并在 NetScaler Console 中注册 CPX 1867
启用许可证的虚拟服务器自动选择 1867
启用 Web 事务和 TCP 事务设置 1868
向微服务发送流量 1869
设置服务网格拓扑的详细步骤 1870
在 NetScaler Console 中配置静态路由 1870
配置所需参数 1871
部署示例应用程序 1873
在 NetScaler Console 中添加 Kubernetes 集群 1875
启用自动选择虚拟服务器进行许可 1877
启用Web事务和TCP事务设置 1878
将流量发送到微服务 1879
数据治理（适用于 14.1-8.x 到 14.1-21.x 版本之间的 NetScaler Console） 1880
数据类别 1880
数据治理（适用于 NetScaler ADM 14.1-4.42 或更早版本） 1881
配置客户身份 1881
工作流 1 - 如果您是新用户 1881

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

工作流 2 - 如果您是升级到最新 ADM 版本的现有用户 1882
诊断和数据收集 1882
为什么要收集数据? 1883
谁可以使用这些数据? 1883
我们会保留您的数据多长时间? 1883
使用维护脚本进行数据库优化 1884
客户用户体验改进计划 1884
CUXIP 收集哪些使用数据? 1884
CUXIP 如何帮助您? 1884
CUXIP 如何工作? 1884
如何在我的 ADM 上禁用 CUXIP? 1885
我们的隐私政策变更 1885
参考 1885
用于 Cloud Connect 的可选遥测数据 1885
NetScaler® 遥测程序的可选遥测数据 1889
NetScaler Console 功能使用情况 1889
Cloud Connect 所需的遥测数据 1895
NetScaler® 遥测程序所需的遥测数据 1900
许可 1900
高可用性 1903
NetScaler Console 高可用性节点之间如何同步许可证? 1904
编排 1904
升级虚拟服务器许可证 1904
验证 1905
管理虚拟服务器 1905
禁用虚拟服务器的自动授权 1906
选择第三方虚拟服务器进行授权 1906
手动应用虚拟服务器许可证 1907

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

配置基于策略的虚拟服务器许可 1907

查看已获得许可的虚拟服务器 1908

为不可寻址的虚拟服务器配置自动许可证支持 1908

备份和恢复 HA 对中的 NetScaler Console 配置 1908

配置系统通知设置 1909

为地理地图配置站点 1913

fix 1915

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

发行说明

NetScaler Console 14.1 发行说明描述了新功能、现有功能的增强以及版本中的已知问题。14.1 版本的发行说明文档包含以下部分：

- **新增功能**：版本中发布的新功能和现有功能的增强。
- **已知问题**：版本中存在的问题及其适用的解决方法。
- **已修复问题**：版本中已解决的问题。

注意：

这些发行说明不包含安全相关修复的文档。有关安全相关修复和建议的列表，请参阅安全公告。NetScaler Console 安全咨询支持识别和修复 CVE。有关最新和现有支持的 CVE 的更多信息，请参阅通过安全咨询支持的 CVE。

要查看版本 14.1 特定版本的发行说明文档，请单击下表中的相应链接。当发行说明更新时，发布日期也会更新。发行说明发布日期可能与版本 GA 日期不同。

NETSCALER CONSOLE 本地部署软件版本 14.1 的发行说明	发布日期
版本 14.1-73.36	Sep 01, 2026
版本 14.1-72.57	May 27, 2026
版本 14.1-66.72	Apr 24, 2026
版本 14.1-60.57	Jan 20, 2026
版本 14.1-56.71	Dec 05, 2025
版本 14.1-51.83	Dec 05, 2025
版本 14.1-47.46	Jul 02, 2025
版本 14.1-43.50	Feb 27, 2025
版本 14.1-38.53	Dec 18, 2024

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

NETSCALER CONSOLE 本地部署软件版本 14.1 的发行说明	发布日期
版本 14.1-34.43	Oct 28, 2024
版本 14.1-29.63	Aug 19, 2024
版本 14.1-25.56	Jul 09, 2024
版本 14.1-21.60	Apr 28, 2024
版本 14.1-17.38	Mar 18, 2024
版本 14.1-12.34	Dec 19, 2023
版本 14.1-8.50	Oct 10, 2023
版本 14.1-4.42	Aug 07, 2023

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

将 NetScaler Console 本地部署迁移到 Citrix Cloud

您可以将 **NetScaler ADM 13.0 64.35 或更高版本**迁移到 Citrix Cloud。如果您的 NetScaler ADM 是 12.1 或更早版本，则必须首先升级到 **13.0 64.35 或更高版本**，然后迁移到 Citrix Cloud。有关更多信息，请参阅 升级 部分。

注意：

NetScaler® ADM 服务现已更名为 NetScaler Console 服务。我们的产品 UI 和文档目前正在更新以反映这些更改。在此期间，您可能会看到旧名称和新名称交替使用。感谢您在此过渡期间的理解。

通过 Citrix Cloud™ 提供的 NetScaler Console 服务可让您获得：

- 更快的发布，大约每两周一次，包含最新的功能更新。
- 基于机器学习的应用程序安全和机器人、性能和使用情况分析。
- 目前仅在 NetScaler Console 服务中支持的各种其他功能，例如高峰期和低谷期分析、基于机器学习的应用程序安全和机器人分析、应用程序 CPU 分析等等。

要成功迁移，您必须：

- 确保 NetScaler Console 本地部署具有互联网连接，以便访问 Citrix Cloud
- 配置 NetScaler 代理
- 从 Citrix Cloud 获取客户端和密钥 CSV 文件
- 验证 NetScaler Console 许可
- 使用脚本进行迁移

将 NetScaler Console 本地部署迁移到 NetScaler Console 服务后，如果您想再次继续使用 NetScaler Console 本地部署，可以使用回滚脚本。有关更多信息，请参阅 回滚到 NetScaler Console 本地部署。

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

配置 NetScaler 代理

要启用 NetScaler 实例与 NetScaler Console 服务之间的通信，您必须配置一个代理。NetScaler 代理默认会自动升级到最新版本。您也可以选择特定的时间进行代理升级。有关详细信息，请参阅配置代理升级设置。

- 如果现有本地 NetScaler Console（独立或 HA 对）未配置代理，则必须为 NetScaler Console 服务至少配置一个代理。
- 如果现有本地 NetScaler Console（独立或 HA 对）已为多站点部署配置了本地代理，则必须为 NetScaler Console 服务配置相同数量的代理。

有关配置代理的更多信息，请参阅入门部分。

从 Citrix Cloud 获取客户端和密钥 CSV 文件

配置代理后，从 Citrix Cloud 页面获取客户端和密钥 CSV 文件：

1. 登录 citrix.cloud.com
2. 单击“**主页**”图标，然后选择“**身份和访问管理**”
3. 在“**API 访问**”选项卡中，输入安全的客户端名称，然后单击“**创建客户端**”。
4. ID 和密钥已生成。单击“**下载**”并将 CSV 文件保存到本地 NetScaler Console 中。

   例如，将 CSV 文件保存到 /var 目录。

验证 NetScaler Console 服务许可证

您必须为 NetScaler 服务获取许可证。

- NetScaler Console 服务中的 VIP 许可证必须大于或等于本地 VIP 许可证。

  注意

  如果 VIP 许可证数量不足，则会随机选择虚拟服务器，并且 NetScaler Console 服务的 VIP 级别配置将失败。

- 如果您使用本地部署的 NetScaler Console 作为许可证服务器，请在迁移前将许可证重新分配给 NetScaler Console 服务。有关详细信息，请参阅如何重新分配许可证文件。

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

- 如果您在本地部署的 NetScaler Console 中使用池化许可证，则必须为 NetScaler Console 服务获取池化许可证，然后将许可证分配给 NetScaler 实例。有关详细信息，请参阅配置池化许可。以下受支持的 NetScaler 版本允许您从 NetScaler Console 修改许可证分配：
  - NetScaler SDX：13.0 74.11 或更高版本。
  - NetScaler VPX 和 MPX：13.0 47.24 或更高版本，12.1 58.14 或更高版本，以及 11.1 65.10 或更高版本。

使用脚本进行迁移

- 使用 NetScaler Console 82.x 版本，您可以选择功能然后进行迁移。
- 对于 NetScaler Console 76.x 或更高版本，迁移脚本 (`servicemigrationtool.py` 和 `config_collect_onprem.py`) 作为版本的一部分提供，可在 `cd /mps/scripts` 获取。
- 对于早于 76.x 版本的 NetScaler Console，您必须下载迁移脚本并将其复制到本地部署的 NetScaler Console 中。

注意

> 确保本地部署的 NetScaler Console 在迁移期间具有互联网连接。

1. 使用 SSH 客户端，登录到本地部署的 NetScaler Console。

   注意

   > 对于 NetScaler Console HA 对，请登录到主节点。

2. 输入 **shell** 并按 **Enter** 键切换到 bash 模式。
3. 复制客户端 ID 和密钥 CSV 文件。例如，将文件复制到 /var 目录。

   复制 CSV 文件后，您可以验证 CSV 文件是否存在。

   添加 CSV(/en-us/netscaler-application-delivery-management-software/media/csv-add-adm.png)

   注意

   > 对于 NetScaler Console HA 对，将 CSV 文件复制到主节点中。

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

4. 对于 NetScaler Console 本地部署 **13.0 82.xx 版本**，运行以下命令以完成迁移：

   a. `cd /mps/scripts`

   b. `python servicemigrationtool.py <path of ClientID/Secret File in on-premises NetScaler Console VM>`

   例如，`python servicemigrationtool.py /var/secureclient.csv`

   运行迁移脚本后，该工具会显示以下选项：

   按功能划分的迁移选项(/en-us/netscaler-application-delivery-management-software/media/migrate-options.png)

   根据您提供的选择，只有该功能会迁移到 NetScaler Console 服务。

   在此示例中，选择了选项 1。该工具会完成管理和监控 (M&M) 迁移并显示以下消息：

   迁移完成(/en-us/netscaler-application-delivery-management-software/media/migrate-option-complete.png)

   管理和监控 (M&M) 功能包括：

   - NetScaler 实例、标签、实例组、配置文件、自定义应用程序、配置作业、SNMP、syslog 配置。
   - 站点、IP 块、网络报告、分析阈值、通知设置、数据清理设置。
   - 配置审计模板、轮询间隔、事件规则和设置。
   - RBAC 组、角色和策略

   分析功能包括：

   - 来自 NetScaler 实例的每个 vserver 的 Appflow 配置。
   - 每个 SDWAN 设备的 Appflow® 配置。

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

注意：

- 即使您选择任何其他功能（2、3 或 4），管理和监控 (M&M) 功能也会自动迁移。
- 您一次只能指定一个功能。
- 完成任何功能的迁移后，如果您以后想迁移任何其他功能，列表中不会显示已迁移的功能。例如，如果您首先完成 **分析** 功能的迁移，下次运行迁移脚本时，您只能看到 **StyleBooks**、**池化许可** 和 **所有** 选项。
- 迁移池化许可时，它会迁移所有类型，包括 vserver。

5. 对于 NetScaler Console 本地部署 **13.0 76.xx 版本**，运行以下命令以完成迁移：

   a. `cd /mps/scripts`

   b. `python servicemigrationtool.py <path of ClientID/Secret File in on-premises NetScaler Console VM>`

   例如，`python servicemigrationtool.py /var/secureclient.csv`

6. 对于早于 13.0 76.xx 版本的 NetScaler Console 本地部署：

   a. 从以下位置下载迁移脚本：`https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigrationtool_27.tgz`

      下载的文件包含两个捆绑脚本：`servicemigrationtool_27.py` 和 `config_collect_onprem_27.py`。

   b. 将这两个脚本保存在 NetScaler Console 本地部署中。例如，保存在 /var 目录中

   c. 运行以下命令进行迁移：

      i. `cd /var`

      ii. `servicemigrationtool_27.py <path of ClientID/Secret File in NetScaler Console on-prem VM>`

      例如，`python servicemigrationtool_27.py /var/secureclient.csv`

运行脚本后，它会检查先决条件，然后继续进行迁移。脚本首先检查许可证可用性。仅当您的 NetScaler Console 服务许可证少于本地部署许可证时，才会显示以下消息。

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

```
bash-3.2# python servicemigrationtool.py /var/baga.csv

 Trying to Get the Customer Id...


 The Customer Id: iaahfc73d8f4

 ADM Service FQDN: baga.adm.cloud.com

 The ADM on-prem IP: 10.106.150.37


 Citrix ADM Deployed with No Agents



-----------------------------------------------------
Checking For Pre-requisites before we start the Migration
-----------------------------------------------------

 The no.of Agents in ADM Service are :1


 VIP licenses available in ADM Service are: 2

 No.of Vservers Licensed in ADM on-prem are: 26


 All the vServers licensed in ADM on-prem will not be licensed in ADM Service since licenses available in service is less.
 vServers will be licensed randomly. Do you want to continue ? [Y|N]
```

如果选择 **Y**，迁移将通过随机许可 VIP 继续。如果选择 **N**，脚本将停止迁移。

如果您的 NetScaler 实例版本不支持池化许可证服务器，则会显示以下消息：

```
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Changing of PooledLicense Server will be effective for below SDX/ADC versions
-------------------------------------------------------------------------------
  For SDX Versions: 13.0 74.11 Onwards
  For ADC Versions: 13.0 47.24 and Onwards
                    12.1 58.14 and Onwards
                    11.1 65.10 and Onwards
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------

 The List of ADCs supported for Pooled License Server change are:
['10.106.150.73', '10.102.60.25']

 The List of SDXs supported for Pooled License Server change are:
[]

 The List of ADCs not supported for Pooled License Server change are:
[]

 The List of SDXs not supported for Pooled License Server chagne are:
['10.102.103.238']

 Migration will change the License Server to ADM Service Agent.
 Do you want to change License Server in all the supported Pooled ADCs/SDXs ? [Y|N] n

 Do you want to continue with rest of the migration ? [Y|N]
```

如果您选择 **Y**，迁移过程将通过更改许可证服务器继续。如果您选择 **N**，脚本会提示您是否要继续进行其余的迁移。如果您选择 **N**，脚本将停止迁移。

根据本地部署配置，迁移完成的大致时间在几分钟到几小时之间。迁移完成后，您将看到以下消息：

```
-----------------------------------------------------------------------------------------
ADM OnPrem to ADM Service Configuration Migration is Complete.
Note: Please Look out for Failures and re-trigger the Tool after taking appropriate action.
-----------------------------------------------------------------------------------------
```

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

一旦所有 NetScaler 实例及其各自的配置成功迁移到 NetScaler Console 服务，迁移即告成功。成功迁移后，本地部署的 NetScaler Console 将停止处理以下实例事件：

- SSL 证书
- Syslog 消息
- 备份
- 代理集群
- 性能报告
- 配置审计
- `Emon` 调度程序

回滚到本地部署的 NetScaler Console

如果您想回滚到本地部署的 NetScaler Console，请确保满足先决条件。

先决条件

如果您的本地部署 NetScaler Console（在迁移到 NetScaler Console 服务之前）是：

- 用作池化许可证服务器时，请确保在 NetScaler Console 本地部署中拥有所需的池化许可证。
- 配置了 NetScaler 代理时，请确保代理处于“UP”状态。

使用回滚脚本

注意

> 回滚后，Analytics、SNMP 和池化许可中的相同配置（迁移前）将再次在 NetScaler Console 本地部署中可用。如果您在迁移后对这些配置进行了任何更改，这些更改将不会反映在 NetScaler Console 本地部署中。

- 对于 **NetScaler Console 82.xx 或更高版本**的内部版本，回滚脚本作为内部版本的一部分提供，可在 `/mps/scripts` 访问。
- 对于 **NetScaler Console 79.xx 之前的版本**，您可以升级到 82.x 版本并使用回滚脚本，或者您可以下载回滚脚本并将其复制到 NetScaler Console 本地部署中。

1. 使用 SSH 客户端登录到 NetScaler Console 本地部署。
2. 键入 shell 并按 Enter 键切换到 bash 模式。
3. 对于 NetScaler Console **13.0 82.xx** 版本，运行以下命令以完成回滚：

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

a. cd /mps/scripts

b. python rollback_to_onprem.py `<path of ClientID/Secret File in NetScaler Console on-prem VM>`

例如，`python rollback_to_onprem.py /var/ secureclient.csv.csv`

该工具将启动回滚操作，并提示您是否要继续。键入 **Y** 以继续。

```
bash-3.2# python rollback_to_onprem.py /var/tmp/baga_prod.csv

The Customer Id: iaahfc73d8f4

ADM Service FQDN: baga.adm.cloud.com

The ADM on-prem IP: 10.106.150.10

--------------------
```

i. `cd /var`

ii. `python rollback_to_onprem_27.py < path of client/secret csv file in NetScaler Console on-prem>`

例如，`python rollback_to_onprem_27.py /var/secureclient.csv`

该工具会启动回滚操作，并提示您是否要继续。键入 **Y** 以继续。

常见问题

NetScaler Console 服务

NetScaler 代理是否像本地 NetScaler 代理一样是可选?

不是。代理对于 NetScaler Console 服务是强制性的，实例与 NetScaler Console 服务之间的所有通信都通过代理进行。在本地 NetScaler Console 中，代理是可选的；但是，您只能配置代理以节省带宽消耗。

为什么选择 NetScaler Console 服务?

通过 Citrix Cloud 提供的 NetScaler Console 服务具有以下优势，无需新的定期构建：

- 基于云的 SaaS 产品，与本地 NetScaler Console 相比，入门更简单，拥有成本更低。
- 发布速度更快，大约每两周更新一次最新功能。
- 基于机器学习的应用程序安全、性能和使用情况分析。
- 目前仅在 NetScaler Console 服务中支持的各种其他功能，例如高峰期和低谷期分析、基于机器学习的 WAF 和机器人应用程序安全分析、应用程序 CPU 分析等等。

如果本地 NetScaler Console 是高可用性对，迁移后会发生什么?

所有配置都将迁移到 Citrix Cloud。无需配置灾难恢复节点。

如果代理因任何原因宕机，会发生什么?

在代理启动并运行之前，可能会出现数据丢失。但是，您也可以为多站点部署配置 NetScaler 代理，以确保在代理故障转移时保持连续性。有关更多信息，请参阅为多站点部署配置代理。

实例备份也会迁移?

备份不包含在迁移中。

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

历史数据也会迁移?

历史数据不会迁移。您可以从本地 NetScaler Console 导出数据。

本地许可证也会迁移吗?

否。本地许可证文件不能用于 NetScaler Console 服务。您必须为 NetScaler Console 服务获取许可证。有关详细信息，请参阅许可。如果您在本地 NetScaler Console 中使用池化许可证，则必须为 NetScaler Console 服务获取池化许可证，然后将许可证分配给实例。

哪些内容不会从本地 NetScaler Console 迁移?

以下功能无法迁移到 NetScaler Console 服务：

- **RBAC** – 在 NetScaler Console 服务中，用户访问基于管理员的邀请。NetScaler Console 服务用户必须在 Citrix Cloud 中拥有帐户。因此，本地 NetScaler Console 用户不会迁移。
- **导出计划** – 导出计划包括来自不同页面的详细信息，例如向下钻取和计划。所有这些详细的导出计划都不会迁移。
- **SSL 证书/密钥/CSR** – NetScaler Console 服务只能显示 NetScaler SSL 证书/密钥/CSR。因此，上传到本地 NetScaler Console 的 SSL 证书/密钥不会迁移到 NetScaler Console 服务。

本地 NetScaler Console 与 Citrix Director 集成后会发生什么?

Director 与 NetScaler Console 的集成目前仅在本地 NetScaler Console 中受支持。

迁移后，是否需要再次许可实例或启用分析?

您必须确保 NetScaler Console 服务中的许可证数量大于或等于本地 VIP 许可证。如果许可证数量已超过本地 NetScaler Console VIP，则虚拟服务器将自动获得许可。否则，许可证将随机分配。

迁移工具

运行迁移脚本后，显示错误消息。可能是什么问题?

将显示一个包含失败原因的日志文件。您可以采取适当的纠正措施并再次运行迁移脚本。通常，在运行迁移脚本之前，请确保：

- 配置 NetScaler® 代理
- 获取 NetScaler Console 服务许可证
- 复制存储客户端和安全 CSV 文件的正确路径

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

NetScaler 实例的版本低于池化许可的限制。如果选择选项“Y”来更改许可证服务器，会发生什么?

许可证服务器的更改仅适用于受支持的 NetScaler MPX、VPX 和 SDX 版本。

如果迁移脚本在 NetScaler 实例配置方面失败，会发生什么?

NetScaler 实例将继续在 NetScaler Console 本地部署上运行。您可以根据建议的失败原因采取必要措施，并再次运行迁移脚本。

如果部分 NetScaler 实例未能迁移到 NetScaler Console 服务，会发生什么？重新运行迁移脚本会有帮助吗?

是的。重新运行脚本后，只有失败的实例会被迁移。假设五个实例中有两个未能迁移。在您采取纠正措施并重新运行迁移脚本后，之前已成功迁移的三个实例会显示“设备已存在”消息。而之前失败的另外两个实例则会成功迁移。

是否有日志文件可以检查迁移状态?

是的，日志文件在 `/var/mps/log/` 目录中生成。使用 python3.7 的 NetScaler Console 的日志文件为 `servicemigrationtool.py.log`，使用 python 2.7 的 NetScaler Console 的日志文件为 `servicemigrationtool_27.py.log`。

如果在运行迁移脚本时会话终止，会发生什么?

您可以重新运行迁移脚本。在新会话中，上次会话中已添加的实例会显示为“设备已存在”，迁移将继续进行。

如果 NetScaler Console 服务许可证少于本地 NetScaler Console 且已启动迁移脚本，会发生什么情况?

运行迁移脚本后，将出现一个建议，提示许可证数量较少，并提示是继续还是停止。如果您想继续使用较少的许可证，虚拟服务器将从可用许可证中随机获得许可。

将本地 NetScaler Console 迁移到 NetScaler Console 服务 Express Account 时会发生什么情况?

NetScaler Console 服务 Express Account 仅包含两个虚拟服务器许可证、两个 StyleBook 配置包和两个配置作业。如果您的本地 NetScaler Console 具有超出这些配置的更多配置，并且您使用 Express Account 启动迁移，则脚本只能迁移适用于 Express Account 的上述配置（两个虚拟服务器许可证、两个 StyleBook 配置包和两个配置作业）。

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

如果 Citrix Cloud 邀请用户（非创建 Citrix Cloud 帐户的管理员用户）尝试迁移本地 NetScaler Console 设置，会发生什么情况?

建议由管理员运行迁移脚本。受邀用户没有管理员权限 (adminExceptSystem_group)。因此，组、角色和策略迁移失败，并显示消息“用户没有权限”。

解决方案是，管理员（创建 Citrix Cloud 帐户的人）可以将与受邀用户关联的组更改为“admin_group”。

回滚脚本

如果在 NetScaler Console 本地 HA 对中使用回滚脚本，会发生什么情况?

NetScaler Console 本地 HA 对将恢复到迁移前可用的所有配置。

使用回滚脚本后，灾难恢复节点会发生什么?

灾难恢复节点也将恢复到迁移前的所有配置。

故障排除

首次运行迁移脚本时，它会检查先决条件并继续进行迁移。如果满足所有先决条件，迁移将顺利完成，不会出现任何错误。如果任何先决条件未能满足，脚本将显示错误消息并说明原因。修复错误后，您必须再次运行该脚本。

注意

> 如果您看到显示“已存在”的错误消息，则表示：

- 您可能已多次运行迁移脚本，并且某些配置已迁移到 NetScaler Console 服务。
- 您可能在运行迁移脚本之前，已在 NetScaler Console 服务中手动创建了相同的配置。

请参阅以下一些错误消息：

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

手动配置文件已添加到 NetScaler Console 服务

```
==================Profiles Addition to ADM Service=====================


60.26 : FAILURE : Profile 60.26 already exists


 The list of ADC profiles added to ADM Service are :

{'60.26': "['FAILURE']"}
```

解决方法：如果您在运行迁移脚本之前已在 NetScaler Console 服务中创建了管理员配置文件，请务必删除这些配置文件并重新运行迁移脚本。

NetScaler 设备已添加到 NetScaler Console 服务

```
==============ADC Device Addition================

10.106.150.53 : FAILURE : Error in contacting Citrix ADC, invalid credentials.
10.102.60.26 : FAILURE :Device with this IP address already exists.


The list of ADCs added to ADM Service are:


['10.102.60.26']
```

解决方法：在 NetScaler Console 中，请确保实例状态并查看您是否可以无任何问题地访问该实例。如果问题仍然存在，请修复问题并重新运行迁移脚本。

StyleBook 自定义模板导入到 NetScaler Console 服务

```
==============Stylebook custom templates Import to ADM Service====================


neustar.citrix.adc.stylebooks_5.0_appfw-signature : FAILURE : There is an existing StyleBook with same namespace, version and name.

neustar.citrix.adc.stylebooks_5.0_customer-template : FAILURE : There is an existing StyleBook with same namespace, version and name.

 Custom stylebooks import status is:{'neustar.citrix.adc.stylebooks_5.0_appfw-signature': 'FAILURE', 'neustar.citrix.adc.stylebooks_5.0_customer-template': 'FAILURE'}
==============Stylebook repository Addition to ADM Service=====================
```

变通方法：此错误消息是已迁移的 StyleBook 的一个示例。如果您在运行迁移脚本之前，在 NetScaler Console 服务中手动创建了具有相同名称、版本和命名空间的 StyleBook，也可能会看到此错误。

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

添加到 NetScaler Console 服务的配置作业

```
===============Config Jobs Addition to ADM Service=====================

config_job2_show_ns_ip : FAILURE : Express user can have maximum 2 config jobs

ConfigJob1_show_ha_node : FAILURE : Express user can have maximum 2 config jobs

 The config jobs status is :
{'config_job2_show_ns_ip': 'FAILURE', 'ConfigJob1_show_ha_node': 'FAILURE'}
```

变通方法：如果您已订阅 Express Account 并且拥有两个以上的配置作业，则会发生此错误。您必须获得有效的订阅才能迁移所有配置作业。

添加到 NetScaler Console 服务的 IP 块

```
====================IP Blocks Addition in ADM Service=======================

ipblock1 : FAILURE : IP Block Name ipblock1 already exists

ipblock3 : FAILURE : IP Block Name ipblock3 already exists

test : FAILURE : IP Block Name test already exists
```

变通方法：删除在 NetScaler Console 服务中手动创建的 IP 块，然后重新运行迁移脚本。

网络控制板报告添加状态

```
================Network Dashboard Reports Addition to ADM Service=================

new456 : FAILURE : Dashboard new456 already exists

new123 : FAILURE : Dashboard new123 already exists

 The network dashoard reports addition status is:
{'new456': "['FAILURE']", 'new123': "['FAILURE']"}
```

变通方法：删除在 NetScaler Console 服务中手动创建的控制板，然后重新运行迁移脚本。

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

所有操作指南文章

NetScaler Application Delivery Management (NetScaler Console)“操作指南文章”是关于 NetScaler Console 功能的简单、相关且易于实施的文章。这些文章包含有关 NetScaler Console 流行功能的信息，例如实例管理、应用程序管理、StyleBooks、证书管理和分析。

单击下表中的功能名称，以查看该功能的操作指南文章列表。

主题				
实例管理	事件管理	StyleBooks	证书管理	NetScaler Console 系统
	配置管理	身份验证	分析	网络功能

实例管理

如何监控全球分布式站点

如何管理 NetScaler 实例的管理员分区

如何将实例添加到 NetScaler Console

如何在 NetScaler Console 上创建实例组

如何在 NetScaler Console 中为地理地图配置站点

如何使用 NetScaler Console 强制故障转移到辅助 NetScaler 实例

如何使用 NetScaler Console 强制辅助 NetScaler 实例保持辅助状态

如何使用 NetScaler Console 备份和恢复实例

如何重新发现多个 NetScaler VPX 实例

如何在 NetScaler Console 中轮询 NetScaler 实例和实体

如何在 NetScaler Console 上取消管理实例

如何从 NetScaler Console 跟踪到实例的路由

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

配置管理

如何在 NetScaler Console 上创建配置作业

如何在配置作业中使用 SCP (put) 命令

如何在 NetScaler Console 中调度使用内置模板创建的作业

如何在 NetScaler Console 中重新安排使用内置模板配置的作业(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-reschedule-jobs.html)

如何重用已执行的配置作业(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-reuse-executed-configuration-jobs.html)

如何使用 NetScaler Console 升级 NetScaler 实例(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-upgrade-netscaler-instances.html)

如何在 NetScaler Console 的配置作业中使用变量(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-use-variables.html)

如何使用配置模板在 NetScaler Console 上创建审计模板(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/use-configuration-templates-to-create-audit-templates.html)

如何在 NetScaler Console 上从纠正命令创建配置作业(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-create-jobs-from-corrective-commands.html)

如何在 NetScaler Console 上将正在运行和已保存的配置命令从一个 NetScaler 实例复制到另一个实例(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/replicate-running-saved-configuration-from-one-netscaler-to-another.html)

如何使用录制和播放功能创建配置作业(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/record-and-play.html)

如何使用配置作业将配置从一个实例复制到多个实例(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/replicate-configuration.html)

如何在 NetScaler Console 上使用主配置模板(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/use-master-configuration-template.html)

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

如何轮询 NetScaler 实例的配置审计(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-audit/how-to-poll-configuration-audit-of-netscaler-instances.html)

如何在配置作业中重用配置审计模板(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-reuse-configuration-audit-templates.html)

如何导入和导出配置模板(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-jobs/how-to-import-and-export-configuration-templates.html)

如何为 ConfigChange SNMP 陷阱生成配置审计差异(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/configuration-audit/generate-configuration-audit-diff-for-configchange-snmp-traps.html)

证书管理

如何在 NetScaler Console 上配置企业策略

如何从 NetScaler Console 在 NetScaler 实例上安装 SSL 证书

如何从 NetScaler Console 更新已安装的证书

如何使用 NetScaler Console 链接和取消链接 SSL 证书

如何使用 NetScaler Console 创建证书签名请求 (CSR)

如何从 NetScaler Console 设置 SSL 证书过期通知

如何在 NetScaler Console 上使用 SSL 控制板

如何从 NetScaler 实例轮询 SSL 证书

StyleBook

如何查看不同组的 StyleBook

如何创建自己的 StyleBook

如何在 NetScaler Console 中使用用户定义的 StyleBook

如何使用 API 从 StyleBook 创建配置

如何对 StyleBook 中定义的虚拟服务器启用分析和配置警报

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

如何创建 StyleBook 以将文件上传到 NetScaler Console

如何使用 API 创建配置以上传任何文件类型

如何创建 StyleBook 以将 SSL 证书和证书密钥文件上传到 NetScaler Console

如何使用 API 创建配置以上传证书和密钥文件

如何在企业中使用 Microsoft Skype for Business StyleBook

如何在企业中使用 Microsoft Exchange StyleBook

如何在企业中使用 Microsoft SharePoint StyleBook

分析

如何在实例上启用分析

如何配置自适应阈值

如何配置 SLA 管理

如何配置用于分析的数据库汇总

如何使用 NetScaler Console 创建阈值和警报

如何从 NetScaler Console 禁用用于分析的 URL 数据收集

事件管理

如何在 NetScaler Console 上设置事件的事件期限

如何使用 NetScaler Console 安排事件过滤器

如何为 NetScaler Console 中的事件设置重复电子邮件通知

如何使用 NetScaler Console 抑制事件

如何使用事件仪表板监控事件

如何在 NetScaler Console 上创建事件规则

如何修改 NetScaler 实例上发生的事件的报告严重性

如何在 NetScaler Console 中查看事件摘要

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

如何在 NetScaler Console 上显示 SNMP 陷阱的事件严重性和偏差

如何使用 NetScaler Console 导出 syslog 消息

如何在 NetScaler Console 中抑制 syslog 消息

如何配置实例事件的清除设置

身份验证

如何启用回退和级联外部身份验证服务器

如何添加 RADIUS 身份验证服务器

如何添加 LDAP 身份验证服务器

如何添加 TACACS 身份验证服务器

如何在 NetScaler Console 中提取身份验证服务器组

如何启用回退本地身份验证

NetScaler Console 系统

如何升级 NetScaler Console

如何重置 NetScaler Console 的密码

如何为 NetScaler Console 生成技术支持文件

如何在单服务器部署中备份和恢复您的 NetScaler Console 服务器

如何在 HA 对中备份和恢复 NetScaler Console 配置

如何在 NetScaler Console 中为非默认用户启用 Shell 访问

如何在 NetScaler Console 上配置 NTP 服务器

如何为 NetScaler Console 配置 SSL 设置

如何为 NetScaler Console 配置 syslog 清除间隔

如何查看 NetScaler Console 的审计信息

如何配置 NetScaler Console 的系统通知设置

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

如何监控 NetScaler Console 的 CPU、内存和磁盘使用情况(/zh-cn/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-monitor-cpu-memory-disk-usage-of-mas.html)

如何为 NetScaler Console 配置密码组(/zh-cn/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-configure-cipher-group-for-mas.html)

如何在 NetScaler Console 上创建 SNMP 陷阱、管理器和用户(/zh-cn/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-create-snmp-traps-managers-users-mas.html)

如何为 NetScaler Console 服务器分配主机名(/zh-cn/netscaler-application-delivery-management-software/current-release/manage-system-settings/how-to-assign-host-name-to-mas-server.html)

如何为 NetScaler Console 配置系统清除设置(/zh-cn/netscaler-application-delivery-management-software/current-release/manage-system-settings/configure-system-prune-settings-mas.html)

如何使用 NetScaler Console 配置系统备份设置(/zh-cn/netscaler-application-delivery-management-software/current-release/manage-system-settings/configure-system-backup-settings.html)

如何在 NetScaler Console 上配置和查看系统警报(/zh-cn/netscaler-application-delivery-management-software/current-release/manage-system-settings/configure-view-system-alarms-mas.html)

网络功能

如何为负载均衡实体生成报告(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/network-functions/how-to-generate-reports-for-load-balancing-entities.html)

如何导出或计划导出网络功能报告(/zh-cn/netscaler-application-delivery-management-software/current-release/networks/network-functions/export-or-schedule-export-of-reports.html)

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

概述

注意：

从 14.1-17.x 版本开始，NetScaler ADM 更名为 NetScaler Console。对于早期版本，产品名称为 NetScaler ADM。

NetScaler Console 是一种集中式管理解决方案，通过为管理员提供企业范围的可见性并自动化需要在多个实例上运行的管理作业来简化操作。您可以管理和监控 NetScaler 产品，包括 NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler CPX 和 NetScaler Gateway。您可以使用 NetScaler Console 从一个统一的控制台管理、监控和排查整个全球应用程序交付基础架构。

NetScaler Console 是一种虚拟设备，可在 Citrix Hypervisor、VMware ESXi 和 Linux KVM 上运行。NetScaler Console 通过收集有关 Web 应用程序和虚拟桌面流量的以下详细信息来解决应用程序可见性挑战：

- 用户会话级别信息
- 网页性能数据
- 流经您站点的 NetScaler 实例的数据库信息，并提供可操作的报告。

NetScaler Console 使 IT 管理员能够在几分钟内排查并主动监控客户问题。

功能和解决方案

NetScaler Console 提供以下功能：

应用程序分析和管理

应用程序性能分析

应用程序评分是评分系统的产物，该系统定义了应用程序的运行状况。它显示了应用程序在响应能力方面是否运行良好，是否不受威胁，以及所有系统是否都已启动并运行。

应用程序安全分析

应用程序安全仪表板提供应用程序安全状态的整体视图。例如，它显示关键安全指标，如安全违规、签名违规、威胁指数。应用程序安全仪表板还显示与攻击相关的信息，例如针对已发现的 NetScaler 实例的 SYN 攻击、小窗口攻击和 DNS 洪水攻击。

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

网络

实例

使您能够管理 NetScaler 和 NetScaler Gateway 实例。

实例组

使您能够按如下方式对实例进行分组：

- 静态组：允许您定义一个设备组，您可以在不同的任务（例如配置作业等）中使用该组。
- 私有 IP 块：使您能够根据地理位置对实例进行分组。

事件管理

当 NetScaler 实例的 IP 地址添加到 NetScaler Console 时，NetScaler Console 会发送一个 NITRO 调用，并隐式地将自身添加为该实例的陷阱目标，以接收其陷阱或事件。

事件表示托管的 NetScaler 实例上发生的事件或错误。

证书管理

NetScaler Console 现在为您简化了证书管理的各个方面。通过一个控制台，您可以建立自动化策略，以确保正确的颁发者、密钥强度和正确的算法，同时密切关注未使用的或即将过期的证书。要开始使用 NetScaler Console SSL 控制面板及其功能，您必须了解什么是 SSL 证书以及如何使用 NetScaler Console 跟踪您的 SSL 证书。

配置管理

NetScaler Console 允许您创建配置作业，帮助您在多个实例上轻松执行配置任务，例如创建实体、配置功能、复制配置更改、系统升级和其他维护活动。配置作业和模板将最重复的管理任务简化为 NetScaler Console 上的单个任务。

配置审计

使您能够监控和识别实例配置中的异常。

- 配置建议：允许您识别配置异常。
- 审计模板：允许您监控特定配置中的更改。

网络报告

您可以通过监控 NetScaler Console 上的网络报告来优化资源使用。

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

编排

云编排

实现了 NetScaler 产品与 OpenStack 云编排的集成。NetScaler Console 和 OpenStack 实现了彼此的 API，从而使 NetScaler 实例的负载均衡功能 (LBaaS) 能够与 OpenStack 云编排集成。

编排

NetScaler Console 通过与不同供应商的 SDN 控制器集成，支持企业网络中的 SDN。NetScaler Console 同时支持 VMware NSX Manager 和 Cisco Application Policy Infrastructure Controller (APIC)。

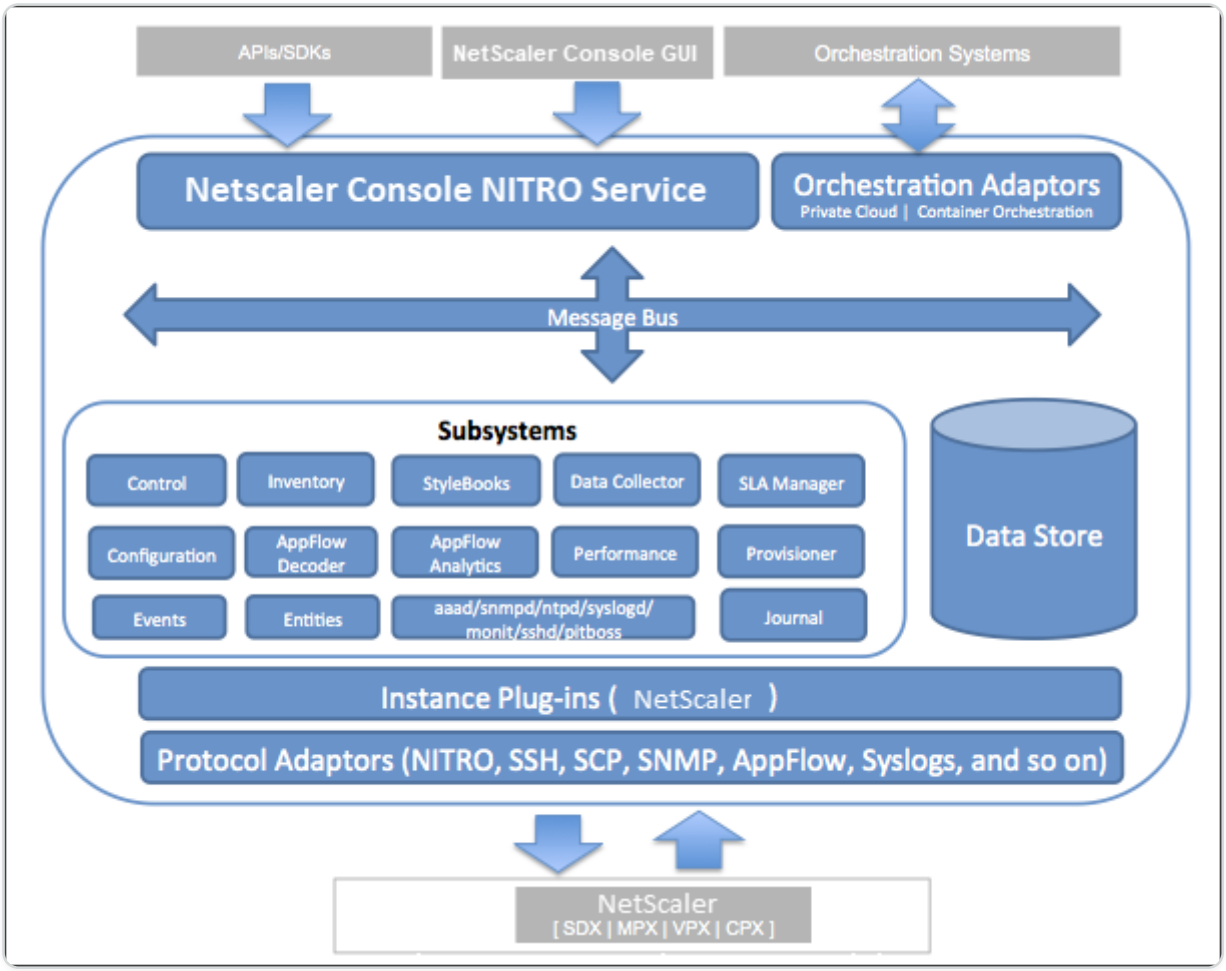
架构

NetScaler Console 数据库与服务器集成，服务器管理所有关键进程，例如数据收集、NITRO 调用。在其数据存储中，服务器存储实例详细信息清单，例如主机名、软件版本、运行和保存的配置、证书详细信息、实例上配置的实体。如果您希望处理少量流量或在有限时间内存储数据，则单服务器部署是合适的。

目前，NetScaler Console 支持两种类型的软件部署：单服务器和高可用性。

下图显示了 NetScaler Console 中的不同子系统以及 NetScaler Console 服务器与托管实例之间如何进行通信。

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



NetScaler Console 中的服务子系统充当 Web 服务器，负责处理从 GUI 或 API 发送到 NetScaler Console 内部子系统的 HTTP 请求和响应，使用端口 80 和 443。这些请求通过 IPC（进程间通信）机制，通过消息总线（消息处理系统）发送到子系统。请求被发送到控制子系统，该子系统要么处理信息，要么将其发送到相应的子系统。其他每个子系统——清单、StyleBooks、数据收集器、配置、AppFlow 解码器、AppFlow 分析、性能、事件、实体、SLA 管理器、配置器和日志——都扮演着特定的角色。

实例插件是共享库，它们对于 NetScaler Console 支持的每种实例类型都是唯一的。信息通过使用 NITRO 调用，或通过 SNMP、安全外壳 (SSH) 或安全复制 (SCP) 协议在 NetScaler Console 和托管实例之间传输。然后，此信息在内部数据库（数据存储）中进行处理和存储。

NetScaler Console 如何发现实例

实例是您希望通过 NetScaler Console 发现、管理和监控的 NetScaler 设备或虚拟设备。要管理和监控这些实例，您必须将它们添加到 NetScaler Console 服务器。您可以将以下 NetScaler 设备和虚拟设备添加到 NetScaler Console：

- NetScaler 实例
  - NetScaler MPX

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

  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
- NetScaler Gateway 实例

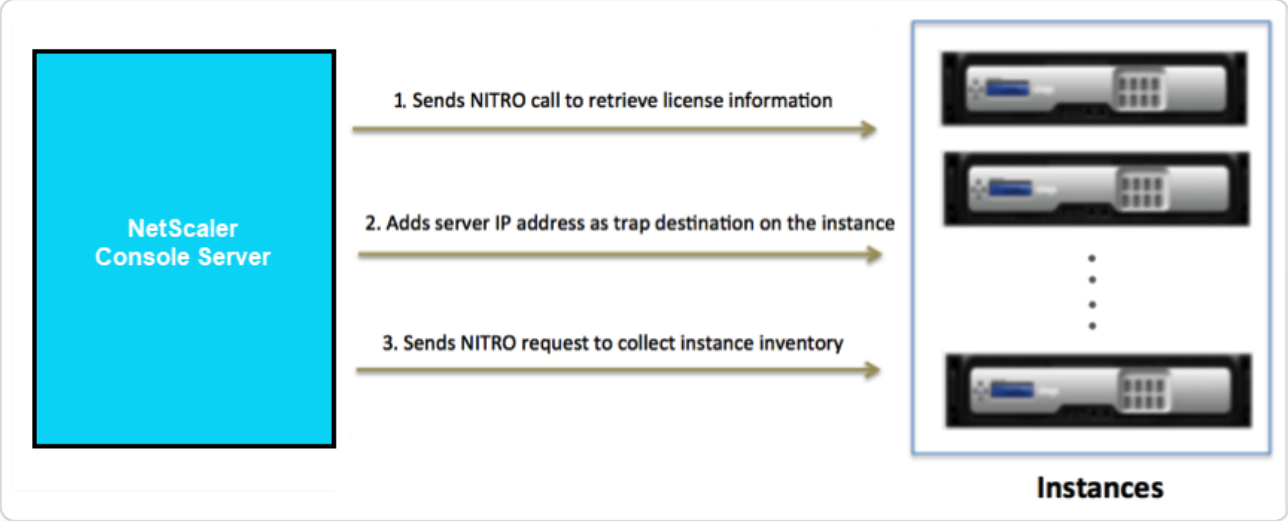
您可以在首次设置 NetScaler Console 服务器时或之后添加实例。

注意

NetScaler Console 使用 NetScaler 实例的 NetScaler IP (NSIP) 地址进行通信。NetScaler Console 还可以发现启用了管理访问权限的子网 IP (SNIP) 地址的 NetScaler 实例。有关 NetScaler 实例和 NetScaler Console 之间必须打开的端口的信息，请参阅 端口。

如果要使用 SNIP 添加 NetScaler HA 对，请确保在 NetScaler HA 对上启用独立网络配置 (INC) 模式。有关添加实例的更多信息，请参阅 添加实例。
当您将实例添加到 NetScaler Console 时，服务器会隐式地将自身添加为该实例的陷阱目标，并收集该实例的清单。

下图描述了 NetScaler Console 如何隐式发现和添加实例。



如图所示，NetScaler Console 会隐式执行以下步骤。

1. NetScaler Console 使用实例配置文件详细信息登录到实例。NetScaler Console 使用 NetScaler NITRO 调用检索实例的许可证信息。根据许可证信息，它确定实例是否为 NetScaler 实例以及 NetScaler 平台的类型（例如，NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler

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

BLX 或 NetScaler Gateway）。成功检测到实例后，它将被添加到 NetScaler Console 数据库中。

如果实例配置文件不包含正确的凭据，此步骤可能会失败。对于 NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler BLX 和 NetScaler Gateway 实例，如果许可证未应用于实例，此步骤也可能会失败。

注意

即使实例上未配置许可证，您也可以使用 HTTP 将所有实例添加到 NetScaler Console。

2. NetScaler Console 将其 IP 地址添加到实例上的陷阱目标列表中。这允许 NetScaler Console 接收在 NetScaler 实例上生成的陷阱。

   如果实例上的陷阱目标数量超过陷阱目标的最大限制，此步骤可能会失败。实例上的最大限制为 20。

3. NetScaler Console 通过发送 NITRO 请求从实例收集清单。它收集实例详细信息，例如主机名、软件版本、运行和保存的配置、证书详细信息以及在实例上配置的实体。

   此步骤可能会因网络或防火墙问题而失败。

   要了解如何将实例添加到 NetScaler Console，请参阅添加实例。

轮询概述

轮询是 NetScaler Console 从 NetScaler 实例收集特定信息的过程。您可能已为您的组织在全球范围内配置了多个 NetScaler 实例。为了通过 NetScaler Console 监控您的实例，NetScaler Console 必须从所有托管的 NetScaler 实例收集某些信息，例如 CPU 使用率、内存使用率、SSL 证书、许可功能、许可证类型等。以下是 NetScaler Console 与托管实例之间发生的各种轮询类型：

- 实例轮询
- 清单轮询
- 性能数据收集
- 实例备份轮询
- 配置审计轮询
- SSL 证书轮询
- 实体轮询

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

NetScaler Console 使用 NITRO 调用、安全外壳 (SSH) 和安全复制 (SCP) 等协议从 NetScaler 实例轮询信息。

NetScaler Console 如何轮询托管实例和实体

NetScaler Console 默认情况下会自动定期轮询。NetScaler Console 还允许您为少数轮询类型配置轮询间隔，并在需要时手动轮询。

下表描述了轮询类型、轮询间隔、使用的协议等详细信息：

轮询类型	轮询间隔	轮询信息	使用的协议	轮询间隔配置
实例轮询	每 1 分钟（默认）	统计信息，例如状态、每秒 HTTP 请求数、CPU 使用率、内存使用率和吞吐量。	NITRO 调用。	否
清单轮询	每 60 分钟（默认）	清单详细信息，例如内部版本、系统信息、许可功能和模式。	NITRO 调用和 SSH	否
性能数据收集	每 5 分钟（默认）	网络报告信息	NITRO 调用	否
实例备份轮询	每 12 小时（默认）	受管 NetScaler 实例当前状态的备份文件	NITRO 调用、SSH 和 SCP。	是。导航到 **Infrastructure > Instances > NetScaler**。选择实例，然后从 **Select Action** 列表中单击 **Backup/ Restore**。
配置审核轮询	每 10 小时（默认）	NetScaler 实例上发生的配置更改（例如，运行中配置与已保存配置）	SSH、SCP 和 NITRO 调用	是。导航到 **Infrastructure > Configuration Audit**。在

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

轮询类型	轮询间隔	轮询信息	使用的协议	轮询间隔配置
				“Configuration Audit”页面上，单击 **Settings** 并配置 “Configuration Audit Polling”的轮询间隔。
				您可以手动轮询配置审核，并将实例的所有配置审核立即添加到 NetScaler Console。为此，请导航到 **Infrastructure > Configuration Audit**，然后单击 **Poll Now**。“**Poll Now**”页面允许您轮询网络中的所有或选定实例。
SSL 证书轮询	默认情况下，每 24 小时	安装在 NetScaler 实例上的 SSL 证书。	NITRO 调用和 SCP	是。导航到 **Infrastructure > SSL Dashboard**。在 SSL Dashboard 页面上，单击 **Settings** 以配置轮询间隔。
				您可以手动轮询 SSL 证书，并将实例的所有证书立即添加到

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

轮询类型	轮询间隔	轮询信息	使用的协议	轮询间隔配置
				NetScaler Console。为此，请导航到 **Infrastructure > SSL Dashboard** 并单击 **Poll Now** 。**Poll Now** 页面允许您轮询网络中的所有或选定实例。
实体轮询				
所有实例	默认情况下，每 720 分钟	实例上配置的所有实体。实体可以是附加到 NetScaler 实例的策略、虚拟服务器、服务或操作。要启用实体轮询，请参阅启用或禁用 NetScaler Console 功能。	NITRO 调用	是。它可以设置为 30 分钟到 1440 分钟之间。要配置，请导航到 **Infrastructure > Network Functions**。在 Networks Function 页面上，单击 **Settings** 以配置轮询间隔。
				您可以手动轮询实体，并将实例的所有实体立即添加到 NetScaler Console。为此，请导航到 **Infrastructure > Network Functions** 并单击 **Poll Now**。**Poll Now** 页面允许您轮询网络

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

轮询类型	轮询间隔	轮询信息	使用的协议	轮询间隔配置
				中的所有或选定实例。
选定的 NetScaler 实例	默认情况下，每 15 分钟	仅轮询在默认轮询周期触发之前发生更改的 NetScaler 实例。	NITRO 调用	是。它可以设置为 5 分钟到 60 分钟之间。导航到 **Infrastructure > Network Functions**，单击 **Settings**，然后在 **Delay time for Network Functions** 文本框中指定时间。

注意

除了轮询之外，NetScaler Console 通过发送到实例的 SNMP trap 接收由托管 NetScaler 实例生成的事件。例如，当发生系统故障或配置更改时，会生成一个事件。

在实例备份期间，SSL 文件、CA 证书文件、NetScaler 模板、数据库信息等会下载到 NetScaler Console。在配置审计期间，ns.conf 文件会下载并存储在文件系统中。从托管 NetScaler 实例收集的所有信息都内部存储在数据库中。

轮询实例的不同方式

以下是 NetScaler Console 对托管实例执行的几种轮询方式：

- 实例的全局轮询
- 实例的手动轮询
- 实体的手动轮询

实例的全局轮询

NetScaler Console 会根据您配置的间隔自动轮询网络中的所有托管实例。尽管默认轮询间隔为 30 分钟，但您可以通过导航到 **Infrastructure > Network Functions** > **Settings** 根据您的要求设置间隔。

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

实例的手动轮询

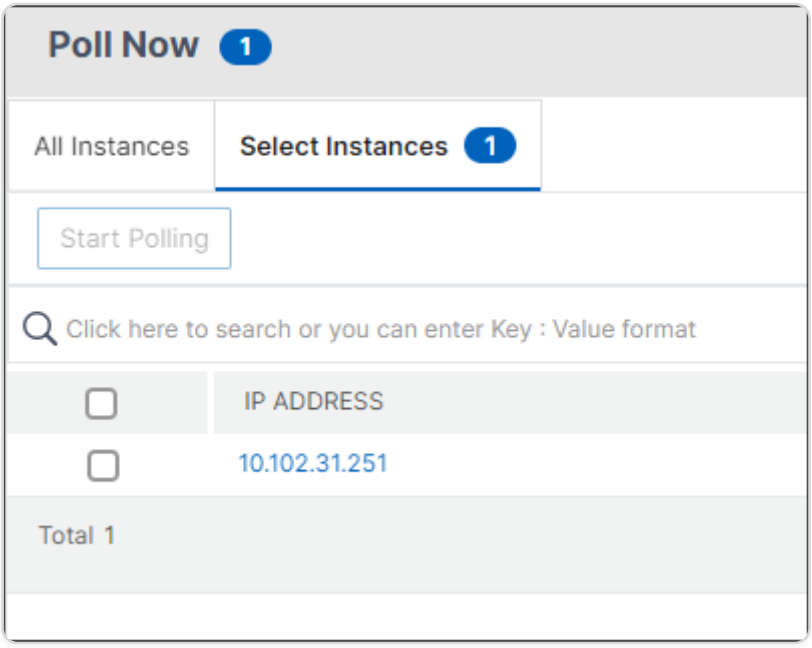
当 NetScaler Console 管理许多实体时，轮询周期需要更长时间才能生成报告，这可能导致屏幕空白或系统仍显示较早的数据。

在 NetScaler Console 中，存在一个最小轮询间隔期，在此期间不会发生自动轮询。如果您添加新的 NetScaler 实例，或者实体已更新，NetScaler Console 在下一次轮询发生之前不会识别新实例或对实体所做的更新。而且，无法立即获取虚拟 IP 地址列表以进行进一步操作。您必须等待最小轮询间隔期过去。尽管您可以手动轮询以发现新添加的实例，但这会导致整个 NetScaler 网络被轮询，从而给网络带来沉重负担。现在，NetScaler Console 允许您在任何给定时间仅轮询选定的实例和实体，而不是轮询整个网络。

NetScaler Console 每天在设定时间自动轮询托管实例以收集信息。选择性轮询可减少 NetScaler Console 显示绑定到这些选定实例的实体的最新状态所需的刷新时间。

在 NetScaler Console 中轮询特定实例：

1. 在 NetScaler Console 中，导航到 **基础架构 > 网络功能**。
2. 在 **Network Functions** 页面右上角，单击 **Poll Now**。
3. 弹出页面 **Poll Now** 提供了轮询网络中所有 NetScaler 实例或轮询选定实例的选项。
   a. **All Instances** 选项卡 - 单击 **Start Polling** 以轮询所有实例。
   b. **Select Instances** 选项卡 - 从列表中选择实例
4. 单击 **开始轮询**。



NetScaler Console 启动手动轮询并添加所有实体。

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

实体的手动轮询

NetScaler Console 还允许您仅轮询绑定到特定实例的少数选定实体。例如，您可以使用此选项来了解实例中特定实体的最新状态。在这种情况下，您无需整体轮询实例即可了解一个已更新实体的状态。当您选择并轮询一个实体时，NetScaler Console 只轮询该实体并更新 NetScaler Console GUI 中的状态。

考虑一个虚拟服务器处于 DOWN 状态的示例。该虚拟服务器的状态可能在下一次自动轮询发生之前已更改为 UP。要查看虚拟服务器的更改状态，您可能只想轮询该虚拟服务器，以便在 GUI 上立即显示正确状态。

您现在可以轮询以下实体以获取其状态的任何更新：服务、服务组、负载平衡虚拟服务器、缓存缩减虚拟服务器、内容切换虚拟服务器、身份验证虚拟服务器、VPN 虚拟服务器、GSLB 虚拟服务器和应用程序服务器。

注意

如果您轮询虚拟服务器，则只轮询该虚拟服务器。关联的实体（例如服务、服务组和服务器）不会被轮询。如果您需要轮询所有关联实体，则必须手动轮询这些实体，或者轮询实例。

在 NetScaler Console 中轮询特定实体：

例如，此任务可帮助您轮询负载平衡虚拟服务器。同样，您也可以轮询其他网络功能实体。

1. 在 NetScaler Console 中，导航到 **基础架构 > 网络功能 > 负载平衡 > 虚拟服务器**。
2. 选择状态显示为 DOWN 的虚拟服务器，然后单击 **立即轮询**。虚拟服务器的状态现在变为 UP。

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

NetScaler® 遥测程序

Citrix 会出于其合法利益（包括许可证合规性）收集基本的许可证遥测数据以及 NetScaler 部署和功能使用遥测数据。您可以自动或手动上传所需的许可证和功能使用数据，以符合 此处 所述的 NetScaler 遥测程序。还会收集 NetScaler Console 配置和功能使用数据，以管理、衡量和改进 Citrix 产品和服务。如果您是现有的 NetScaler Console 客户，则必须确保符合 NetScaler 遥测程序。我们强烈建议将 NetScaler 实例添加到 NetScaler Console，以全面改进和简化您的 NetScaler 操作，并通过发送 NetScaler 功能使用数据来支持我们产品的增强。了解更多。

您可以通过以下方式上传所需的遥测数据：

- **自动收集模式** - 升级到 **14.1-25.56 或更高版本 / 13.1-53.22 或更高版本** 后，此模式默认启用。自动模式会创建出站连接以使用自动启用的通道（端点 URL），并自动上传遥测数据。您只需确保端点 URL 可访问。由于上传是自动进行的，因此除非先决条件失败，否则您无需执行任何操作。有关详细信息，请参阅 自动收集模式。
- **手动收集模式** - 仅当自动模式禁用时，此模式才启用。您必须从本地 NetScaler Console 中的 NetScaler 遥测主页下载所需的遥测数据，并在 30 天内完成首次上传到 NetScaler Console 服务。后续上传必须每 90 天进行一次，以保持合规。有关详细信息，请参阅 手动收集模式。

建议使用自动遥测模式并自动上传所需数据，但您也可以选择禁用自动模式并手动上传。在自动和手动模式下，都需要上传数据以符合 NetScaler 遥测程序。您可以选择禁用可选遥测数据不包含在数据上传中，但必需的许可证合规性和功能使用遥测数据必须在自动和手动模式下提供。

为保持合规，自上次成功上传以来的天数不得超过 90 天。

作为 NetScaler 遥测程序的一部分，以下配置已推送到受管 NetScaler 实例：

- AppFlow 配置：`enable ns feature AppFlow`
- 遥测指标配置文件配置：`add analytics profile telemetry_metrics_profile -type timeseries -outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "./telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency 300`

注意：

为实现最佳遥测数据收集，我们建议您升级到最新的 NetScaler Console 版本。

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

- 从 **14.1-43.x / 13.1-57.x** 版本开始，如果 NetScaler 实例中存在遥测指标配置文件配置，NetScaler Console 将会将其删除。遥测指标配置文件配置的删除不会影响 NetScaler 实例中的任何现有功能。
- 如果您未使用 NetScaler 或 NetScaler Console 分析功能，可以使用以下命令删除 AppFlow 配置：

  `disable ns feature AppFlow`

下表提供了有关最新版本和早期版本中 AppFlow® 和遥测指标配置文件配置的详细信息：

版本	作为遥测计划一部分推送的配置	遥测模式	所需操作
14.1-43.x / 13.1-57.x	否	自动和手动	配置不会推送到 NetScaler 实例，如果存在，遥测指标配置文件配置将从 NetScaler 实例中删除。如果您未使用 NetScaler 或 NetScaler Console 分析功能，您可以使用 `disable ns feature AppFlow` 删除 AppFlow 配置。
14.1-29.x / 13.1-55.x	否	自动和手动	配置不会作为 NetScaler 遥测计划的一部分推送。如果这些配置存在于您的 NetScaler 实例中并且您想要删除这些配置，请在 NetScaler 上运行 `rm analytics profile telemetry_metrics_profile` 命令以删除遥测指标配置文件配置，并使用 `disable ns feature AppFlow` 删除 AppFlow 配置。

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

版本	作为遥测计划一部分推送的配置	遥测模式	所需操作
14.1-25.56 / 13.1-53.22	是。AppFlow 和遥测指标配置文件配置	自动化（所有先决条件均已满足）	配置作为 NetScaler 遥测程序的一部分被推送，但不会每 24 小时检查一次。要删除这些配置，请在 NetScaler 上运行 `rm analytics profile telemetry_metrics_profile` 命令以删除遥测指标配置文件配置，并使用 `disable ns feature AppFlow` 删除 AppFlow 配置。
		自动化（任何先决条件未满足）或手动	如果这些配置缺失，NetScaler Console 会继续每 24 小时检查一次这些配置并将其推送到 NetScaler 实例。如果您不希望推送这些配置，则必须处于自动化模式（所有先决条件均已满足）或升级到最新版本。

注意：

- `/nsconfig/.telemetry.conf` 文件会使用以下命令更新，用于网关遥测。如果此命令缺失，NetScaler Console 会每小时检查一次并添加它：

```
ns_telemetry_server,&lt;Console IP>,5140
```

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

- 某些遥测参数是通过从 NetScaler Console 推送到 NetScaler 实例的脚本收集的。这些脚本是只读的，不会更改 NetScaler 中的任何内容。
- 通过遥测收集的信息，例如电子邮件地址、用户名和 IP 地址，通过使用单向哈希算法在源头对信息进行哈希处理，从而安全地进行匿名化。因此，Citrix 无法访问或读取这些值。此遥测数据仅用于逻辑资产匹配目的。

下表提供了作为 NetScaler 遥测程序一部分收集的参数详细信息：

类别	描述	我们用它做什么？	必需/可选
许可证，以及 NetScaler 部署和使用遥测数据	有关许可证权利、分配、使用、高级 NetScaler 部署数据以及 NetScaler 功能使用情况的信息。	许可证合规性，以及管理、衡量和改进服务。	必需
NetScaler Console 部署和功能使用遥测数据	有关 Console 部署和功能使用情况的信息。	用于管理、衡量和改进服务。	可选

有关可选和必需遥测参数列表的更多信息，请参阅数据治理。

Citrix 要求您从 **2024 年 6 月 18 日**起在 3 个月内过渡到最新的 NetScaler Console 版本（14.1-25.56 或更高版本 / 13.1–53.22 或更高版本）。升级到 NetScaler Console 14.1-25.56 或更高版本 / 13.1–53.22 或更高版本后，其中一种遥测模式（自动或手动）必须处于活动运行状态。除非您选择手动报告，否则您同意根据需要调整防火墙以允许自动遥测报告。

注意事项：

- 遥测模块在 NetScaler 上执行多个 SSH 命令，并使用 NetScaler Console 的 SSH 实用程序读取响应中的输出。如果满足以下任一条件，SSH 实用程序将无法正常工作，并且遥测将失败：
  - NetScaler OS 主机名中包含“#”字符。
  - NetScaler motd（每日消息）中包含“#”字符。
  - NetScaler PS1 提示符中包含“#”字符。
- 您必须确保在 **2024 年 9 月 18 日** 之前过渡到最新版本 (14.1–25.56 及更高版本 / 13.1–53.22 及更高版本)。
- 如果您选择手动遥测模式，首次上传必须在您过渡到上述版本后的 30 天内完成，但不得迟于 2024 年 10 月 18 日。此后，您的 NetScaler Console 本地部署版必须每 90 天进行一次手动遥测上传，才能符合 NetScaler 遥测计划的要求。

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

如果未能遵守这些要求，Citrix 可能会暂停或终止您的 Citrix 支持，恕不承担任何责任，此外，Citrix 还可采取法律或衡平法规定的任何其他补救措施。在法律或法规禁止的范围内，这些要求不适用。有关更多信息，请参阅 Citrix 许可证遥测常见问题解答。

遥测数据收集模式

自动化遥测数据收集模式

升级到 NetScaler Console on-prem 14.1-25.53 / 13.1-53.22 或更高版本后，此模式默认启用。

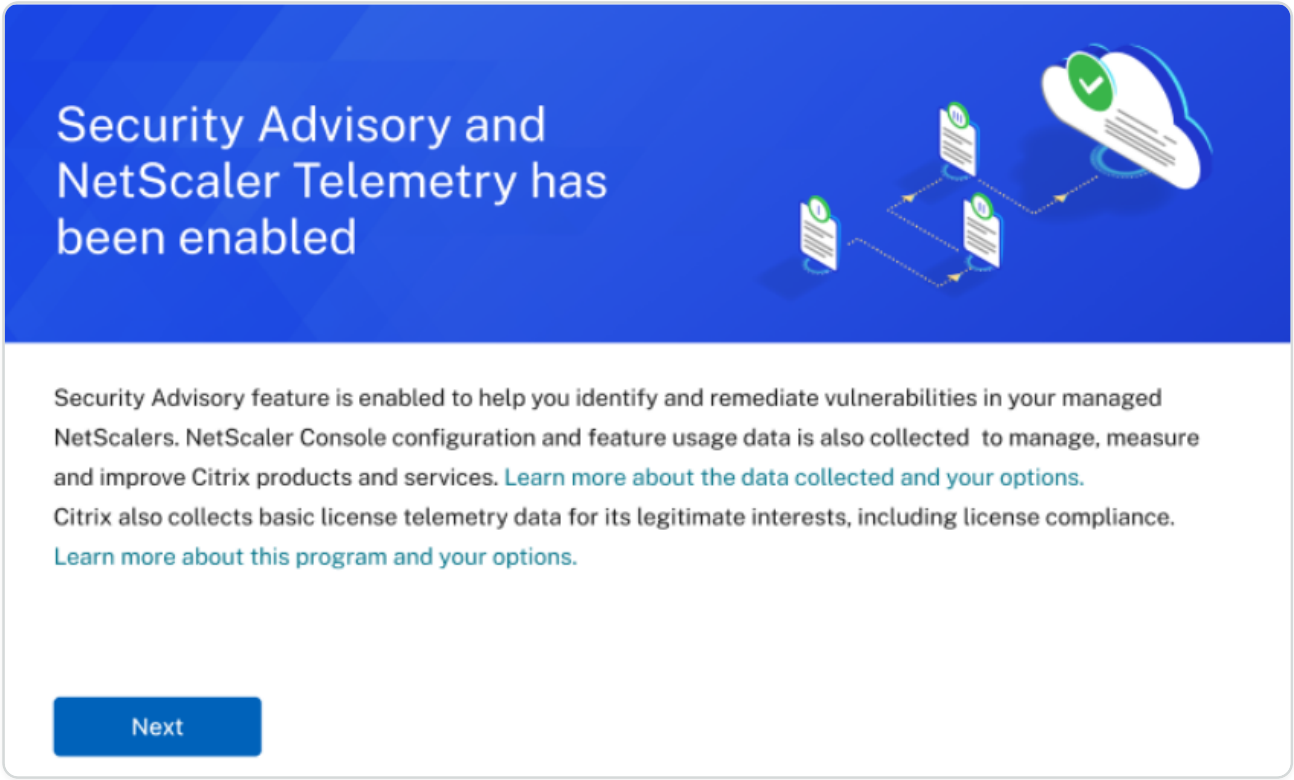
自动化遥测数据收集模式的先决条件：

- 确保您已连接互联网，或者在 NetScaler Console on-prem 中配置了代理服务器以访问 Citrix Cloud。有关更多信息，请参阅系统要求。
- 确保以下端点 URL 可访问：
  - 下载服务 URL: `https://download.citrixnetworkapi.net`
  - 服务 URL: `https://adm.cloud.com`（仅在 14.1-43.x 或更早版本中需要）。
  - 自动启用通道: `https://safehaven.adm.cloud.com`
- 确保以下端口已打开：

端口	类型	详细信息	通信方向
5140	UDP	接收 NetScaler Gateway 遥测数据的端口	NetScaler 到 NetScaler 控制台

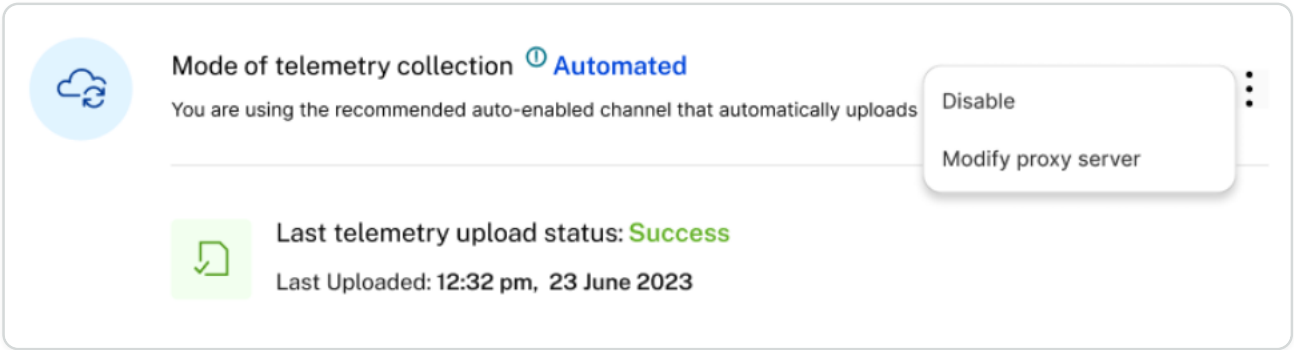
升级到 14.1-25.53 或 13.1-53.22 版本并导航到 **NetScaler 遥测**页面后，在以下弹出窗口中单击**下一步**：

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



手动遥测收集模式

要使用手动遥测收集模式，您必须首先禁用**安全建议**，然后单击垂直省略号并选择**禁用**。



在弹出窗口中，单击**我同意手动上传数据**以禁用自动遥测收集。遥测收集模式将自动更改为**手动**。在手动遥测模式下，新的 CVE 更新不可用，您只能使用现有或上次更新的 CVE 的安全建议。

选择手动模式后，您必须在 30 天内下载遥测数据并在 NetScaler Console 服务中完成首次上传。此后，后续上传每 90 天进行一次。

注意：

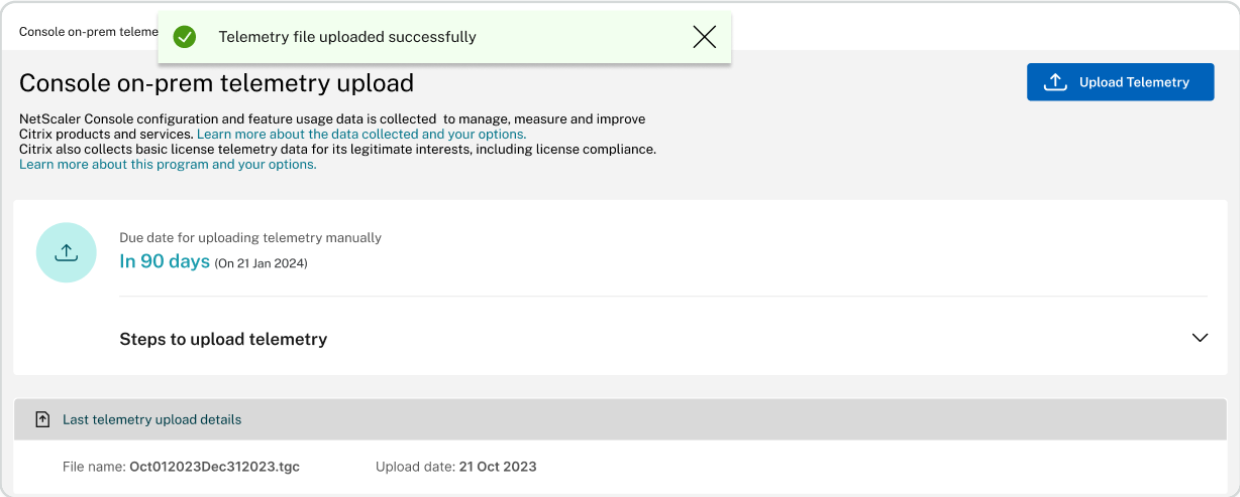
最多使用 2 GB 的 NetScaler Console 磁盘空间来保存 90 天的遥测数据。

在 **NetScaler 遥测**主页上，单击**下载遥测数据**以下载包含所需遥测数据的捆绑包 (.tgz) 文件。

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

下载遥测文件后，您必须将其上传到 NetScaler Console 服务。要在 NetScaler Console 服务中上传：

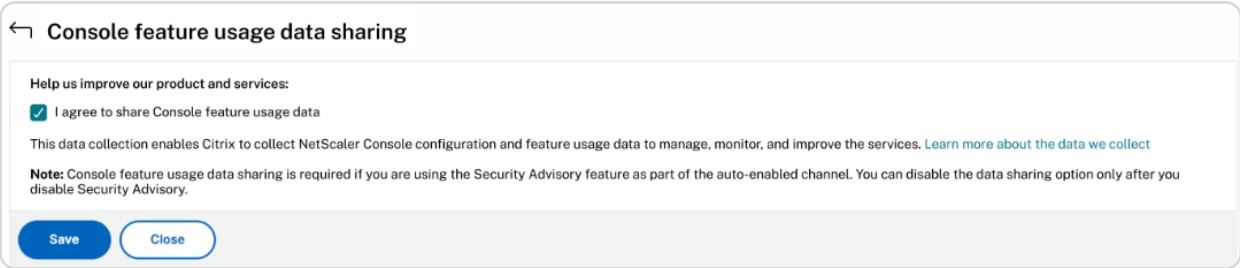
1. 登录到 Citrix Cloud (citrix.cloud.com)。如果您没有 Citrix Cloud 帐户，请注册一个新帐户。有关更多信息，请参阅创建 Citrix Cloud 帐户。
2. 选择一个帐户。
3. 在 **NetScaler Console Service** 下，单击 **Manage**。
4. 设置 Console 服务帐户。
5. 在 NetScaler Console 服务中，导航到 **设置 > 控制台本地遥测上传**。
6. 单击 **Upload Telemetry** 并选择已下载的 (.tgz) 文件以完成上传过程。
7. 在选择手动模式后的 30 天内完成首次上传。此后，每 90 天重复相同的步骤并上传遥测文件。



注意：

- 如果文件不是有效的 (.tgz) 格式或文件未通过完整性检查，则上传失败。建议重新下载并重试上传。如果问题仍然存在，请联系客户服务。
- 您可以禁用上传可选遥测数据。要禁用，您必须首先在 **NetScaler Telemetry** 页面中禁用 **Security Advisory**，然后导航到 **Settings > Administration > Enable or disable the Console feature data sharing**，并清除 **I agree to share Console feature usage data** 复选框。

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



- 在您的本地 NetScaler Console 中，上传截止日期前 7 天会显示提醒横幅。

用于排查遥测数据收集和上传问题的诊断

在版本 14.1 build 56.x 之前，诊断功能有助于检查到这些端点 URL 的出站连接，并告知您它们是否处于可访问状态。NetScaler On-prem 版本 14.1 build 56.x 及更高版本提供了增强的诊断功能，用于识别和排查收集器级别（控制台）和设备级别（单个 NetScaler 实例）的遥测数据收集和上传问题。

从版本 14.1 build 56.x 开始的诊断行为

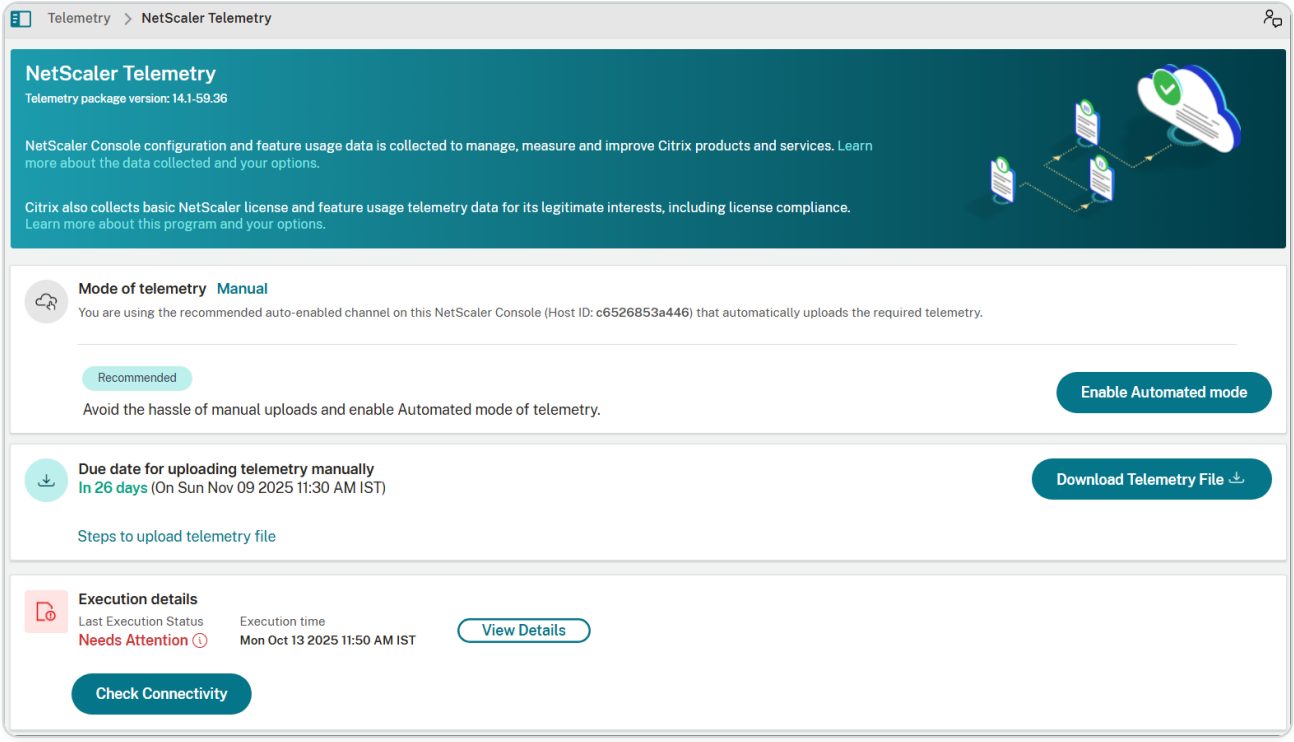
注意：

> 从版本 14.1 build 56.x 开始，遥测诊断功能得到增强，可以识别和排查收集器级别（控制台）和设备级别（单个 NetScaler 实例）的遥测数据收集和上传问题。

所有受管的 NetScaler 实例都必须发送遥测数据以保持合规。但是，由于连接或配置问题，遥测数据上传和收集会失败。 Console on-prem 的 NetScaler 遥测页面上的诊断功能可帮助您快速识别和排查这两个级别的问题：

- 收集器级别（控制台）：检查数据是否已成功上传。
- 设备级别（单个 NetScaler 实例）：检查是否已从 NetScaler 实例收集数据。

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



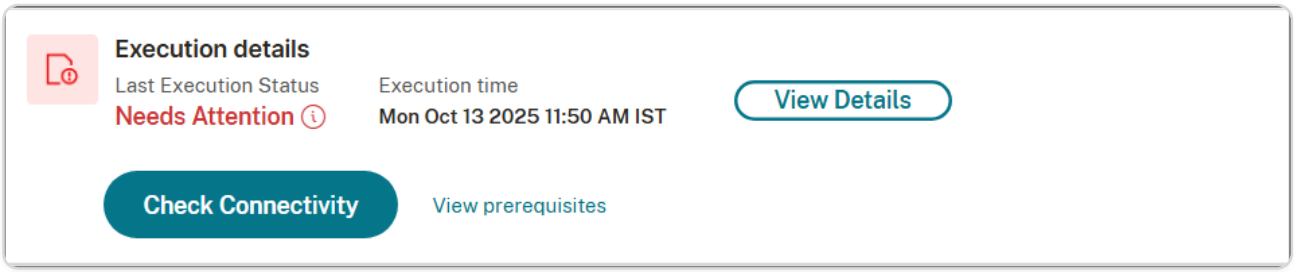
工作原理

以下是诊断过程中的高级步骤：

- 自动运行：诊断功能每 24 小时自动运行一次。
- 按需运行：用户可以根据需要手动运行诊断，尤其是在尝试修复问题之后。
- 状态指示器：结果以清晰的状态显示：
  - 成功：未检测到任何问题。
  - 需要注意：一个或多个问题需要用户操作。

注意：

单击**查看详细信息**或错误突出显示的区域，以获取深入的错误日志和缓解步骤。

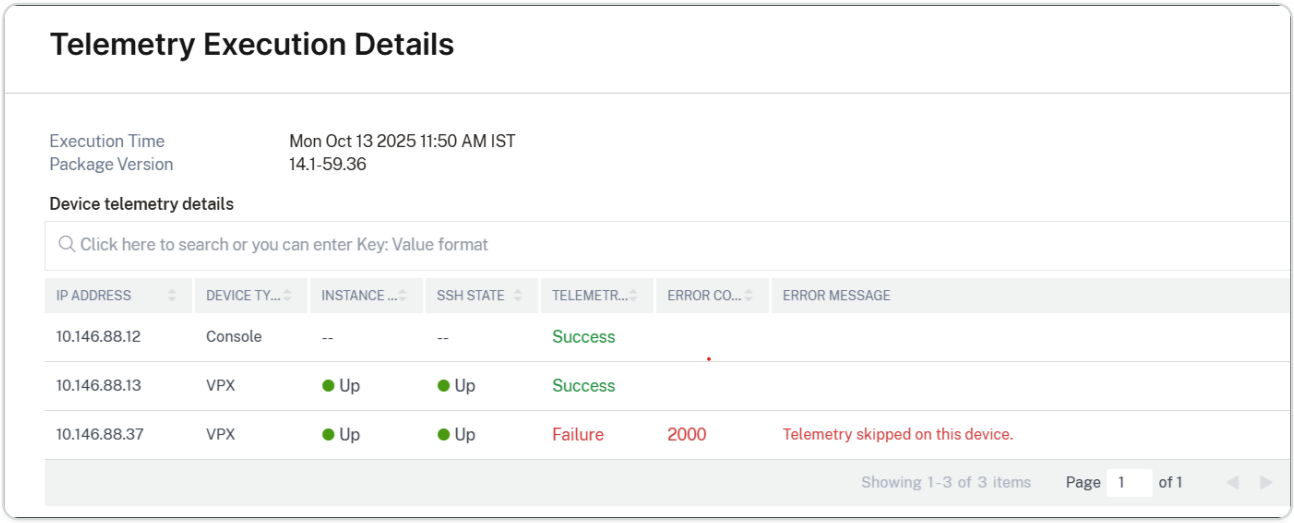


收集器级别（控制台）诊断

本节检查 NetScaler Console 是否成功从托管设备收集数据并将其上传到所需目标。

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

检查字段	描述
执行时间	上次从托管 NetScaler 实例收集遥测数据的时间戳。
软件包版本	此检查可识别 Console 本地安装的遥测软件包版本，确保收集到最新数据集。
常青下载状态	（仅限自动模式）Console 本地每 24 小时检查一次下载服务 URL 中是否有更新的遥测脚本包。将鼠标悬停在信息 (i) 图标上可查看具体的故障原因。要获取有关缓解步骤的更多详细信息，请单击“失败”状态。
连接状态	(仅自动模式) 确认所需的 URL 已列入白名单且可访问。连接问题（例如代理配置错误）会阻止控制台访问这些 URL。将鼠标悬停在信息 (i) 图标上可查看无法访问的具体原因。要获取有关缓解步骤的更多详细信息，请单击**不可访问状态**。
	- 下载服务 URL：最新遥测包下载的来源。
	- 自动启用通道 URL：用于上传遥测数据的目标。



设备级 (NetScaler) 诊断

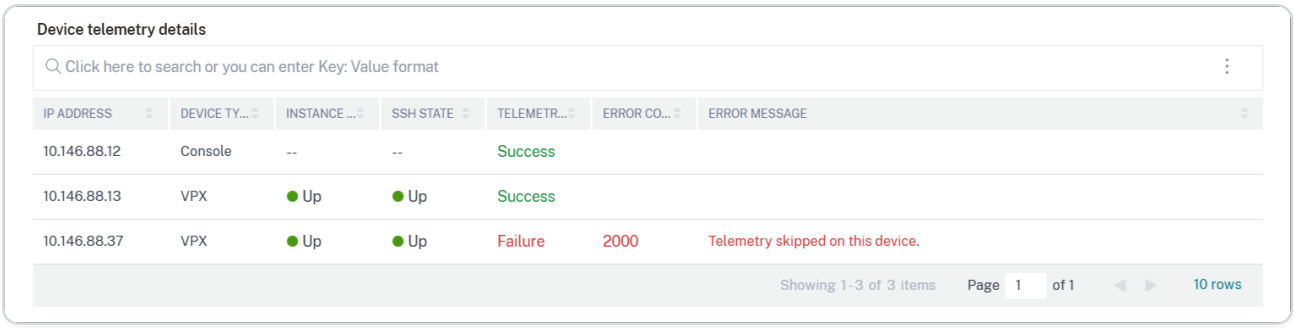
控制台通过将遥测收集脚本推送到每个托管的 NetScaler 实例、收集数据并准备上传来运行设备级诊断。

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

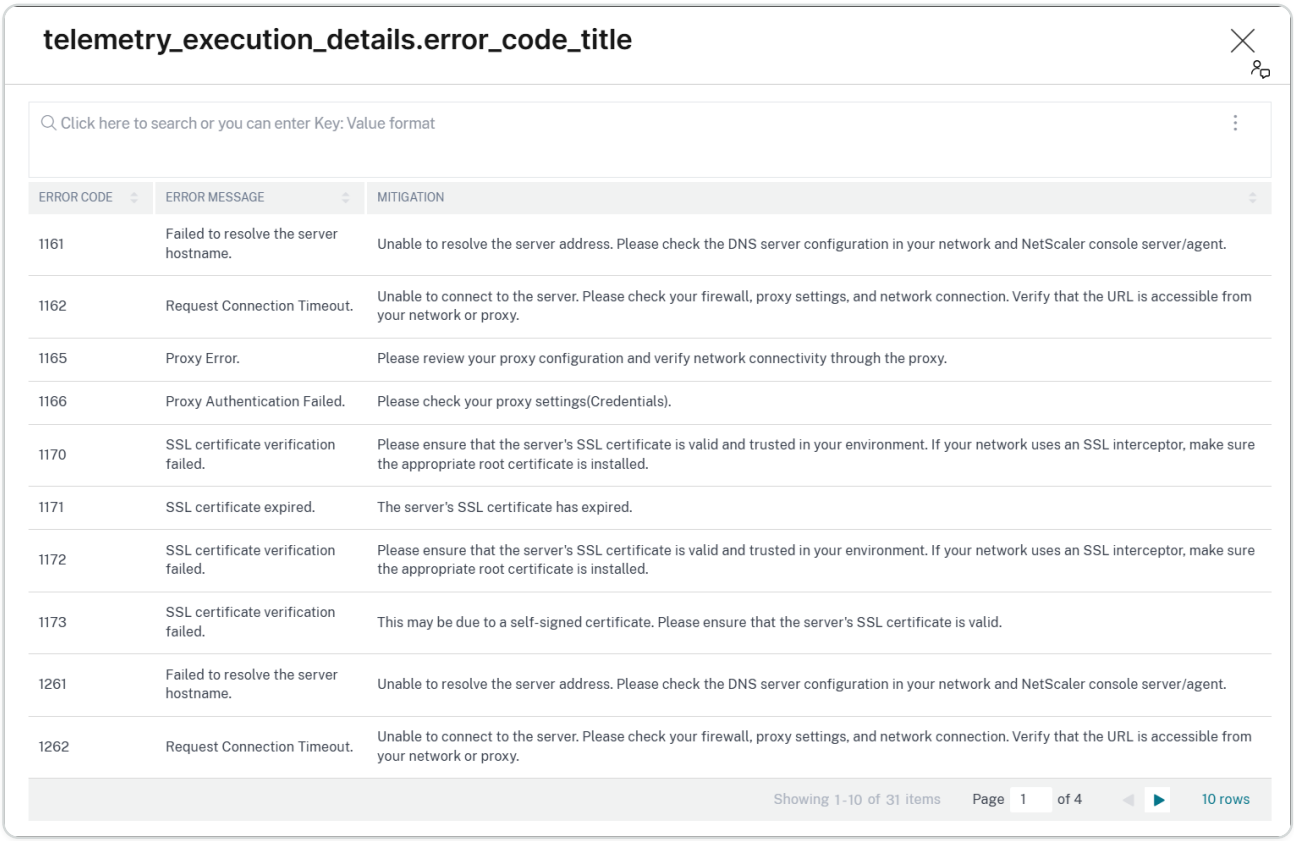
设备遥测详细信息表提供了此过程的结果，包括：

- 设备详细信息
- 遥测状态
- 错误代码和错误消息

有关详细的错误信息和缓解步骤，请单击红色突出显示的错误详细信息。



缓解措施：每个错误代码都映射到缓解表中的推荐解决方案。请遵循建议来解决问题。



错误表映射

错误代码	错误消息	客户操作
1161	无法解析服务器主机名	无法解析服务器地址。请检查您的网络和 NetScaler 控制台

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

错误代码	错误消息	客户操作
		服务器/代理中的 **DNS 服务器配置**。
1162	无法解析服务器地址。请检查您的网络和 NetScaler 控制台服务器/代理中的 **DNS 服务器配置**。	无法连接到服务器。请检查您的 **防火墙、代理设置和网络连接**。另外，请验证您的网络或通过代理是否可以访问 URL `download.citrixnetworkapi.net`。
1165	代理错误	请检查您的 **代理配置** 并确保网络连接通过代理正常工作。
1166	代理身份验证失败	请在 NetScaler 控制台中检查您的**代理凭据**。
1170	SSL 证书验证失败。	如果您的网络使用 **SSL 拦截器**，请确保在 NetScaler 控制台中**安装了相应的根证书**。
1171	SSL 证书已过期	**SSL 证书已过期**。
1172	SSL 证书验证失败。	如果您的网络使用 **SSL 拦截器**，请确保在 NetScaler 控制台中**安装了相应的根证书**。
1173	SSL 证书验证失败。	这可能是由于**自签名证书**。如果您的网络使用 **SSL 拦截器**，请确保在 NetScaler 控制台中**安装了相应的根证书**。
1261	无法解析服务器主机名	无法解析服务器地址。请检查您的网络和 NetScaler 控制台服务器/代理中的 **DNS 服务器配置**。
1262	请求连接超时	无法连接到服务器。请检查您的**防火墙、代理设置和网络连接**。验证这两个 URL (`download.citrixnetworka`

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

错误代码	错误消息	客户操作
		`pi.net`, `safehaven.adm.cloud.com`) 可从您的网络或通过您的代理访问。
1265	代理错误	请检查您的**代理配置**，并确保网络连接通过代理正常工作。
1266	代理身份验证失败。	请在 NetScaler 控制台中检查您的**代理凭据**。
1270	SSL 证书验证失败	如果您的网络使用 **SSL 拦截器**，请确保在 NetScaler 控制台中**安装了相应的根证书**。
1271	SSL 证书已过期。	服务器的 **SSL 证书已过期**。
1272	SSL 证书验证失败	如果您的网络使用 **SSL 拦截器**，请确保在 NetScaler 控制台中**安装了相应的根证书**。
1273	SSL 证书验证失败	这可能是由于**自签名证书**造成的。如果您的网络使用 **SSL 拦截器**，请确保在 NetScaler 控制台中**安装了相应的根证书**。
1361	无法解析服务器主机名	无法解析服务器地址。请检查您的网络和 NetScaler 控制台服务器/代理中的 **DNS 服务器配置**。
1362	请求连接超时。	无法连接到服务器。请检查您的**防火墙、代理设置和网络连接**。验证 URL `safehaven.adm.cloud.com` 是否可从您的网络或通过您的代理访问。
1365	代理错误	请检查您的**代理配置**，并确保网络连接通过代理正常工作。

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

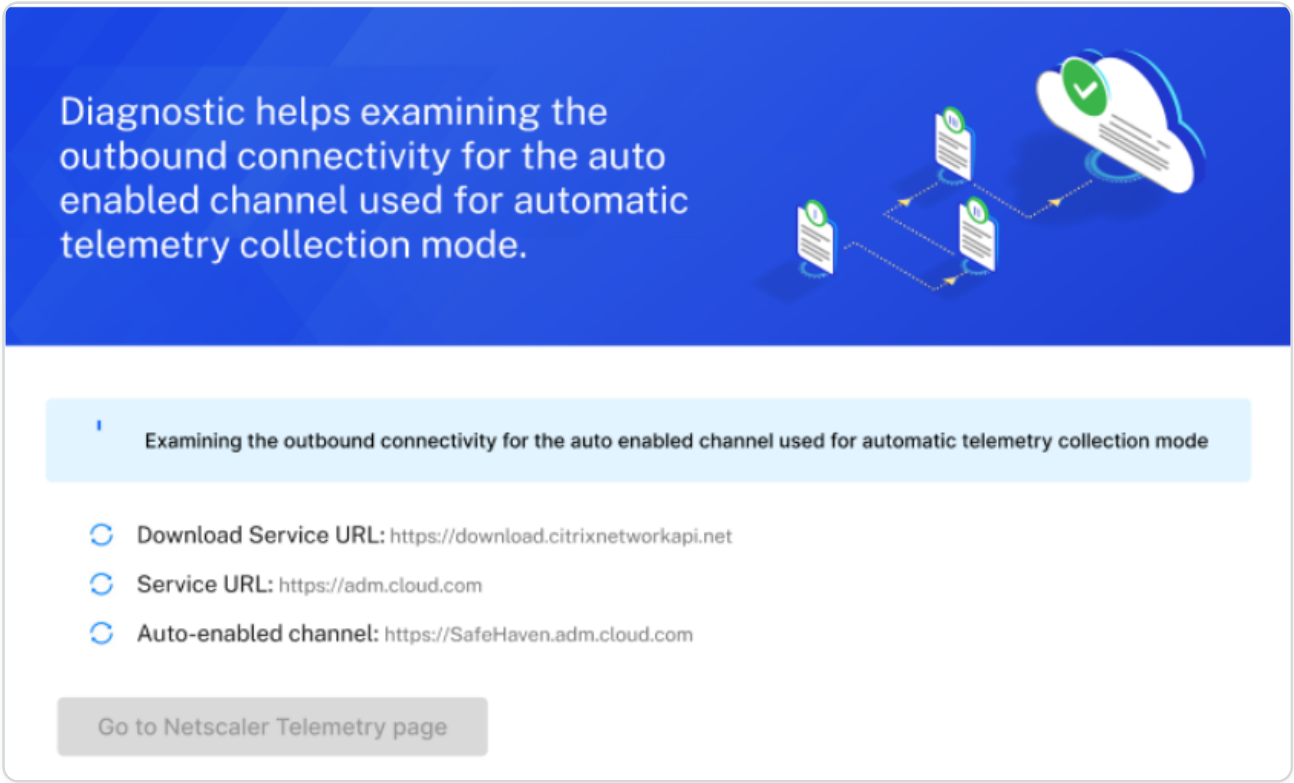
错误代码	错误消息	客户操作
1366	代理身份验证失败	请在 NetScaler 控制台中检查您的**代理凭据**。
1370	SSL 证书验证失败。	如果您的网络使用 **SSL 拦截器**，请确保在 NetScaler 控制台中**安装了相应的根证书**。
1371	SSL 证书已过期	服务器的**SSL 证书已过期**。
1372	SSL 证书验证失败。	如果您的网络使用 **SSL 拦截器**，请确保在 NetScaler 控制台中**安装了相应的根证书**。
1373	SSL 证书验证失败。	这可能是由于**自签名证书**造成的。如果您的网络使用 **SSL 拦截器**，请确保在 NetScaler 控制台中**安装了相应的根证书**。
2000	此设备上的遥测已跳过。	这可能是因为此设备**由另一个 NetScaler Console/Service/Agent 管理**。请确保其他收集器正在成功发送遥测数据。
2100	实例状态为关闭或不可达。	请确保**实例正在运行且可达**。
2250	SSH 身份验证错误	请确保在 NetScaler 控制台中为该设备**正确配置了设备配置文件**。
2251	SSH 连接超时/拒绝。	连接可能被防火墙或网络策略暂时阻止，或者设备可能不可达。请**验证网络连接**并确保 **SSH 端口可访问**。
2252	主机密钥验证失败	与管理员核实服务器身份，然后删除旧密钥：`ssh-keygen -R <server_address>`。

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

错误代码	错误消息	客户操作
2350	SSH 身份验证错误。	请确保在 NetScaler 控制台中为设备**正确配置了设备配置文件**。
2351	SSH 连接设备失败	连接可能被防火墙或网络策略暂时阻止，或者设备可能无法访问。请**验证网络连接**并确保 **SSH 端口可访问**。

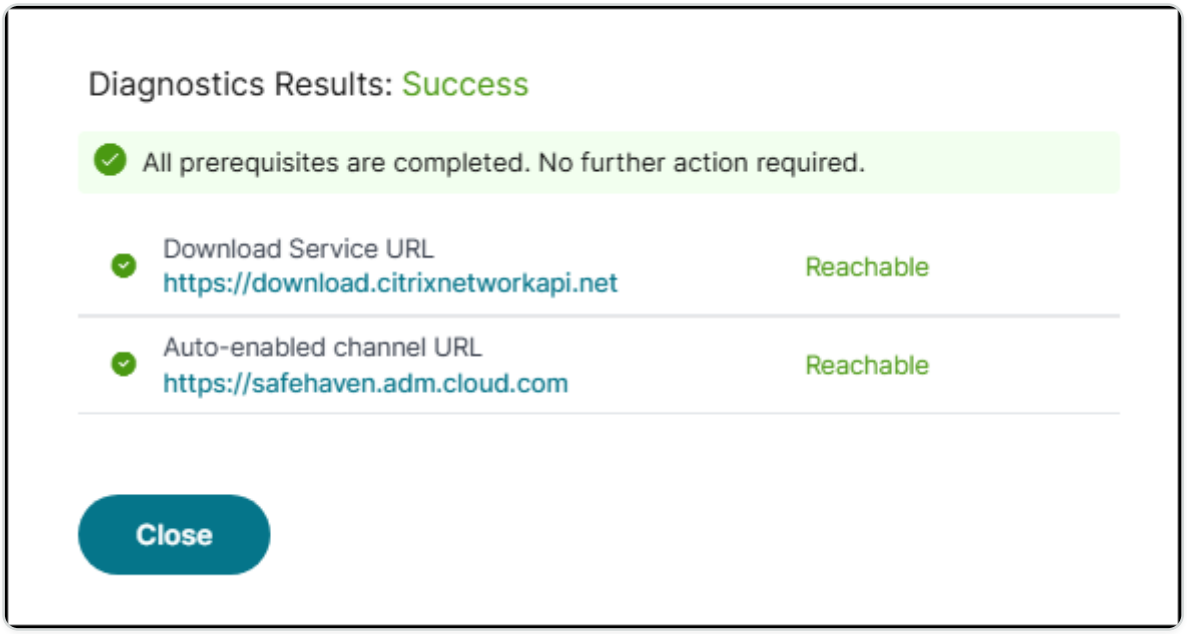
14.1 build 56.x 版本之前的诊断行为

在 14.1 build 51.x 及更早版本中，诊断功能有助于检查到这些端点 URL 的出站连接，并告知您它们是否处于可访问状态。

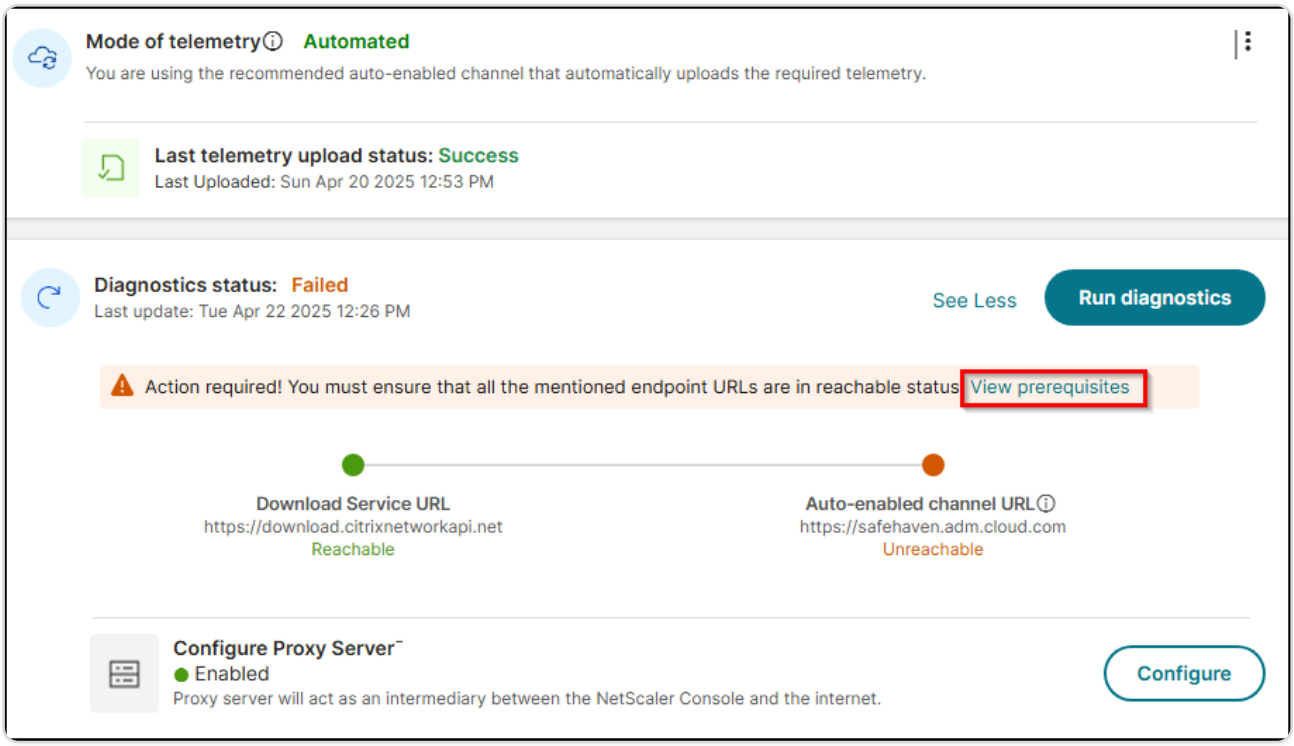


在您看到端点 URL 处于可访问状态后，单击“**转到 NetScaler® Telemetry**”页面。

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

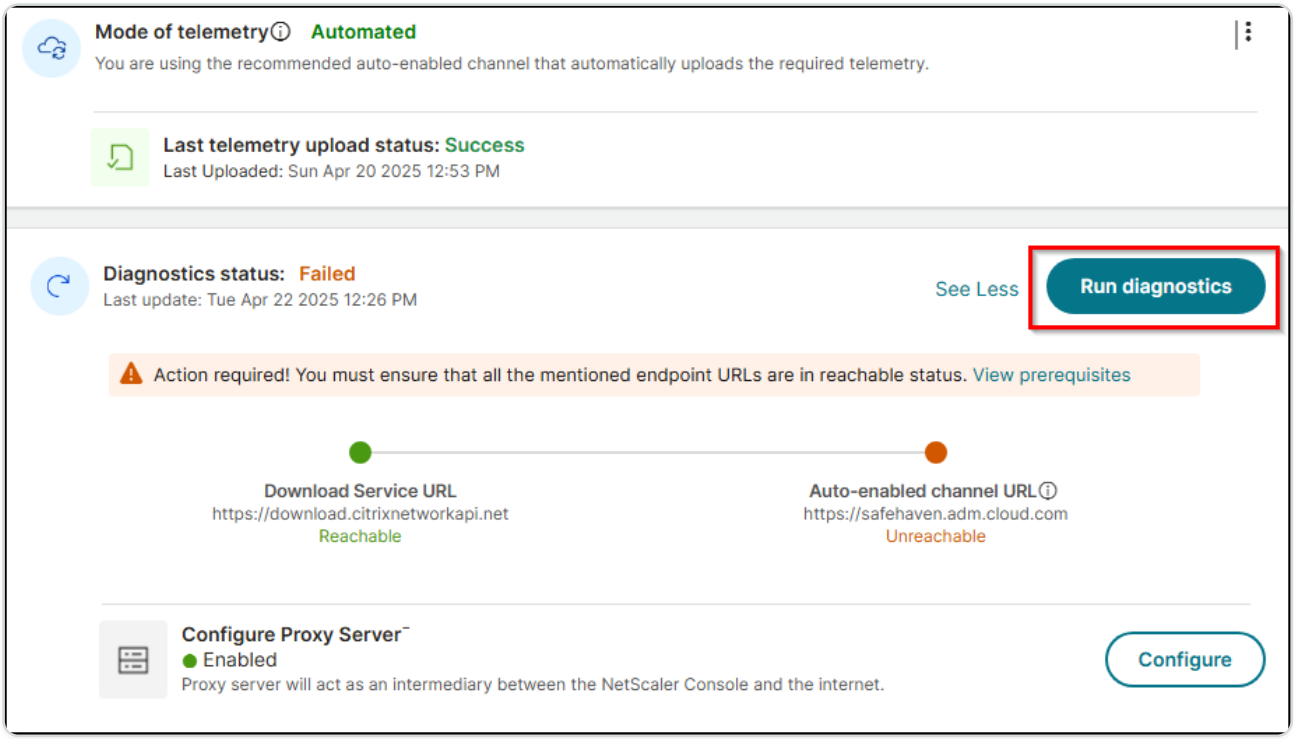


如果任何先决条件失败，诊断检查会显示不可访问的端点，您必须确保 URL 可访问。单击“**查看先决条件**”以查看详细信息。



您可以通过点击**运行诊断**来运行诊断，以确认端点 URL 是否可达。

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

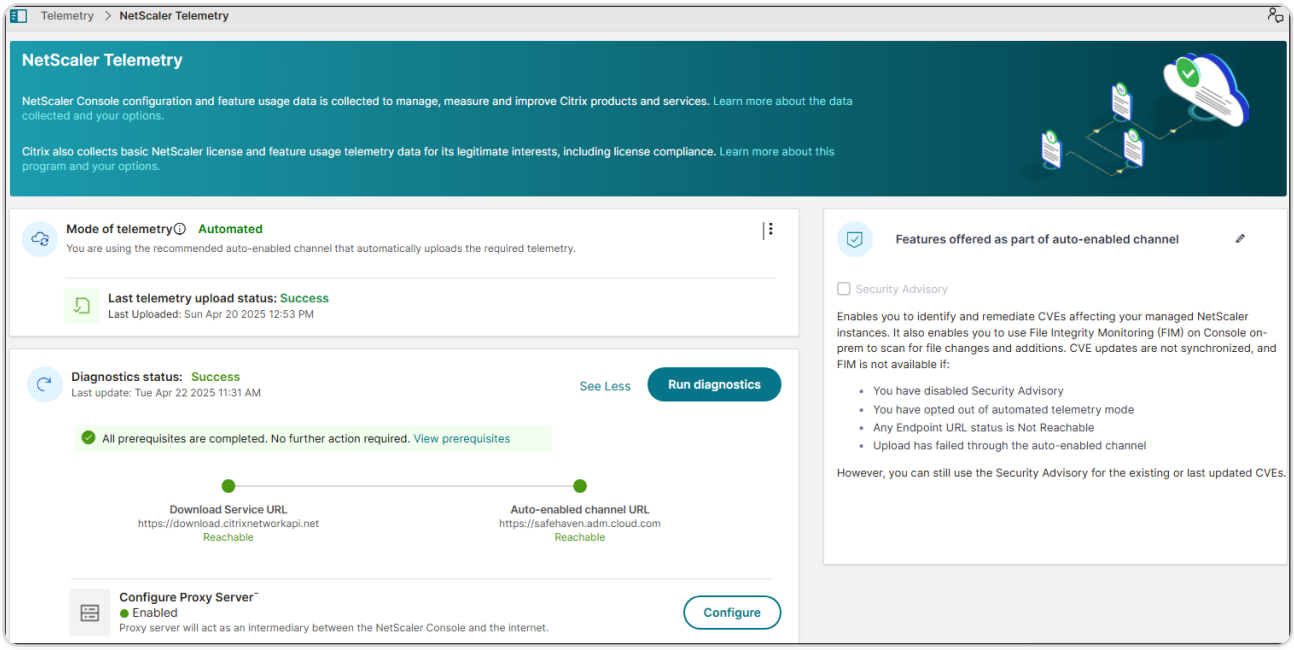


如果不采取任何措施，您的本地 NetScaler Console 可能不符合 NetScaler 遥测计划的要求。

作为自动启用通道的一部分，您可以在本地 NetScaler Console 中使用具有最新 CVE 更新的**安全建议**功能。安全建议功能使您能够识别使 NetScaler 实例面临风险的 CVE，并推荐补救措施。您可以在安全建议中查看影响 NetScaler 实例的最新 CVE 详细信息。有关更多信息，请参阅安全建议。

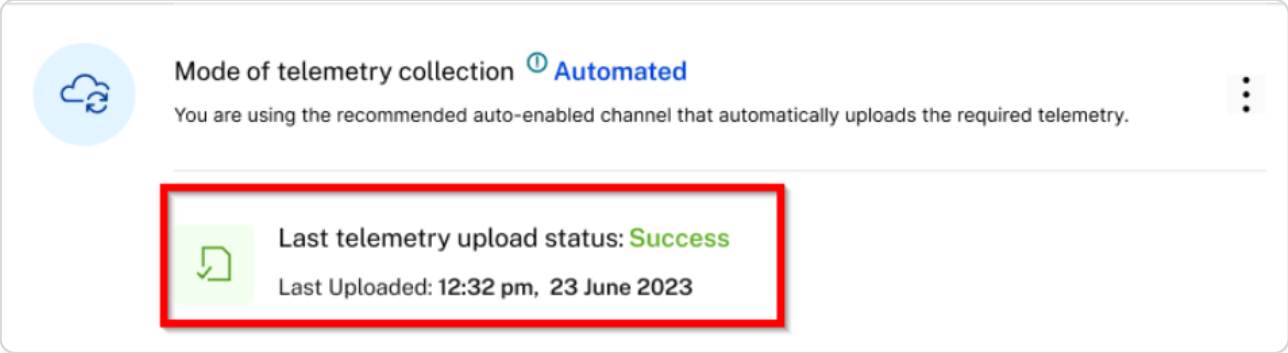
注意：

您也可以禁用安全建议。如果您禁用**安全建议**，或选择退出自动遥测模式，或任何先决条件失败，则新的 CVE 更新将不可用，您只能使用现有或上次更新的 CVE 的安全建议。



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

成功启用自动遥测收集后，首次上传将在 24 小时内进行。后续上传将每 24 小时自动进行。上传完成后，状态将变为**成功**。



如果上传失败，请确保端点 URL 可达。如果状态显示可达但上传仍然失败，请联系客户服务。

遥测上传通知

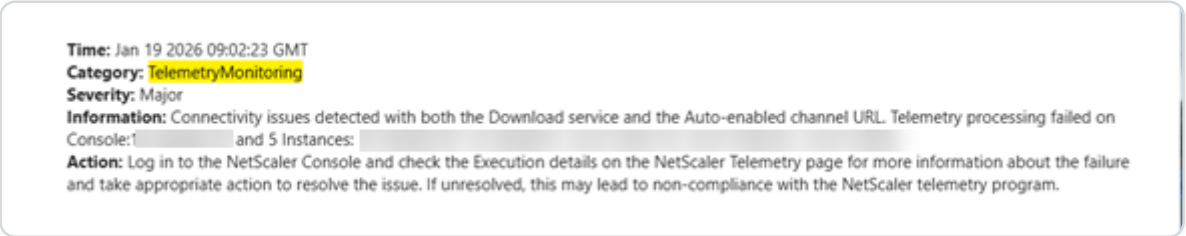
默认情况下，遥测上传的电子邮件通知处于启用状态。接收电子邮件通知的先决条件是配置电子邮件分发列表。有关更多信息，请参阅配置通知设置。作为管理员，您会收到以下情况的电子邮件通知：

- **遥测收集失败** - 电子邮件通知每 24 小时发送一次，直到问题解决。通知中包含受此问题影响的 NetScaler 和 Console IP 地址。
- **通过自动模式上传失败** - 电子邮件通知每 24 小时收到一次，直到问题解决。
- **手动上传的截止日期临近**（仅当启用手动模式时） - 事件发生时收到一封电子邮件通知，上传完成后收到另一封电子邮件。
- **超出手动上传截止日期**（仅在启用手动模式时）- 事件发生期间会收到一封电子邮件通知，上传完成后会收到另一封电子邮件。

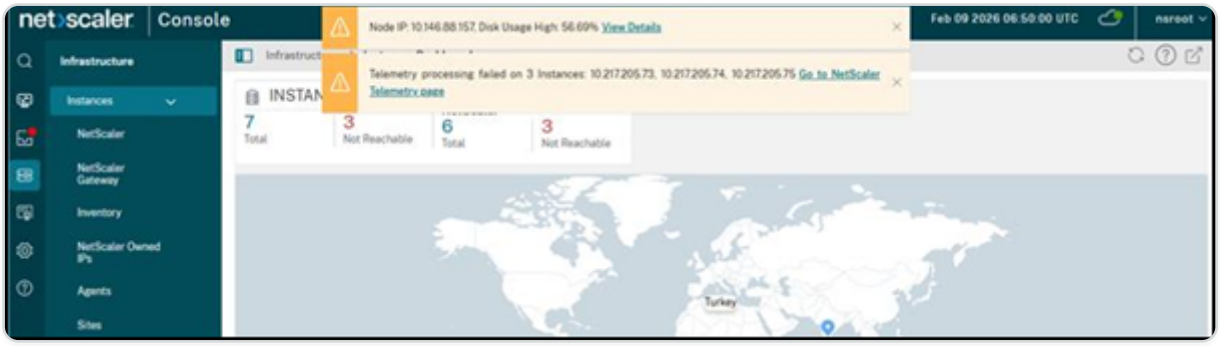
注意：

每当用户登录控制台用户界面时，NetScaler 设备上遥测数据收集问题的通知也会以横幅形式显示。

以下是 NetScaler 设备上遥测数据收集失败的电子邮件和横幅通知示例：

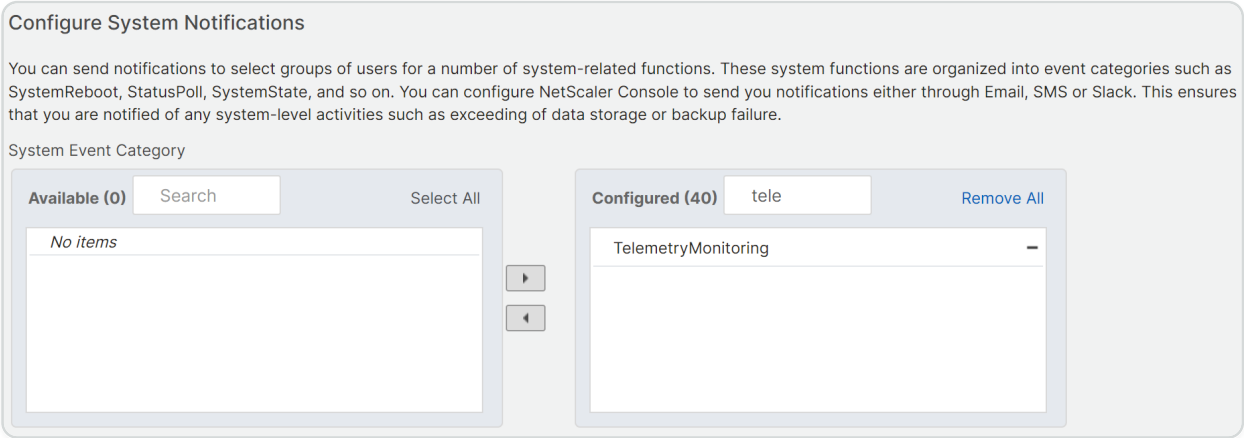


© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以禁用电子邮件通知。要禁用：

1. 导航到 **设置 > 管理 > 配置事件通知和摘要**。
2. 在 **事件通知 > 配置系统通知** 中，搜索 **TelemetryMonitoring**，删除此通知，然后单击 **保存**。



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

数据治理

所有现有的 NetScaler Console 客户都必须通过自动或手动模式上传所需的遥测数据，以遵守 NetScaler 遥测计划。NetScaler 遥测计划从 14.1-25.53 及更高版本 / 13.1-53.22 及更高版本开始启用。有关更多信息，请参阅NetScaler 遥测计划。

Citrix 收集基本的许可证遥测数据以及 NetScaler® 部署和功能使用遥测数据，以维护其合法权益，包括许可证合规性。NetScaler Console 配置和功能使用数据也用于管理、衡量和改进 Citrix 产品和服务。

自动遥测数据收集模式使您能够使用 NetScaler Console 本地部署中的**安全建议**功能，该功能收集可选的遥测参数。您可以禁用可选参数，但不能禁用必需参数。

注意：

- 在您升级到 NetScaler Console **14.1-25.53 或更高版本 / 13.1-53.22 或更高版本**后，以下配置将通过 NetScaler Console 自动推送到您的 NetScaler 实例。此配置会在您的 NetScaler 实例中收集并存储遥测指标：

```
enable ns feature AppFlow

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

- 如果您处于手动模式或自动模式（未满足任何先决条件），NetScaler Console 会每 24 小时继续检查上述配置，如果此配置缺失，则将其推送到 NetScaler 实例。如果您不希望推送此配置，则必须处于自动模式（并满足所有先决条件）或升级到即将发布的版本（**14.1-29.x** 或 **13.1-55.x**）。
- `/nsconfig/.telemetry.conf` 文件将使用以下命令进行更新，用于 Gateway 遥测。NetScaler Console 每小时检查此命令，如果缺失则添加此命令：

```
ns_telemetry_server,&lt;Console IP>,5140
```

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

- 某些遥测参数通过从 NetScaler Console 推送到 NetScaler 实例的脚本收集。这些脚本是只读的，不会更改 NetScaler 中的任何内容。
- 通过遥测收集的信息（例如电子邮件地址、用户名和 IP 地址）通过使用单向哈希算法在源头对信息进行哈希处理，从而安全地进行假名化。因此，Citrix 无法访问或读取这些值。此遥测数据仅用于逻辑资产匹配目的。

下表提供了作为 NetScaler 遥测计划一部分收集的参数详细信息：

类别	描述	我们用它做什么？	必需/可选
许可证，以及 NetScaler 部署和使用遥测数据	有关许可证权利、分配、使用、高级 NetScaler 部署数据以及 NetScaler 功能使用情况的信息。	许可证合规性以及管理、衡量和改进服务。	必需
NetScaler Console 部署和功能使用遥测数据	有关 Console 部署和功能使用情况的信息。	用于管理、衡量和改进服务。	可选

要禁用可选参数：

1. 在本地 NetScaler Console 中，导航到 **NetScaler Telemetry** 并禁用 **Security Advisory**。
2. 导航到 **设置 > 管理 > 启用或禁用控制台功能数据共享**，然后清除 **我同意共享控制台功能使用数据** 复选框。

如果您的 NetScaler Console 版本介于 14.1-8.x 和 14.1-21.x 之间，则在您配置 Cloud Connect 并启用安全建议功能后，数据收集将启用。有关更多信息，请参阅 Cloud Connect 的数据治理

如果您的 NetScaler Console 版本为 14.1-4.x 或更低，您可以在 Citrix Cloud 上创建客户身份，以将有关 NetScaler Console 运行状况、状态和其他指标的重要统计信息从本地 NetScaler Console 部署发送到 Citrix Cloud 帐户。Citrix 收集统计信息以了解 NetScaler Console 的使用情况。有关更多信息，请参阅 客户身份的数据治理。

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

IoC 信息使用条件

使用 IoC 信息（定义见下文），即表示您承认并同意以下使用条件：

Citrix Systems, Inc. 和/或其关联公司（以下简称“Citrix”）已开发妥协指标逻辑脚本以及有关妥协指标的相关指南（统称为“IoC 信息”），以帮助组织确定其环境是否可能受到入侵。

IoC 信息不涵盖威胁行为者在攻击相关环境时可能使用的所有技术、策略或程序（“TTP”）。此外，威胁行为者会频繁更改 TTP 和基础设施。由于这些原因及其他原因，IoC 信息可能具有有限的取证价值，并且可能无法识别实际入侵。强烈建议您聘请经验丰富的取证调查员来评估您的环境。

IoC 信息按“原样”提供。Citrix 不对 IoC 信息作任何明示或暗示的保证或陈述，包括但不限于 IoC 信息无错误或符合任何适销性或特定用途适用性条件。

IoC 信息是 Citrix 的机密和专有信息，并受这些材料接收方与 Citrix 之间适用的保密协议条款和条件的约束。未经 Citrix 事先明确书面许可，不得以任何形式或任何方式复制、再分发或传输 IoC 信息的任何部分给任何第三方。

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

NetScaler Console 许可

许可

当实例通过 `https` 协议发现时，NetScaler Console 需要经过验证的 NetScaler 许可证来管理和监控 NetScaler 实例。

NetScaler Console 支持以下许可证版本。请联系您的 NetScaler 销售代表或合作伙伴购买 NetScaler Console 许可证。

Express 版 – 您可以使用 Express 版许可证管理和监控任意数量的实例。默认情况下，将应用 Express 版许可证。

高级版 - 它允许管理发现的应用程序，并查看已购买的虚拟服务器以及免费虚拟服务器的分析数据。

注意事项：

- 对于版本 **13.1-9.x 或更早版本**，您可以管理多达 30 个已发现的应用程序或虚拟服务器并查看分析数据。超出 30 个已发现的应用程序或 30 个虚拟服务器后，您必须购买并应用高级许可证。例如，如果您购买 100 个虚拟服务器许可证，则您有权使用多达 130 个虚拟服务器许可证。
- 对于版本 **13.1-12.x 或更高版本**，您可以管理多达两个已发现的应用程序或虚拟服务器并查看分析数据。超出两个已发现的应用程序或两个虚拟服务器后，您必须购买并应用高级许可证。例如，如果您购买 100 个虚拟服务器许可证，则您有权使用多达 102 个虚拟服务器许可证。

升级到 13.1-12.x 至 14.1-17.x 版本后：

- 所有 Express 默认免费虚拟服务器在 30 天内保持功能正常。您可以在 30 天内选择两个虚拟服务器并应用两个默认许可证。如果在升级后 30 天内未采取任何用户操作，NetScaler Console 将随机向两个虚拟服务器应用许可证，并取消其余虚拟服务器的许可证。您必须购买并应用新的高级许可证才能启用这些虚拟服务器。
- 升级后，NetScaler Console 的行为发生以下变化：
  - NetScaler Console 额外提供 30 天时间来执行所需操作。
  - 在 30 天内，将阻止为 30 个 Express 免费虚拟服务器分配新的虚拟服务器。

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

- 例如，如果您在升级到 12.x 之前可用的虚拟服务器许可证数量为 30 个，并且只使用了 20 个已许可的虚拟服务器，则您只能使用这 20 个虚拟服务器，并且在 30 天内不允许许可剩余的 10 个虚拟服务器。

- 但是，在 30 天内，作为管理员，您仍然可以应用高级 NetScaler Console 许可证并分配新的虚拟服务器。

下表提供了许可详细信息：

功能	选项	EXPRESS 版本	ADVANCE 版本	NETSCALER 许可证
应用程序	应用程序仪表板	最多两个虚拟服务器。	有权使用所有已购买的虚拟服务器许可证和额外的两个虚拟服务器。	应用程序仪表板上与 NetScaler Web App Firewall 相关的信息需要 Premium（或）Advanced with App Firewall 许可证。
	网络洞察	最多两个虚拟服务器。	有权使用所有已购买的虚拟服务器许可证和额外的两个虚拟服务器。	不适用
	服务图	最多两个虚拟服务器。	适用于所有已购买的虚拟服务器许可证和额外的两个虚拟服务器。	不适用
	配置 > StyleBooks	无限制	无限制	不适用
安全	安全仪表板	最多两个虚拟服务器。	适用于所有已购买的虚拟服务器许可证和额外的两个虚拟服务器。	安全仪表板上与 NetScaler Web App Firewall 相关的信息需要 Premium（或）Advanced with

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

功能	选项	EXPRESS 版本	ADVANCE 版本	NETSCALER 许可证
				App Firewall 许可证。
	安全违规	最多两个虚拟服务器。	有权获得所有已购买的虚拟服务器许可证以及额外的两个虚拟服务器。	高级版（或）带应用程序防火墙许可证的增强版
	用户和端点	最多两个虚拟服务器。	有权获得所有已购买的虚拟服务器许可证以及额外的两个虚拟服务器。	不适用
网关	HDX 洞察	最多两个虚拟服务器。	有权获得所有已购买的虚拟服务器许可证以及额外的两个虚拟服务器。	增强版（报告 < 1 小时）高级版（报告 = 无限制）
	网关洞察	最多两个虚拟服务器。	有权获得所有已购买的虚拟服务器许可证以及额外的两个虚拟服务器。	增强版（报告 < 1 小时）高级版（报告 = 无限制）
基础架构	基础架构分析	无限制	无限制	不适用
	实例	无限制	无限制	不适用
	SSL 控制板	无限制	无限制	不适用
	事件	无限制	无限制	不适用
	网络功能	无限制	无限制	不适用
	网络报告	无限制	无限制	不适用
	池化许可证	无限制	无限制	不适用

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

功能	选项	EXPRESS 版本	ADVANCE 版本	NETSCALER 许可证
	配置 > 配置作业、配置模板和配置建议	无限制	无限制	不适用
	升级作业	无限制	无限制	不适用
	编排	无限制	无限制	不适用
设置	RBAC 和外部身份验证（实例级别）	无限制	无限制	不适用
	RBAC 和外部身份验证	无限制	无限制	不适用

*对于 Citrix Director 与 NetScaler Console 的集成支持 – Citrix Director 必须拥有高级许可证。

更多虚拟服务器的许可证以 10 个虚拟服务器包的形式提供。您可以通过 NetScaler Console GUI 获取有效许可证并将其添加到 NetScaler Console 服务器上。

高可用性

NetScaler Console 服务器可以包含 VIP、CICO 和池容量许可证。当许可证颁发给 NetScaler Console 服务器时，许可证将绑定到服务器的主机 ID。限制将许可证分配给不同的 NetScaler Console 服务器。

如果您将 NetScaler Console 高可用性对配置为许可证服务器，则主服务器和辅助服务器必须具有相同的许可证文件。因此，在 NetScaler Console 高可用性部署中，NetScaler Console 支持将相同的许可证文件分配给两台服务器。

注意

- 如果您安装了 NetScaler Console 12.1-49.x 或更早版本，您有 30 天的时间来维护辅助节点上的许可。30 天后，您必须联系 Citrix 重新托管原始许可证。
- 在 12.1-50.x 及更高版本中，NetScaler Console 许可证会自动同步到辅助节点。
- 在 12.1-50.x 及更高版本中，池许可证会自动同步到辅助节点。

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

NetScaler Console 高可用性节点之间如何同步许可证?

当发生故障转移时，辅助服务器将承担主服务器的角色。主服务器的真实主机 ID 被配置为新主服务器的虚拟主机 ID。许可证文件使用虚拟主机 ID 识别新的主服务器。

- **真实主机 ID** - 此 ID 是从 NetScaler Console 服务器的 MAC 地址生成的。每个 NetScaler Console 独立部署都有一个唯一的主机 ID。
- **虚拟主机 ID** - 此 ID 在 HA 部署期间自动生成。NetScaler Console 主服务器的真实主机 ID 用作辅助服务器的虚拟主机 ID。此 ID 以加密格式存储在 NetScaler Console 数据库中，并且限制对该 ID 的任何修改。虚拟主机 ID 优先于真实主机 ID。

NetScaler Console 高可用性节点之间同步的许可证(/en-us/netscaler-application-delivery-management-software/media/license-ha-support-console.png)

假设 Node-1 是主服务器，Node-2 是辅助服务器。Node-1 的虚拟主机 ID 与 Node-2 同步。

1. Node-1 中可用的许可证文件同步到 Node-2。
2. Node-1 上的任何新许可证文件会定期同步到 Node-2。
3. NetScaler Console 确保许可证服务器仅在 Node-1 上运行，以避免许可证容量翻倍。
4. NetScaler 实例使用浮动 IP 地址从 Node-1 签出许可证。

许可证锁定到 NetScaler 实例。要从 NetScaler Console HA 签出许可证，实例需要特定的 NetScalerNetScaler IP 地址。当您在负责许可的主服务器上应用许可证时，它将应用于该实例上的所有未来许可证。您只能从安装了许可证的服务器中删除许可证。

编排

编排模块独立于许可，并且始终可用。

升级虚拟服务器许可证

您可以升级 NetScaler Console 上的许可，以监控和管理 NetScaler 上托管的更多虚拟服务器。

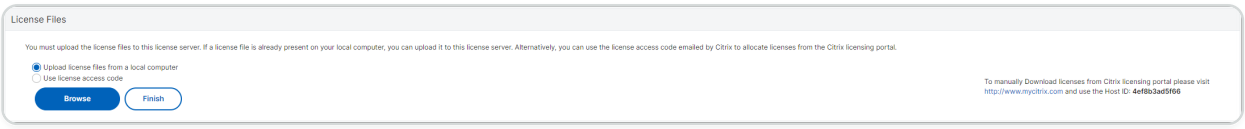
要升级您的 NetScaler 许可证：

1. 使用管理员凭据登录到 NetScaler Console。
2. 导航到 **基础架构 > 池化许可**。
3. 转到 **License Files**，然后选择以下选项之一：
    - **从本地计算机上传许可证文件**。如果您的本地计算机上已存在许可证，请单击 **Browse** 并选择要用于分配许可证的许可证文件 (.lic)。单击 **Finish**。

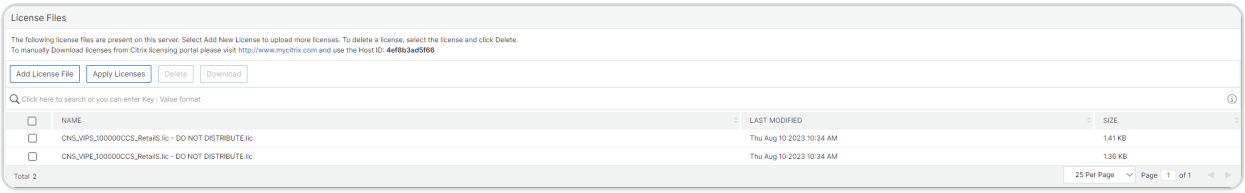
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **使用许可证激活码**。Citrix 会通过电子邮件发送您购买的许可证的许可证访问码。在文本框中输入许可证访问码，然后单击 **Get Licenses**。

> **注意**
>
> 如果您选择此选项，NetScaler Console 必须连接到 Internet，或者必须有可用的代理服务器。



4. 您可以随时从“许可证设置”页面添加更多许可证。



验证

您可以通过导航到 **Settings > Licensing & Analytics Configuration** 来验证 NetScaler Console 上安装的许可证。

管理虚拟服务器

您可以选择要通过 NetScaler Console 管理和监视的虚拟服务器或第三方虚拟服务器。

> **注意事项**
>
> - 默认情况下，NetScaler Console 在每个虚拟服务器轮询周期后随机自动授权虚拟服务器。
> - 如果您的 NetScaler Console 中发现的虚拟服务器总数低于已安装的虚拟服务器许可证数量，则 NetScaler Console 默认授权所有虚拟服务器。

要手动选择虚拟服务器，或将授权限制为有限的虚拟服务器，您必须首先禁用虚拟服务器的自动授权，然后选择要管理的虚拟服务器。

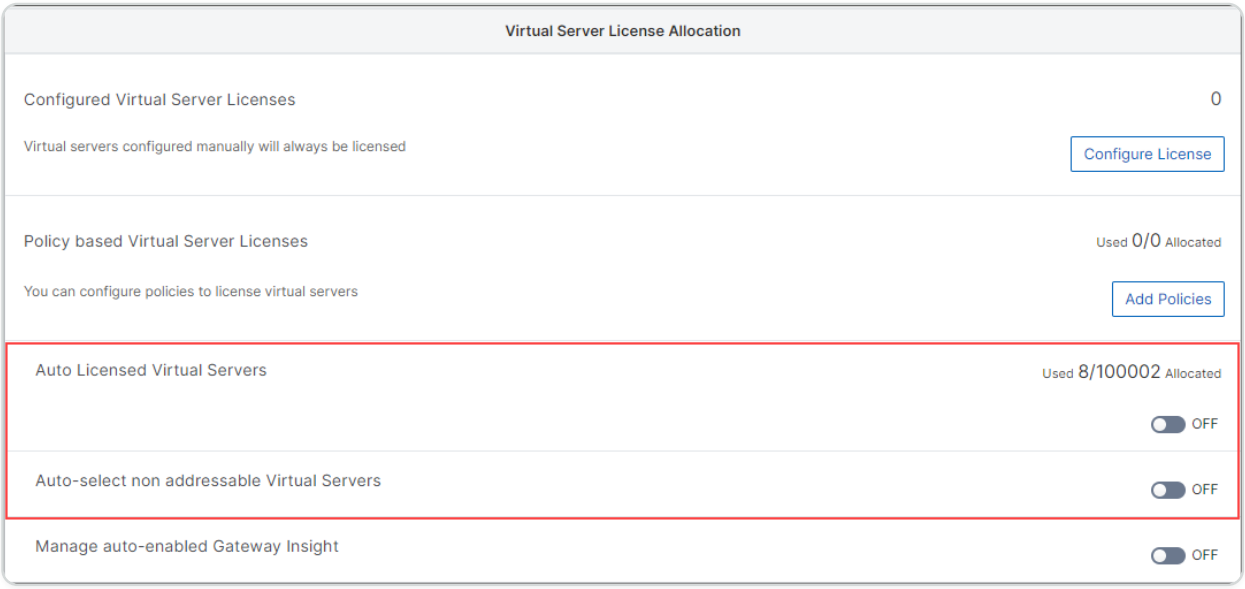
© 1997–2026 Citrix Systems, Inc. All rights reserved.

禁用虚拟服务器的自动授权

1. 导航到 **设置 > 许可与分析配置**。

   控制板显示可用的虚拟服务器许可证、托管的虚拟服务器及其类型以及许可证到期信息。

2. 在 **虚拟服务器许可证分配** 中，禁用 **自动许可的虚拟服务器** 和 **自动选择不可寻址的虚拟服务器**。

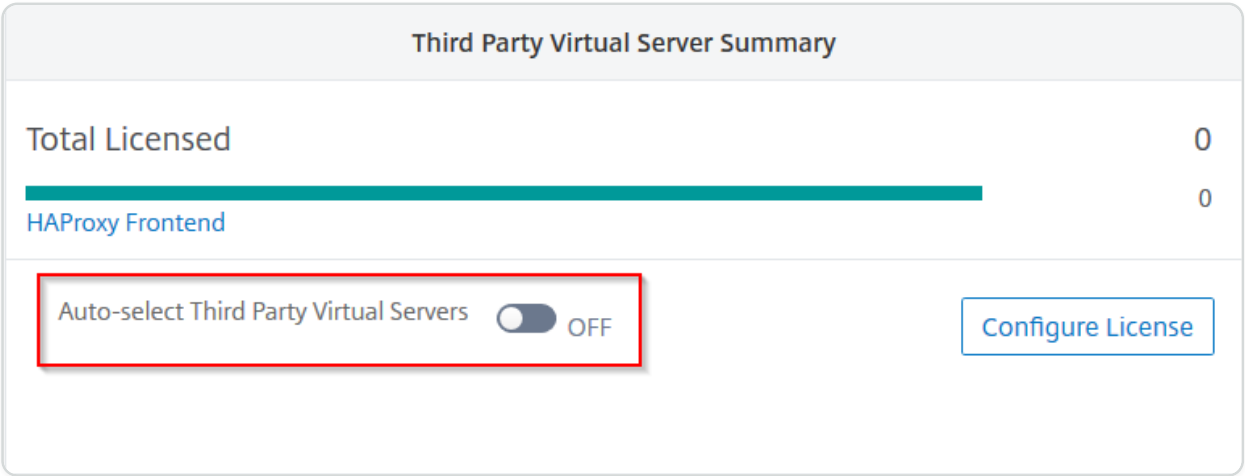


选择第三方虚拟服务器进行授权

1. 导航到 **设置 > 许可与分析配置**。

   控制板显示可用的虚拟服务器许可证、托管的虚拟服务器及其类型以及许可证到期信息。

2. 在 **第三方虚拟服务器摘要** 中，禁用 **自动选择第三方虚拟服务器**。



手动应用虚拟服务器许可证

您可以手动将许可证应用于单个虚拟服务器。

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

1. 在 **虚拟服务器许可证分配** 中，选择 **配置许可证**。

   将显示 **所有虚拟服务器** 页面。

2. 使用属性 `Licensed: No` 筛选未获得许可的虚拟服务器。
3. 选择要获得许可的虚拟服务器。
4. 单击 **许可证**。

配置基于策略的虚拟服务器许可

您可以配置策略以将许可证应用于虚拟服务器。此策略控制要自动许可的虚拟服务器数量。它还仅将许可证应用于所选实例的虚拟服务器。

单击 **编辑策略**，您可以指定以下内容：

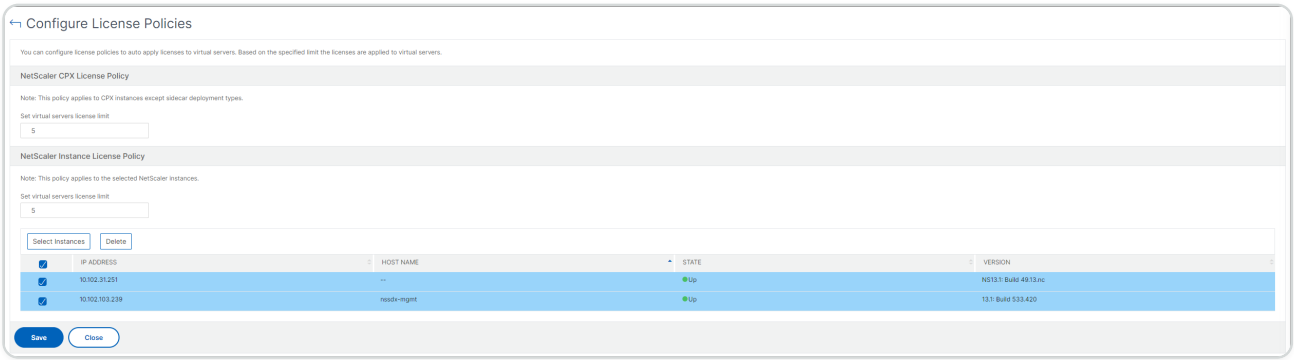
- 单独设置 CPX 实例上的虚拟服务器限制以应用许可证。NetScaler Console 将许可证应用于 CPX 实例上的虚拟服务器，直至达到指定限制。

  重要

  此限制适用于 CPX 实例，但 sidecar 部署类型除外。

  要查看 sidecar 部署类型的 CPX 实例，请使用属性 `License Type: Freely Managed` 筛选虚拟服务器。

- 在选定的 NetScaler 实例 (MPX/VPX/BLX) 上设置虚拟服务器限制以应用许可证。NetScaler Console 将许可证应用于 NetScaler 实例上的虚拟服务器，直至达到指定限制。
- 选择优先级 NetScaler 实例以应用虚拟服务器许可证。因此，NetScaler Console 只能将许可证应用于所选实例的虚拟服务器。



查看已获得许可的虚拟服务器

将许可证应用于虚拟服务器后，您可以查看已获得许可的虚拟服务器或第三方虚拟服务器。

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

1. 导航到 **设置 > 许可和分析配置**。
2. 在 **虚拟服务器许可证摘要** 中的 **总许可** 部分中单击虚拟服务器类型。

为不可寻址的虚拟服务器配置自动许可证支持

NetScaler Console 默认情况下不会自动将许可证应用于不可寻址的虚拟服务器。要许可不可寻址的虚拟服务器，您必须禁用自动许可选项并手动选择不可寻址的虚拟服务器。这会增加您在最初应用许可证时手动选择不可寻址服务器的工作量。此外，每当新的不可寻址虚拟服务器添加到您的网络时，您还需要手动选择它们。

NetScaler Console 在 **虚拟服务器许可证分配** 下提供了一个选项。如果您启用 **自动选择不可寻址虚拟服务器** 选项，许可证将自动应用于不可寻址的虚拟服务器。

注意

- NetScaler Console 默认情况下仍然不会自动选择不可寻址的虚拟服务器进行许可。
- 应用程序分析（应用程序仪表板）是目前唯一在已获得许可的不可寻址虚拟服务器上支持的分析功能。

许可

从 **14.1-21.x** 版本开始，已移除许可 VIP 的概念。NetScaler Console 本地部署版现在提供无限数量的 VIP。您不再需要购买 NetScaler Console 虚拟服务器许可证，因为 VIP 许可证 SKU 即将停止销售 (EOS) 和停止续订 (EOR)。

下表提供了许可详细信息：

功能	选项	NETSCALER 许可证
应用程序	应用程序仪表板	应用程序仪表板上的 NetScaler Web App Firewall 相关信息需要 Premium（或）Advanced 许可证以及 App Firewall 许可证。
	Web 洞察	不适用
	服务图	不适用

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

功能	选项	NETSCALER 许可证
	配置 > StyleBooks	不适用
安全	安全仪表板	安全仪表板上与 NetScaler Web App Firewall 相关的信息需要 Premium（或）Advanced with App Firewall 许可证。
	安全违规	尊享版（或）带 App Firewall 许可证的高级版
	用户和端点	不适用
网关	HDX 洞察	Advanced（报告 < 1 小时） Premium（报告 = 无限制）
	网关洞察	Advanced（报告 < 1 小时） Premium（报告 = 无限制）
基础架构	基础架构分析	不适用
	实例	不适用
	SSL 仪表板	不适用
	事件	不适用
	网络功能	不适用
	网络报告	不适用
	池化许可证	不适用
	配置 > 配置作业、配置模板和配置建议	不适用
	升级作业	不适用
	编排	不适用
设置	RBAC 和外部身份验证（实例级别）	不适用

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

功能	选项	NETSCALER 许可证
	RBAC 和外部身份验证	不适用

*对于 Citrix Director 与 NetScaler Console 集成支持 – Citrix Director 必须拥有高级许可证。

高可用性

NetScaler Console 服务器可以包含 VIP、CICO 和池化容量许可证。当许可证颁发给 NetScaler Console 服务器时，许可证将绑定到服务器的主机 ID。限制将许可证分配给不同的 NetScaler Console 服务器。

如果您将 NetScaler Console 高可用性对配置为许可证服务器，则应用于主服务器的许可证文件将同步到辅助服务器。

注意：

- 在 12.1-50.x 及更高版本中，NetScaler Console 许可证会自动从主节点同步到辅助节点。

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

系统要求

在安装 NetScaler Console 之前，您必须了解软件要求、浏览器要求、端口信息、许可证信息和限制。

NetScaler Console 的要求

组件	要求
内存	32 GB
虚拟 CPU	8 个 CPU
	注意： 我们建议在 NetScaler Console 部署中使用固态硬盘 (SSD) 技术。
存储空间	所需的默认存储空间为 120 GB。实际存储要求取决于 NetScaler Console 的大小估算。
	如果您的 NetScaler Console 存储要求超过 120 GB，则必须连接一个额外的磁盘。您只能添加一个额外的磁盘。
	我们建议您在初始部署时估算存储并连接额外的磁盘。
	有关更多信息，请参阅 如何将额外磁盘连接到 NetScaler Console。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps 的速率

NetScaler Console 本地代理的要求

组件	要求
RAM	32 GB

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

组件	要求
虚拟 CPU	8 个 CPU
存储空间	30 GB
虚拟网络接口	1
吞吐量	1 吉比特每秒

注意

AMD 处理器支持：

- **NetScaler Console 13.1 内部版本 4.43 或更高版本。**
- **NetScaler agent 13.1 内部版本 17.42 或更高版本。**

NetScaler Console 功能所需的最低 NetScaler 版本

重要

NetScaler Console 的版本和内部版本必须**等于或高于**您的 NetScaler 版本和内部版本。例如，如果您已安装 NetScaler Console 12.1 内部版本 50.39，则请确保您已安装 NetScaler 12.1 内部版本 50.28/50.31 或更早版本。

NETSCALER CONSOLE 功能	NETSCALER 软件版本
StyleBooks	10.5 及更高版本
OpenStack/CloudStack 支持	11.0 及更高版本（如果需要分区）
	11.1 及更高版本，如果需要共享虚拟 LAN 上的分区
NSX 支持	11.1 Build 47.14 及更高版本 (VPX)
Mesos/Marathon 支持	10.5 及更高版本
备份/还原	对于 NetScaler，10.1 及更高版本

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

NETSCALER CONSOLE 功能	NETSCALER 软件版本
	对于 NetScaler SDX，11.0 及更高版本
使用作业进行监视/报告和配置	10.1 及更高版本
分析功能	
网络洞察	10.5 及更高版本
HDX 洞察	10.1 及更高版本
WAF 安全违规	11.0.65.31 及更高版本
网关洞察	11.0.65.31 及更高版本
缓存洞察	10.5 及更高版本*
SSL 洞察	12.0 及更高版本

* NetScaler Console 不支持运行版本 11.0 build 66.x 的 NetScaler 实例的集成缓存指标。

NetScaler Console 分析的要求

NetScaler Console 功能所需的最低 Citrix Virtual Apps and Desktops 版本

NETSCALER CONSOLE 功能	CITRIX 虚拟应用和桌面 版本
HDX 洞察	Citrix Virtual Apps and Desktops 7.0 及更高版本

注意

NetScaler Gateway 功能（在 9.3 和 10.x 版本中品牌为 Access Gateway Enterprise）必须在 NetScaler 实例上可用。NetScaler Console 不支持独立的 Access Gateway Standard 设备。

NetScaler Console 可以为发布在 Citrix Virtual Apps 或 Citrix Virtual Desktops 上并通过 Citrix Workspace 访问的应用程序生成报告。但是，此功能取决于安装 Workspace 的操作系统。目前，

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

NetScaler 不会解析通过在 iOS 或 Android 操作系统上运行的 Citrix Workspace 访问的应用程序或桌面的 ICA 流量。

HDX™ Insight 支持的瘦客户端

- 戴尔 Wyse 基于 Windows 的瘦客户端
- 戴尔 Wyse 基于 Linux 的瘦客户端
- 戴尔 Wyse 基于 ThinOS 的瘦客户端
- 10ZiG 基于 Ubuntu 的瘦客户端
- IGEL UD3 W7+ (M340)
- IGEL UD3 W7 (M340C)

HDX Insight 所需的 NetScaler 实例许可证

NetScaler Console 为 HDX Insight 收集的数据取决于所监控 NetScaler 实例的版本和许可证。HDX Insight 报告仅显示适用于运行 10.5 及更高版本的 NetScaler Premium 和 Advanced 设备。

NETSCALER 许可证/持续时间	5 分钟	1 小时	1 天	1 周	> 1 个月
标准版	否	否	否	否	否
高级版	是	是	否	否	否
高级版	是	是	是	是	是

支持的虚拟机管理程序

下表列出了 NetScaler Console 支持的虚拟机管理程序：

虚拟机管理程序	版本
XenServer	7.1、7.4 和 8.0
威睿 ESX	6.0、6.5、6.7、7.0、8.0（从 14.1-21.x 及更高版本开始）和 8.0.2b（从 14.1-25.x 及更高版本开始）
微软 Hyper-V	2012 R2、2016、2019 和 2022

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

虚拟机管理程序	版本
通用 KVM	RHEL 7.4、RHEL 8.0、Ubuntu 16.04 和 Ubuntu 18.04
Nutanix 虚拟机监控程序 (AHV)	6.5.2（从 14.1-38.x 及更高版本）

支持的操作系统和 Workspace 版本

下表列出了 NetScaler Console 支持的操作系统，以及每个系统当前支持的 Citrix Workspace 版本：

操作系统	WORKSPACE 版本
视窗	4.0 标准版
林纳克斯	13.0.265571 及更高版本
Mac	11.8, build 238301 及更高版本
HTML5	1.5
Chrome 应用	1.5

支持的浏览器

下表列出了 NetScaler Console 支持的 Web 浏览器：

WEB 浏览器	版本
微软 Edge	79 及更高版本
谷歌 Chrome	51 及更高版本
苹果 Safari	10 及更高版本
火狐浏览器	52 及更高版本

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

支持的端口

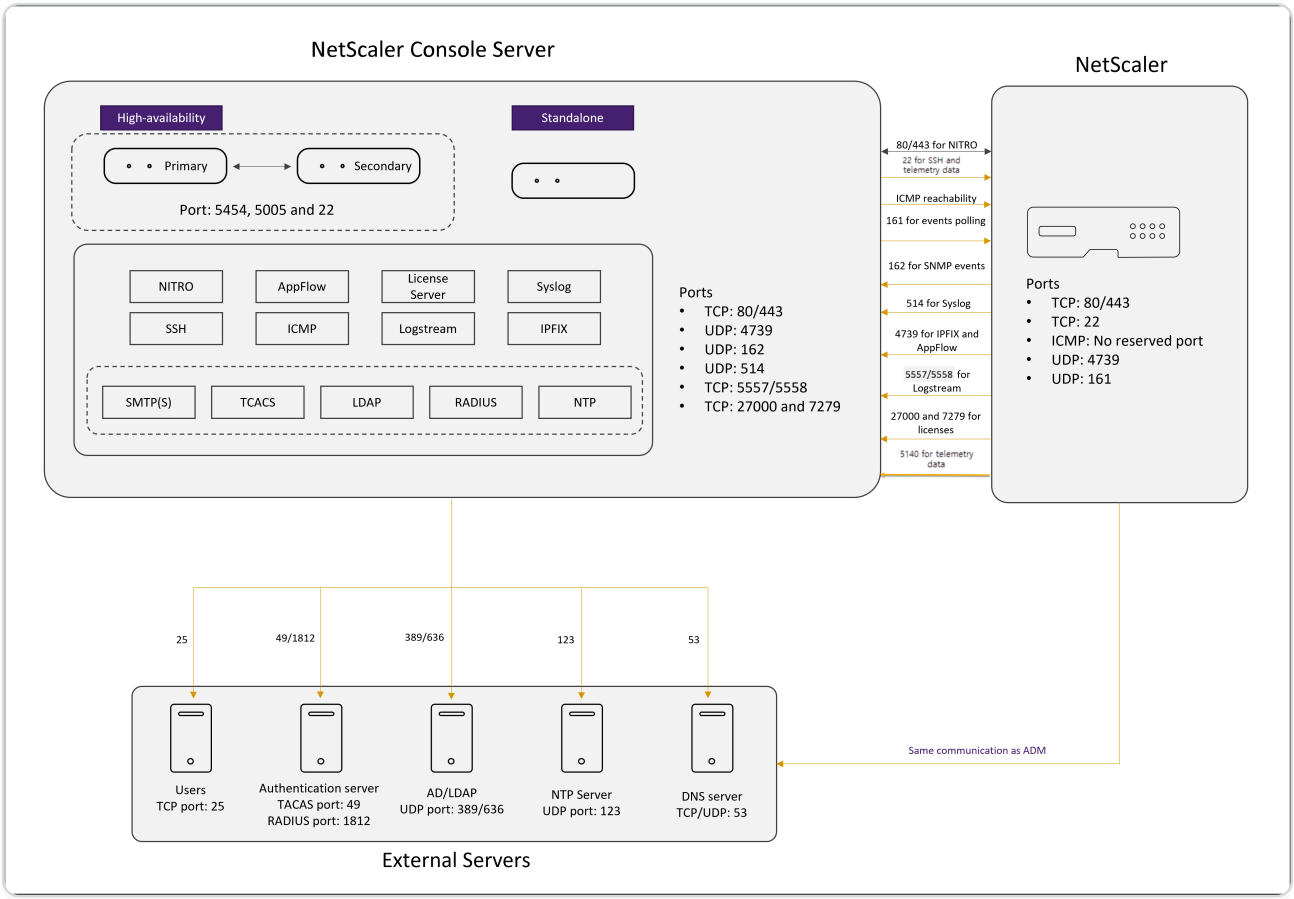
NetScaler Console 使用 NetScaler IP（称为 NSIP）地址与 NetScaler 通信。您可以使用代理作为 NetScaler 实例和 NetScaler Console 之间的中介。要与这些服务器建立通信，请打开所需的端口。

- 对于从 NetScaler 到 NetScaler Console 的 AppFlow 和日志流通信，使用子网 IP 地址（称为 SNIP）。
- 对于从 NetScaler 到 NetScaler Console 的许可证相关通信，使用 NSIP 地址。
- 如果 SNIP 地址已启用管理访问，并且 NetScaler 是通过 SNIP 地址添加到 NetScaler Console 中的，则 SNIP 地址将用作事件和系统日志的源 IP 地址。

注意

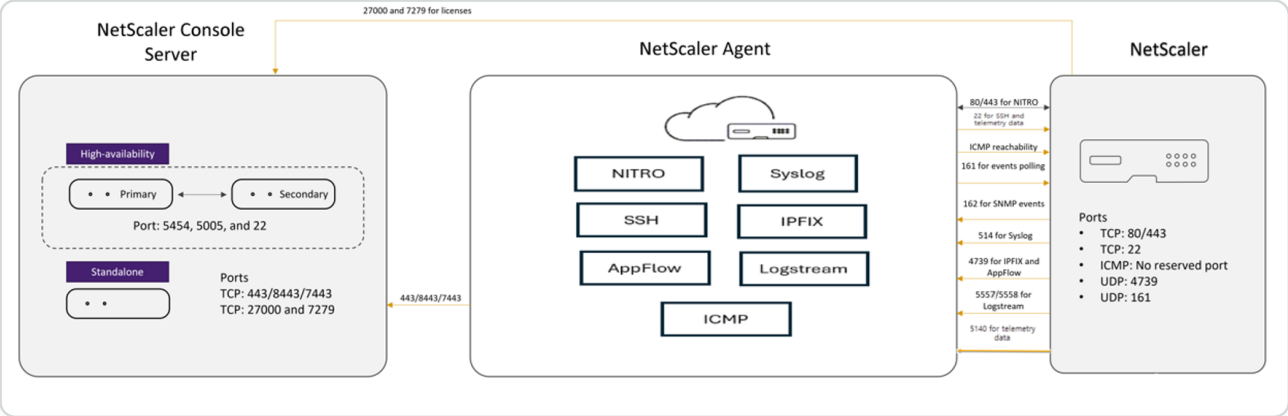
如果您已在高可用性模式下配置 NetScaler，NetScaler Console 将使用 NSIP 与 NetScaler 通信，并且所需的端口保持不变。

无代理部署的网络端口图：

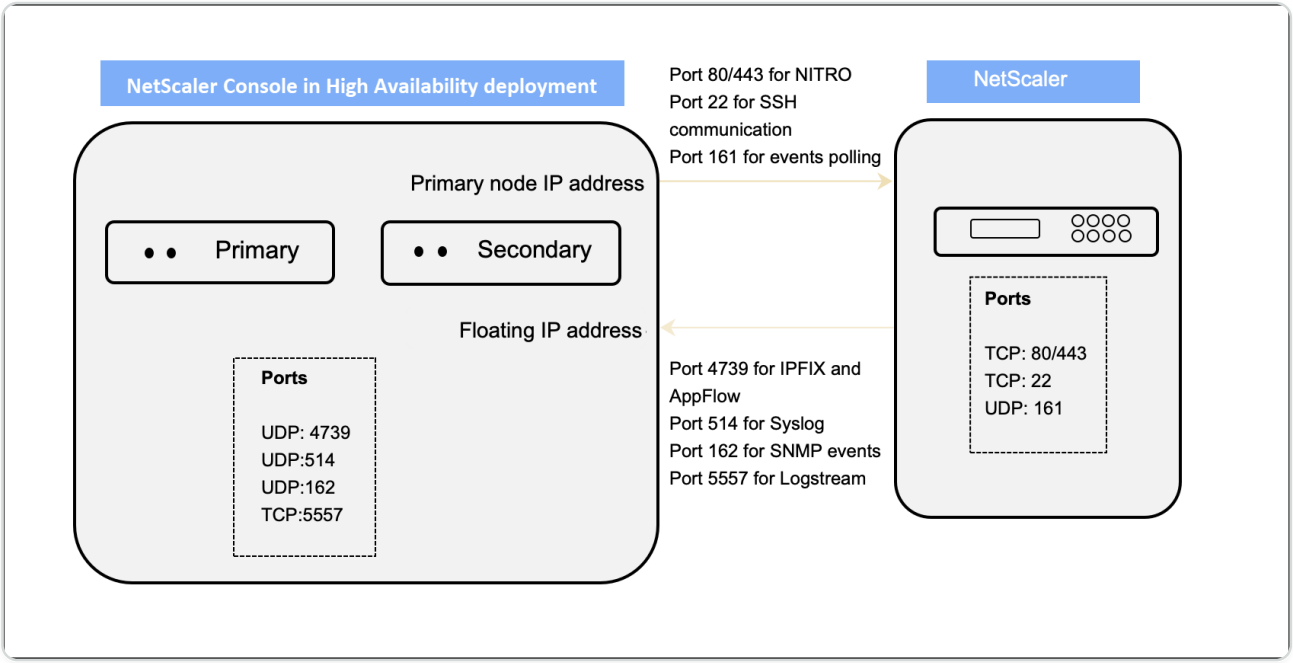


包含 NetScaler® 代理的部署的网络端口图：

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



NetScaler Console 高可用性部署的网络端口图：



如果在高可用性模式下设置了两个 NetScaler Console 服务器，则在添加实例时：

- NetScaler Console 通过主 IP 地址与 NetScaler 通信。
- NetScaler 通过 NetScaler Console 浮动 IP 地址与 NetScaler Console 建立连接。这意味着 NetScaler 将所有 SNMP、Syslog 和分析流量定向到 NetScaler Console 浮动 IP 地址。

以下部分说明了所需的端口及其用途：

- NetScaler Console 服务器
- NetScaler 代理
- NetScaler 实例
- 外部服务器

NetScaler Console 服务器的端口

下表说明了 NetScaler Console 服务器上必须打开的所需端口。

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

端口	类型	详细信息	通信方向
80/443/5454/22	TCP	高可用性模式下 NetScaler Console 节点之间通信和数据库同步的默认端口。**注意：**此端口也用于 NetScaler 遥测。	NetScaler Console 主节点到 NetScaler Console 辅助节点
443/8443/7443	TCP	NetScaler 代理与 NetScaler Console 之间通信的端口。	NetScaler 代理启动与 NetScaler Console 的通信。然后，NetScaler Console 和代理相互交互。
27000 和 7279	TCP	NetScaler Console 许可证服务器与 NetScaler 实例之间通信的许可证端口。这些端口也用于 NetScaler 池化许可证。	NetScaler 与 NetScaler Console 之间的通信
5005	UDP	HA 节点之间交换心跳的端口。	NetScaler Console 主节点到辅助节点。NetScaler Console 辅助节点到主节点。
5140	UDP	接收 NetScaler Gateway 遥测数据的端口。	网思乐 到 网思乐控制台

如果 NetScaler Console 和 NetScaler 实例不使用代理进行通信，请在 NetScaler Console 服务器上打开以下端口：

端口	类型	详细信息	通信方向
80/443	TCP	用于从 NetScaler Console 到 NetScaler 实例的 NITRO 通信。	NetScaler 代理到 NetScaler 以及 NetScaler 到 NetScaler 代理

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

端口	类型	详细信息	通信方向
4739	UDP	用于从 NetScaler 实例到 NetScaler Console 的 AppFlow 通信。	NetScaler 到 NetScaler 代理
162	UDP	用于从 NetScaler 实例接收 SNMP 事件到 NetScaler Console。	NetScaler 到 NetScaler 代理
514	UDP	用于从 NetScaler 实例接收 syslog 消息到 NetScaler Console。	NetScaler 到 NetScaler 代理
5557/5558	TCP	用于从 NetScaler 到 NetScaler Console 的日志流通信（适用于 WAF 安全违规、Web Insight 和 HDX Insight）。	NetScaler 与 NetScaler Console 之间的通信
5563	TCP	用于从 NetScaler 实例接收 NetScaler 指标（计数器）、系统事件和审计日志消息到 NetScaler Console	网思乐 到 网思乐 控制台

代理端口

下表说明了代理上必须打开的所需端口。

端口	类型	详细信息	通信方向
80/443	TCP	用于从 NetScaler Console 到 NetScaler 实例的 NITRO 通信。	NetScaler 代理到 NetScaler 以及 NetScaler 到 NetScaler 代理
4739	UDP	用于从 NetScaler 实例到 NetScaler	NetScaler 到 NetScaler 代理

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

端口	类型	详细信息	通信方向
		Console 的 AppFlow 通信。	
162	UDP	用于从 NetScaler 实例接收 SNMP 事件到 NetScaler Console。	NetScaler 到 NetScaler 代理
514	UDP	用于从 NetScaler 实例接收 syslog 消息到 NetScaler Console。	NetScaler 到 NetScaler 代理
5557/5558	TCP	用于从 NetScaler 到 NetScaler Console 的日志流通信（适用于 WAF 安全违规、Web Insight 和 HDX Insight）。	NetScaler 到 NetScaler 控制台

NetScaler 实例的端口

下表说明了 NetScaler 实例上必须打开的所需端口。

端口	类型	详细信息	通信方向
80/443	TCP	用于从 NetScaler Console 到 NetScaler 实例的 NITRO 通信。用于高可用性模式下 NetScaler Console 服务器之间的 NITRO 通信。	NetScaler Console 到 NetScaler 以及 NetScaler 到 NetScaler Console
22	TCP	用于从 NetScaler Console 到 NetScaler 实例的 SSH 通信。用于高可用性模式下部署的 NetScaler Console 服务器之间的同步。此外，NetScaler	NetScaler Console 到 NetScaler。或者，NetScaler 代理到 NetScaler。

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

端口	类型	详细信息	通信方向
		Console 代理与 NetScaler 之间的 SSH 通信需要此端口。	
无保留端口	ICMP	用于检测 NetScaler Console 与 NetScaler 实例之间的网络可达性，或高可用性模式下部署的辅助 NetScaler Console 服务器。	NetScaler Console 与 NetScaler 之间的连接
161	UDP	从 NetScaler 实例轮询事件。	NetScaler Console 与 NetScaler 之间的连接

NetScaler 内置代理的端口

下表说明了 NetScaler 内置代理必须打开的所需端口。

端口	类型	详细信息	通信方向
443	TCP	用于从 NetScaler Console 到 NetScaler 内置代理的所有通信	NetScaler Console 到 NetScaler 内置代理以及 NetScaler 内置代理到 NetScaler Console

注意：

在 NetScaler Console 高可用性部署中，所有来自 NetScaler Console 的通信都使用主节点 IP 地址。

外部服务器端口

下表说明了必须在外部服务器上打开的所需端口：

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

端口	类型	详细信息	通信方向
25	TCP	用于将 SMTP 通知从 NetScaler Console 发送给用户。	NetScaler Console 到用户。
389/636	TCP	身份验证协议的默认端口。用于 NetScaler Console 与 LDAP 外部身份验证服务器之间的通信。	NetScaler Console 到 LDAP 外部身份验证服务器
123	UDP	用于与多个时间源同步的默认 NTP 服务器端口。	NetScaler Console 到 NTP 服务器
1812	RADIUS	身份验证协议的默认端口。用于 NetScaler Console 与 RADIUS 外部身份验证服务器之间的通信。	NetScaler Console 到 RADIUS 外部身份验证服务器
49	TACACS	身份验证协议的默认端口。用于 NetScaler Console 与 TACACS 外部身份验证服务器之间的通信。	NetScaler Console 到 TACACS 外部身份验证服务器

限制

从 NetScaler ADM 12.1 或更高版本开始，支持 IP 地址的 IPv6 格式。要配置 IPv6，请导航到“**设置 > 管理**”，在“**网络配置**”下选择“**IP 地址、第二个 NIC、主机名和代理服务器**”，启用“**IPv6**”，提供 IPv6 配置详细信息，然后单击“**保存**”。

下表描述了 IPv6 支持和不支持的功能列表：

IPV6 支持的功能	IPV6 不支持的功能
NetScaler ADM GUI 的管理访问	高可用性浮动 IP

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

IPV6 支持的功能	IPV6 不支持的功能
NetScaler 的管理访问	从支持 IPv6 的 ADC 接收的系统日志
注册和清单	支持 IPv6 的 ADC 上的 StyleBooks
网络仪表板	分析
SSL 仪表板	池化许可
配置作业	
配置审计	
网络功能	
网络报告	
ADC 实例的备份和恢复	
来自 NetScaler 实例的 SNMP 事件	

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

开始使用

本文档将指导您首次部署和设置本地 NetScaler Console。本文档适用于管理 Citrix 网络设备（NetScaler 和 NetScaler Gateway）的网络和应用程序管理员。无论您计划使用 NetScaler Console 管理何种类型的设备，请遵循本文档中的步骤。

如果您是 NetScaler Console 的现有用户，建议您在将服务器升级到最新版本的 NetScaler Console 之前，查看发行说明、系统要求 和 许可 详细信息。

步骤 1 - 查看系统要求

在数据中心部署 NetScaler Console 之前，请查看软件要求、浏览器要求、端口信息、许可证信息和限制。

- **许可证信息**。您可以添加任意数量的实例和实体，而无需许可证。但是，在不应用许可证的情况下，您只能查看两个虚拟服务器的分析信息。要查看两个以上虚拟服务器的分析，您必须购买相应的许可证。了解更多。
- **操作系统和接收器要求**。查看此信息以确保您拥有受支持操作系统的正确接收器版本。了解更多。
- **浏览器要求**。要访问 NetScaler Console GUI，您必须确保拥有所需的浏览器和正确的版本。了解更多。
- **端口**。确保打开所需的端口，以便 NetScaler Console 与 NetScaler 实例通信。了解更多。
- **NetScaler 实例要求**。不同的 NetScaler Console 功能支持不同的 NetScaler 软件版本。查看此信息以确保您已将 NetScaler 实例升级到正确的版本。了解更多。

步骤 2 - 部署 NetScaler Console

要管理和监控应用程序和网络基础架构，您必须首先在其中一个虚拟机管理程序上安装 NetScaler Console。您可以将 NetScaler Console 部署为单个服务器或高可用性模式。如果您正在使用 NetScaler Insight Center，则可以迁移到 NetScaler Console，除了分析功能外，还可以利用管理、监控、编排和应用程序管理功能。

- **单服务器部署**。在 NetScaler Console 单服务器部署中，数据库与服务器集成，单个服务器处理所有流量。您可以使用 Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V 和 Linux KVM 部署 NetScaler Console。请参阅：

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

  - NetScaler 控制台与 Citrix Hypervisor
  - NetScaler 控制台与 Microsoft Hyper-V
  - NetScaler 控制台 与 威睿 ESXi
  - NetScaler Console 与 Linux KVM 服务器

- **高可用性部署。** 两个 NetScaler Console 服务器的高可用性部署 (HA) 可提供不间断的操作。在高可用性设置中，两个 NetScaler Console 节点必须以主动-被动模式部署在同一子网上，使用相同的软件版本和内部版本，并且必须具有相同的配置。通过 HA 部署，在 NetScaler Console 主节点上配置浮动 IP 地址的能力消除了对单独的 NetScaler 负载均衡器的需求。要了解更多信息，请参阅 [在高可用性部署中配置。

  ```
  ](deploy/high-availability-deployment.md)
  ```

步骤 3 - 将实例添加到 NetScaler Console

在 NetScaler Console 中，您可以发现、管理和监控所有部署在本地或云上的 NetScaler 实例。如果要管理和监控这些实例，则必须将实例添加到 NetScaler Console 服务器。您可以将以下实例添加到 NetScaler Console：

- NetScaler
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
  - NetScaler 网关

当您将实例添加到 NetScaler Console 服务器时，服务器会隐式地与这些实例通信并收集这些实例的清单。

了解更多

步骤 4 - 在虚拟服务器上启用分析

要查看应用程序流量的分析数据，您必须在接收特定应用程序流量的虚拟服务器上启用分析功能。

了解更多

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

步骤 5 - 在 NetScaler Console 上配置 NTP 服务器

您必须在 NetScaler Console 中配置网络时间协议 (NTP) 服务器，以使其时钟与 NTP 服务器同步。配置 NTP 服务器可确保 NetScaler Console 时钟与网络上的其他服务器具有相同的日期和时间设置。

了解更多

步骤 6 - 配置系统设置以优化 NetScaler Console 性能

在开始使用 NetScaler Console 管理和监控实例和应用程序之前，建议您配置一些系统设置，以确保 NetScaler Console 服务器的最佳性能。

- **配置系统警报**。配置系统警报以确保您了解任何严重或主要的系统问题。例如，您可能希望在 CPU 使用率过高或服务器登录失败次数过多时收到通知。
- **配置系统通知**。您可以向选定的用户组发送各种系统相关功能的通知。您可以在 NetScaler Console 中设置通知服务器，并且可以配置电子邮件和短消息服务 (SMS) 网关服务器，以向用户发送电子邮件和文本通知。这可确保您收到任何系统级活动（例如用户登录或系统重启）的通知。
- **配置系统清除设置**。为了限制 NetScaler Console 服务器数据库中存储的报告数据量，您可以指定 NetScaler Console 保留网络报告数据、事件、审计日志和任务日志的时间间隔。默认情况下，此数据每 24 小时（00:00 时）清除一次。
- **配置系统备份设置**。NetScaler Console 每天 00:30 自动备份系统。默认情况下，它会保存三个备份文件。您可能希望保留更多数量的系统备份。
- **配置实例备份设置**。如果您备份 NetScaler 实例的当前状态，则可以使用备份文件在实例变得不稳定时恢复稳定性。在执行升级之前，这样做尤其重要。默认情况下，每 12 小时进行一次备份，并在系统中保留三个备份文件。
- **配置实例事件清除设置**。为了限制 NetScaler Console 服务器数据库中存储的事件消息数据量，您可以指定 NetScaler Console 保留网络报告数据、事件、审计日志和任务日志的时间间隔。默认情况下，此数据每 24 小时（00:00 时）清除一次。
- **配置实例 syslog 清除设置**。为了限制数据库中存储的 syslog 数据量，您可以指定要清除 syslog 数据的时间间隔。您可以指定从 NetScaler Console 中删除以下 syslog 数据的天数：
  - 通用 Syslog 数据
  - AppFirewall 数据
  - NetScaler Gateway 数据。

    了解更多

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

接下来

部署并设置 NetScaler Console 后，您可以开始管理和监控您的实例和应用程序。

管理 NetScaler 实例和应用程序。 所有 NetScaler Console 功能都支持 NetScaler 实例。您可以开始使用任何功能。

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

增强型图形用户界面

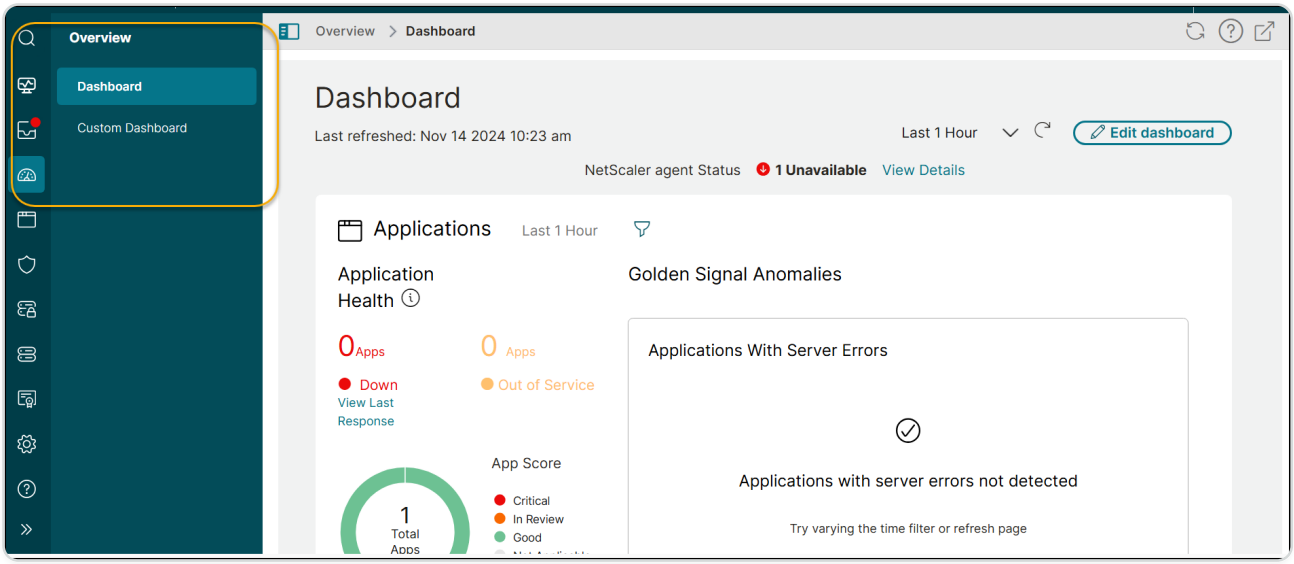
NetScaler Console 图形用户界面 (GUI) 提供了丰富的使用体验，具有以下几个关键功能。这些功能提供：

- **优化屏幕空间：** 用户可以根据自己的偏好显示或隐藏侧边栏。
- **快速访问收藏夹：** 固定常用菜单项以加快导航速度。
- **增强子菜单可见性：** 将鼠标悬停在菜单项上可显示子菜单，从而更清晰地查看所有可用选项。
- **改进的子菜单结构：** 一致的三级子菜单系统确保了 NetScaler Console 中的无缝导航，提供统一的体验。

本页面将引导您了解 NetScaler Console GUI 的功能，从而提供丰富的用户体验。

悬停显示菜单

以前，二级子菜单以树状结构显示。NetScaler Console GUI 提供了无缝导航，二级菜单在悬停时出现，显示子菜单。这种导航通过显示所有子菜单选项而无需滚动，提升了查看体验。



精简的菜单层级结构

菜单层级结构已精简为最多三级。以前显示在第三级之外的子菜单现在已定位到第三级。以下导航已更新：

- **基础架构 > 配置**

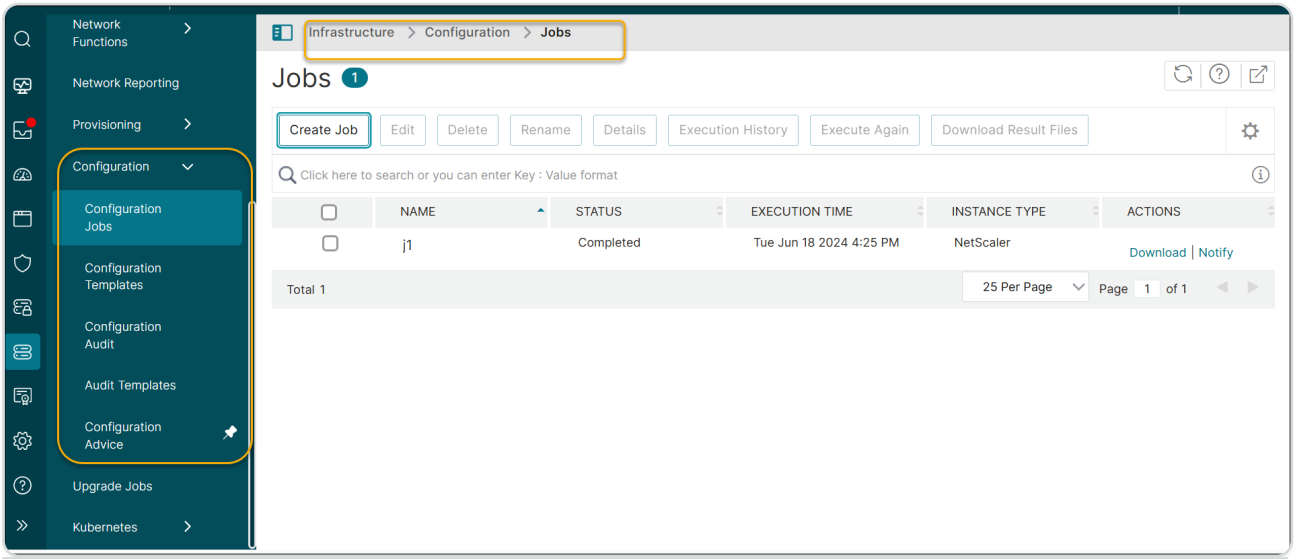
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **NetScaler® 许可 > 池化许可**
- **网关 > HDX™ Insight**

更新的子菜单标签

为与此导航方法保持一致，部分子菜单的名称已更改。屏幕导航更改和子菜单标签更新如下：

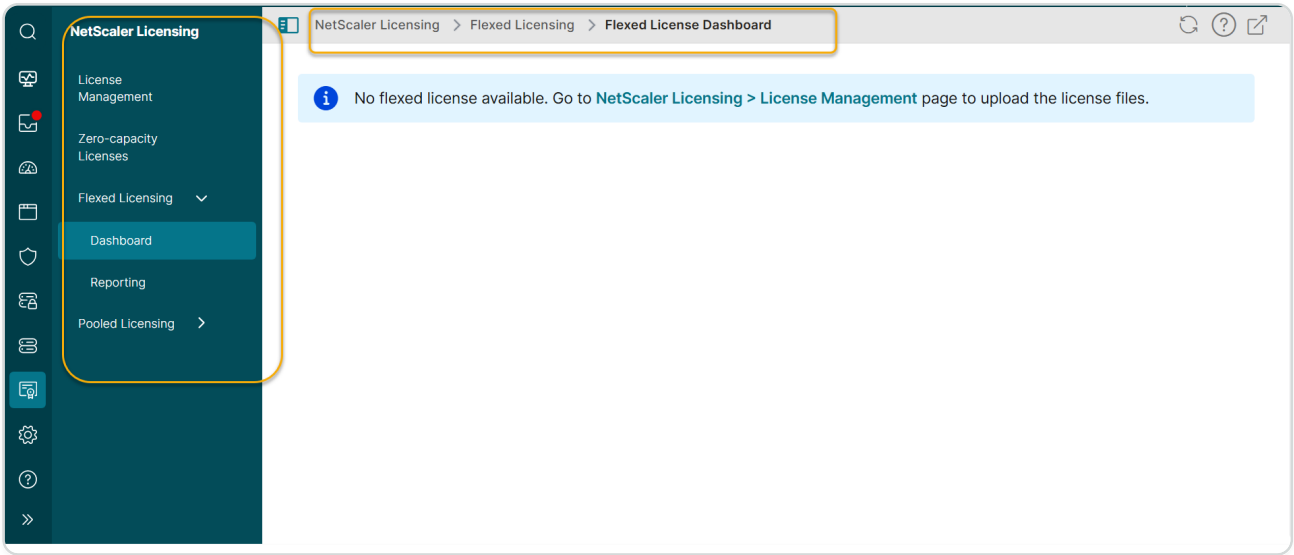
基础架构 > 配置



以前的屏幕导航	更改后的屏幕导航	子菜单标签有变化吗？
配置 > 配置作业 > 作业	配置 > 配置作业	是
配置 > 配置作业 > 配置模板	配置 > 配置模板	否
配置 > 配置审计 > 概述	配置 > 配置审计	是
配置 > 配置审计 > 审计模板	配置 > 审计模板	否
配置 > 配置审计 > 配置建议	配置 > 配置建议	否

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

NetScaler 许可 > 许可池



以前的屏幕导航	更改后的屏幕导航	子菜单标签有变化吗？
许可池 > 吞吐量容量许可证 > 吞吐量容量	许可池 > 吞吐量容量	否
许可池 > 吞吐量容量许可证 > CPX 许可证	许可池 > CPX 许可证	否
许可池 > 吞吐量容量许可证 > CICO	许可池 > CICO	否
许可池 > 吞吐量容量许可证 > FIPS 实例	许可池 > FIPS 实例	否
许可池 > 自管理 > 许可证到期信息	许可池 > 自管理到期信息	是
许可池 > 自管理 > 吞吐量容量许可证 > 自管理池	许可池 > 自管理吞吐量	是
池化许可 > 自行管理 > 自行管理 VCPU	池化许可 > 自行管理 VCPU	否

网关 > HDX Insight

以前的屏幕导航	更改后的屏幕导航	子菜单标签有变化吗？
HDX Insight > 许可证 > SSL VPN 许可证	HDX Insight > 许可证	是

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

设置

除了子菜单标签或名称的修改之外，**设置**下没有其他更改。

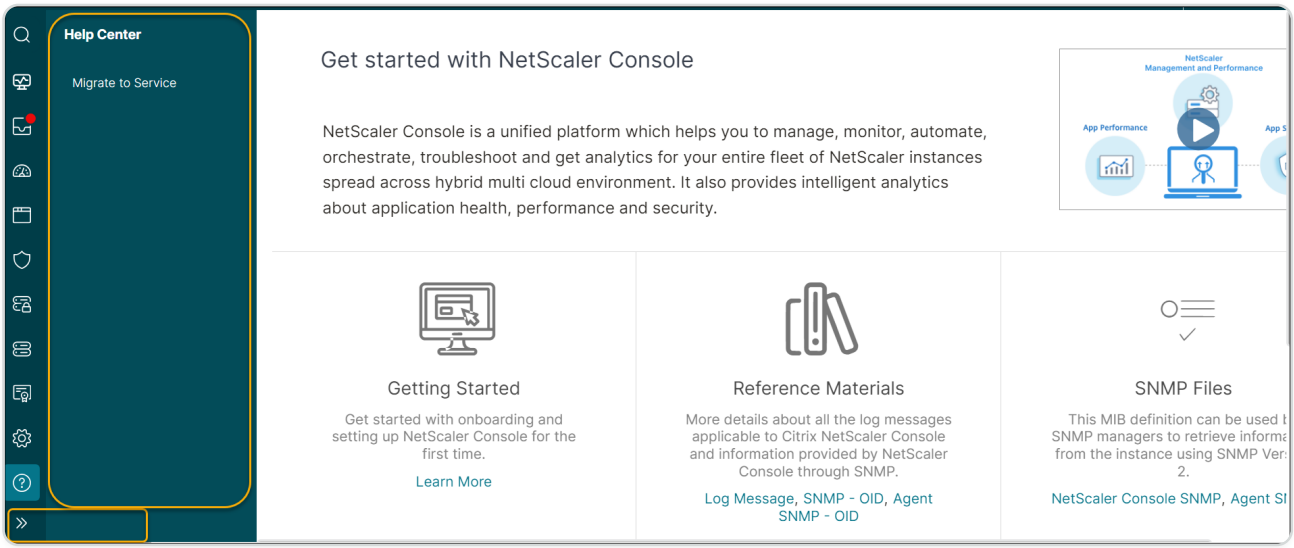
以前的屏幕导航	更改后的屏幕导航	子菜单标签有变化吗？
设置 > 数据存储管理	屏幕导航没有变化。	子菜单标签已更改为 **设置 > 数据存储**

可折叠菜单

您可以通过单击图标折叠或展开整个菜单。

展开的菜单

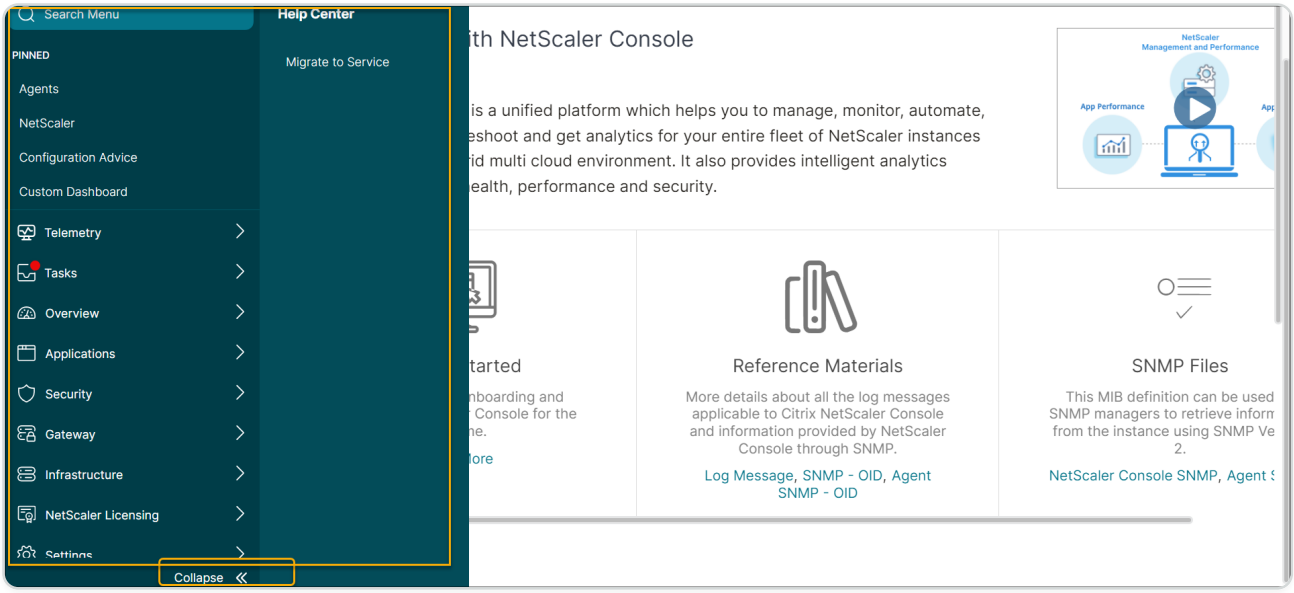
单击窗格中的图标 **>>** 以展开整个菜单。



折叠的菜单

单击窗格中的 **Collapse <<** 以折叠整个菜单。

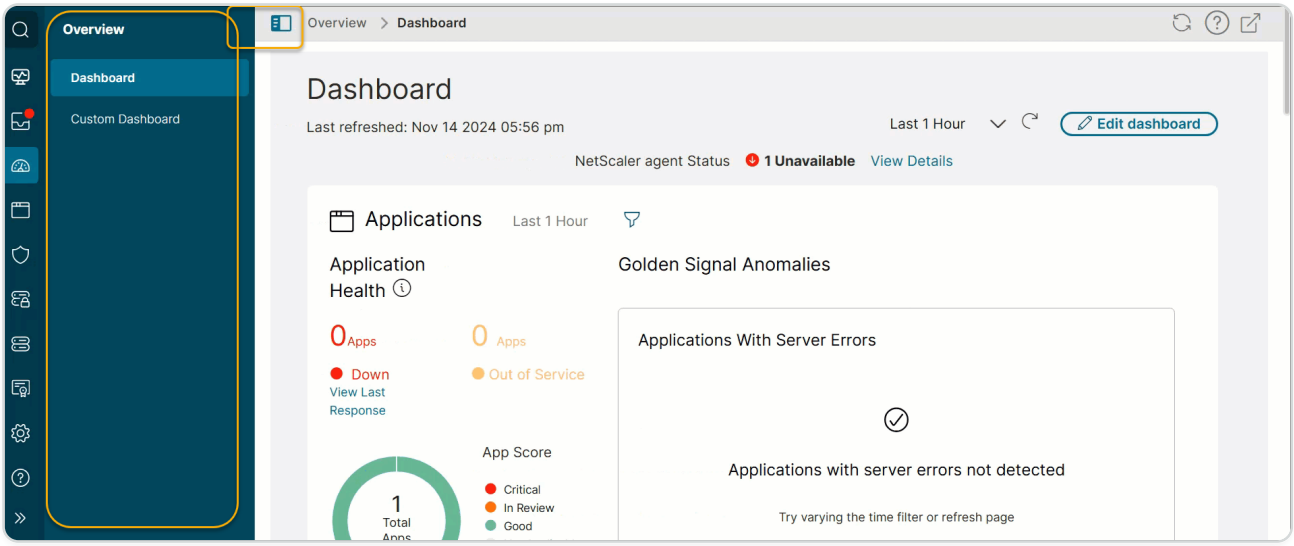
© 1997–2026 Citrix Systems, Inc. All rights reserved.



侧边栏切换

您可以通过切换侧边栏可见性来优化屏幕空间。单击面包屑中的切换按钮以隐藏或显示侧边栏。

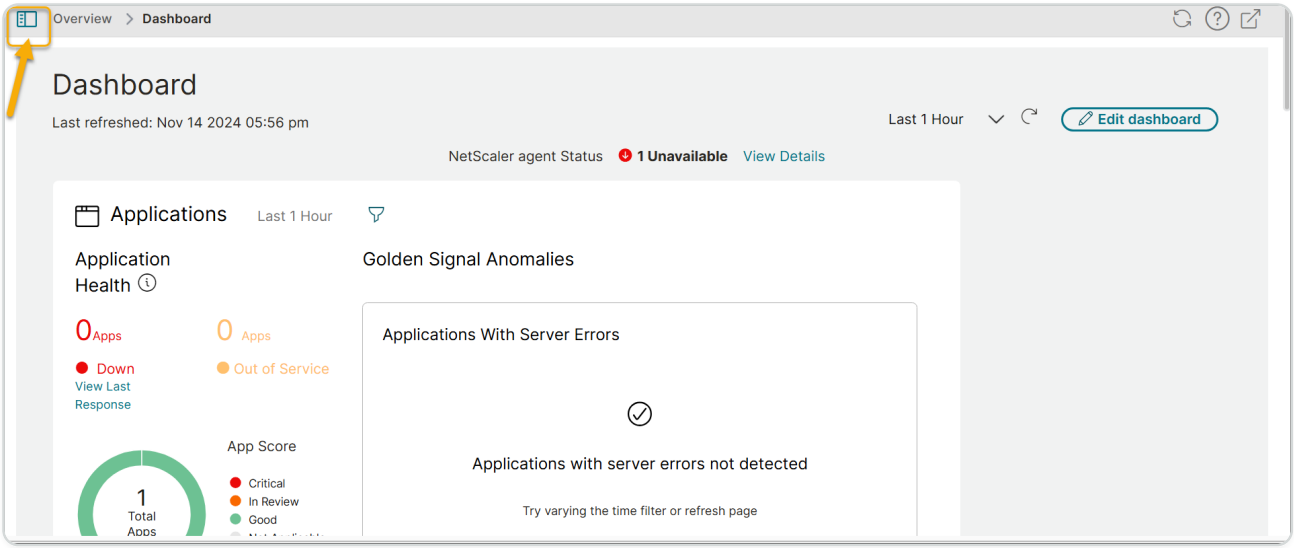
显示侧边栏



隐藏侧边栏

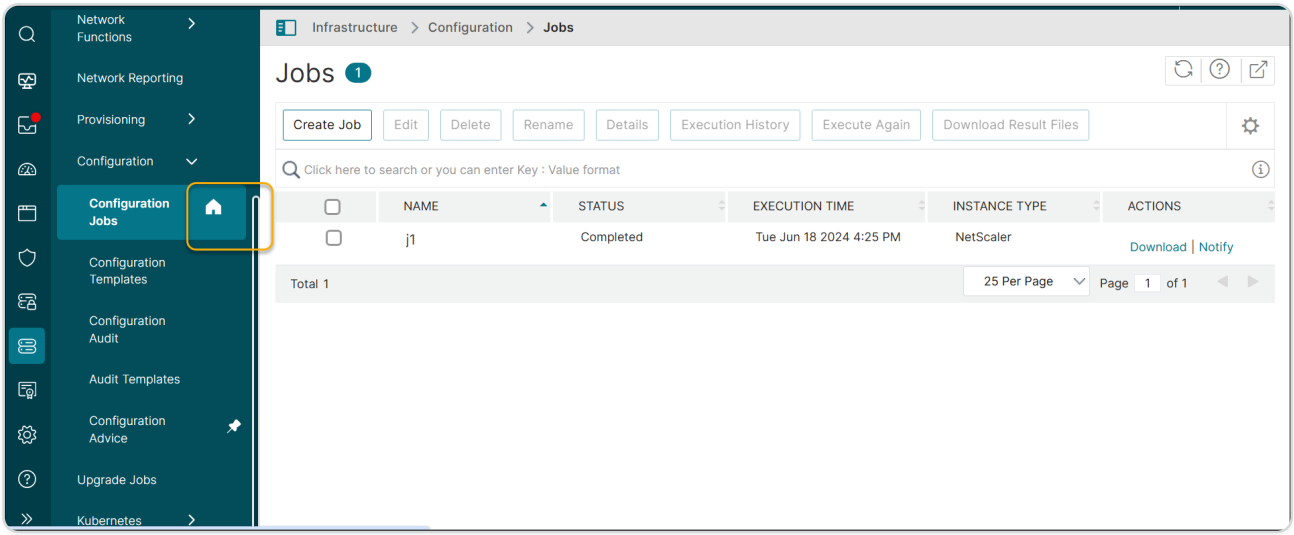
此选项通过隐藏侧边栏来优化屏幕空间。

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



设置为主屏幕

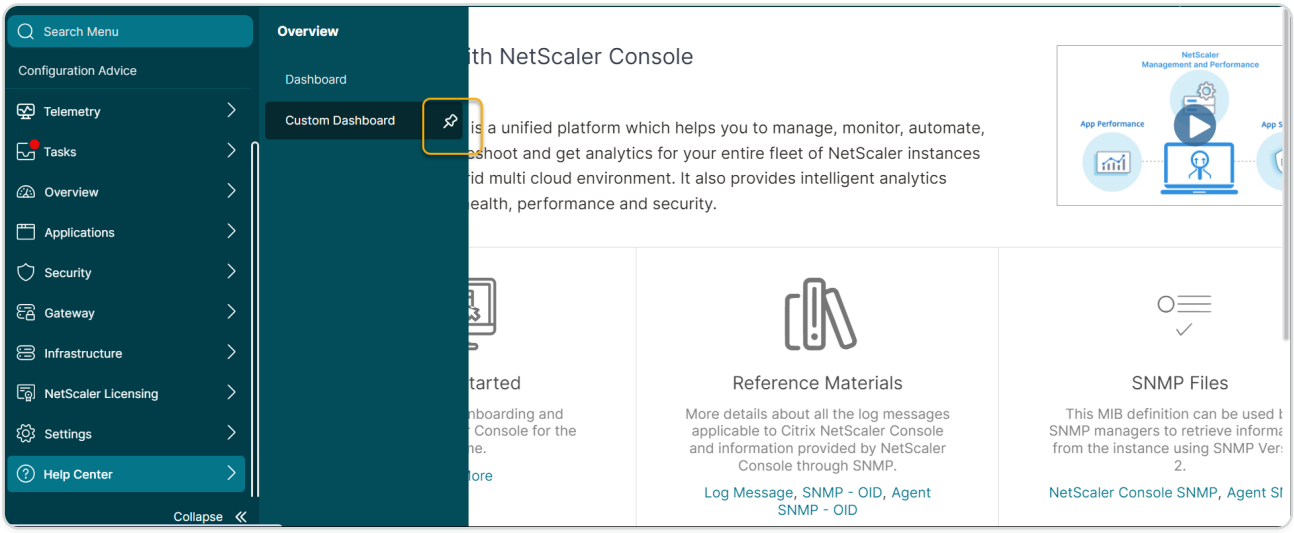
NetScaler Console GUI 在显示为页面的子菜单名称旁边有一个图标。主屏幕图标允许您设置着陆页。它仅在您位于该特定页面时显示。要从主页中删除该页面，只需再次单击该图标。



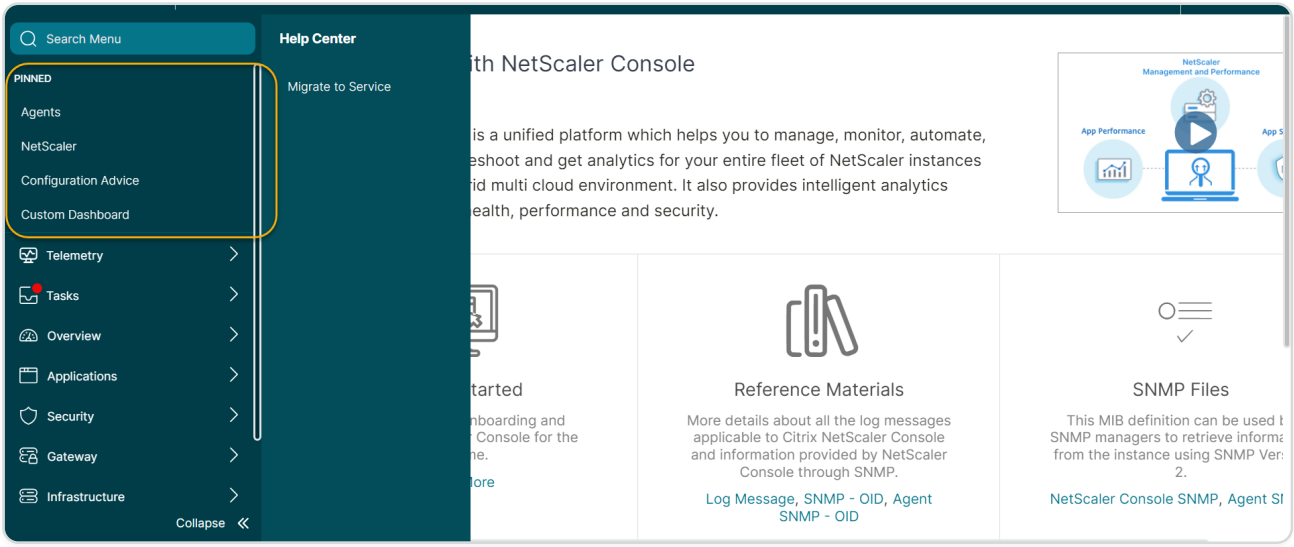
固定收藏项

固定功能可让您更快地访问收藏项。要固定菜单或子菜单，请将鼠标悬停在其上方，然后单击其名称旁边出现的图钉图标。

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



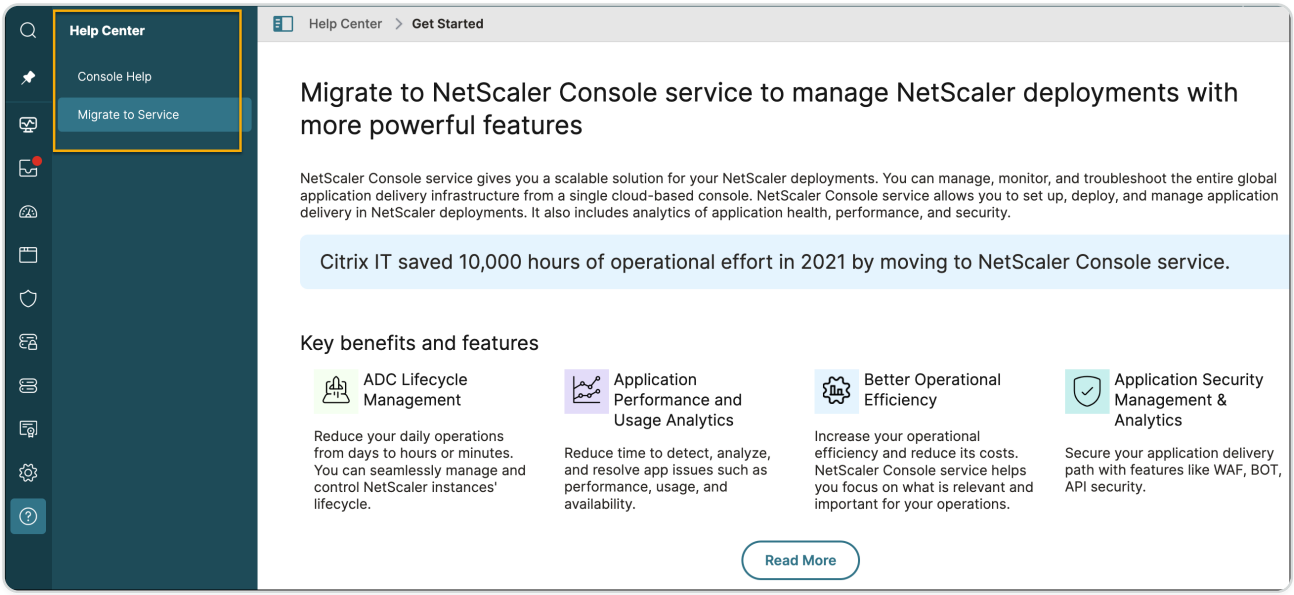
固定菜单显示在侧边栏的 **已固定** 下方，方便访问。



迁移到服务

迁移到服务 选项现在作为 **帮助中心** 的子菜单提供。以前，此选项在导航窗格中可用。这简化了适当菜单项下的可用选项。

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



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

部署

在使用 NetScaler Console 管理和监控您的应用程序和网络基础设施之前，您必须首先将其安装在其中一个虚拟机管理程序或 Kubernetes 集群上。如果您在虚拟机管理程序上部署 NetScaler Console，则可以将其部署为单个服务器或高可用性模式。高可用性模式不适用于 Kubernetes 集群。如果您正在使用 NetScaler Insight Center，则可以迁移到 NetScaler Console，除了分析功能之外，还可以利用其管理、监控、编排和应用程序管理功能。

- **单服务器部署**：对于部署在虚拟机管理程序上的独立 NetScaler Console，数据库与服务器集成，单个服务器处理所有流量。您可以使用 Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V 和 Linux KVM 部署 NetScaler Console。请参阅：
  - Citrix 虚拟机监控程序上的 NetScaler 控制台
  - Microsoft Hyper-V 上的 NetScaler 控制台
  - Azure 上的 NetScaler 控制台
  - VMware ESXi 上的 NetScaler 控制台
  - Linux KVM 服务器上的 NetScaler Console
  - Nutanix 虚拟机管理程序 (Acropolis) 上的 NetScaler Console
  - Kubernetes 集群上的 NetScaler Console
- **高可用性 (HA) 部署**：两个 NetScaler Console 服务器的 HA 部署可提供不间断的操作。在 HA 设置中，两个 NetScaler Console 节点都必须以主动-被动模式部署在同一子网上，使用相同的软件版本和内部版本，并且必须具有相同的配置。通过 HA 部署，在 NetScaler Console 主节点上配置浮动 IP 地址的能力消除了对单独的 NetScaler 负载均衡器的需求。请参阅：在高可用性部署中进行配置。

  注意：

  高可用性不适用于部署在 Kubernetes 集群上的 NetScaler Console。

- **轻量级部署**：如果您计划仅将 NetScaler Console 用于池化或弹性许可，则可以使用较低的规格进行部署。有关更多信息，请参阅先决条件。
- **从 NetScaler Insight Center 迁移到 NetScaler Console**：您可以将 NetScaler Insight Center 部署迁移到 NetScaler Console，而不会丢失现有配置、设置或数据。使用 NetScaler

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

Console，您不仅可以查看 NetScaler 生成的各种分析，还可以从一个统一的控制台管理、监控和排查整个全球应用程序交付基础设施。请参阅：从 NetScaler Insight Center 迁移到 NetScaler Console

- **将 NetScaler Console 与 Director 集成**：Director 与 NetScaler Console 集成，以进行网络分析和性能管理。请参阅：将 NetScaler Console 与 Director

安装 NetScaler Console 的先决条件

您可以将 NetScaler Console 作为虚拟设备下载并安装到 Microsoft HyperV、 VMware ESXi、Linux KVM 和 Citrix Hypervisor™ 平台。在安装 NetScaler Console 之前，您必须了解所有这些平台上的软件要求、浏览器要求、端口 信息、许可证信息和限制。

有关特定平台要求和安装 NetScaler Console 的详细步骤，请参阅以下主题：

- NetScaler 控制台 和 Citrix Hypervisor
- NetScaler 控制台 和 Microsoft HyperV
- NetScaler 控制台 和 VMware ESXi
- NetScaler Console 与 Linux KVM 服务器

NetScaler Console 的一般要求

组件	要求
内存	32 GB
虚拟 CPU	8 个 CPU
存储空间	Citrix 建议在 NetScaler Console 部署中使用固态硬盘 (SSD) 技术。
	所需的默认存储空间为 120 GB。实际存储要求取决于 NetScaler Console 的大小估算。
	如果您的 NetScaler Console 存储要求超过 120 GB，则必须连接一个额外的磁盘。
	Citrix 建议您在初始部署时估算存储并连接一个额外的磁盘。您只能添加一个额外的磁盘。
	有关更多信息，请参阅 如何将额外磁盘连接到 NetScaler Console。

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

组件	要求
虚拟网络接口	1
吞吐量	1 千兆位/秒

仅适用于池化或弹性许可的轻量级 NetScaler® Console

您只能将 NetScaler Console 用于具有较低规格的 池化或弹性许可：

组件	要求
RAM	8 GB
虚拟 CPU	4
存储	120 GB

注意：

Citrix 建议您将 NetScaler Console VHD 托管在本地存储上。当托管在 SAN 中的存储设备上时，NetScaler Console 可能无法按预期工作。因此，不支持在 SAN 上部署 NetScaler Console。

思杰虚拟化管理程序上的 NetScaler Console

要在 Citrix Hypervisor（以前称为 XenServer）上安装 NetScaler Console，您需要首先将 NetScaler Console .xva 映像文件下载到本地计算机。您需要使用 Citrix XenCenter 执行 NetScaler Console 安装。

注意：

NetScaler Console 不支持 XenMotion。

先决条件

在安装 NetScaler Console 之前，请验证是否满足以下要求：

- Citrix Hypervisor 7.1 或更高版本已安装在满足最低要求的硬件上。

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

- XenCenter 已安装在满足最低要求的管理工作站上。您必须使用 XenCenter 在 Citrix Hypervisor 上安装 NetScaler Console。
- 您已下载 NetScaler Console .XVA 映像文件。

XenCenter® 系统要求

XenCenter 是一个 Windows 客户端应用程序。它不能在与 Citrix Hypervisor™ 主机相同的计算机上运行。下表描述了最低系统要求。

组件	要求
操作系统	Windows 7 操作系统、Windows Server 2003 操作系统或 Windows 10 操作系统
.NET 框架	2.0 或更高版本
CPU	750 MHz (MHz)，建议：1 千兆赫 (GHz) 或更快
RAM	1 GB，建议：2 GB
NIC	100 兆位/秒 (Mbps) 或更快的 NIC

安装 NetScaler® 应用交付管理

1. 将 XVA 映像文件导入到您的 Citrix Hypervisor，然后从“**控制台**”选项卡配置初始网络配置选项。

2. 指定所需的 IP 地址后，保存配置设置。
3. 出现提示时，使用 nsrecover/nsroot 凭据登录。

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

```
login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

bash-3.2#
```

注意

登录后，如果您想更新初始网络配置，请键入 `networkconfig`，更新配置，然后保存配置。

4. 在 shell 提示符下键入命令以运行部署脚本：`/mps/deployment_type.py`

```
bash-3.2# deployment_type.py
-------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
```

5. 选择部署类型为 **NetScaler Console Server**。如果您未选择任何选项，则默认将其部署为服务器。

```
-------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

6. 键入 **Yes** 以将 NetScaler Console 部署为独立部署。
7. 键入 **Yes** 以重新启动 NetScaler Console 服务器。

注意

安装 NetScaler Console 后，您可以稍后更新初始配置设置。

验证

服务器安装完成后，您可以通过在 Web 浏览器中键入 NetScaler Console 服务器的 IP 地址来访问 GUI。登录服务器的默认管理员凭据是 nsroot/nsroot。

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

浏览器将显示 NetScaler Console 配置实用程序。

在 Microsoft Hyper-V 虚拟化平台上的 NetScaler Console

要在 Microsoft Hyper-V 上安装 NetScaler Console，您必须首先将 NetScaler Console 映像文件下载到本地计算机。此外，请确保您的系统具有硬件虚拟化扩展，并验证 CPU 虚拟化扩展是否可用。

先决条件

在安装 NetScaler Console 虚拟设备之前，请验证是否满足以下要求：

- Microsoft Hyper-V 6.2 或更高版本已安装在满足最低要求的硬件上。
- 在满足最低系统要求的管理工作站上安装 Microsoft Hyper-V Manager。
- 您已下载 NetScaler Console 映像文件。

Microsoft Hyper-V 系统要求

Microsoft Hyper-V 是一个 Windows 客户端应用程序。下表描述了最低系统要求。

组件	要求
操作系统	Windows Server 2012 R2 操作系统
.NET 框架	版本 2.0 或更高版本
CPU	750 MHz (MHz)，推荐：1 千兆赫 (GHz) 或更快
RAM	1 GB，推荐：2 GB
网卡	100 兆位/秒 (Mbps) 或更快的网卡

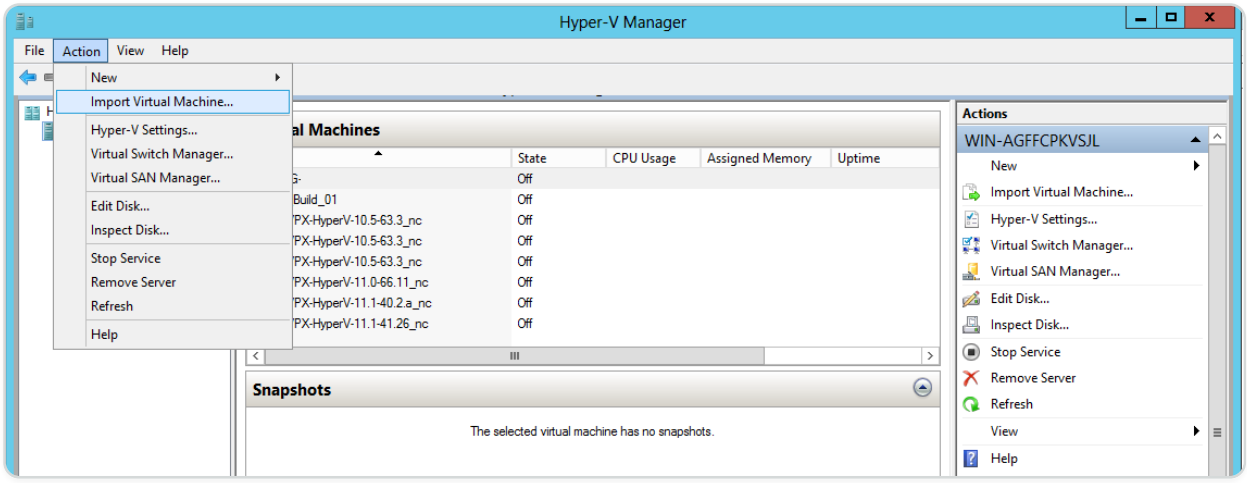
安装 NetScaler® 应用交付管理

您可以安装的 NetScaler Console 服务器数量取决于 Hyper-V 服务器上可用的内存。

安装 NetScaler Console：

1. 在您的工作站上启动 Hyper-V 管理器客户端。
2. 在“**操作**”菜单上，单击“**导入虚拟机**”。

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



3. 导入 Hyper-V 映像，并执行以下操作：

   a. 在“导入虚拟机”对话框的“**定位文件夹**”部分中，浏览到您保存 NetScaler Console Hyper-V 映像的文件夹，选择该文件夹，然后单击“**下一步**”。

   b. 在“选择虚拟机”部分中，选择相应的虚拟机名称。

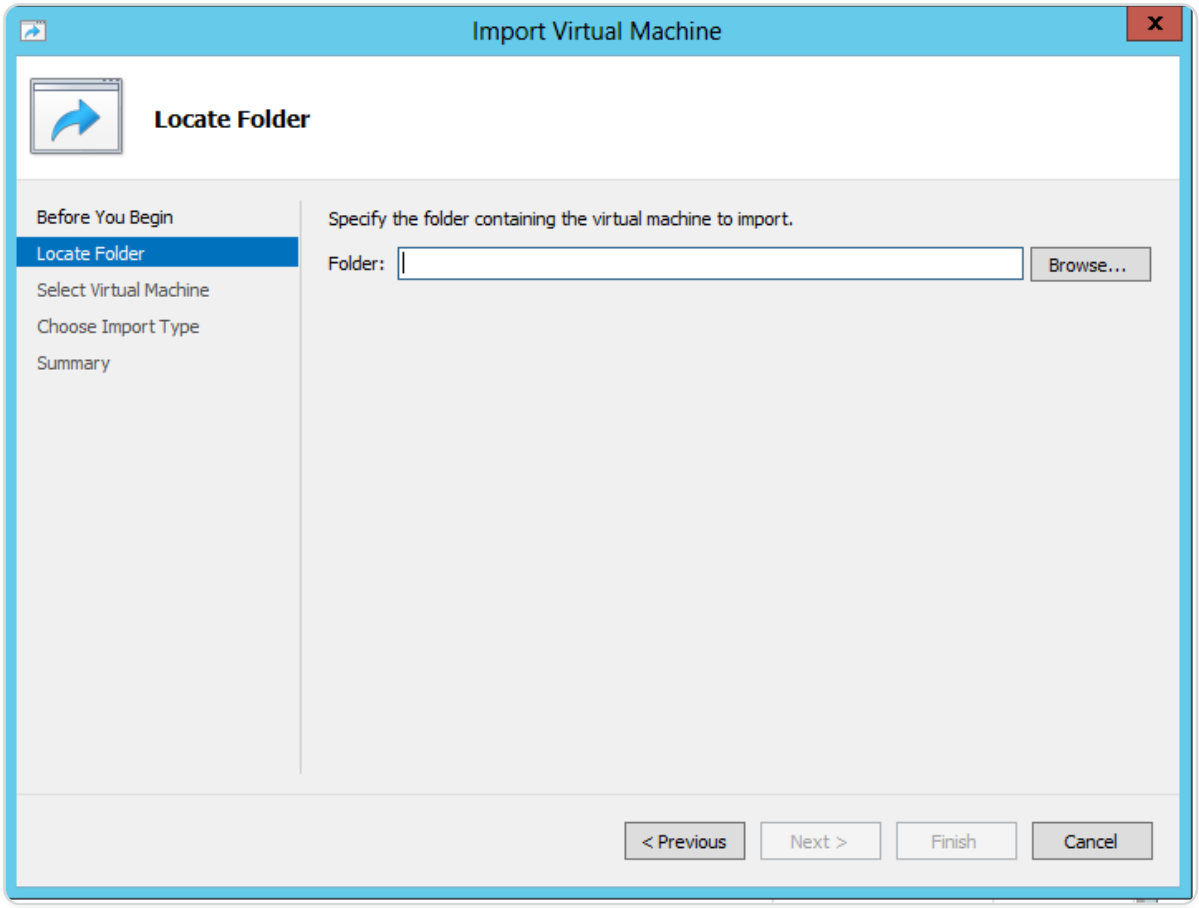
   c. 在“**选择导入类型**”部分，选择“复制虚拟机（创建新的唯一 ID）”选项，然后单击“下一步”。

   d. 在“**选择目标**”部分，您可以指定用于存储虚拟机文件的文件夹。

注意

默认情况下，向导会将虚拟机文件导入到本地主机上的默认 Hyper-V 文件夹。

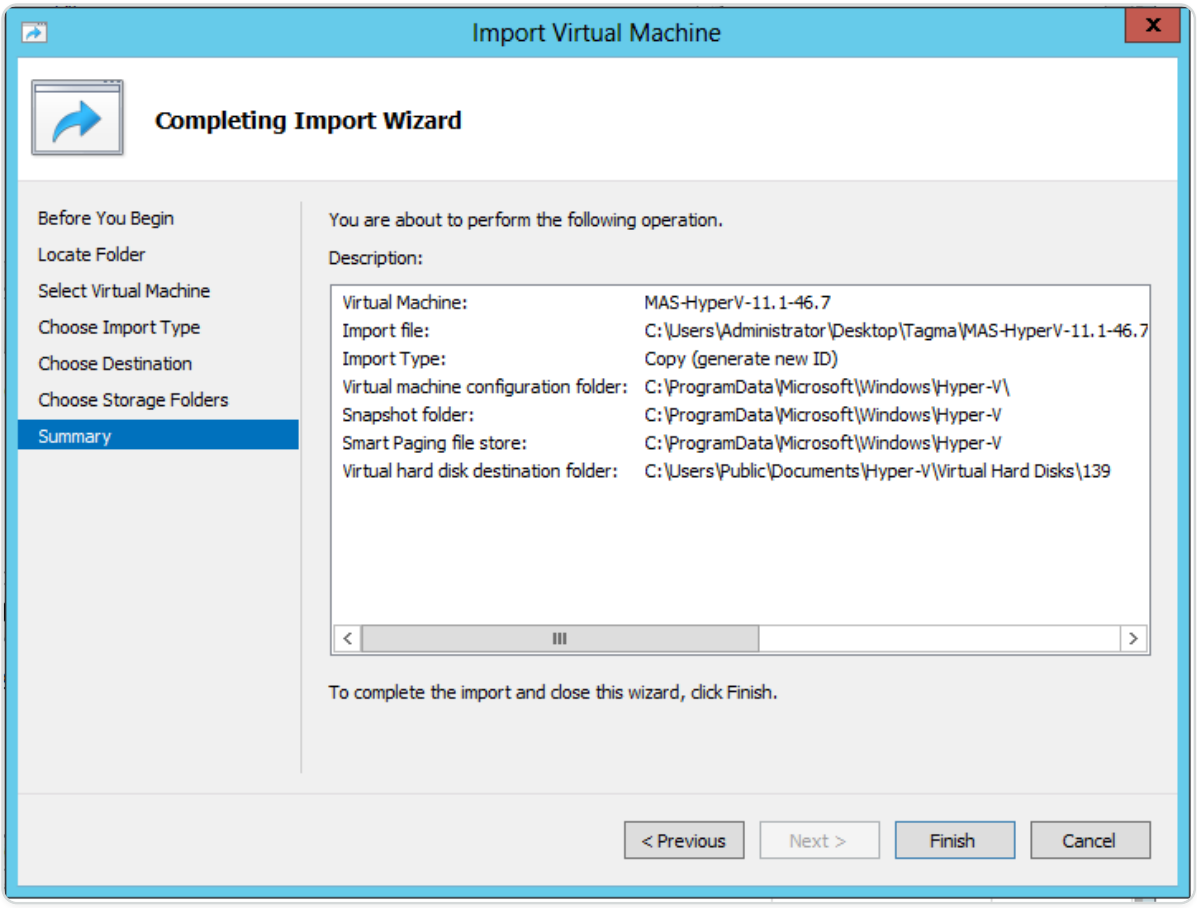
© 1997–2026 Citrix Systems, Inc. All rights reserved.



e. 在“**选择存储文件夹**”部分，您可以选择要存储虚拟硬盘的位置，然后单击“**下一步**”。

f. 您可以在摘要窗格中验证虚拟机详细信息，然后单击“**完成**”。

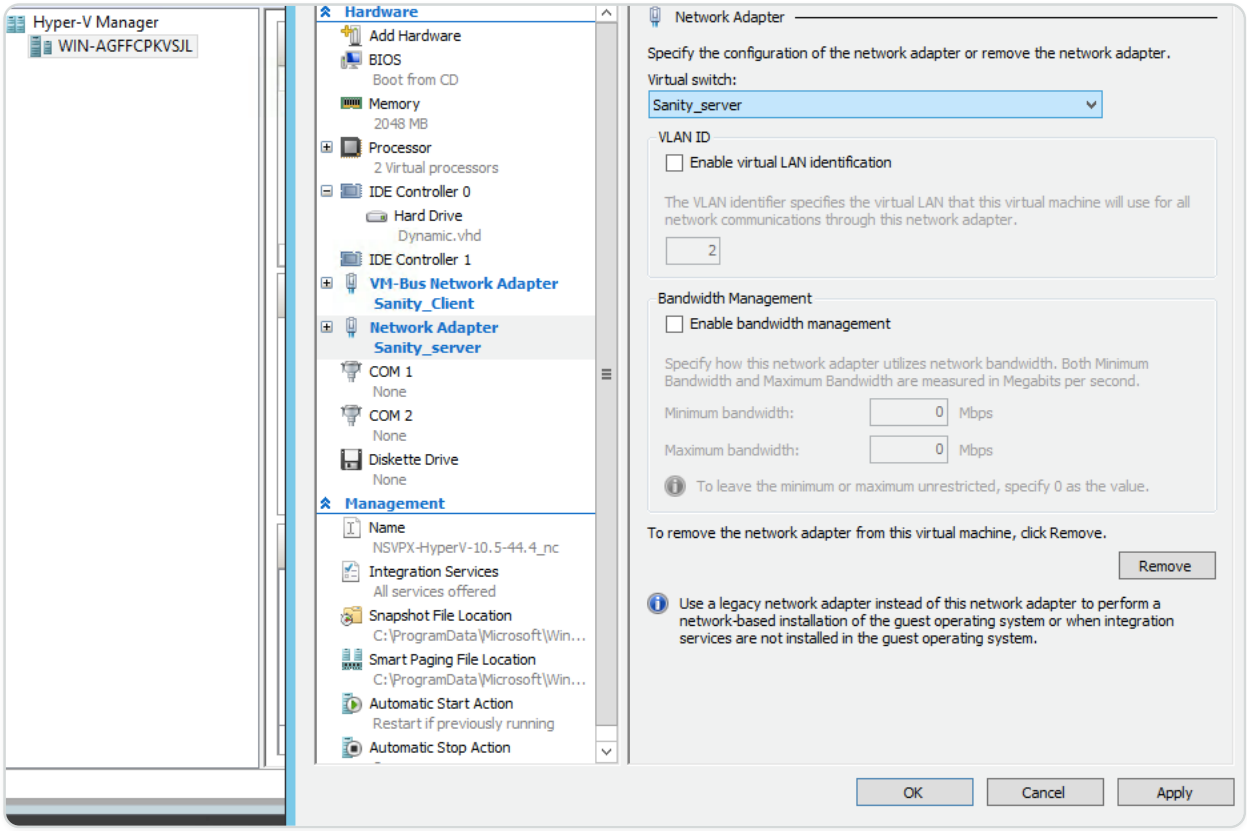
© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler Console Hyper-V 映像显示在右侧窗格中。

4. 右键单击 NetScaler Console Hyper-V 映像，然后单击“**设置**”。
5. 在出现的对话框的左侧窗格中，导航到“**硬件**” \> “**VM_Bus 网络适配器**”，并在右侧窗格中，从“网络”列表中选择相应的网络。

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



6. 单击“**应用**”，然后单击“**确定**”。
7. 右键单击 NetScaler Console Hyper-V 映像，然后单击“**连接**”。
8. 在控制台窗口中，单击“**启动**”按钮。
9. 配置初始网络配置选项。

```
-------------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-------------------------------------------------------------------------

      1. Citrix ADM Host Name [ADMHA1]:
      2. Citrix ADM IPv4 address [10.102.29.52]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

Select a menu item from 1 to 7 [7]:
```

10. 指定所需的 IP 地址后，保存配置设置。
11. 出现提示时，使用 nsrecover/nsroot 凭据登录。

```
login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

bash-3.2#
```

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

注意

登录后，如果要更新初始网络配置，请键入 `networkconfig`，更新配置，然后保存配置。

12. 在 shell 提示符下键入命令以运行部署脚本：

```
deployment_type.py
```

```
bash-3.2# deployment_type.py
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
```

13. 选择部署类型为 **NetScaler Console Server**。如果未选择任何选项，则默认将其部署为服务器。

```
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

14. 键入 **Yes** 以将 NetScaler Console 部署为独立部署。
15. 键入 **Yes** 以重新启动 NetScaler Console 服务器。

注意

安装 NetScaler Console 后，您可以稍后更新初始配置设置。

验证

服务器安装完成后，您可以通过在浏览器地址栏中键入 NetScaler Console 服务器的 IP 地址来访问 GUI。登录服务器的默认管理员凭据是 nsroot/nsroot。

浏览器将显示 NetScaler Console 配置实用程序。

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

NetScaler 控制台 在 VMware ESXi 上

本文档介绍了如何使用 VMware vSphere 客户端在 VMware ESXi 上安装 NetScaler Console 虚拟设备。

先决条件

在开始安装虚拟设备之前，请验证以下要求：

- 安装受支持的 VMware ESXi 版本。有关支持的版本列表，请参阅 Supported hypervisors。
- 在满足最低系统要求管理工作站上安装 VMware Client。
- 下载 NetScaler Console 安装文件。

注意

- VMotion 仅在 **NetScaler Console 13.0 Build 47.22 或更高版本**中受支持。您可以计划和自动化部署在 ESXi 虚拟机管理程序上的 NetScaler Console 服务器的迁移，包括 vSphere 高可用性和 vSphere DRS 设置。
- 适用于 NetScaler Console 的 VMware Tools 作为软件版本的一部分提供，无法单独升级或修改。

安装 NetScaler Console

请按照以下步骤在 VMware ESXi 上安装 NetScaler Console 虚拟设备。

注意

这些步骤和屏幕截图基于 VMware ESXi 6.0 版本。GUI 在其他 ESXi 版本中可能有所不同。VMware ESXi 7.0.1c 版本（内部版本号 17325551，带 VMXNET3 适配器）在 **NetScaler Console 13.0 71.40 或更高版本**中受支持。有关特定于版本的步骤，请参阅 VMware 文档。

1. 在您的工作站上启动 VMware vSphere 客户端。
2. 在 **IP 地址 / 名称** 文本框中，键入要连接的 VMware ESXi 服务器的 IP 地址。
3. 在 **用户名** 和 **密码** 文本框中，键入管理员凭据，然后单击 **登录**。
4. 在 **文件** 菜单上，单击 **部署 OVF 模板**。
5. 在 **部署 OVF 模板** 对话框中，在 **从文件或 URL 部署** 中，选择 .ovf 文件，然后单击 **下一步**。

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

注意

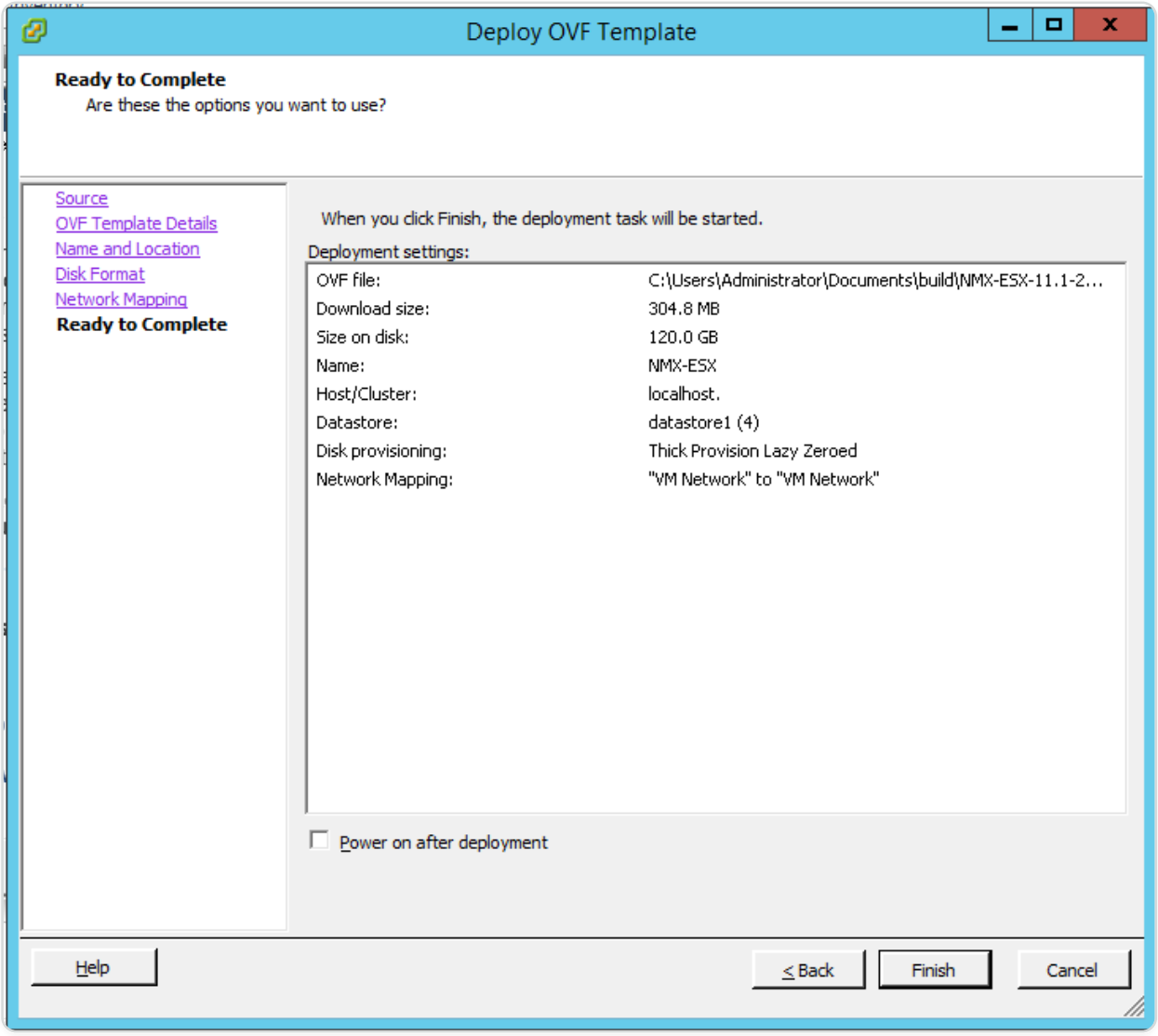
如果出现警告消息，其中包含以下文本：“所选主机不支持操作系统标识符，请检查 VMware 服务器是否支持 FreeBSD 操作系统。”单击 **是**。

6. 在 **OVF 模板详细信息** 页面上，单击 **下一步**。
7. 键入 NetScaler Console 虚拟设备的名称，然后单击 **下一步**。
8. 通过选择精简置备格式或厚置备格式来指定磁盘格式。

注意

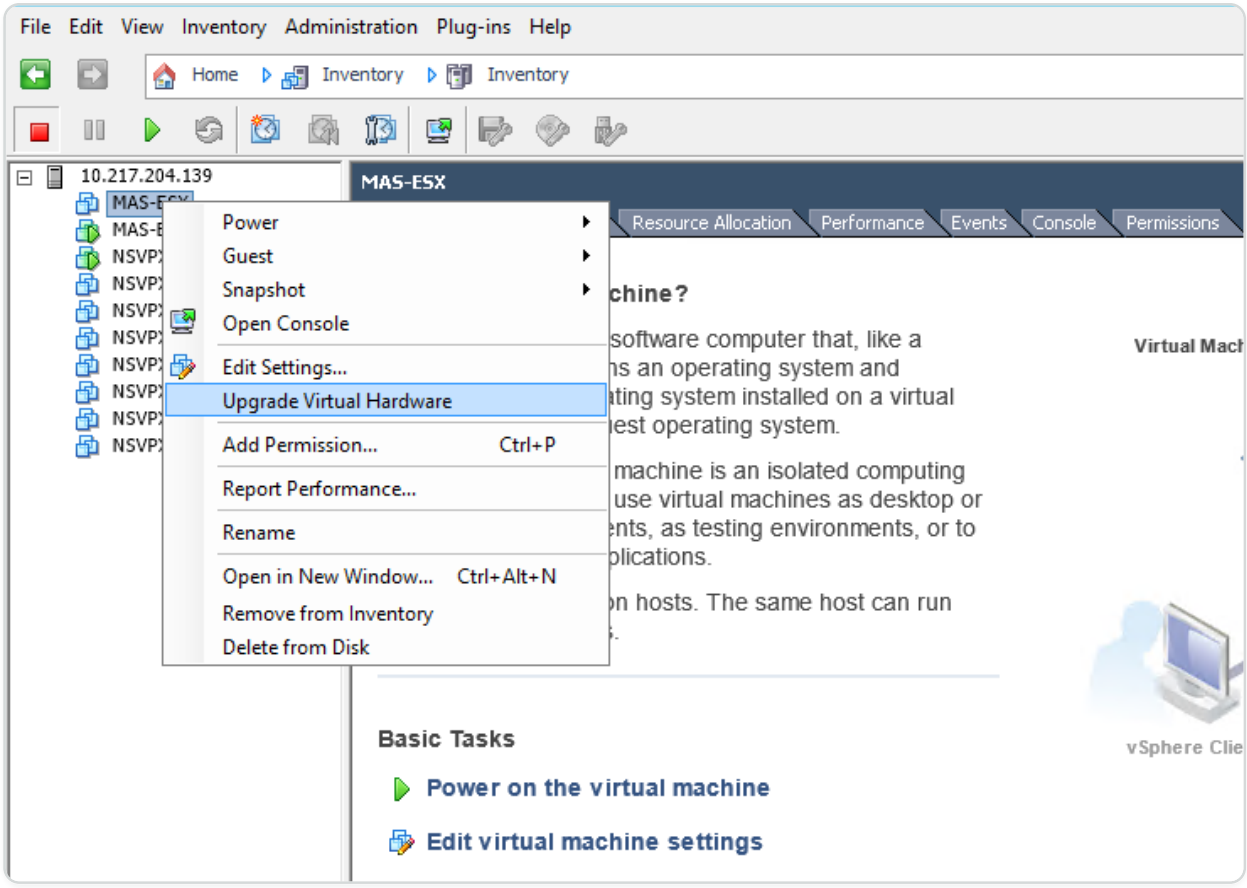
我们建议您选择 **厚置备格式**。

9. 单击 **完成** 以开始安装过程。



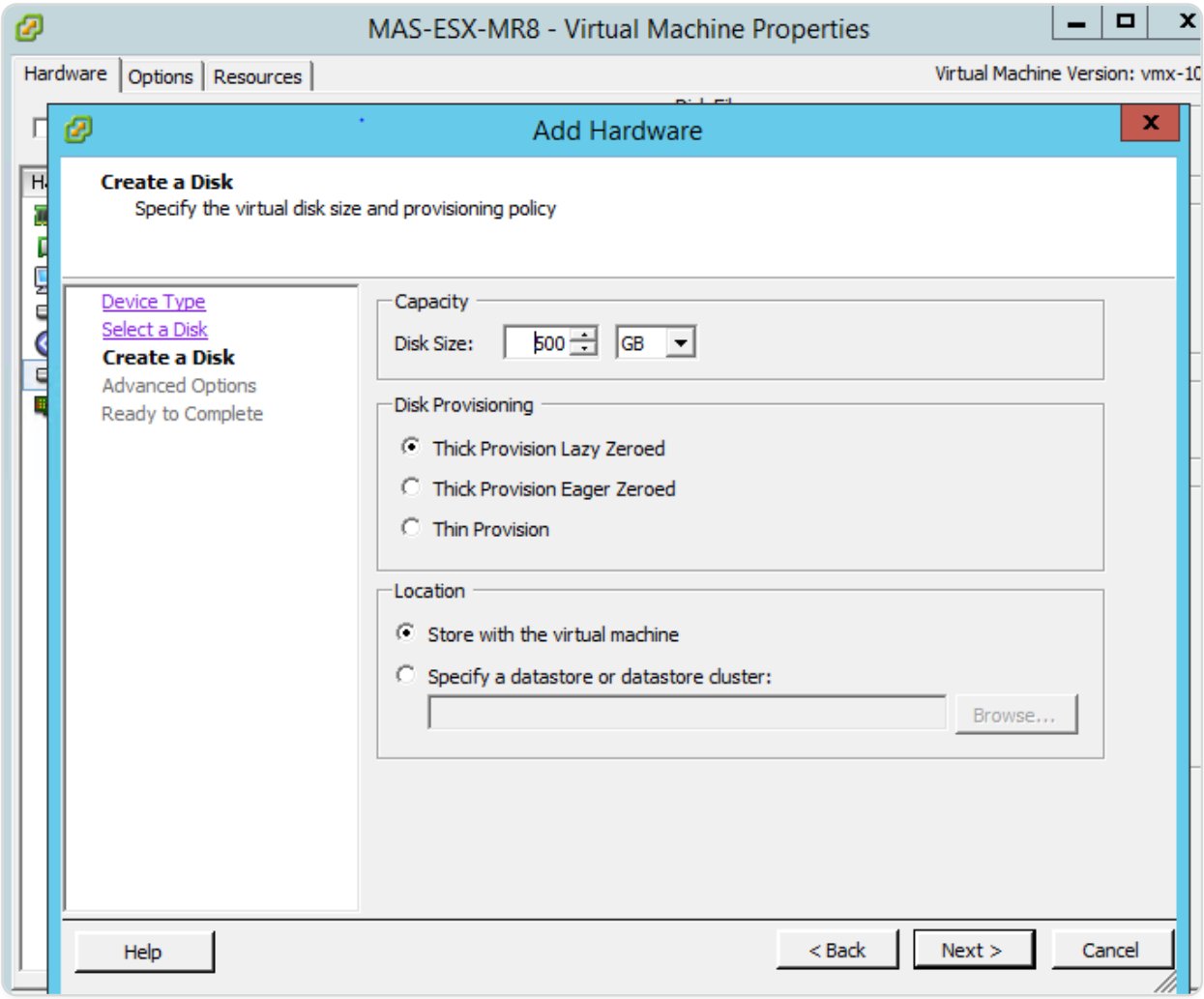
© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. 您现在可以启动 NetScaler Console 虚拟设备了。
11. 在导航窗格中，选择您安装的虚拟设备。在 **清单** 菜单中，右键单击 **虚拟机**，然后单击 **升级虚拟硬件**。在 **确认虚拟机** 对话框中，单击 **是**。



12. 在**清单**菜单中，单击**虚拟机**，然后单击**编辑设置**。
13. 在**虚拟机属性**对话框中，在**硬件**选项卡上，单击**内存**，然后在右侧窗格中将**内存大小**指定为 32 GB。
14. 单击**CPU**，然后在右侧窗格中，将 CPU 指定为 8。单击**确定**。
15. 根据您的要求添加一个额外磁盘。

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



16. 在导航窗格中，选择您安装的虚拟设备。从**清单**菜单中，单击**虚拟机**，单击**电源**，然后单击**开机**。

17. 单击**控制台**选项卡以显示 NetScaler Console 初始网络配置选项。

18. 指定所需的 IP 地址后，保存配置设置。

19. 出现提示时，使用 nsrecover/nsroot 凭据登录。

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

```
login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

bash-3.2#
```

注意

登录后，如果要更新初始网络配置，请键入 `networkconfig`，更新配置，然后保存配置。

20. 通过在 shell 提示符处键入命令来运行部署脚本：

```
deployment_type.py
```

初始配置(/en-us/netscaler-application-delivery-management-software/media/ha-deploymenttype.png)

21. 选择部署类型为 **NetScaler Console Server**。如果未选择任何选项，则默认将其部署为服务器。

初始配置(/en-us/netscaler-application-delivery-management-software/media/ha-deploymentconfig.png)

22. 键入 **Yes** 以将 NetScaler Console 部署为独立部署。
23. 键入 **Yes** 以重新启动 NetScaler Console 服务器。

注意

安装 NetScaler Console 后，您可以稍后更新初始配置设置。

验证

服务器安装完成后，您可以通过在浏览器中键入 NetScaler Console 服务器的 IP 地址来访问 GUI。登录服务器的默认管理员凭据为 nsroot/nsroot。

浏览器将显示 NetScaler Console 配置实用程序。

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

注意

NetScaler Console 在 VMware ESXi 上的典型安装时间约为 10 分钟，但在某些系统上可能需要更长时间。

在 VMware ESXi 上自动部署 NetScaler® 代理

NetScaler Console 允许您在 VMware ESXi 上自动部署 NetScaler 代理。

作为管理员，您可以自动执行以下操作：

- 配置 NetScaler 代理
- 注册 NetScaler 代理并更改代理的默认密码。

配置 NetScaler 代理

要自动配置代理，请在 .ovf 文件中添加以下参数的值：

1. `IPAddress`
2. `Netmask`
3. `Gateway`
4. `Nameserver`
5. `Hostname`

注意：

.ovf 文件在代理映像文件中。要下载 NetScaler 代理文件，请转到 `<https://www.citrix.com/downloads/citrix-application-management/>`。代理映像文件的命名模式如下：**MASAGENT-ESX-releasenumber-buildnumber.zip**

注册 NetScaler 代理并更改默认密码

注意：

在注册和更改默认密码之前，请确保您已添加 (#configure-the-netscaler-agent) 中指定的参数。

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

要自动注册 NetScaler 代理并更改默认密码，请在同一个 .ovf 文件中添加以下参数的值：

1. `NetScaler Console Server IP`
2. `NetScaler Console Username`
3. `NetScaler Console Password`
4. `Agent New Password`

先决条件

在开始安装虚拟设备之前，请确保您已完成以下操作：

- 在满足最低系统要求管理工作站上安装 VMware vSphere 8.x。
- 下载 NetScaler Console 安装文件。

如何配置和注册 NetScaler 代理

1. 下载并编辑 .OVF 文件
2. 在 VMware ESXi 上安装 NetScaler Console 虚拟设备
3. 验证

步骤 1：下载并编辑 .OVF 文件

1. 将文件从 **MASAGENT-ESX-releasenumber-buildnumber.zip** 解压到所需位置。将解压以下文件：
   - .ovf 文件
   - .vmdk 文件
   - .ova 文件
   - .mf 文件
2. 在任何编辑器中打开 .ovf 文件， 并在 `</VirtualHardwareSection>` 标签后添加以下 `<ProductSection>..</ProductSection>` 示例代码

```
<ProductSection>

<Info>Information about the installed software</Info>

<Product>Application Delivery management</Product>

<Vendor>Citrix</Vendor>
```

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

```
<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.ip">

<Label>IPAddress</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.netmask">

<Label>Netmask</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.gateway">

<Label>Gateway</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.nameserver">

<Label>Nameserver</Label>

</Property>
```

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

```
<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.hostname">

<Label>Hostname</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.ServerIP">

<Label>NetScaler Console Server IP</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:value="VALUE"
ovf:type="string"

ovf:key="eth0.ServerUname">

<Label>NetScaler Console Username</Label>

</Property>



<Property ovf:userConfigurable="true" ovf:password="true"
ovf:value="VALUE"

ovf:type="string" ovf:key="eth0.ServerPassword">

<Label>NetScaler Console Password</Label>

</Property>
```

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

```
<Property ovf:userConfigurable="true" ovf:password="true"
ovf:value="VALUE"

ovf:type="string" ovf:key="eth0.NewPassword">

<Label>Agent New Password</Label>

</Property>



</ProductSection>
```

3. 对于要配置的参数，请在 ovf:value="VALUE" 中添加其相应的值

   - 要配置 NetScaler 代理，请将值添加到以下参数：
     - `IPAddress`
     - `Netmask`
     - `Gateway`
     - `Nameserver`
     - `Hostname`
   - 要注册并更改 NetScaler 代理的默认密码，请将值添加到以下参数：
     - `NetScaler Console Server IP`
     - `NetScaler Console Username`
     - `NetScaler Console Password`
     - `Agent New Password`

注意：

- 在注册并更改代理的默认密码之前，必须配置 NetScaler 代理。
- 如果未在 .ovf 文件中注册并更改默认密码，请在部署 VM 后手动执行这些操作。

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

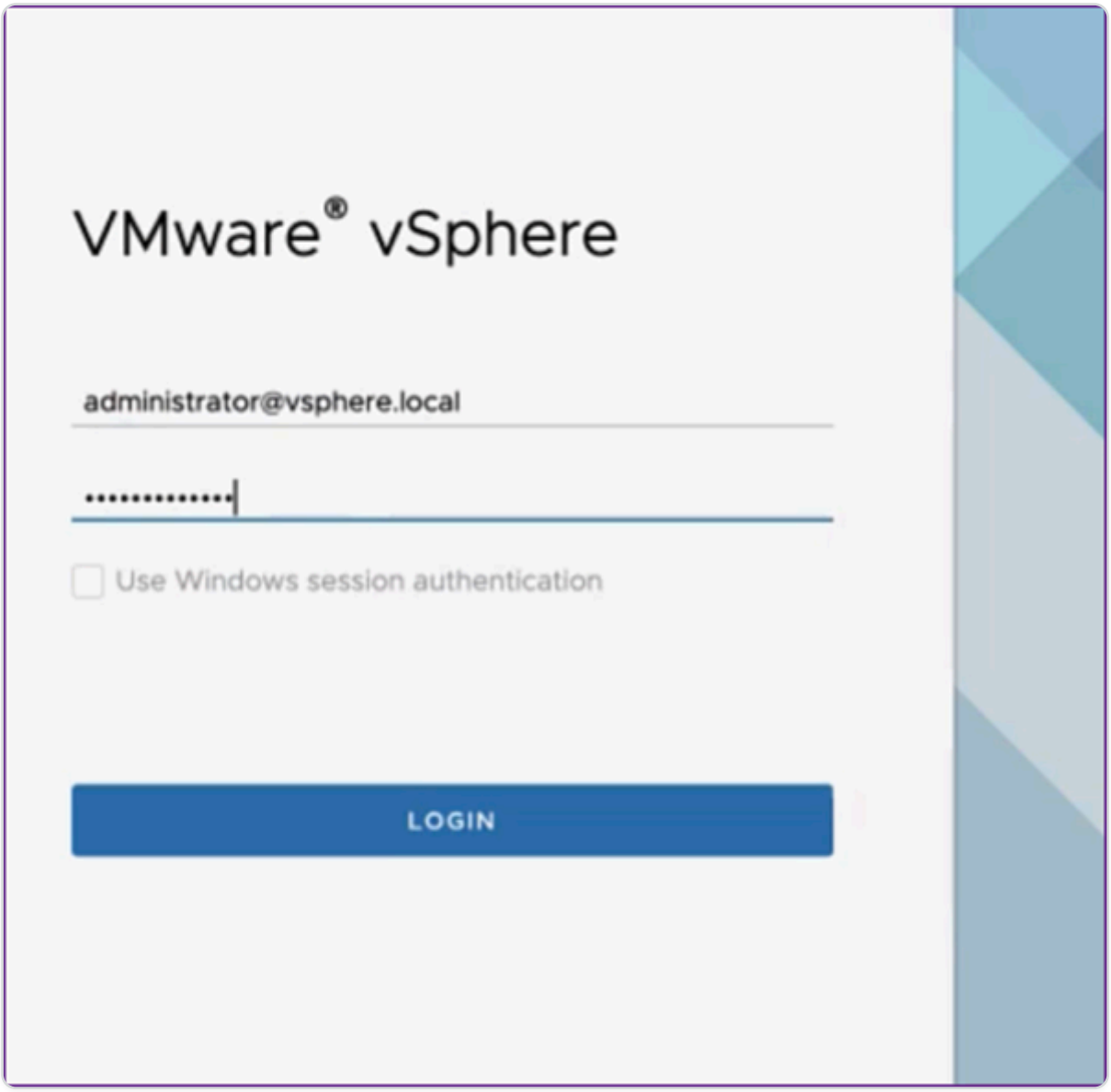
```
  <Property ovf:key="guestinfo.ovfEnvTransport" ovf:value="com.vmware.guestInfo"/>
</VirtualHardwareSection>
<ProductSection>
  <Info>Information about the installed software</Info>
  <Product>Application Delivery management</Product>
  <Vendor>Citrix</Vendor>
  <vssd:Transport ovf:required="true">
    <vssd:TransportName>com.vmware.guestInfo</vssd:TransportName>
  </vssd:Transport>
  <Property ovf:userConfigurable="true" ovf:value="10.106.100.98" ovf:type="string" ovf:key="eth0.ip">
    <Label>IPAddress</Label>
    <Description/>
  </Property>
  <Property ovf:userConfigurable="true" ovf:value="255.255.255.0" ovf:type="string" ovf:key="eth0.netmask">
    <Label>Netmask</Label>
    <Description/>
  </Property>
  <Property ovf:userConfigurable="true" ovf:value="10.106.100.1" ovf:type="string" ovf:key="eth0.gateway">
    <Label>Gateway</Label>
    <Description/>
  </Property>
  <Property ovf:userConfigurable="true" ovf:value="10.105.99.99" ovf:type="string" ovf:key="eth0.nameserver">
    <Label>Nameserver</Label>
    <Description/>
  </Property>
  <Property ovf:userConfigurable="true" ovf:value="admagent" ovf:type="string" ovf:key="eth0.hostname">
    <Label>Hostname</Label>
    <Description/>
  </Property>
  <Property ovf:userConfigurable="true" ovf:value="10.106.100.50" ovf:type="string" ovf:key="eth0.ServerIP">
```

4. 添加参数及其值后，保存 .ovf 文件。

步骤 2：在 VMware ESXi 上安装 NetScaler Console 虚拟设备

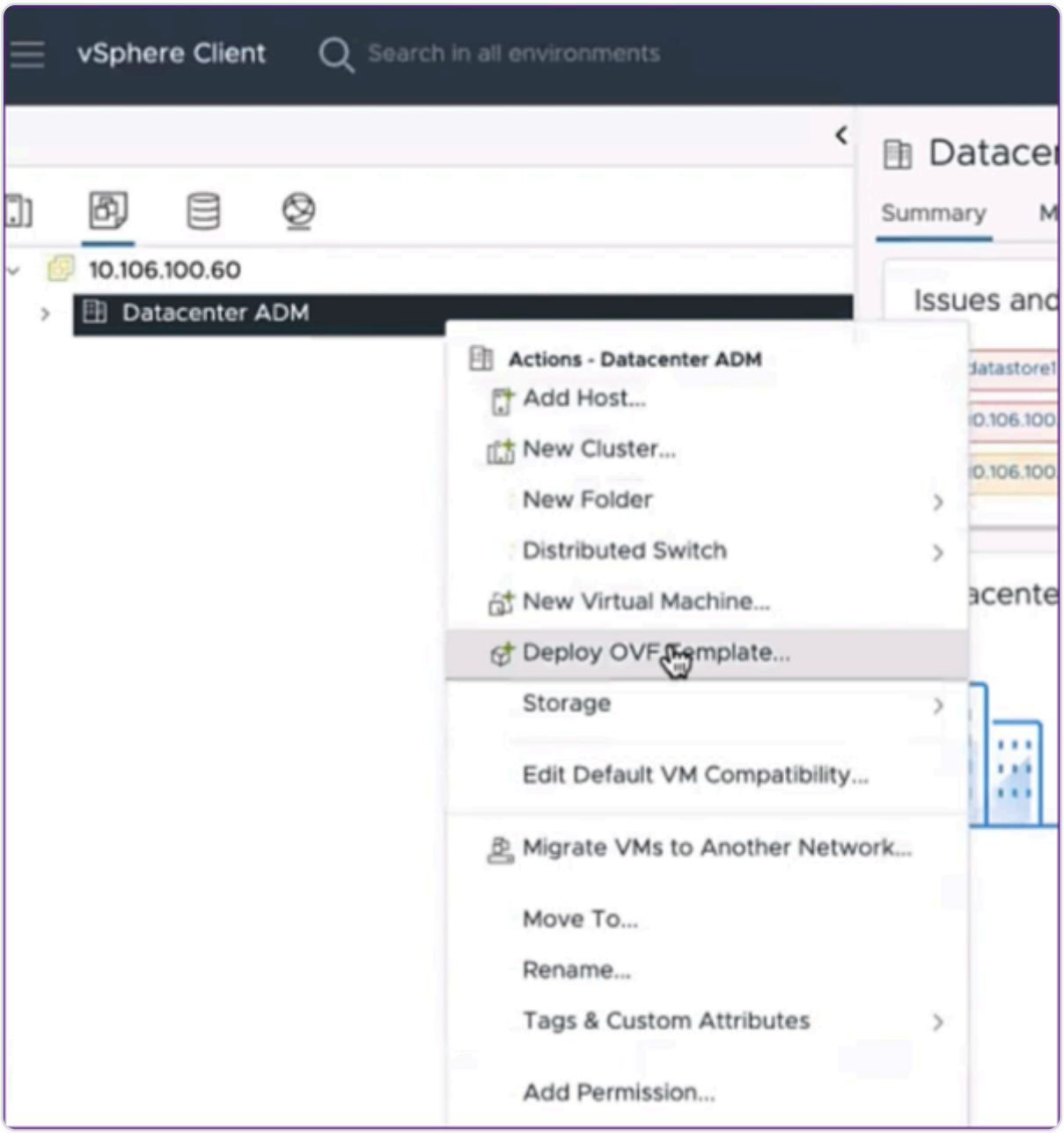
1. 登录到 **VMWare vSphere Client** 并键入管理员凭据。单击 **Login**。

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



2. 选择您的 ESXi 服务器，然后右键单击以选择 **Deploy OVF Template**。

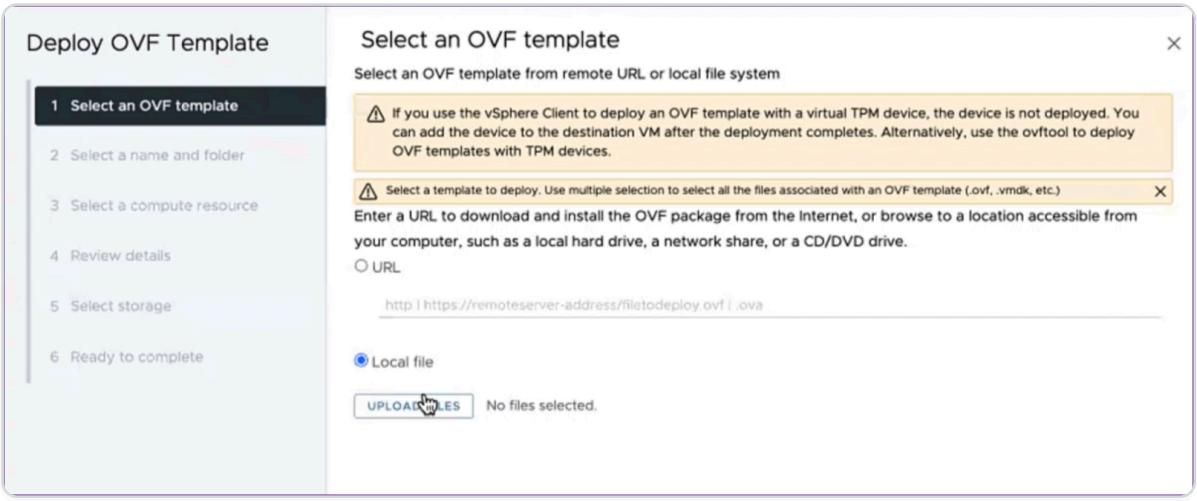
© 1997–2026 Citrix Systems, Inc. All rights reserved.



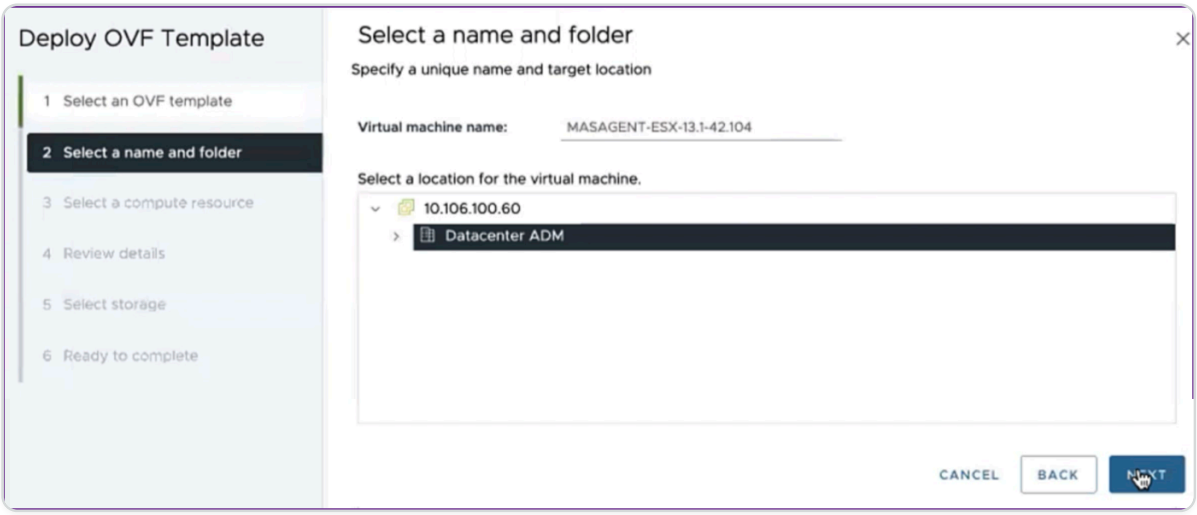
3. 在 **Deploy OVF Template** 页面中：

   a. **选择 OVF 模板**：选择**本地文件**，然后导航到您保存已编辑的 .ovf 文件和 .vmdk 文件的位置。选择这些文件，然后单击**打开**以上传它们。单击**下一步**。

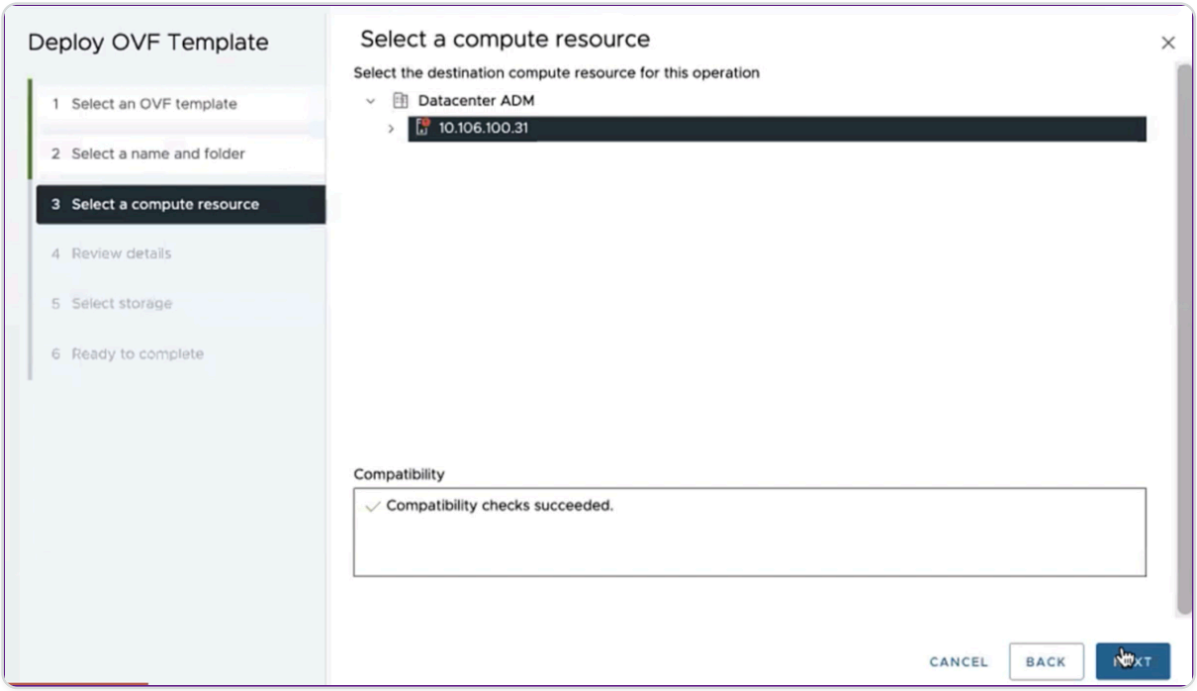
© 1997–2026 Citrix Systems, Inc. All rights reserved.



b. **选择名称和文件夹**：为虚拟设备添加名称，然后选择要在 ESXi 上部署虚拟机的位置。单击**下一步**。

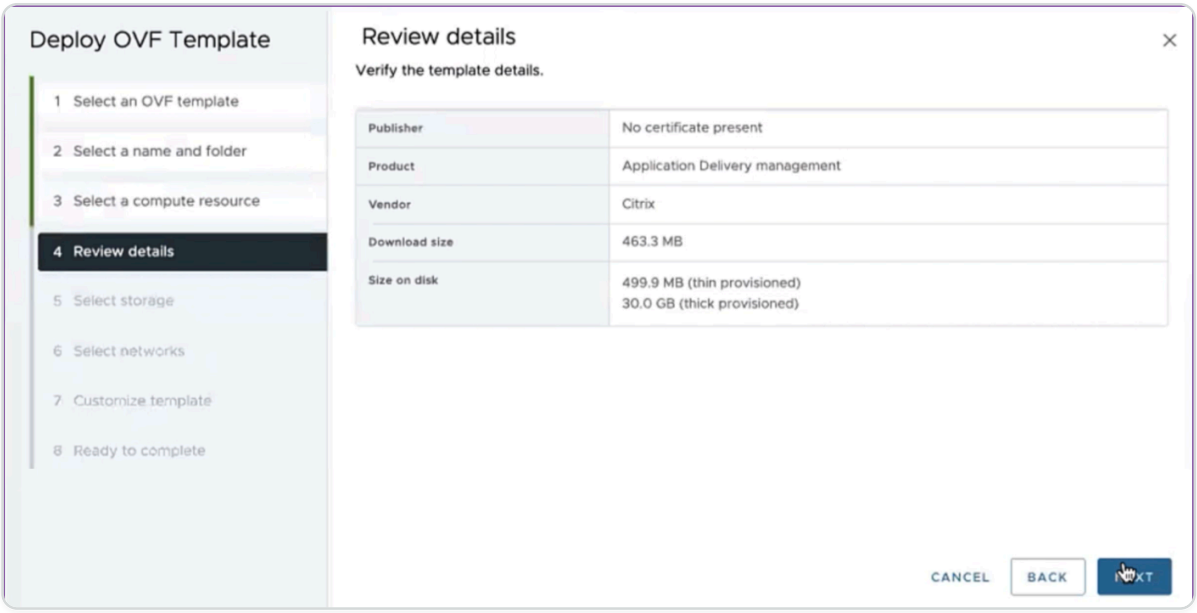


c. **选择计算资源**：选择部署模板后要在其上运行的资源。单击**下一步**。

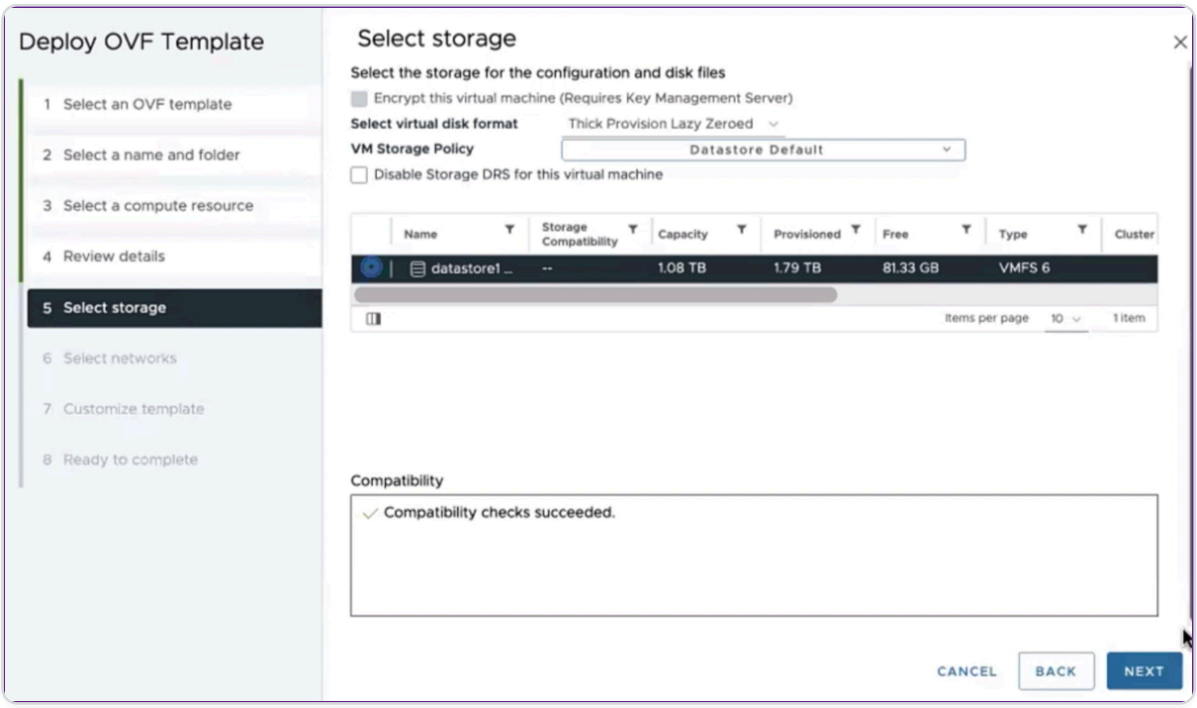


© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. **审查详细信息**：验证 OVF 模板详细信息。单击**下一步**。

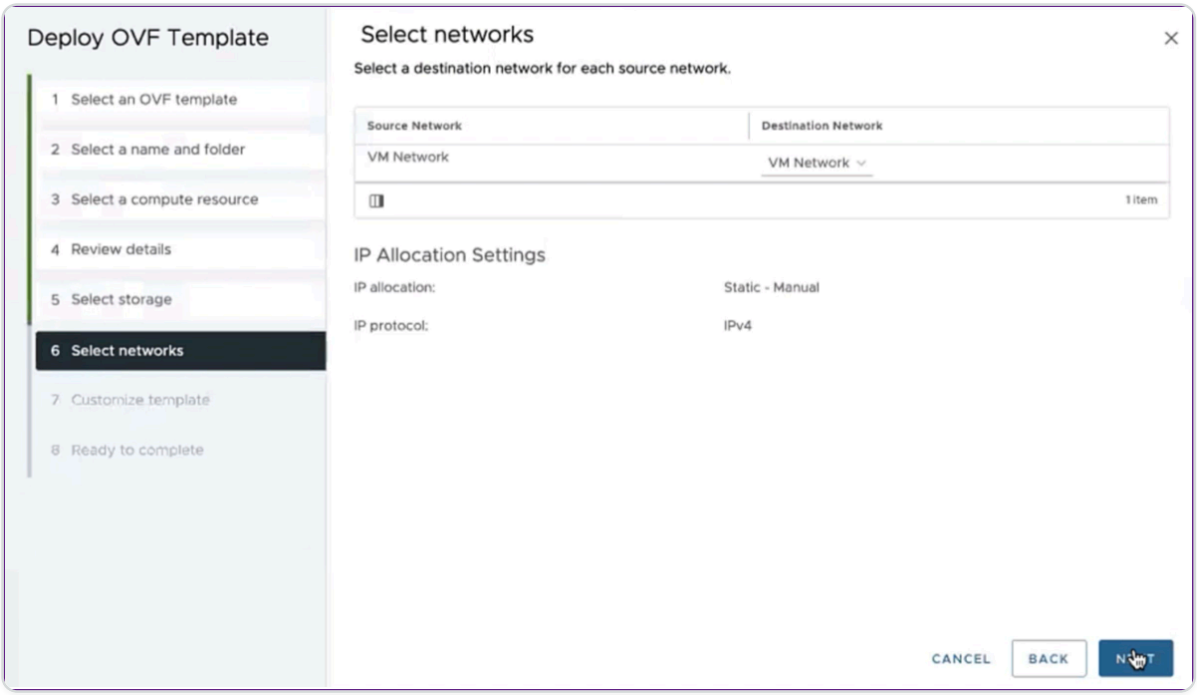


e. **选择存储**：选择一个数据存储来存储 OVF 模板。单击**下一步**。

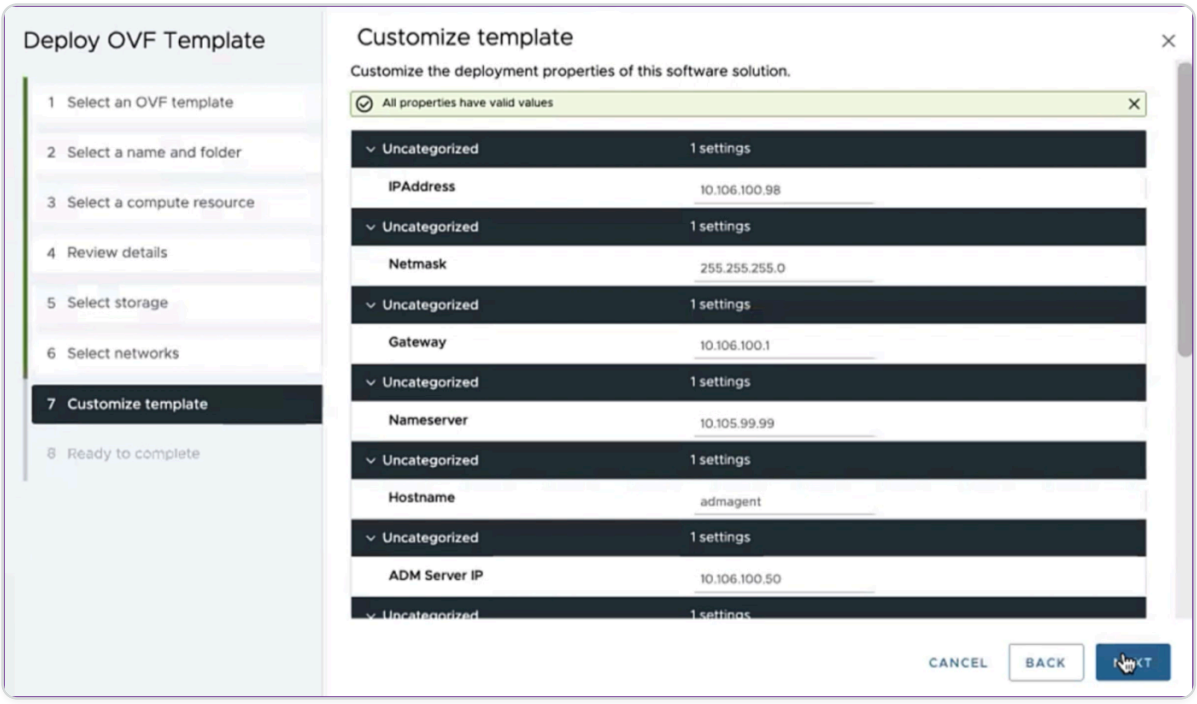


f. **选择网络**：继续使用默认设置。单击**下一步**。

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

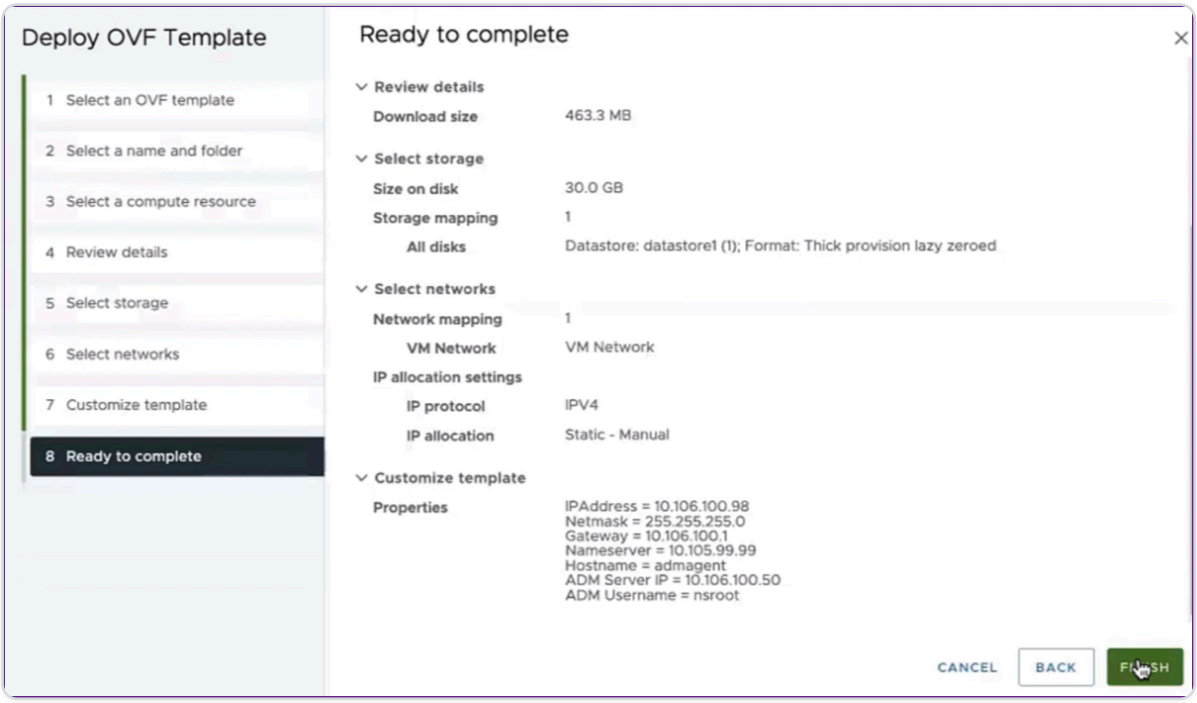


g. **自定义模板**：审查 OVF 模板的所有属性。在 下载并编辑 .OVF 文件 部分中，您在 .ovf 文件中添加的所有参数和值都将显示。

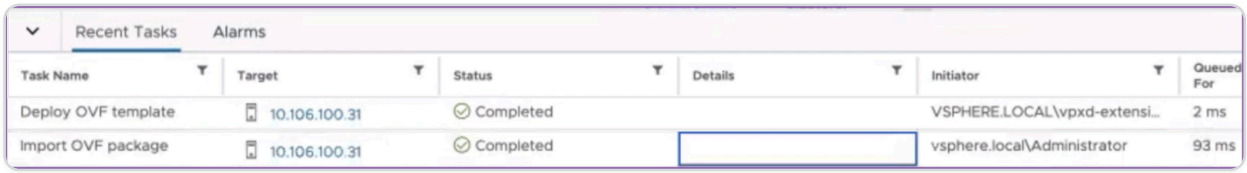


h. **准备完成**：要保存设置并开始部署过程，请单击**完成**。

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



等待部署完成。在“**部署 OVF 模板**”操作状态为 100% 完成后，您的代理即已部署。

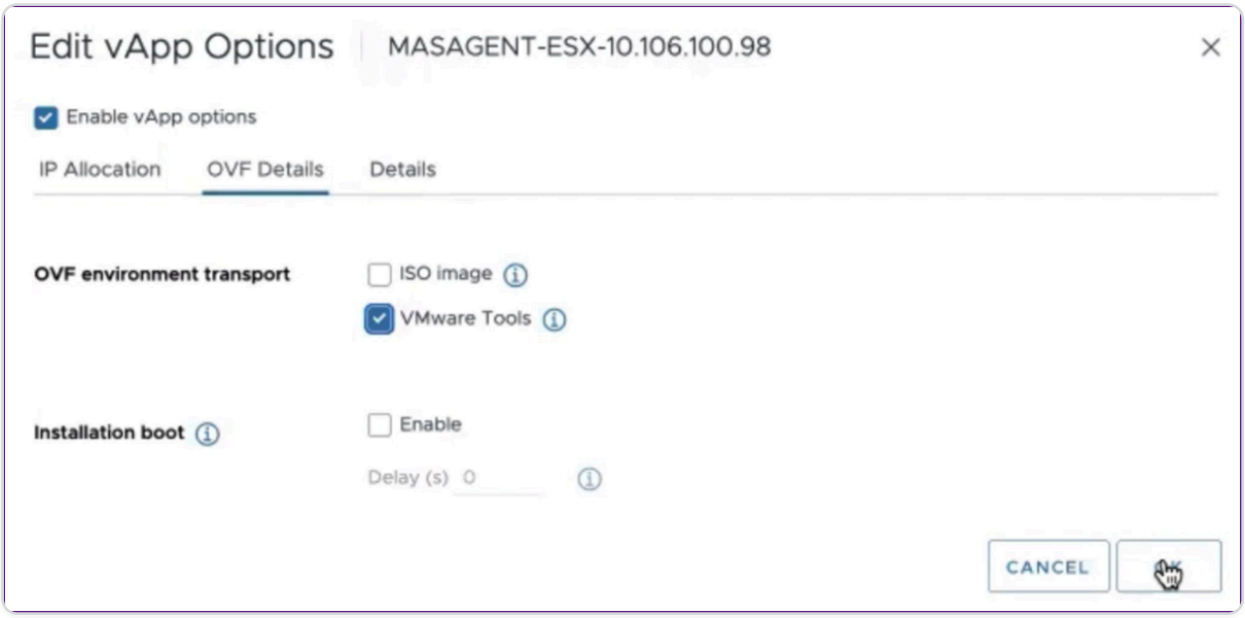


重要提示：

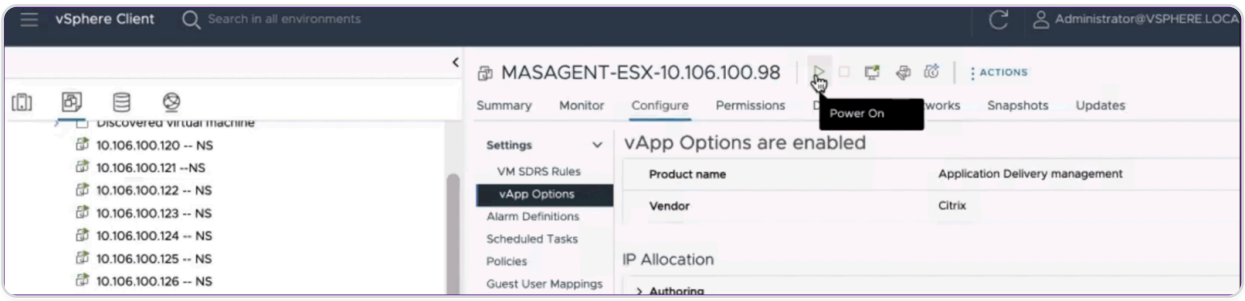
在编辑设置之前，请勿启动虚拟设备。

4. 单击您安装的新虚拟设备，然后导航到“**配置 > 设置 > vApp 选项 > 编辑**”。
5. 在“**编辑 vApp 选项**”窗口中，导航到“**在 OVF 详细信息 > OVF 环境传输**”，然后选择“**VMware Tools**”。单击“**确定**”。

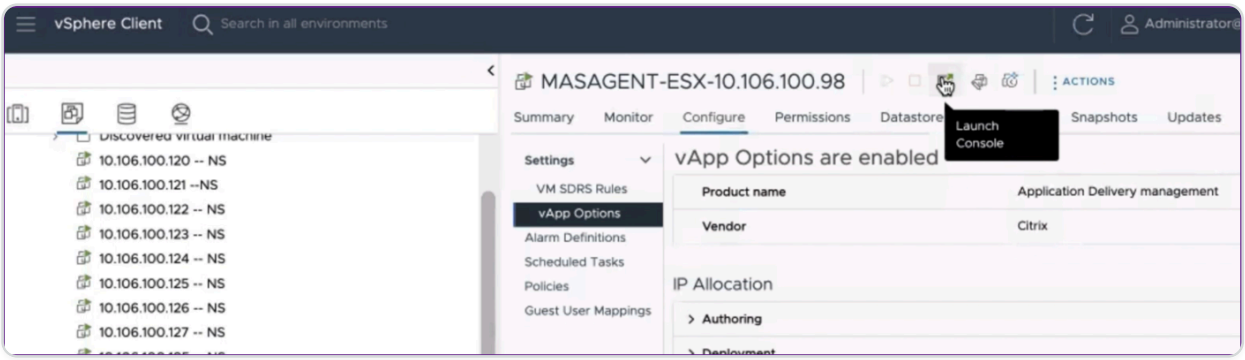
© 1997–2026 Citrix Systems, Inc. All rights reserved.



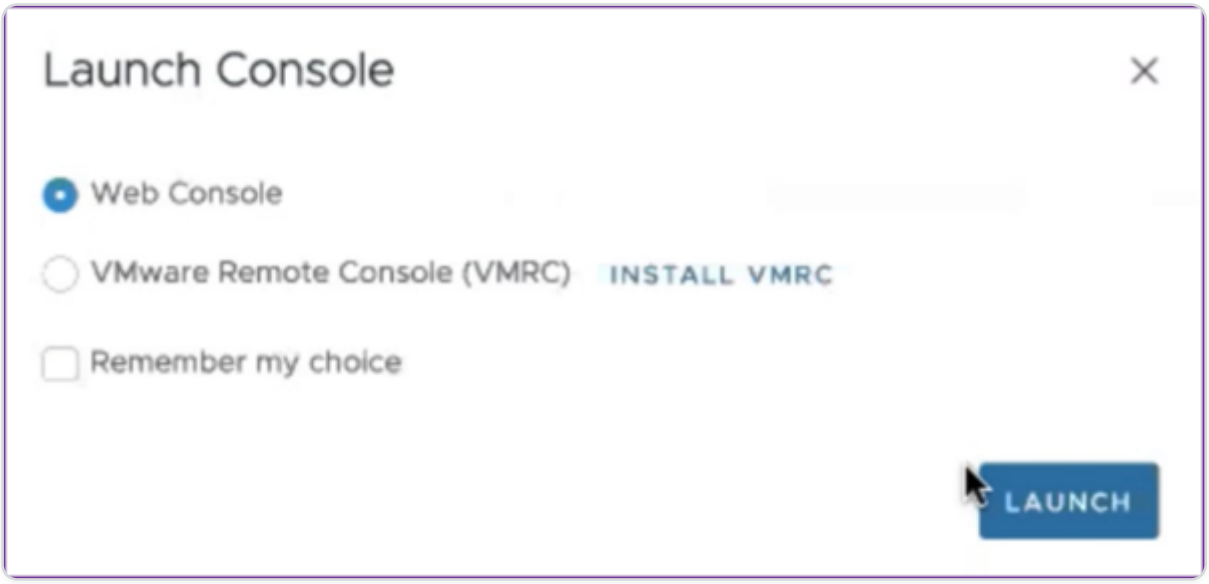
6. 右键单击虚拟机，然后单击“**启动**”。或者，您可以选择虚拟机的“**摘要**”选项卡，然后单击“**启动**”。



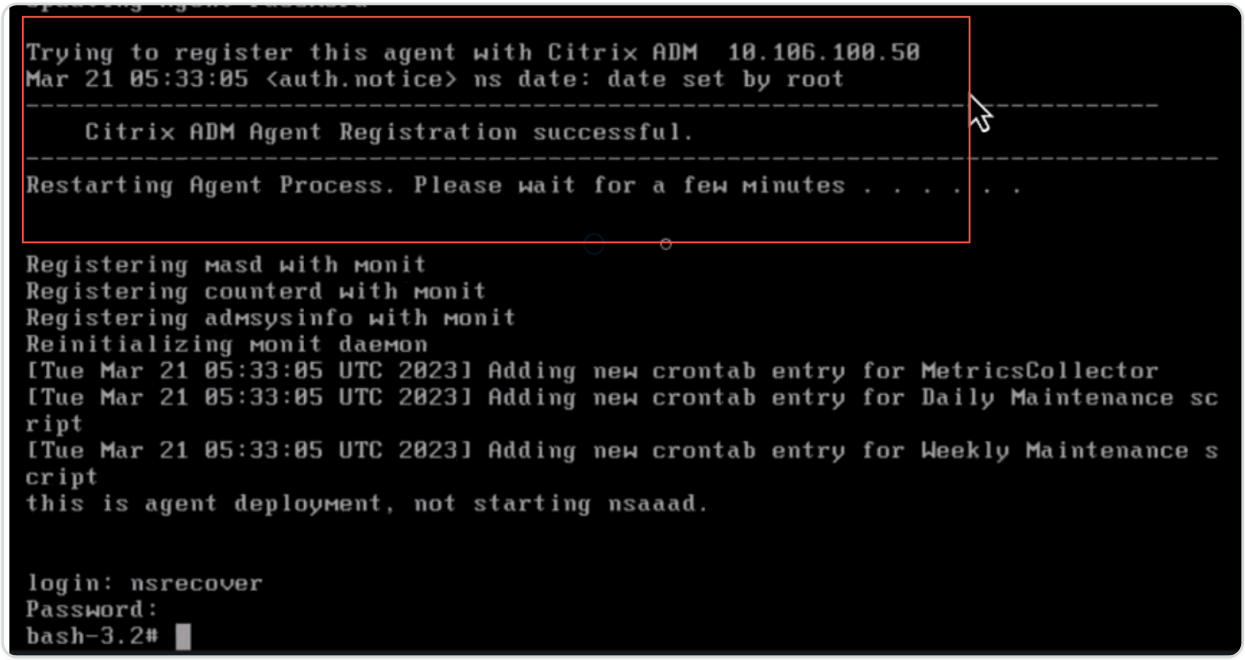
7. 在“**摘要**”选项卡中，选择“**启动 Web 控制台**”。 在“**启动控制台**”窗口中，选择“**Web 控制台**”。单击“**启动**”。



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



8. 在控制台中，NetScaler 代理注册到 NetScaler Console 服务器后，将显示一条成功注册消息。要验证 NetScaler 代理是否已部署且默认密码已更改，请使用 NetScaler 代理 用户名和新密码登录。



步骤 3: 验证

要验证 NetScaler 代理已部署：

1. NetScaler 代理部署后，通过在浏览器中键入 NetScaler Console 服务器的 IP 地址来访问 NetScaler Console GUI。
2. 使用您的凭据登录服务器。
3. 导航到 **Infrastructure > Instances > Agents**。 新部署的代理将显示在 ESX 平台上。

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

Kubernetes 集群上的 NetScaler Console

在 Kubernetes 集群上安装 NetScaler Console 虚拟设备之前，请阅读先决条件部分。

先决条件

在安装 NetScaler Console 之前，请确保满足以下先决条件。

Kubernetes 集群

- Kubernetes 集群必须是以下版本或更高版本：
  - 服务器版本 v1.20
  - 客户端版本 v1.20

  键入命令 `kubectl version` 以检查版本。
- 集群上安装的 Helm 应用程序的客户端版本必须为 v3.4.0 或更高版本。

  使用命令 `helm version` 检查版本。
- Kubernetes 集群 CNI (Container Network Interface) 必须是 Calico v3.21.1 或更高版本。
- 集群中的所有从属节点都必须安装 NFS 客户端。这是因为 NetScaler Console 应用程序将数据和配置持久化到挂载在网络文件服务器上的卷中。要在基于 Ubuntu 的从属节点上安装 NFS 客户端，请键入以下命令：

`apt-get update` `apt install nfs-common`

- NetScaler Console 应用程序需要 32 GB 内存、8 个 vCPU（跨集群）以及 NFS 上 120 GB 的空间。

NFS 共享

NetScaler Console 应用程序需要持久卷来存储配置、证书、镜像等数据。为此，NetScaler Console 需要 NFS 挂载。该应用程序需要共享网络挂载中的两个文件夹：

- 一个用于存储证书、镜像等文件
- 另一个用于数据库

注意

> 建议使用带有 SSD 的 NFS。

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

这两个文件夹可以不同，也可以相同。两个文件夹都必须具有 777 权限。第一个文件夹必须至少有 10 GB 空间。第二个文件夹的大小取决于需要持久化到数据库中的数据量。最小大小为 100 GB。对于生产环境，我们建议使用生产级 NFS 解决方案。

NetScaler 设备

NetScaler 设备作为入口设备是必需的。NetScaler 使所需的应用程序服务在 Kubernetes 集群外部可用。NetScaler 设备必须位于 Kubernetes 集群外部，并且工作节点必须可从 NetScaler 访问。执行以下步骤：

- 在 NetScaler 上配置一个 SNIP。NetScaler 使用此 SNIP 访问 Kubernetes 集群的工作节点。
- 确定一个空闲 IP 地址，用作虚拟服务器 IP 地址，以使所需的应用程序服务在 Kubernetes 集群外部可用。

在 Kubernetes 集群上安装 NetScaler Console

按照以下步骤在 Kubernetes 集群上安装 NetScaler Console 设备：

1. 访问 NetScaler 站点 并下载适用于 Kubernetes 的 NetScaler Console Helm Chart 文件。
2. 将下载的 Helm Chart tarball 解压到 Kubernetes 集群主节点的 /var 目录中。
3. 在 `/var/citrixadm` 目录下打开 `values.yaml` 文件。
4. 在文件中 `dbpasswd` 字段中输入数据库密码。
5. 更改以下值。NetScaler Console 应用程序使用这些值来配置 NetScaler 设备，以便服务暴露给外部世界：
   - `ingressIP`：在 NetScaler 中配置的用于访问应用程序的虚拟 IP。
   - `applicationID`：一个唯一 ID，用于将入口配置与 NetScaler 设备上的其余配置区分开来。
   - `ingressADCIP`：NetScaler IP 地址 (NSIP)，用作 NetScaler Console 应用程序的入口。
   - `ingressADCUsername`：用于访问 NetScaler 设备的用户名称。此用户必须具有写入权限。
   - `ingressADCPassword`：用户名的密码。

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

```
# ingressIP is the Virtual IP configured in the Citrix ADC for accessing the application
ingressIP: "xx.xx.xx.xx"

# coreDumpFilePath is the directory on slave nodes of the cluster which will be used to store core dumps files in case
application runs into faulty state
# this setting is optional
# Admin needs to create this directory on each of the slave nodes and then run the command: "echo <coreDumpFilePath_value>/
core.%h.%e.%p > /proc/sys/kernel/core_pattern"
coreDumpFilePath: "/var/mps/cores"

# applicationID is the identifier for ingress configuration
applicationID: "citrixadm"

# ingressADCIP is the NSIP of the northbound ADC used to expose the ADM application to the outside world
ingressADCIP: "xx.xx.xx.xx"

# ingressADCUsername is the username of the northbound ADC
ingressADCUsername: "nsroot"

# ingressADCUsername is the password for above username
ingressADCPassword: "nsroot"
```

6. 更改 **storage** 部分中的以下值。这些值指定了存储 NetScaler Console 应用程序所需文件所需的持久性。

   - `nfsServer`：NFS 服务器的主机名或 IP 地址
   - `path`：用于存储应用程序文件的文件夹的挂载路径。
   - `size`：至少 10 GB。

   注意

   > 此值的单位是 Gi。例如，10Gi、20Gi。

7. 导航到 `pg-datastore` 下的 **存储** 部分，并更改以下值。这些值指定了用于创建数据库的持久性。

   - `nsfServer`：NFS 服务器的主机名或 IP 地址。
   - `size`：挂载用于数据存储的文件夹路径。
   - `path`：至少 100 GB。

   注意

   > 此值的单位是 Gi。例如，100Gi、200Gi。

8. 转到主节点中的 /var/citrix 目录，并运行以下命令以安装 NetScaler Console 应用程序：`helm install -n citrixadm --namespace <name> ./citrixadm`

   注意

   > 此 helm 命令在 helm 3.x 版本中不受支持。

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

此命令还会在您的集群中安装所需的 Pod。命名空间参数是可选的。如果未提供命名空间，Helm 会将 NetScaler Console 安装在默认命名空间中。为了便于管理，请将 NetScaler Console 安装在单独的命名空间下。

9. 打开浏览器并键入 `http://< virtual server IP address >`，然后使用 `nsroot/nsroot` 作为凭据登录到 NetScaler Console。对于安全访问，请键入 `https://< virtual server IP address >`。

注意

> 在部署期间，NetScaler Console 应用程序会在数据存储中创建表，这可能需要一些时间。根据 Kubernetes 为 NetScaler Console 应用程序的各个 Pod 分配的资源，服务启动可能需要 5-15 分钟。

Linux KVM 服务器上的 NetScaler Console

可以预配 NetScaler Console 的虚拟化平台包括 Linux-KVM。

在 Linux-KVM 上安装 NetScaler Console 之前，请确保您的系统具有硬件虚拟化扩展，并验证 CPU 虚拟化扩展是否可用。验证管理程序上是否提供了 `virsh`（用于管理虚拟机的命令行工具）。

使用您的管理员凭据登录 Citrix.com 网站，访问最新的 NetScaler Console 安装文件，并将其下载到您的计算机上。然后，在您的 Linux-KVM 平台上安装 NetScaler Console 并为您的网络进行配置。

先决条件

在安装 NetScaler Console 虚拟设备之前，请验证 Linux-KVM 3.6.11-4 或更高版本是否已安装在满足最低要求的硬件上。

硬件要求

组件	要求
CPU	具有 Intel VT-X 处理器中包含的硬件虚拟化功能的 64 位 x86 处理器。为托管 Linux-KVM 提供至少 2 个 CPU 核心。**注意** 要测试您的 CPU 是否支持 Linux 主机，请在主机 Linux shell 提示符下输入以下命令：`*. egrep'\^flags.* ( vmx | svm ) '/proc/cpuinfo*`。如果扩展的 BIOS 设置已禁用，则必须在 BIOS 中启用

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

组件	要求
	它们。对处理器速度没有具体建议，但速度越高，NetScaler Console 的性能越好。
内存 (RAM)	主机 Linux 内核至少需要 4 GB 内存。根据 VM 的要求添加额外内存。
硬盘	计算主机 Linux 内核和 VM 要求的空间。单个 NetScaler Console VM 需要 120 GB 磁盘空间。

注意

指定的内存和硬盘要求适用于在 OpenStack 平台上部署 NetScaler Console，前提是主机上没有运行其他虚拟机。OpenStack 的硬件要求取决于其上运行的虚拟机数量。

软件要求

我们建议使用较新的内核，例如 64 位版本的 3.6.11-4 内核或更高版本。

网络要求

NetScaler Console 仅支持一个 virtIO 半虚拟化网络接口。请确保将此接口连接到 Linux-KVM 主机的管理网络，以便 NetScaler Console 和 Linux-KVM 可以通信。

下载 NetScaler Console 安装文件

要从 `www.citrix.com` 下载 NetScaler Console 安装文件，请执行以下操作：

1. 打开 Web 浏览器并在地址栏中键入 www.citrix.com。
2. 将鼠标悬停在“**登录**”选项上，然后单击“**我的帐户**”，输入您的 Citrix 凭据，然后再次单击“**登录**”。
3. 导航到“**下载**”部分。
4. 从“**下载**”列表中，选择“**NetScaler® Application Delivery Management**”。
5. 在“**NetScaler Application Delivery Management**”页面上，选择版本。例如，选择“**Release 13.0**”。
6. 单击“**产品软件**”以展开它，然后单击最新版本。例如，选择“**NetScaler MAS Release (Feature Phase) 13.0 Build 36.27**”。

   将显示所选版本页面。

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

7. 在“**跳转到下载**”列表中，选择“**适用于 KVM 的 NetScaler MAS 映像，13.0 Build xx.xx**”
8. 单击“**下载文件**”，接受 EULA，并将压缩映像文件下载到本地计算机上的任意文件夹。

在 Linux-KVM 上安装 NetScaler 应用交付管理

1. 使用 SSH 登录到 KVM 主机。
2. 在 CLI 提示符下，使用任何文件传输程序将映像复制到服务器上的文件夹。
3. 导航到您已保存下载映像的目录。
4. 在命令行执行以下操作：
   a. 列出目录中的文件，验证映像文件是否存在。
   b. 使用 tar 命令解压 NetScaler Application Delivery Management 映像文件。解压后的软件包包含以下组件：
      i. 一个指定 NetScaler Console 属性的域 XML 文件
      ii. 一个指定域磁盘映像校验和的文本文件
      iii. 一个域磁盘映像

```
tar -xvfz MAS-KVM.tgz

MAS-KVM.xml

MAS-KVM.qcow2

checksum.txt
```

      一个域磁盘映像(/en-us/netscaler-application-delivery-management-software/media/netscaler-mas-linux-kvm-1.png)

      iv. 将 MAS-KVM.xml 复制为 MAS1-KVM.xml，作为备份选项。使用 vi 编辑器打开 MAS1-KVM.xml 文件。
      v. 编辑 MAS1-KVM.xml 以配置以下网络属性：
         i. `name` - 指定名称。
         ii. `mac` - 指定 MAC 地址。
         iii. `source file` - 指定绝对磁盘映像源路径。文件路径必须是绝对路径。

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

> **注意**
>
> 域名和 MAC 地址必须是唯一的。

iv. `mode` - 指定模式。

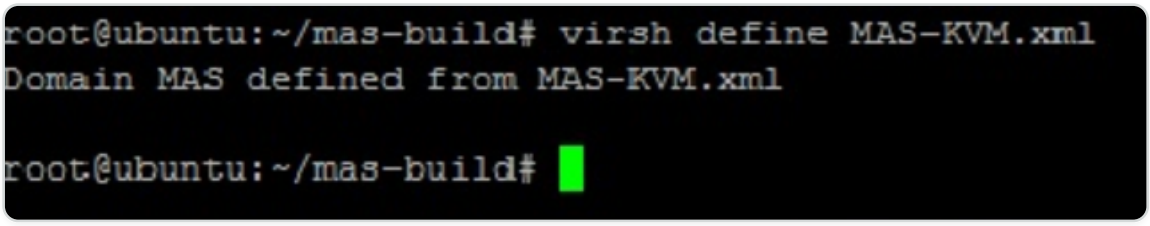
v. `model type` - 设置为 virtIO。

vi. `source dev` - 指定接口。

```
<name> MAS1-KVM</name>

<mac address='52:54:00:29:74:b3'/>

<source file='/var/ MAS-KVM.qcow2'/>

<source dev='eth0' mode='bridge'/>

<model type='virtio'/>
```

vi. 使用以下命令在 MAS1-KVM.xml 文件中定义 VM 属性：`virsh define \<FileName\>.xml`

```
virsh define MAS-KVM.xml

Domain MAS defined from MAS-KVM.xml
```



vii. 通过输入以下命令启动 NetScaler Console：`virsh start \[\<DomainName\> | \<DomainUUID\>\]`

```
virsh start MAS

Domain MAS started
```

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

```
root@ubuntu:/home/mas-build# virsh start MAS
Domain MAS started

root@ubuntu:/home/mas-build#
```

viii. 您可以使用以下命令连接到 NetScaler Console 虚拟机：`virsh console \<DomainName\>`

```
virsh console MAS

Connected to domain MAS

Escape character is ^]
```

```
root@ubuntu:/home/mas-build# virsh console MAS
Connected to domain MAS
Escape character is ^]
```

配置 NetScaler 应用交付管理

注意

在某些 Linux KVM 主机上，如果 FreeBSD 访客虚拟机具有多个 CPU，则无法正常重启。当 NetScaler Console 虚拟设备重启时，NetScaler Console CLI 和 GUI 会变得无响应。有关详细信息，请参阅 `<https://bugs.launchpad.net/qemu/+bug/1329956>`

为避免 NetScaler Console 虚拟设备重启时 NetScaler Console CLI 和 GUI 变得无响应，请关闭 KVM 主机上的所有虚拟机，并在 KVM 主机上执行以下操作：

1. 使用以下命令移除 kvm_intel 模块：`rmmod kvm\_intel`
2. 使用以下命令禁用 **APICv** 并重新加载 kvm_intel 模块：`modprobe kvm\_intel enable\_apicv=N`
3. 启动 KVM 主机上的虚拟机。

安装 NetScaler Console 后，请等待大约 10 分钟，直到服务可用，然后登录 NetScaler Console。

1. 在命令行中，使用默认系统管理员凭据登录系统：

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

- 用户名：`nsroot`
- 密码：`nsroot`

注意

首次登录后，请更改管理员密码。然后，配置 MAS 以在您的网络中运行。您可以从 NetScaler Console 用户界面更改密码。在 NetScaler Console 主页上，导航到 **Settings > User Administration > Users**。选择用户并单击 **Edit**，然后在 Password 字段中更新密码。

2. 在提示符下，键入：*shell*
3. 键入 **networkconfig** 以进入 NetScaler Console 初始网络配置菜单。配置管理 IP 地址。
4. 要完成 NetScaler Console 的初始网络配置，请按照提示操作。控制台显示 NetScaler Console 的初始网络配置选项，用于设置 NetScaler Console 的以下参数。主机名默认已填充。

   a. 输入 **2** 以更新 NetScaler Console IPv4 地址 - 您访问 NetScaler Console 的管理 IP 地址

   b. 输入 **3** 以更新子网掩码 - 与管理 IP 地址关联的子网掩码

   c. 输入 **4** 以更新网关 IPv4 地址 - NetScaler Console 管理 IP 地址子网的默认网关 IP 地址

   d. 输入 **7** 以保存并退出 - 保存您的配置更改并退出系统。

```
-----------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-----------------------------------------------------------------------
      1. Citrix ADM Host Name [ADMHA1]:
      2. Citrix ADM IPv4 address [10.102.29.52]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

Select a menu item from 1 to 7 [7]:
```

5. 在 shell 提示符下键入命令以运行部署脚本：`deployment_type.py`
6. 在出现的部署屏幕中，选择部署类型为 **NetScaler Console 服务器**。

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

```
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

7. 键入 **Yes** 以将 NetScaler Console 部署为独立部署。
8. 键入 **Yes** 以重新启动 NetScaler Console 服务器。
9. NetScaler Console 服务器重新启动后，通过命令行或 GUI 使用默认管理员凭据 nsroot/nsroot 登录到 NetScaler Console。

   您稍后可以通过在浏览器地址栏中键入 NetScaler Console 服务器的 IP 地址来访问 NetScaler Console。登录服务器的默认管理员凭据是 *nsroot/nsroot*。

NetScaler Console 在 Nutanix 虚拟机监控程序 (Acropolis) 上

注意：

此功能在版本 14.1-38.xx 及更高版本中可用。

您可以使用 KVM 软件映像在 Nutanix 虚拟机监控程序上配置 NetScaler® Console 服务器。在开始之前，请确保您已配置 Nutanix Prism 以创建 NetScaler Console 的 VM。

硬件要求

组件	要求
CPU	64 位 x86 处理器，具有 Intel VT-X 处理器中包含的硬件虚拟化功能。提供至少 8 个 CPU 核心以托管 Linux-KVM。
内存 (RAM)	主机 Linux 内核最低 4 GB。根据 VM 的要求添加额外内存。

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

组件	要求
硬盘	计算主机 Linux 内核和 VM 要求的空间。单个 NetScaler Console VM 需要 120 GB 磁盘空间。

下载 NetScaler Console 安装文件

要下载 NetScaler Console 安装文件：

1. 登录 www.citrix.com/downloads 页面。
2. 从产品列表中选择 **NetScaler Console**。
3. 在 **Release 14.1** 下，选择 14.1-38.x 或更高版本。

   将显示所选版本页面。
4. 在 **Jump to Download** 列表中，选择 **Citrix ADM image for KVM, 14.1 Build xx.xx**
5. 单击 **Download File**，接受 EULA，并将压缩映像文件下载到本地计算机上的任何文件夹。

在 Nutanix 管理程序上配置 NetScaler Console

1. 解压 `.tgz` 文件。
2. 登录到 Nutanix Prism。
3. 导航到 **Settings** 并选择 **Image Configuration**。

   a. 指定映像名称。

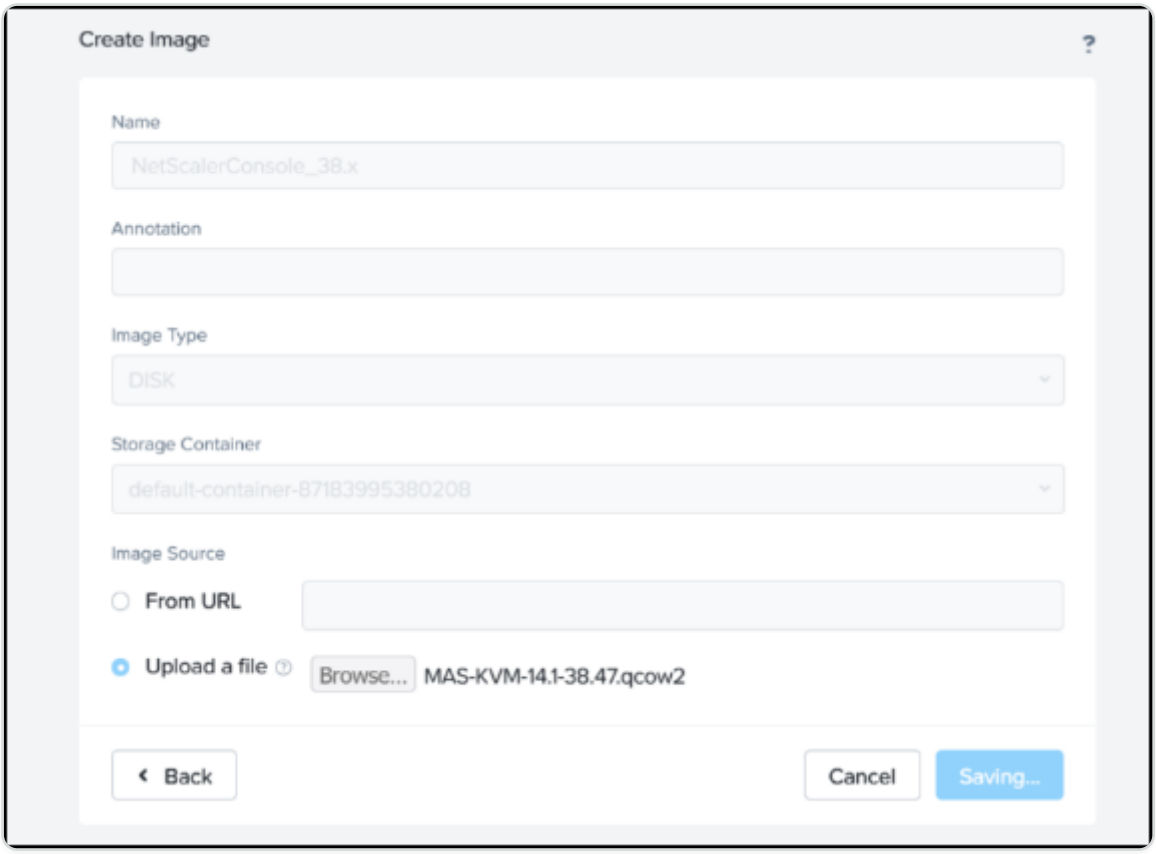
   b. 选择 **DISK** 作为映像类型。

   c. 选择存储容器。

   d. 在 **Image Source** 中，选择“上传文件”，并上传扩展名为 `.qcow2` 的文件。

   e. 单击 **Save**。

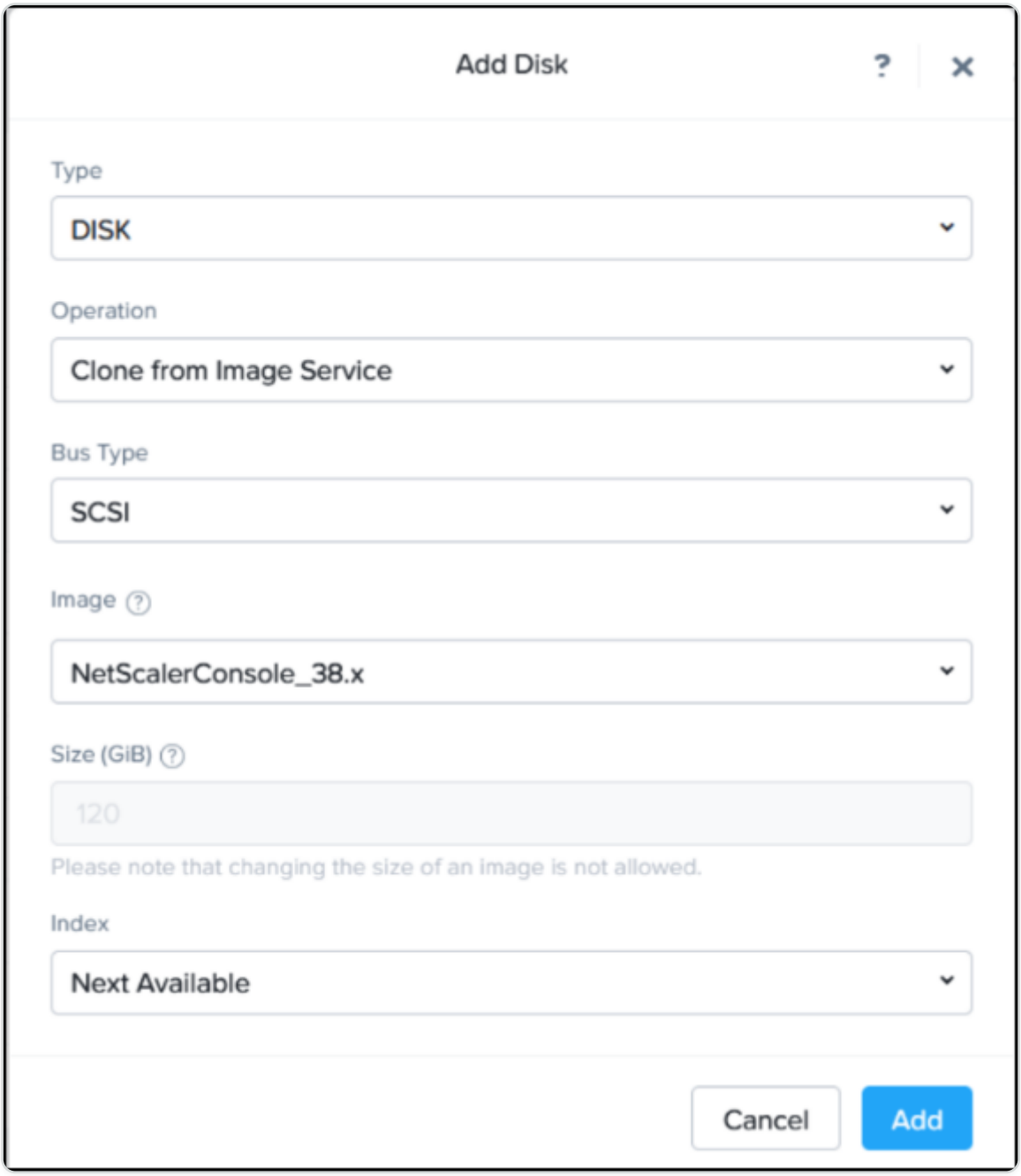
© 1997–2026 Citrix Systems, Inc. All rights reserved.



上传并保存后，将显示映像及其状态：

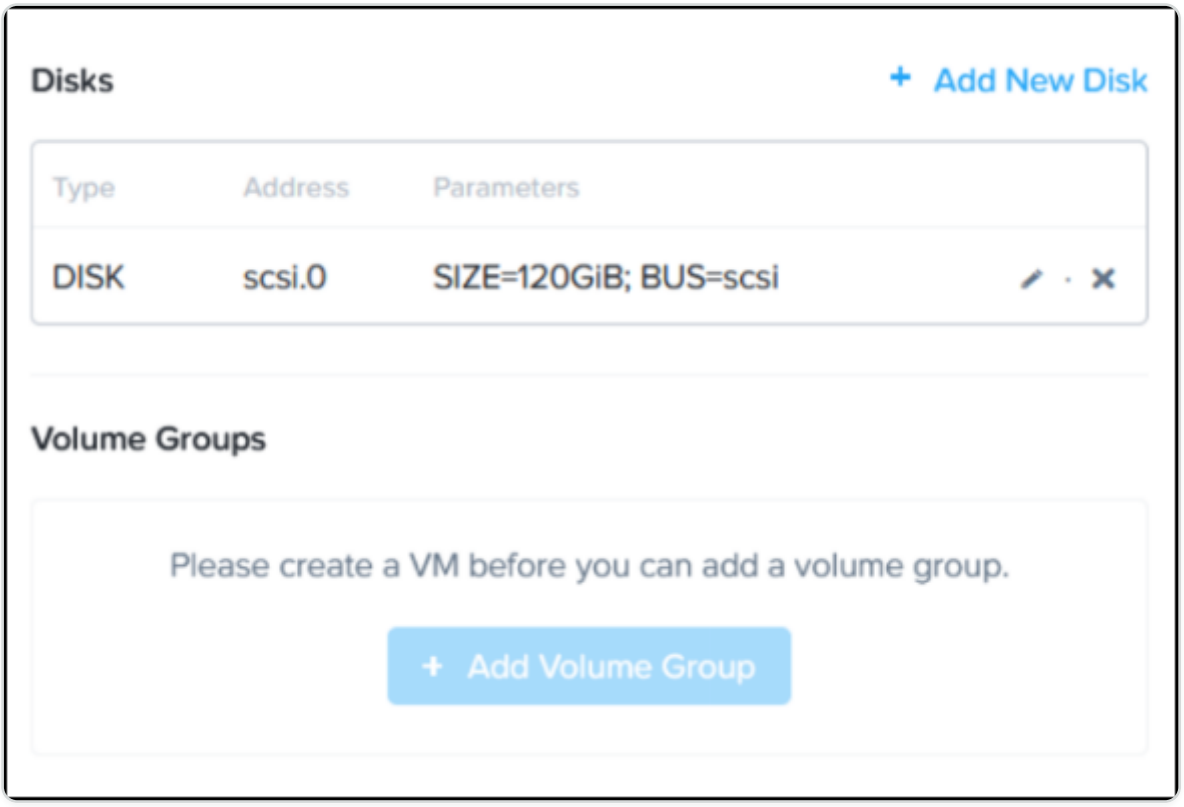
4. 导航到虚拟机，然后单击**创建虚拟机**。
5. 在**创建虚拟机**页面上，移除**CD ROM 驱动器**。
6. 添加新磁盘。
   a. 从**类型**列表中选择**磁盘**。
   b. 从**操作**列表中选择**从映像服务克隆**。
   c. 从**总线类型**列表中选择**SCSI**。
   d. 从列表中选择 NetScaler Console 映像。
   e. 单击**添加**。

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

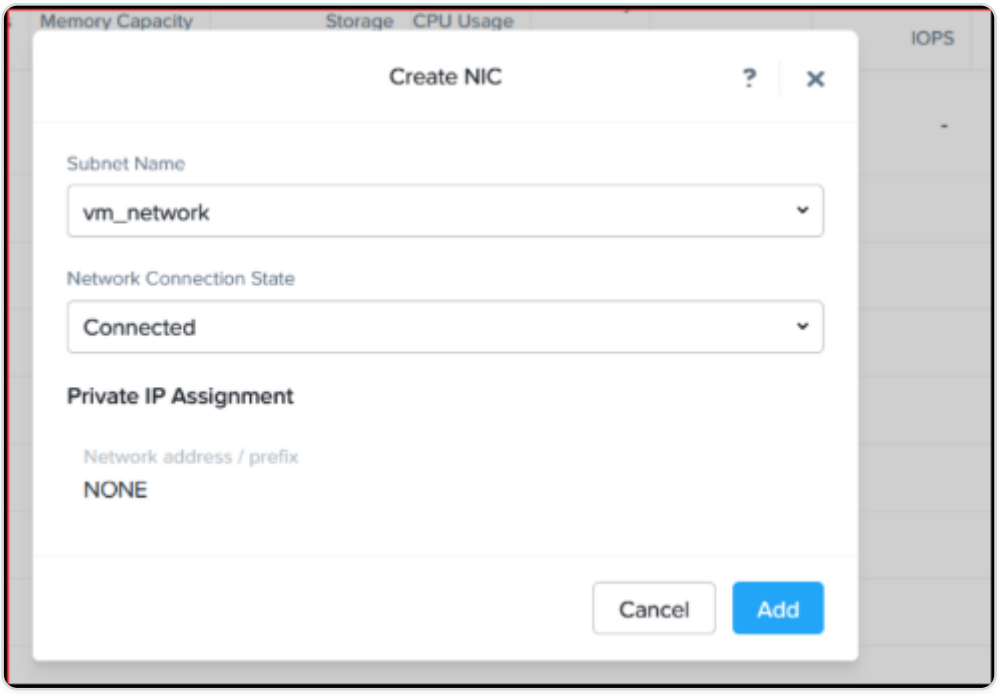


磁盘已添加。

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



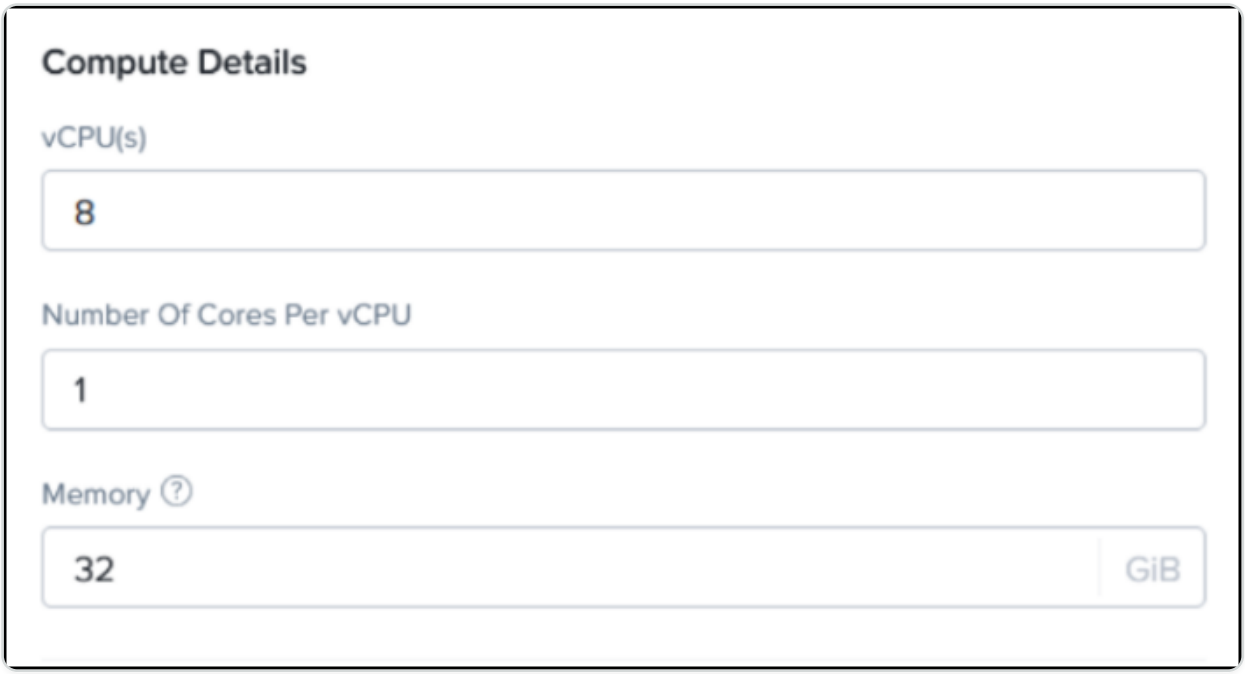
7. 将以下 NIC 详细信息添加到虚拟机：



8. 单击 **保存**。

9. 指定计算详细信息。对 NetScaler Console 和 NetScaler 代理使用默认值。

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



10. 单击 **保存**。

    VM 列出并显示为已关机后，您必须添加串行端口才能启动 VM。

11. 使用您为该帐户设置的用户名和密码通过 SSH 连接到控制器 VM (CVM)。您可以在 Prism Element 控制台的“硬件”部分找到 CVM IP 地址列表。

12. 输入 **ACLI**。

13. 使用以下命令创建串行端口。在 `vmname` 中键入 VPX 设备名称。

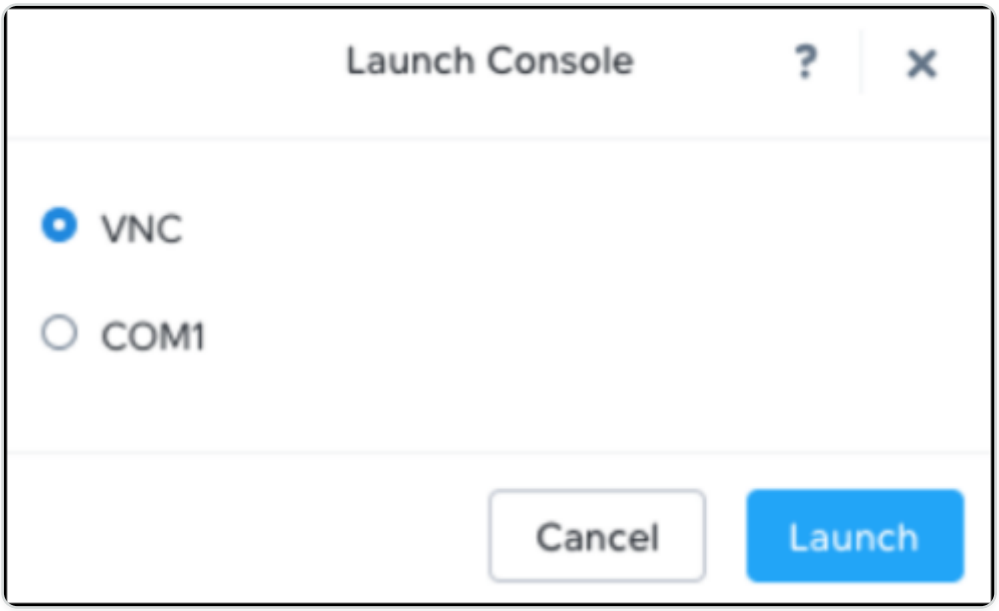
    ```
    vm.serial_port_create <vmname> type=kServer index=0
    ```

网络配置

1. 启动 VM。

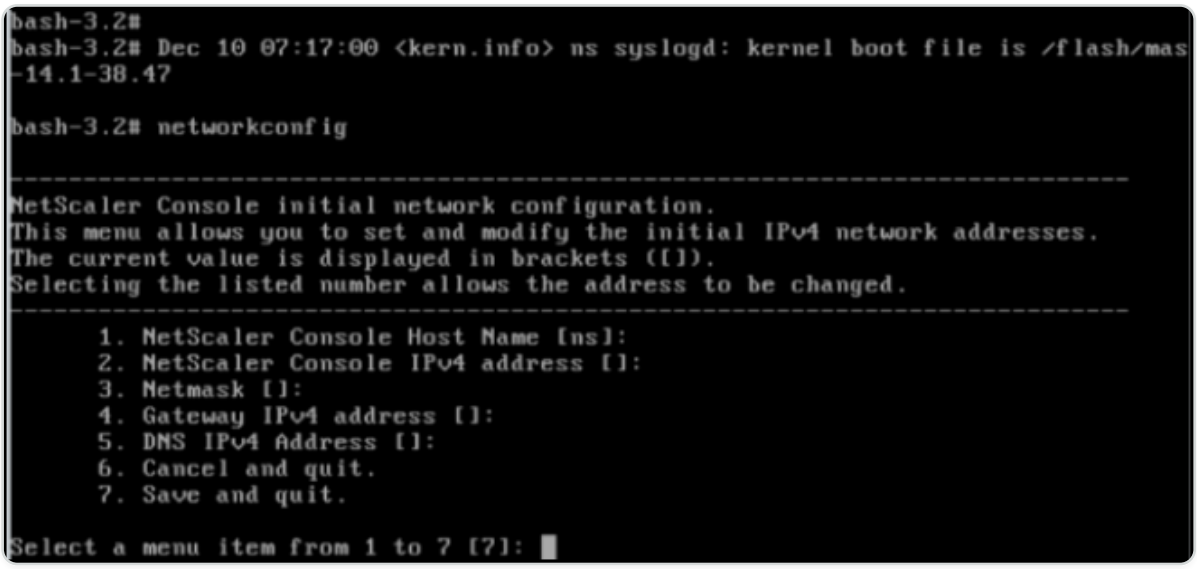
2. 启动 VNC 控制台。

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



3. VM 启动后，使用默认凭据 (**nsrecover**/**nsroot**) 登录。
4. 在提示符下，键入：*shell*
5. 键入 **networkconfig** 以进入 NetScaler Console 初始网络配置菜单。配置管理 IP 地址。
6. 要完成 NetScaler Console 的初始网络配置，请按照提示操作。控制台显示 NetScaler Console 初始网络配置选项，用于设置以下参数。主机名默认已填充。

   a. 输入 **2** 以更新 NetScaler Console IPv4 地址 - 用于访问 NetScaler Console 的管理 IP 地址。
   b. 输入 **3** 以更新子网掩码 - 与管理 IP 地址关联的子网掩码。
   c. 输入 **4** 以更新网关 IPv4 地址 - NetScaler Console 管理 IP 地址子网的默认网关 IP 地址。
   d. 输入 **7** 以保存并退出 - 保存您的配置更改并退出系统。



您可以通过在浏览器地址栏中键入 NetScaler Console 服务器的 IP 地址来访问 NetScaler Console。登录服务器的默认管理员凭据是 *nsroot/nsroot*。

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

NetScaler Console 在 红帽 OpenShift 虚拟化 上

注意：

在 NetScaler Console 版本 14.1-72.xx 及更高版本中，支持在 Red Hat® OpenShift® Virtualization (RHOCPV) 上安装 NetScaler Console。

您可以将 NetScaler® Console 作为虚拟机部署在 Red Hat® OpenShift® Virtualization (RHOCPV) 上。这使您能够在基于 OpenShift 的环境中管理 NetScaler 实例。

硬件要求

组件	最低要求
CPU	最低 8 个 vCPU
内存 (RAM)	最低 32 GiB
硬盘	最低 120 GiB（引导磁盘）

注意：

硬件要求适用于部署在 RHOCPV 上的 NetScaler Console 虚拟机。这些值基于部署期间使用的推荐通用型（U 系列 – 2xlarge）实例类型。请确保您的 RHOCPV 群集节点具有足够的容量，可以根据这些要求运行 NetScaler Console 虚拟机。

先决条件

平台要求

- 已部署 RHOCPV (OpenShift Virtualization) 集群
- 访问 OpenShift Web 控制台或 CLI (oc)
- 已启用 KubeVirt

注意：

对于部署在 RHOCPV 上的 NetScaler，支持的最低版本是 14.1–66.64。有关更多信息，请参阅 Red Hat OpenShift® Virtualization (RHOCPV) 上的 NetScaler VPX 实例。

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

部署架构

- NetScaler Console 作为虚拟机在 RHOCPV 上运行
- NetScaler Agent 可以部署在 RHOCPV 上

在 红帽 OpenShift 虚拟化 上安装 NetScaler Console

执行以下步骤以在 RHOCPV 上安装 NetScaler Console。

步骤 1 - 准备环境

1. 确保您的 RHOCPV 集群已启动并正在运行。
2. 验证您是否具有创建虚拟机的管理员访问权限。
3. 确保已启用虚拟化操作员以创建和管理虚拟机。

步骤 2 - 下载 NetScaler Console 安装文件

要下载 NetScaler Console 安装文件：

1. 登录到 `<https://www.citrix.com/downloads>` 页面。
2. 从产品列表中选择 **NetScaler Console**。
3. 在 **Release 14.1** 下，选择 14.1-72.x 或更高版本。将显示所选版本的页面。
4. 在 **跳转到下载** 列表中，选择 **NetScaler Console/NetScaler Console Agent 适用于 KVM 的映像, 14.1 Build 72.57**。
5. 单击 **Download File**，接受 EULA，并将压缩的映像文件下载到本地计算机上的任何文件夹。

步骤 3 - 将映像上传到 RHOCPV 可引导卷

1. 登录到您的 Red Hat OpenShift 控制台。
2. 在仪表板中，导航到 **Virtualization > Bootable Volumes**。
3. 单击右上角的 **Add volume**，然后选择 **with form** 以将可引导卷添加到群集。
4. 在 **Upload PVC image** 字段中，上传带有 `.qcow2` 扩展名的 NetScaler Console/Agent 映像文件。
5. 指定 **Volume name** 并选择可用的 **Storage**。
6. 将 **Volume metadata Preference** 字段指定为 **legacy**。
7. 点击 **保存**。

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

Add volume

Add a new bootable volume to the cluster.

Source type

Volume

Source details

Upload PVC image *

MAS-KV[redacted]72.57.qcow2 | Upload | Clear

☐ This is an ISO file

Destination details

StorageClass

SC lvms-vg1

Volume Mode

- ○ Filesystem (Recommended)
- ◉ Block (Highly recommended)

Access Mode

- ◉ Single user (RWO) (Highly recommended)
- ○ Shared access (RWX) (Not recommended)
- ○ Read only (ROX) (Not recommended)

Disk size *

− 120 + GiB

Volume name *

adm7257

Destination project

PR default

Volume metadata

Preference *

VMCP legacy

Default InstanceType

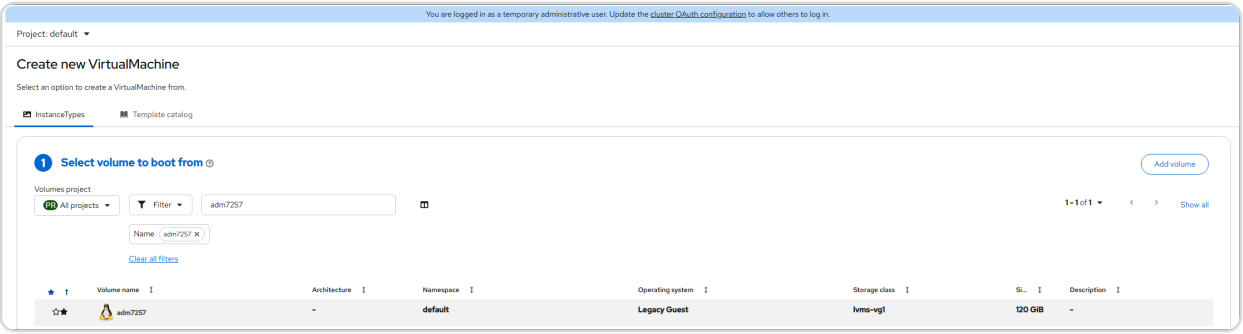
Select InstanceType

Architecture

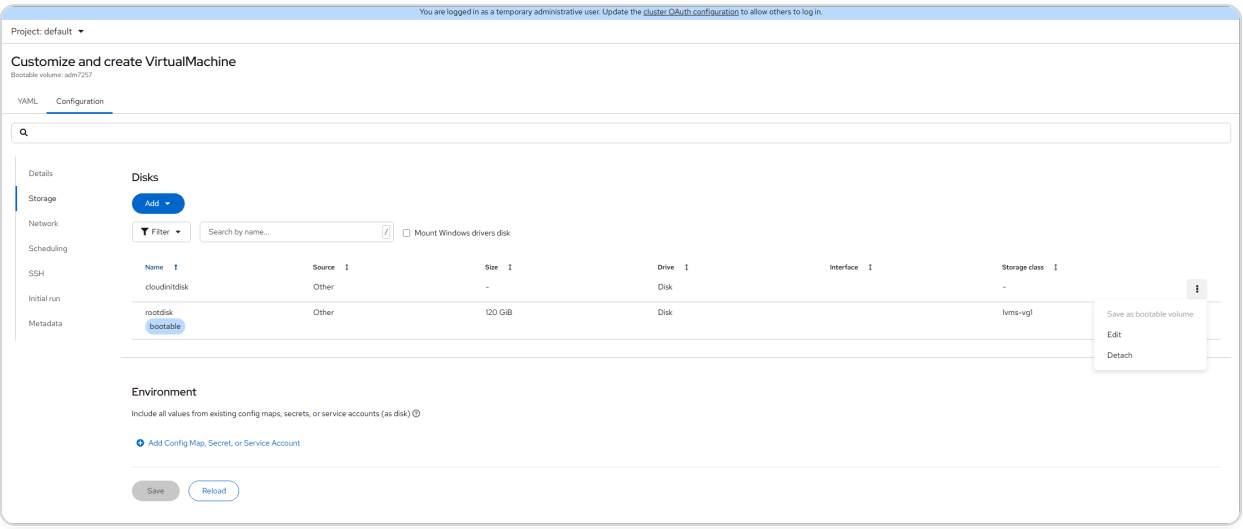
步骤 4 - 创建虚拟机

要从实例类型创建虚拟机：

1. 转到 **虚拟化 > 虚拟机** 并点击 **创建**。
2. 选择 **实例类型** 选项卡。
3. 选择您在 步骤 3 中创建的可启动卷。

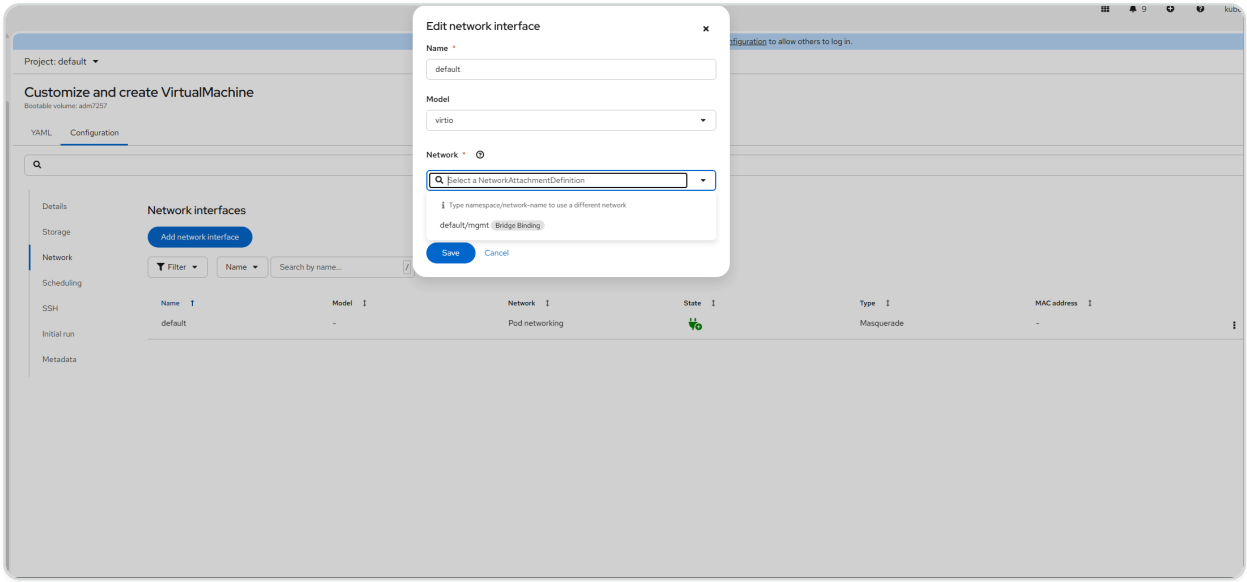


4. 选择与您的 NetScaler Console 模型虚拟机硬件规格匹配的实例类型。有关详细信息，请参阅 硬件要求。
5. 输入虚拟机的名称。
6. 点击 **自定义虚拟机**。
7. 分离默认磁盘（此处 `cloudinitdesk`）（如果存在），并保留 120 GB 可启动磁盘。



8. 在 **网络** 部分中，选择 `virtio` 作为接口模型，然后从列表中选择所需的网络。

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



9. 单击 **创建虚拟机**。

步骤 5. 启动虚拟机

启动虚拟机并验证其是否达到运行状态。

步骤 6. 访问 NetScaler Console

使用以下 URL 访问 NetScaler Console：

```
https://<console-ip-address>
```

Azure 云上的 NetScaler Console

从 14.1-43.x 开始，NetScaler Console 提供了更多部署选项，其中 NetScaler Console 可以通过 Azure 政府版市场作为虚拟机 (VM) 部署在 Azure 上。对于云部署采用气隙隔离且缺乏互联网连接的客户，NetScaler Console 服务不是一个可行的选择。将 NetScaler Console 作为 VM 部署在 Azure 上，使您能够在 Azure 部署中高效地管理和监控您的 NetScaler VPX 实例。

注意：

Azure 云上的 NetScaler Console 仅在 Azure 政府版市场提供。

先决条件

在配置之前，请确保您拥有 Azure 云和资源组的访问权限。

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

注意：

我们建议您在预置 NetScaler Console 之前，创建 资源组、网络安全组、虚拟网络 以及其他所需的实体。

配置 NetScaler Console

在 Azure 云中：

1. 转到市场，搜索 NetScaler Console，然后单击“**选择**”。

   选择映像后，您将被重定向到“**创建虚拟机**”工作流。

2. 指定以下内容：

   a. **资源组** - 从列表中选择一个资源组。

   b. **虚拟机名称** - 您选择的名称。

   c. **区域** - 从列表中选择一个区域。

   d. **映像** - 由于您已从市场中选择它，因此会自动填充。

   e. 从列表中选择 VM 大小（建议使用 8 个 vCPU、32 GB RAM）。

   f. **身份验证类型** - 选择 SSH 公钥。

   注意：

   不支持密码选项。

   g. **用户名** - 将名称更改为 `nsroot`。访问 NetScaler Console 的默认用户名为 `nsroot`。

   h. **SSH 公钥源** - 您可以使用现有密钥对或创建新密钥对。

   i. **公共入站端口** - 选择 **无**。

   j. 单击 **查看 + 创建**。

      将显示 VM 摘要。验证所有内容，然后单击 **创建**。

   k. VM 部署显示状态正在进行中。部署完成后，单击 **转到资源**。

      将显示有关 VM 的信息，您可以在 **网络** 下查看 VM 的公共 IP 和私有 IP。您可以通过浏览器使用公共 IP 登录 (`nsroot` / `nsroot`)。

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

> **注意：**
>
> 如果您想使用私有 IP 地址，请确保您在同一 Azure 云网络中运行 Azure 虚拟桌面，以便通过私有 IP 地址访问 NetScaler Console。

l. 通过使用 SSH 登录到虚拟机，并使用用户名 `nsrecover` 和密码 `nsroot`，验证 NetScaler Console 进程是否正在运行。

m. 后端进程启动并运行后，您可以使用 `nsroot` 密码登录到 NetScaler Console GUI。首次登录时，系统会提示您更改默认密码。

Azure 云上的 NetScaler Console HA 对

在 Azure 中，NetScaler Console 的高可用性通过 Azure 负载均衡器 (ALB) 实现。ALB 通过向主节点和辅助节点发送健康探测来监控实例。主实例响应 `200 OK`，而辅助实例不响应。根据这些响应，ALB 仅将流量发送到主实例。在故障转移事件中，新的主实例开始响应 `200 OK`，ALB 会自动将流量发送到它。

HA 对架构(/en-us/netscaler-application-delivery-management-software/media/console-azure-ha-architecture.png)

先决条件

确保：

- 您有权访问 Azure 云和资源组。

> **注意：**
>
> 建议您在部署 NetScaler Console 之前创建 资源组、网络安全组、虚拟网络 以及其他所需的实体。

- 您在 Azure 云上创建两个独立的 NetScaler Console 实例。
- 所需端口已打开以进行通信。有关更多信息，请参阅 系统要求。

配置 NetScaler Console HA 对

在您配置两个独立的 NetScaler Console 实例之后：

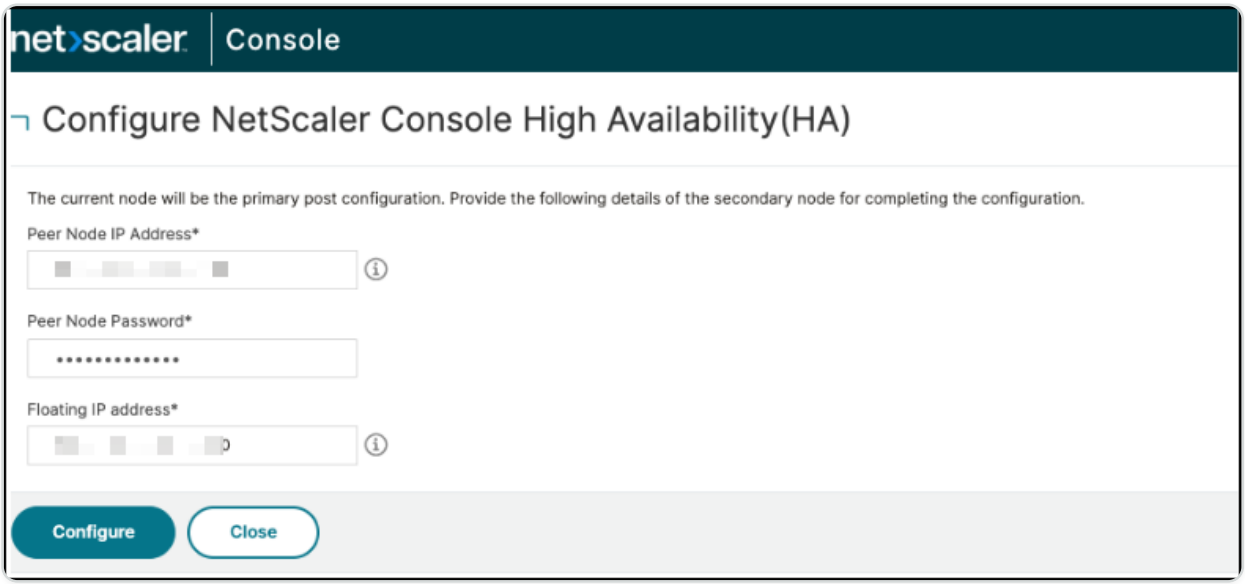
1. 登录到其中一个 NetScaler Console GUI。
2. 导航到 **设置 > 高可用性设置**。

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

注意：

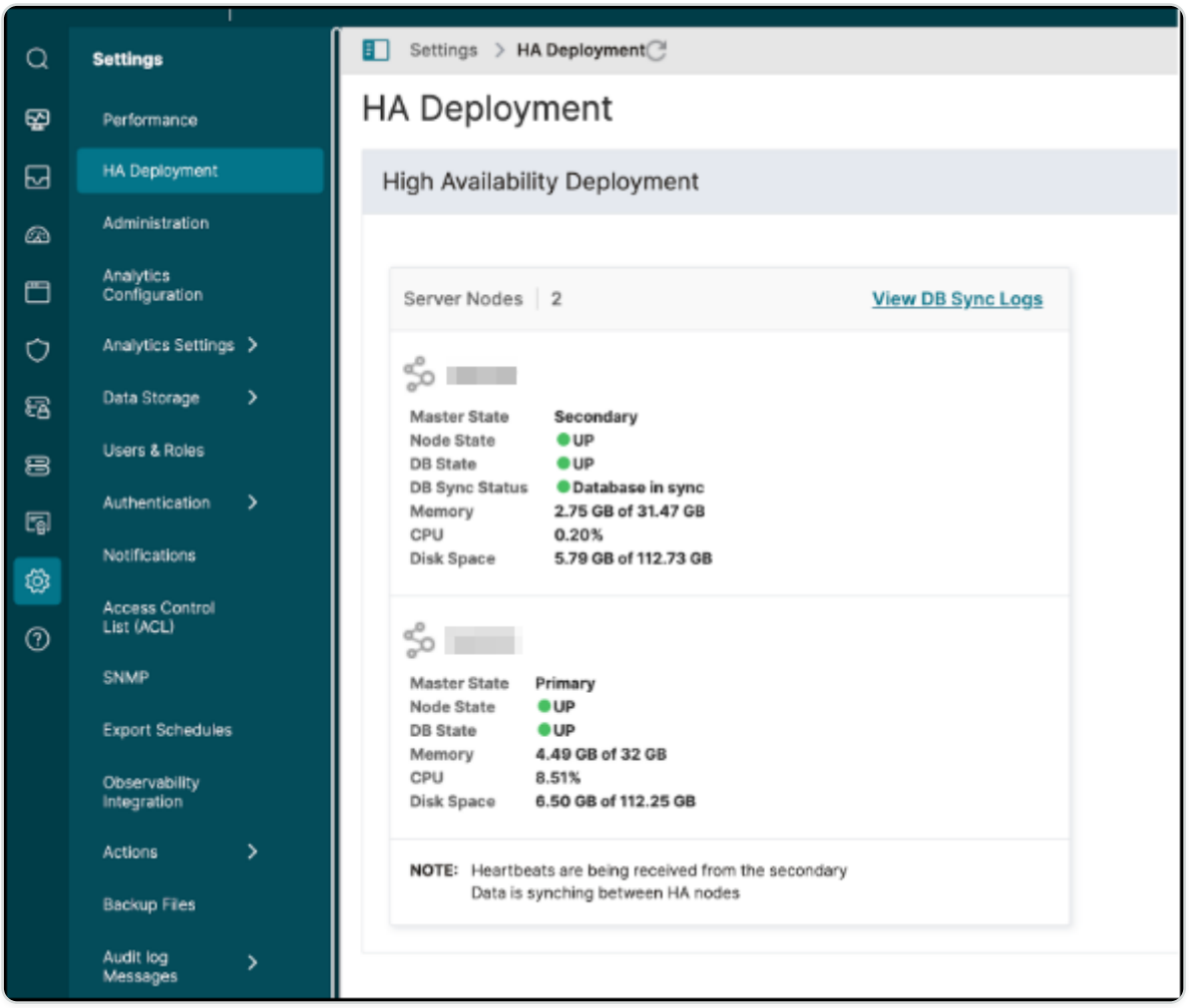
- 要配置 HA 对，您必须提供另一个 NetScaler Console 的私有 IP 地址。
- 浮动 IP 可以是 Azure VNet (虚拟网络) 中的任何可用 IP。

3. 单击 **配置 NetScaler Console 高可用性 (HA)**，然后提供辅助节点详细信息、浮动 IP 地址，并单击 **配置**。



4. 在确认窗口中，单击 **是**。NetScaler Console 实例将重新启动以形成 HA 对。
5. HA 对配置完成后，登录到主 NetScaler Console 并导航到 **设置 > HA 部署** 以验证主节点和辅助节点。

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



下一步是将浮动 IP 地址配置为 Azure 云中 Azure 负载均衡器的前端 IP。在 Azure 云门户中，搜索负载均衡器，在结果中选择 **负载均衡器**，然后单击 **创建**：

1. 在 **基本信息** 中，在配置 Console VM 的同一资源组和区域中创建 Azure 负载均衡器 (ALB)。
   a. 在 **实例详细信息** 下，选择 SKU: **标准**，类型: **内部**，以及层: **区域**。
2. 在 **前端 IP 配置** 中，添加一个前端 IP，其浮动 IP 已为 Console HA 对配置。
3. 在 **后端池** 中，添加两个 Console 实例的 IP 地址。
4. **负载均衡规则**：配置以下规则，并启用协议、端口、后端端口、运行状况探测和浮动 IP：

规则名称	协议	端口	后端端口	浮动 IP
规则-80	TCP	80	80	是
规则-443	TCP	443	443	是
规则-5454	TCP	5454	5454	是

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

规则名称	协议	端口	后端端口	浮动 IP
规则-22	TCP	22	22	是
规则-8443	TCP	8443	8443	是
规则-7443	TCP	7443	7443	是
规则-27000	TCP	27000	27000	是
规则-7279	TCP	7279	7279	是
规则-5563	TCP	5563	5563	是
规则-4739	UDP	4739	4739	是
规则-5140	UDP	5140	5140	是
规则-162	UDP	162	162	是
规则-514	UDP	514	514	是
规则-5557	UDP	5557	5557	是
规则-5558	UDP	5558	5558	是

5. **健康探测**：创建 HTTP 健康检查，其中包含步骤 4 中列出的所有必需端口。此健康探测将主 Console 启用为活动状态，将辅助 Console 启用为被动状态。例如：

   a. 端口: 443

   b. URL: `/mas_health`

   c. 预期响应代码: 200

   有关创建负载均衡器的更多信息，请参阅 Azure 文档中的创建负载均衡器。

   配置负载均衡器后，您可以使用 ALB 的前端 IP 地址访问 NetScaler Console。

   注意：

   确保您在同一 Azure 网络中运行 Azure 虚拟桌面，以便通过前端 IP 地址访问 NetScaler Console。

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

亚马逊网络服务 (AWS) 上的 NetScaler 控制台

从 **14.1-47.x** 开始，您可以通过在 **AWS GovCloud** 中使用 AWS Marketplace 上的 AMI 来部署 NetScaler Console。

先决条件

要使用 Amazon GUI 在 AWS 虚拟私有云 (VPC) 中启动 NetScaler Console AMI，您需要：

- 一个 AWS 账户
- 一个 AWS 虚拟私有云 (VPC)
- 确保在 AWS 中创建安全组时，所需的端口（例如 22、80 和 443）已打开。有关更多信息，请参阅 系统要求。

配置 NetScaler Console

1. 使用您的 AWS 凭据登录 AWS Marketplace。
2. 搜索 AMI 并选择 **AMIs**。
3. 在搜索框中，键入 NetScaler Console，选择 NetScaler Console，然后单击 **从 AMI 启动实例**。
4. 在 **实例类型** 下，从列表中选择 8 个 vCPU 和 32 GB 内存选项。

   注意：

   默认情况下，NetScaler Console AMI 为 500 GB。

5. 在 **密钥对（登录）** 下，选择现有密钥对或创建新密钥对。
6. 在**网络设置**下，单击**编辑**，然后：

   a. 从列表中选择 VPC。

   b. 选择或创建新子网。

   c. 启用**自动分配公共 IP**，以使用公共 IP 地址启动 NetScaler Console。

   d. 选择或创建安全组。

   注意：

   确保所需的端口（例如端口 22、443 和 80）已打开。有关详细信息，请参阅系统要求。

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

e. 单击**启动实例**。将创建一个实例 ID。

7. 单击实例 ID。

   您可能需要等待**状态检查**显示为已通过（绿色复选标记）。

8. 安全检查通过后，单击实例 ID 以查看详细信息。

   使用 IP 地址启动 NetScaler Console GUI。如果要使用私有 IP 地址，请确保您在 AWS 中拥有 VDI。

   下表描述了通过 SSH、GUI 和串行控制台（可从 AWS 访问的控制台）的 AWS 登录过程：

   | | SSH | | 串行控制台 | | GUI | |

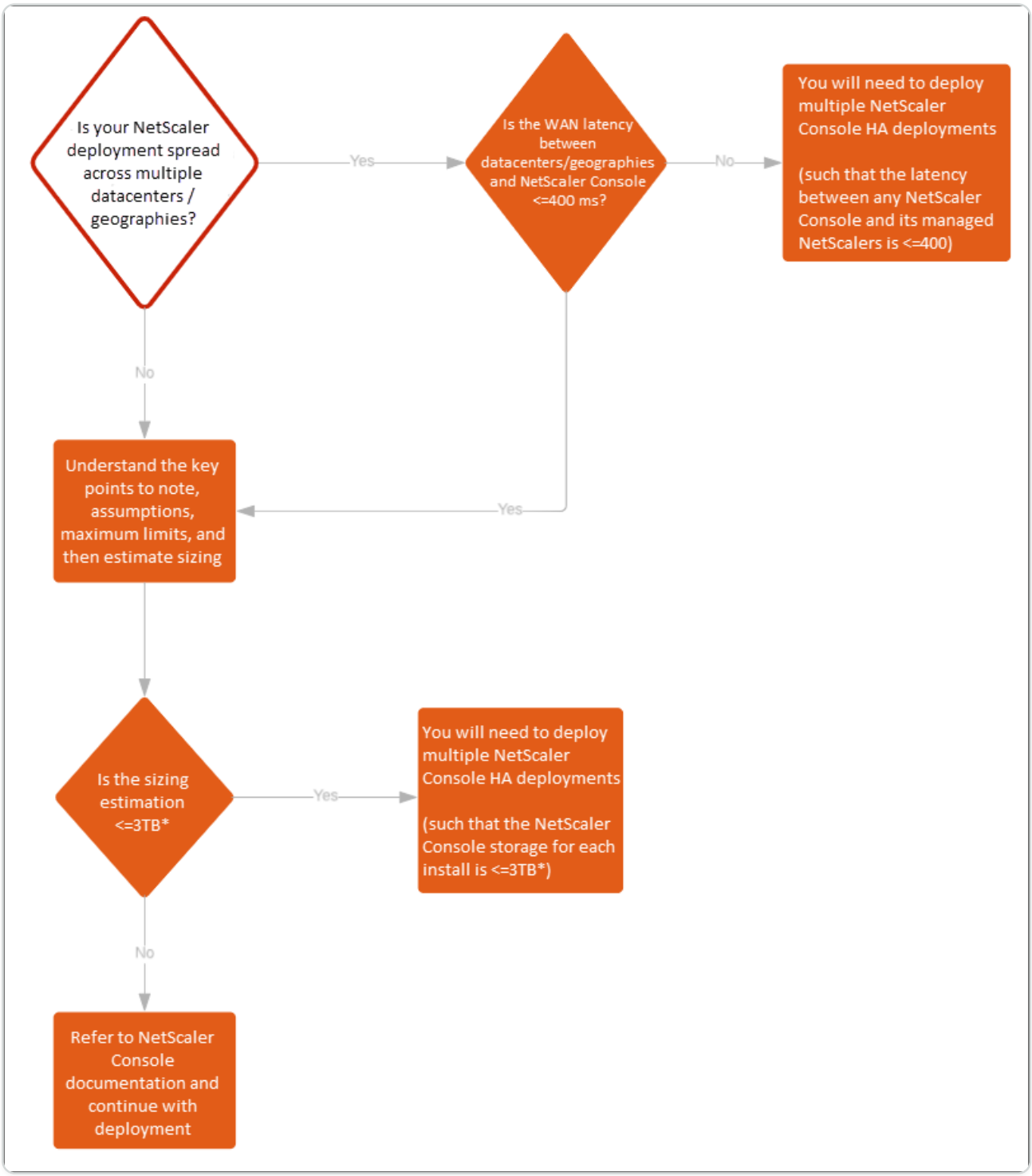
	ns根	**ns恢复**	**nsroot** 用户	**nsrecover** 用户	**nsroot**	**自定义用户**
密码	允许（默认密码为 `nsroot`）	允许（默认密码为 `nsroot`）	不允许	允许（默认密码为 `nsroot`）	允许（默认密码为 `nsroot`）	允许（用户定义的密码）
公钥	允许	不适用	不适用	不适用	不适用	不适用

配置高可用性部署

高可用性 (HA) 是指一个系统始终可供用户使用，而不会中断服务。高可用性设置在系统停机、网络或应用程序故障期间至关重要，是任何企业的关键要求。两个 NetScaler Console 节点以主动-被动模式进行高可用性部署，并采用相同的配置，可提供不间断的操作。

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

部署场景



注意

单个 NetScaler Console HA 部署的经验证最大存储限制为 3 TB。有关详细信息，请参阅部署指南。

重要

要使用 HTTPS 访问 NetScaler Console 12.1 build 48.18 或更高版本：

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

如果您已配置 NetScaler 实例以在高可用性模式下对 NetScaler Console 进行负载平衡，请首先移除该 NetScaler 实例。然后，配置一个浮动 IP 地址以在高可用性模式下访问 NetScaler Console。
以下是 NetScaler Console 中高可用性部署的优势：

- 改进了监视主节点和辅助节点之间心跳的机制。
- 提供数据库的物理流式复制，而不是逻辑双向复制。
- 能够在主节点上配置浮动 IP 地址，从而无需单独的 NetScaler 负载平衡器。
- 使用浮动 IP 地址可轻松访问 NetScaler Console 用户界面。
- NetScaler Console 用户界面仅在主节点上提供。通过使用主节点，可以消除访问和更改辅助节点的风险。
- 配置浮动 IP 地址可处理故障转移情况，并且无需重新配置实例。
- 提供内置功能，可检测和处理脑裂情况。

下表描述了高可用性部署中使用的术语。

术语	描述
主节点	在高可用性部署中注册的第一个节点。
辅助节点	在高可用性部署中注册的第二个节点。
心跳	在高可用性设置中用于在主节点和辅助节点之间交换消息的机制。这些消息确定每个独立节点上应用程序的状态和运行状况。
浮动 IP 地址	浮动 IP 是一种 IP 地址，可以在同一子网中的一个节点与另一个节点之间即时移动。在内部，它被设置为主节点网络接口上的别名。如果发生故障转移，浮动 IP 地址将从旧主节点无缝移动到新主节点。它在高可用性设置中很有用，因为它允许客户端使用单个 IP 地址与高可用性节点通信。

注意：

有关端口和协议详细信息的更多信息，请参阅端口。

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

高可用性架构的组件

下图显示了以高可用性模式部署的两个 NetScaler Console 节点的架构。

HA 架构(/en-us/netscaler-application-delivery-management-software/media/haarchitecture-console.png)

在高可用性部署中，一个 NetScaler Console 节点配置为主节点 (MAS 1)，另一个配置为辅助节点 (MAS 2)。如果主节点因任何原因发生故障，辅助节点将接管成为新的主节点。

监控工具

监控工具是一个内部进程，用于监控、警报和处理故障转移情况。该工具在高可用性中的每个节点上都处于活动运行状态。它负责启动子系统、在两个节点上初始化数据库、在发生故障转移时决定主节点或辅助节点等。

主节点

主节点接受连接并管理实例。所有进程（例如 AppFlow、SNMP、LogStream、syslog 等）都由主节点管理。NetScaler Console 用户界面可在主节点上访问。浮动 IP 地址在主节点上配置。

辅助节点

辅助节点侦听来自主节点的心跳消息。辅助节点上的数据库仅处于只读副本模式。辅助节点中没有活动进程，并且 NetScaler Console 用户界面在辅助节点上不可访问。

物理流复制

主节点和辅助节点通过心跳机制同步。通过数据库的物理流复制，辅助节点以只读副本模式启动。辅助节点侦听从主节点接收到的心跳消息。如果辅助节点在 180 秒内未收到任何心跳，则认为主节点已关闭。然后，辅助节点接管成为主节点。

心跳消息

心跳消息是主节点和辅助节点之间发送和接收的用户数据报协议 (UDP) 数据包。它监控 NetScaler Console 的所有子系统和数据库，以交换有关节点状态、运行状况、进程等信息。信息每秒在高可用性节点之间共享。如果发生故障转移或高可用性状态中断，则会向管理员发送通知作为警报。

浮动 IP 地址

浮动 IP 地址与高可用性设置中的主节点关联。它是分配给主节点 IP 地址的别名，客户端可以使用它连接到主节点中的 NetScaler Console。由于浮动 IP 地址配置在主节点上，因此在发生故障转移时无需重新配置实例。实例会重新连接到相同的 IP 地址以访问新的主节点。

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

关键注意事项

- 在高可用性设置中，两个 NetScaler Console 节点都以主动-被动模式部署。它们必须位于相同的子网中，使用相同的软件版本和内部版本，并具有相同的配置。
- 浮动 IP 地址：
  - 浮动 IP 地址配置在主节点上。
  - 如果发生故障转移，实例无需重新配置。
  - 您可以通过使用主节点 IP 或浮动 IP 地址从用户界面访问高可用性节点。

    注意：

    我们建议您使用浮动 IP 地址访问用户界面。

- 数据库：
  - 在高可用性设置中，所有配置文件每隔一分钟自动从主节点同步到辅助节点。
  - 数据库同步通过数据库的物理复制即时发生。
  - 辅助节点上的数据库处于只读副本模式。
- NetScaler Console 升级：
  - 内部进程会隐式地将 NetScaler Console 从早期版本升级。

    注意：

    升级成功后，您必须配置浮动 IP 地址。

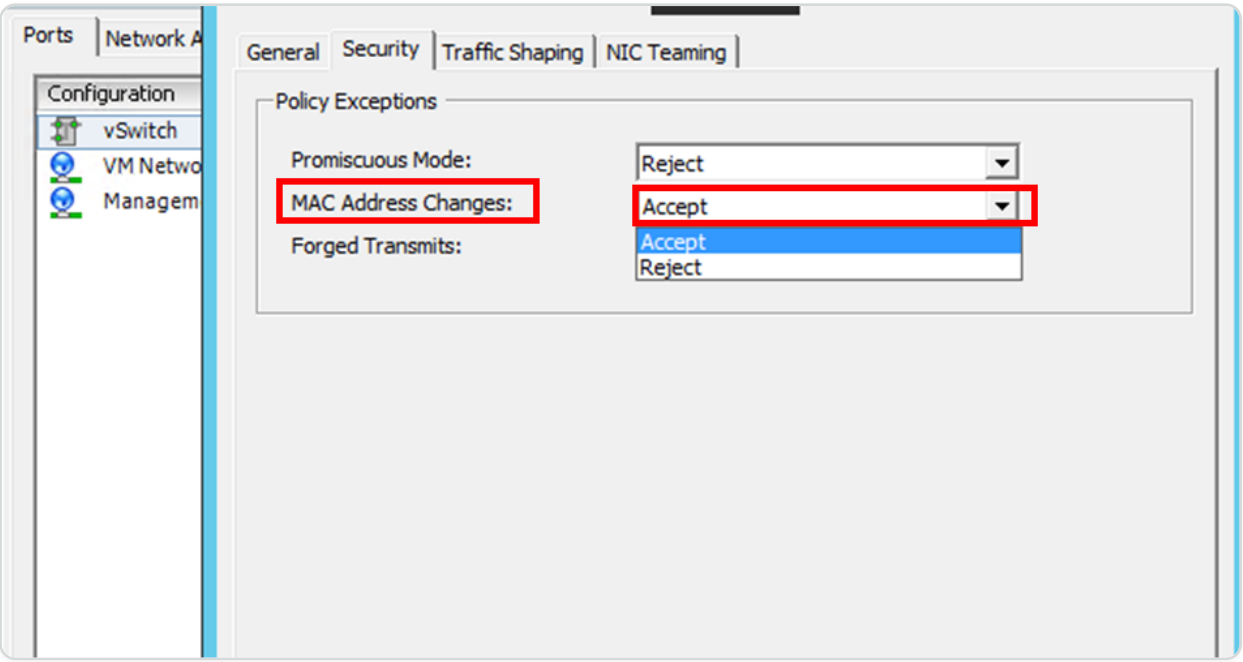
- 两个节点上都提供了 UDP 默认端口 5005，用于发送心跳和接收消息。
- MAC 地址 管理程序中“MAC 地址更改”选项的设置会影响虚拟机接收的流量。允许在虚拟交换机上启用 MAC 地址更改，以便在故障转移后浮动 IP 地址无缝移动到新的主节点。 例如，在 VMware ESXi 上部署 NetScaler Console 高可用性时，请确保接受 MAC 地址更改。ESXi 现在允许将活动 MAC 地址更改为初始 MAC 地址以外的地址。

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

注意：

对于部署在 ESXI 6.7 版上的 NetScaler Console，您也可以将“**MAC 地址更改**”选项设置为“**拒绝**”。故障转移后，无论“**MAC 地址更改**”设置如何，流量都会无缝流向新的主节点。因此，接受 MAC 地址更改不是强制性的。

如果 NetScaler Console 部署在低于 6.7 的 ESXI 版本上，请确保“**MAC 地址更改**”选项仅设置为“**接受**”。



先决条件

在为 NetScaler Console 节点设置高可用性之前，请注意以下先决条件：

- NetScaler Console 高可用性部署从 NetScaler Console 12.0 build 51.24 版本开始支持。
- 从 NetScaler 站点下载 NetScaler Console 映像文件 (.xva)：`<https://www.citrix.com/downloads/>`

我们建议您将 CPU 优先级（在虚拟机属性中）设置为最高级别，以改善调度行为和网络延迟。

下表列出了虚拟计算资源的最低要求：

组件	要求
内存	**32 GB**
虚拟 CPU	**8 个 CPU**

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

组件	要求
存储空间	我们建议您在 NetScaler Console 部署中使用固态硬盘 (SSD) 技术。默认值为 120 GB。实际存储要求取决于 NetScaler Console 的大小估算。如果您的 NetScaler Console 存储要求超过 120 GB，则必须连接一个额外的磁盘。**注意：**您只能添加一个额外的磁盘。我们建议您在初始部署时估算存储并连接额外的磁盘。有关更多信息，请参阅 如何将额外磁盘连接到 NetScaler Console。
虚拟网络接口	1
吞吐量	1 千兆位/秒 或 100 兆位/秒
虚拟机管理程序	**版本**
思杰管理程序	6.2 和 6.5
威睿 ESXi	5.5 和 6.0
微软 Hyper-V	2012 R2
利努克斯 KVM	乌班图 和 费多拉

在高可用性模式下设置 NetScaler Console

从版本 14.1 build 17.x 开始，您可以直接从主节点的 NetScaler Console GUI 部署高可用性设置。

1. 注册第一个服务器（主节点）。
2. 注册第二个服务器（辅助节点）。
3. 在主节点 GUI 中部署高可用性设置。

注册第一个服务器（主节点）

要注册主节点：

1. 使用从 NetScaler 站点下载的 .xva 映像文件并将其导入到您的管理程序中。

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

> **注意：**
>
> 导入并启动 .xva 镜像文件可能需要几分钟。您可以在屏幕底部查看状态。

XVA 文件(/en-us/netscaler-application-delivery-management-software/media/importvm.png)

2. 导入成功后，右键单击并点击 **Start**。

   启动文件(/en-us/netscaler-application-delivery-management-software/media/startvm.png)

3. 在 **Console** 选项卡中，使用初始网络配置来配置 NetScaler Console。

   网络配置(/en-us/netscaler-application-delivery-management-software/media/admha-initialconfig.png)

4. 初始网络配置完成后，系统会提示登录。使用以下凭据登录 – *nsrecover/nsroot*。

> **注意：**
>
> 登录后，如果您想更新初始网络配置，请键入 `networkconfig`，更新配置，然后保存配置。

注册第二个服务器（辅助节点）

1. 使用从 NetScaler 站点下载的 **.xva** 镜像文件并将其导入到您的虚拟机管理程序中。
2. 在 **Console** 选项卡中，按照下图所示配置 NetScaler Console 的初始网络配置。
3. 初始网络配置完成后，系统会提示登录。使用以下凭据登录 – *nsrecover/nsroot*。

> **注意：**
>
> - 登录后，如果您想更新初始网络配置，请键入 `networkconfig`，更新配置，然后保存配置。
> - 如果配置中存在任何问题，系统将显示错误消息。
> - 系统将重新启动，配置生效需要几分钟。

从主节点 GUI 部署高可用性设置

注册主节点和辅助节点后，登录主节点 GUI 以设置高可用性对。

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

注意：

- 在将节点部署到高可用性对之前，请确保辅助节点在初始网络配置后已完成重新启动。

要从主节点部署高可用性对，请按照以下步骤操作：

1. 登录主节点 GUI。
2. 导航到 **设置 > 管理 > 高可用性设置 > 配置 NetScaler Console 高可用性 (HA)**。
3. 在 **配置 NetScaler Console 高可用性 (HA) 页面**上，输入辅助节点的以下详细信息：
   - 对等节点 IP 地址
   - 对等节点密码
   - 浮动 IP 地址
4. 单击“配置”。
5. 在“**确认**”页面上，单击“**是**”。

   配置高可用性对(/en-us/netscaler-application-delivery-management-software/media/configure-ha-pair.png)

   主节点和辅助节点都会重新启动以形成高可用性对，通常需要大约 10 分钟。

   备注：

   - 您现在可以开始使用**浮动 IP 地址**。
   - 浮动 IP 地址对于节点的高可用性部署是强制性的。
   - 高可用性部署完成后，使用浮动 IP 地址访问 NetScaler Console 用户界面。

6. 导航到**设置 > 部署**以验证部署。

   注意：

   辅助节点可能需要大约 10 分钟才能启动。在此之前，辅助节点状态显示为**关闭**。

有关详细信息，请参阅常见问题。

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

禁用高可用性

您可以在 NetScaler Console 高可用性对上禁用高可用性，并将节点转换为独立的 NetScaler Console 服务器。

注意：

从主节点禁用高可用性。

要禁用高可用性：

1. 在 Web 浏览器中，输入 NetScaler Console 服务器主节点的 IP 地址。
2. 在**用户名**和**密码**字段中，输入管理员凭据。
3. 在**系统**选项卡上，导航到**部署**，然后单击**中断 HA**。

   将显示一个对话框。单击**是**以中断高可用性部署。

重新部署高可用性

将高可用性禁用为独立部署后，您可以将其重新部署到高可用性模式。重新部署高可用性与首次部署高可用性类似。有关更多详细信息，请参阅从主节点 GUI 部署高可用性设置。

注意：

禁用 NetScaler® Console 高可用性后，只能使用一个控制台节点作为独立许可证服务器。第二个节点必须重新配置。

高可用性故障转移场景

如果遇到以下任一情况，则会发生故障转移：

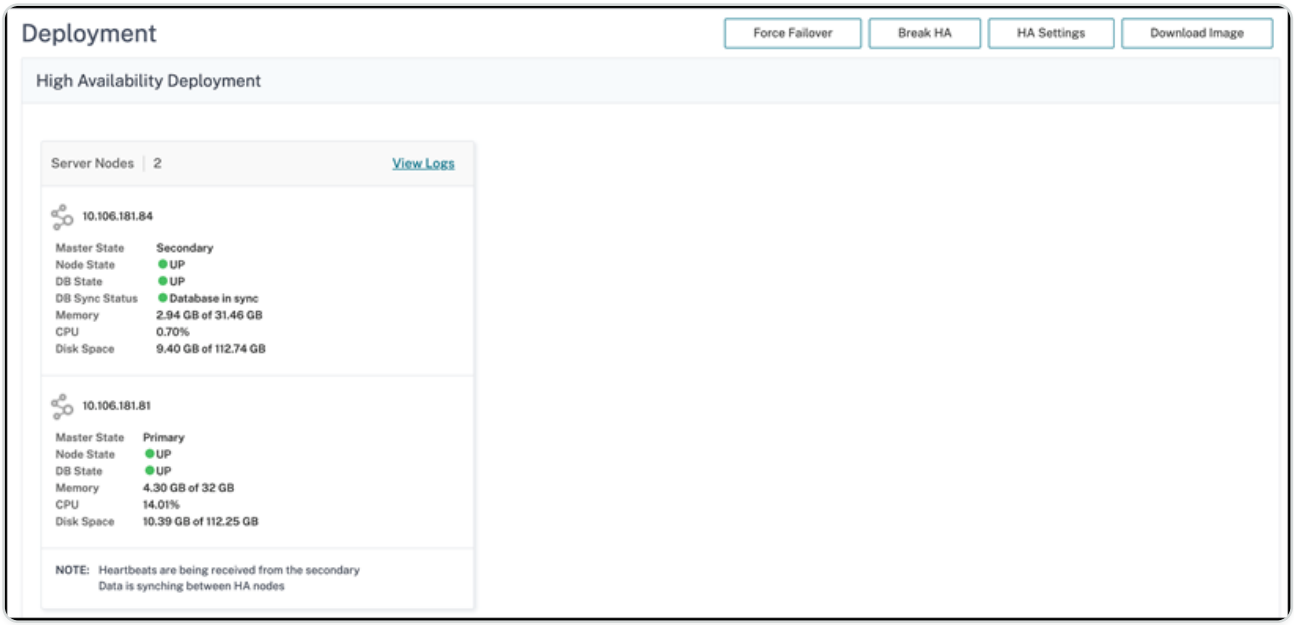
- **节点故障**：主节点关闭，180 秒内未检测到来自主节点的心跳。
- **应用程序运行状况故障**：主节点已启动并正在运行，但其中一个 NetScaler Console 进程已关闭。

查看数据库同步日志消息

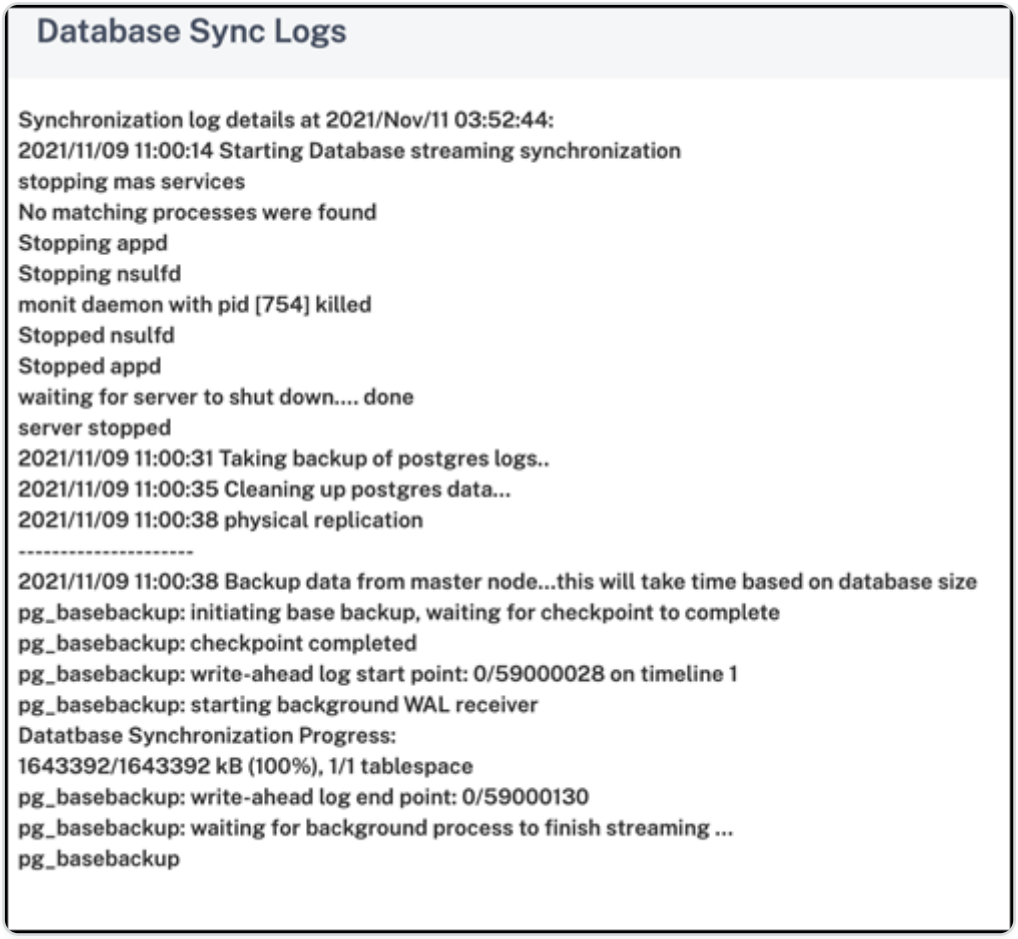
在 NetScaler Console HA 对中，配置文件会自动从主节点同步到辅助节点，并发生数据库的物理流式复制。

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

但是，如果存在流式复制错误，则会显示**同步数据库**按钮。您可以单击**同步数据库**按钮以启动数据库同步过程。



要查看数据库同步进度，请单击 **查看日志**。此时将显示 **数据库同步日志** 消息，您可以实时查看同步进度的详细信息。



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

脑裂场景

当由于网络链路停机导致两个节点之间没有通信时，则：

- 主节点继续作为主节点运行
- 由于未能接收到心跳，辅助节点接管成为主节点
- 两个节点都将运行各自的数据库实例

例如，在企业中，两个 NetScaler Console 节点已部署为主节点和辅助节点。由于可能的网络链路停机，两个 NetScaler Console 节点之间的通信完全中断。由于超过 180 秒没有心跳交换，两个节点都认为自己是主节点。两个节点都作为活动节点运行自己的数据库实例。

从 NetScaler Console 12.1 或更高版本开始，在网络链路和心跳恢复后，此脑裂情况将得到妥善处理。高可用性同步会自动恢复。恢复时间取决于数据量和节点之间链路的速度。

注意：

在脑裂情况下，当旧主节点重新加入高可用性时，其上发生的更改将与新主节点同步并重置。在脑裂期间在新主节点上发生的更改保持不变。

许可

NetScaler Console 服务器可以包含 VIP、CICO 和池化容量许可证。当许可证颁发给 NetScaler Console 服务器时，许可证将绑定到服务器主机 ID。禁止将许可证分配给其他 NetScaler Console 服务器。

如果您将 NetScaler Console 高可用性对配置为许可证服务器，则应用于主节点的许可证文件将同步到辅助节点。

注意：

- 在 12.1-50.x 及更高版本中，NetScaler Console 许可证会自动从主节点同步到辅助节点。

配置跨不同第 3 层子网的高可用性 (L3 上的 HA)

从版本 14.1-66.x 开始，NetScaler Console 支持跨不同第 3 层 (L3) 子网的高可用性 (HA) 部署。

此增强功能提供以下功能：

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

- 主 NetScaler Console 节点和辅助 NetScaler Console 节点可以部署在不同的 L3 子网或数据中心中。
- 浮动 IP 地址 (VIP) 由外部负载均衡器配置和拥有。
- 负载均衡器将客户端流量转发到活动的 NetScaler Console 节点。
- 节点间的 HA 同步保持不变。

有关常规 HA 概念、节点角色和同步行为，请参阅 HA 文档。

NetScaler Console 通过使用外部负载均衡器管理浮动 IP 地址，支持跨不同子网的 HA 部署，从而消除 L2 依赖性。

以前，NetScaler Console 要求主节点和辅助节点驻留在同一子网中，因为浮动 IP 地址由 HA 对内部拥有和管理。这产生了第 2 层依赖性，并限制了跨分段或地理上分离网络的部署。这限制了 HA 部署到第 2 层环境，并阻止客户进行以下操作：

- 跨不同子网部署 HA。
- 跨数据中心分发节点。
- 与路由的企业网络架构保持一致。

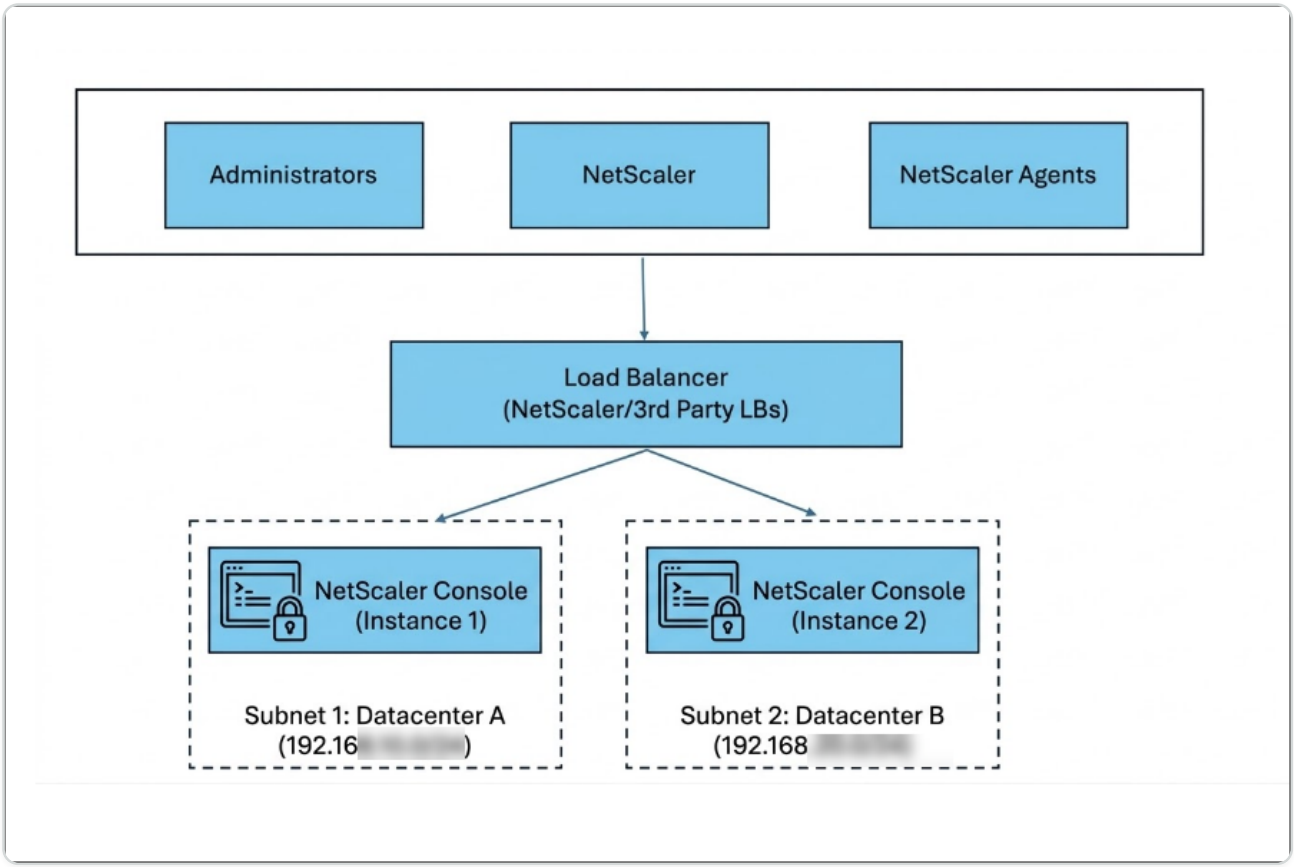
高级架构

- 浮动 IP 地址 (VIP) 配置在外部负载均衡器上。
- NetScaler Console 在此部署中不拥有 VIP。
- 负载均衡器根据健康检查将流量转发到活动节点。
- HA 同步通过 L3 连接直接在节点之间继续进行。
- NetScaler Console 中不使用基于 ARP 的 VIP 接管。

注意：

推荐的负载均衡器是 NetScaler，但也支持第三方负载均衡器。

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



部署和配置

先决条件

- 部署了外部第 3 层负载均衡器，并且可由以下对象访问：
  - 客户端
  - 两个 NetScaler Console 节点
- 主节点和辅助节点之间的网络连接。

工作流程

1. 在单独的 L3 子网或数据中心中部署两个 NetScaler Console 节点（主节点和辅助节点）。
2. 部署并配置外部负载均衡器。
3. 在负载均衡器（前端）上创建浮动 IP 地址 (VIP)，并将两个 NetScaler Console 节点添加为后端目标。
4. 使用以下协议和端口为 VIP 创建负载均衡规则。

LB 虚拟服务器	协议	端口
HTTP	TCP	80

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

LB 虚拟服务器	协议	端口
HTTPS	TCP	443
数据库和高可用性	TCP	5454
NTP	UDP	123
SNMP	UDP	162
SYSLOG	UDP	514
许可证	TCP	27000
供应商守护进程	TCP	7279

5. 在所有后端目标上配置健康监视器，以便负载均衡器仅将流量转发到活动节点。

监视器 / 用途	协议 / 端口
HA 和 DB	TCP / 5454
SNMP	UDP / 162
系统日志	UDP / 514
NTP	UDP / 123

6. 配置 NetScaler Console HA 对，并指定浮动 IP 地址是在外部配置的。

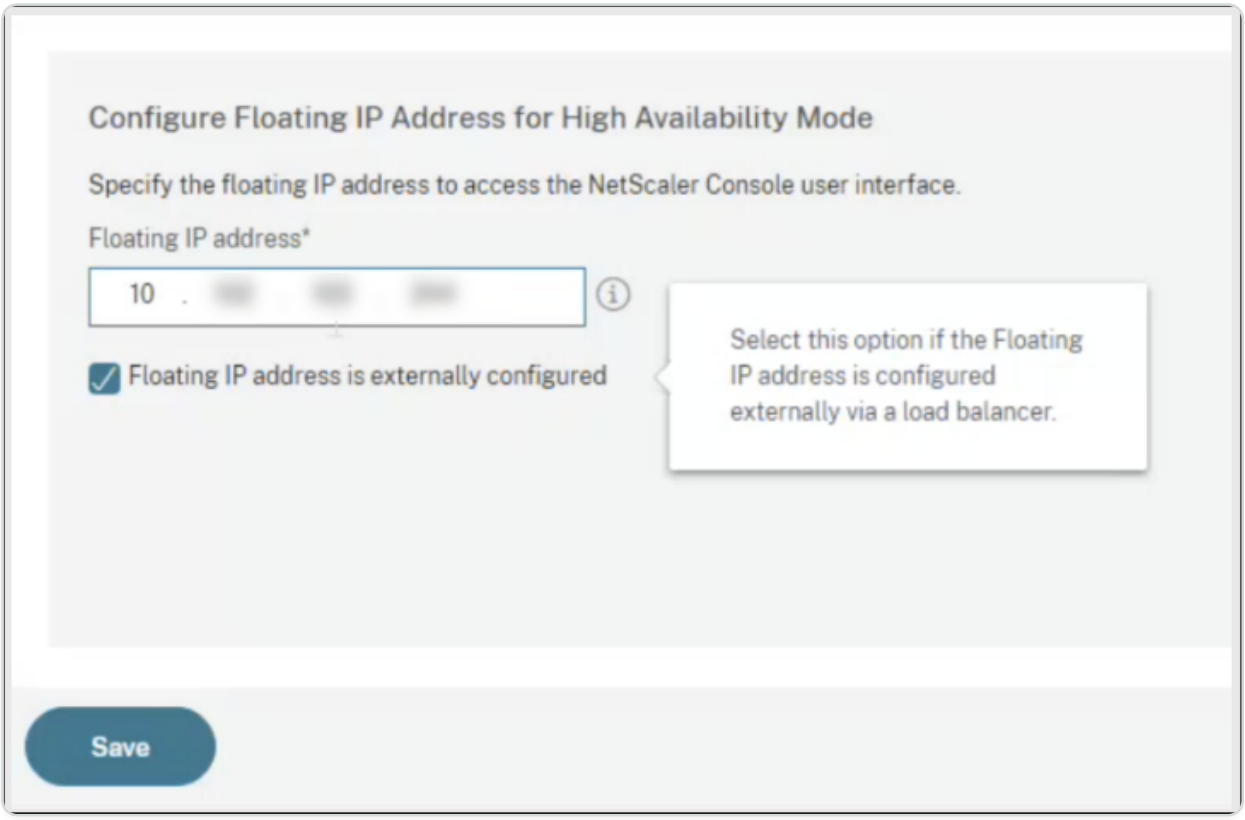
在 NetScaler Console 中配置 HA

1. 登录到您要配置为主节点的 NetScaler Console GUI。
2. 转到 **设置 > 高可用性设置**。
3. 选择 **配置 NetScaler Console 高可用性 (HA)** 并提供辅助节点详细信息。
4. 输入在外部负载均衡器上配置的 VIP，然后选择 **浮动 IP 地址是外部配置的**，并单击 **保存**。

注意：

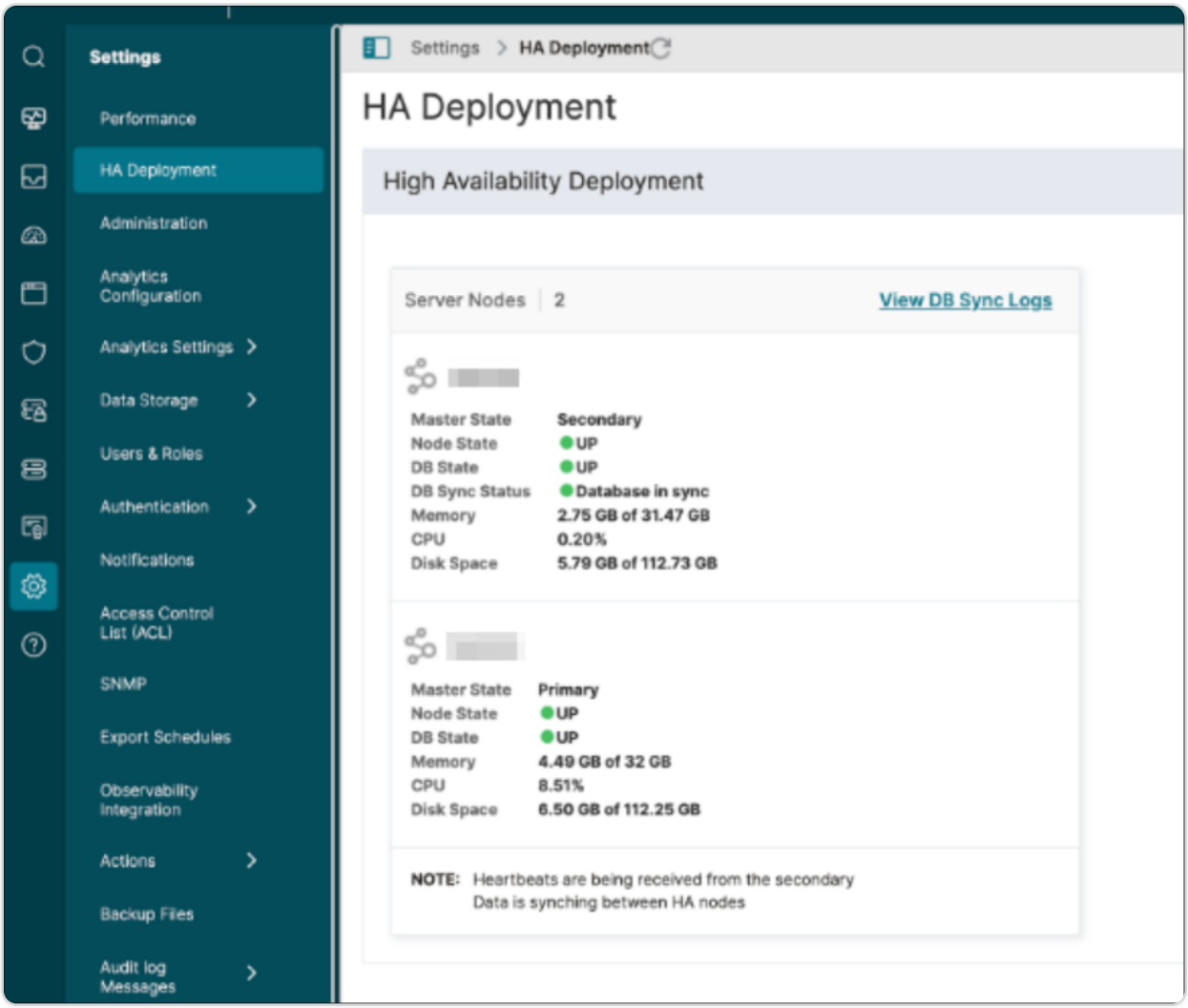
在外部负载均衡器上配置浮动 IP 地址 (VIP)。在不同子网的 HA 模型中，NetScaler Console 不拥有或管理此 VIP。

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



5. NetScaler Console 实例将重新启动以形成 HA 对。
6. 配置 HA 后，登录主节点并转到 **设置 > HA 部署** 以验证主节点和辅助节点的状态。

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



将 NetScaler 配置为外部负载均衡器

在外部负载均衡器上配置浮动 IP 地址 (VIP) 和转发规则，以便客户端流量仅发送到活动的 NetScaler Console 节点。具体步骤因负载均衡器供应商而异。以下要求普遍适用，并且可以在 NetScaler 或第三方负载均衡器上实施：

1. 创建所有具有相同虚拟 IP 地址（前端）的虚拟服务器，客户端使用该地址访问 NetScaler Console。
2. 为每个虚拟服务器创建服务组，并将两个 NetScaler Console 节点绑定为服务组成员。
3. 将服务组与相应的虚拟服务器绑定。
4. 创建可可靠指示活动节点的监视器，并将其绑定到在步骤 2 中配置的服务组。

注意：

确保负载均衡器和两个 NetScaler Console 节点之间所有必要的端口都已打开，如 系统要求 中所定义。

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

NetScaler 负载均衡配置脚本示例

添加负载均衡虚拟服务器

```
add lb vserver ADM-LB HTTP <EXTERNAL_VIP> 80 -persistenceType NONE
-cltTimeout 180



add lb vserver ADM-LB-HTTPS SSL <EXTERNAL_VIP> 443 -persistenceType NONE
-cltTimeout 180



add lb vserver ADM-LB-SNMP UDP <EXTERNAL_VIP> 162 -persistenceType NONE
-cltTimeout 120



add lb vserver ADM-LB-SYSLOG UDP <EXTERNAL_VIP> 514 -persistenceType NONE
-cltTimeout 120



add lb vserver ADM-LB-DB_HA TCP <EXTERNAL_VIP> 5454 -persistenceType NONE
-cltTimeout 9000



add lb vserver ADM-LB-LICENSE TCP <EXTERNAL_VIP> 27000 -persistenceType
NONE -cltTimeout 9000



add lb vserver ADM-LB-NTP UDP <EXTERNAL_VIP> 123 -persistenceType NONE
-cltTimeout 120



add lb vserver ADM-LB-VENDOR-DEMON TCP <EXTERNAL_VIP> 7279
-persistenceType NONE -cltTimeout 9000
```

添加服务组

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

```
add serviceGroup ADM-SVCG-HTTP HTTP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB
NO -CMP NO



add serviceGroup ADM-SVCG-HTTPS SSL -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport YES

-cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO



add serviceGroup ADM-SVCG-SNMP UDP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport NO -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO
-CMP NO



add serviceGroup ADM-SVCG-SYSLOG UDP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport NO -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO
-CMP NO



add serviceGroup ADM-SVCG-DB_HA TCP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport YES -cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB
NO -CMP NO



add serviceGroup ADM-SVCG-NTP UDP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport NO -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO
-CMP NO



add serviceGroup ADM-SVCG-LICENSE TCP -maxClient 0 -maxReq 0 -cip DISABLED
-usip NO -useproxyport YES -cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB
NO -CMP NO
```

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

```
add serviceGroup ADM-SVCG-VENDOR-DEMON TCP -maxClient 0 -maxReq 0 -cip
DISABLED -usip NO -useproxyport YES -cltTimeout 9000 -svrTimeout 9000 -CKA
NO -TCPB NO -CMP NO
```

将负载均衡虚拟服务器绑定到服务组

```
bind lb vserver ADM-LB ADM-SVCG-HTTP



bind lb vserver ADM-LB-HTTPS ADM-SVCG-HTTPS



bind lb vserver ADM-LB-SNMP ADM-SVCG-SNMP



bind lb vserver ADM-LB-SYSLOG ADM-SVCG-SYSLOG



bind lb vserver ADM-LB-DB_HA ADM-SVCG-DB_HA



bind lb vserver ADM-LB-NTP ADM-SVCG-NTP



bind lb vserver ADM-LB-LICENSE ADM-SVCG-LICENSE



bind lb vserver ADM-LB-VENDOR-DEMON ADM-SVCG-VENDOR-DEMON
```

将服务组绑定到 NetScaler Console 节点

```
bind serviceGroup ADM-SVCG-HTTP <PRIMARY_IP> 80
```

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

```
bind serviceGroup ADM-SVCG-HTTP <SECONDARY_IP> 80


bind serviceGroup ADM-SVCG-HTTPS <PRIMARY_IP> 443


bind serviceGroup ADM-SVCG-HTTPS <SECONDARY_IP> 443


bind serviceGroup ADM-SVCG-SNMP <PRIMARY_IP> 162


bind serviceGroup ADM-SVCG-SNMP <SECONDARY_IP> 162
```

添加负载均衡监视器

```
add lb monitor monitor-snmp UDP-ECV -send "Udp data" -destPort 162


add lb monitor monitor-syslog UDP-ECV -send "Udp data" -LRTM DISABLED
-destPort 514


add lb monitor monitor-db TCP-ECV -LRTM DISABLED -destPort 5454


add lb monitor monitor-ntp UDP-ECV -send "Udp data" -LRTM DISABLED
-destPort 123
```

将监视器和成员绑定到服务组

```
bind serviceGroup ADM-SVCG-SNMP -monitorName monitor-snmp
```

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

```
bind serviceGroup ADM-SVCG-SYSLOG <PRIMARY_IP> 514

bind serviceGroup ADM-SVCG-SYSLOG <SECONDARY_IP> 514

bind serviceGroup ADM-SVCG-SYSLOG -monitorName monitor-syslog

bind serviceGroup ADM-SVCG-DB_HA <PRIMARY_IP> 5454

bind serviceGroup ADM-SVCG-DB_HA <SECONDARY_IP> 5454

bind serviceGroup ADM-SVCG-DB_HA -monitorName monitor-db

bind serviceGroup ADM-SVCG-NTP <PRIMARY_IP> 123

bind serviceGroup ADM-SVCG-NTP <SECONDARY_IP> 123

bind serviceGroup ADM-SVCG-NTP -monitorName monitor-ntp

bind serviceGroup ADM-SVCG-LICENSE <PRIMARY_IP> 27000

bind serviceGroup ADM-SVCG-LICENSE <SECONDARY_IP> 27000
```

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

```
bind serviceGroup ADM-SVCG-VENDOR-DEMON <PRIMARY_IP> 7279


bind serviceGroup ADM-SVCG-VENDOR-DEMON <SECONDARY_IP> 7279
```

启用模式并更新服务组

```
enable ns mode USIP


enable ns mode MBF


set serviceGroup ADM-SVCG-SYSLOG -usip YES


set serviceGroup ADM-SVCG-SNMP -usip YES
```

优势

- **灵活且弹性部署**：在不同子网或数据中心之间启用 HA，从而改善故障隔离和可用性。
- **与现代网络架构保持一致**：支持路由 (L3) 和分段的企业环境，不受第 2 层限制。
- **利用现有基础架构**：与 NetScaler ADC 或第三方负载均衡器集成，实现可扩展且灵活的流量管理。

为高可用性配置灾难恢复

灾难是由自然灾害或人为事件引起的业务功能突然中断。灾难会影响数据中心运营，之后必须完全重建和恢复灾难现场丢失的资源和数据。数据丢失或数据中心停机至关重要，会中断业务连续性。

NetScaler Console 灾难恢复 (DR) 功能为以高可用性模式部署的 NetScaler Console 提供完整的系统备份和恢复功能。恢复时，恢复站点中提供证书、配置文件和完整的数据库备份。

下表描述了在 NetScaler Console 中配置灾难恢复时使用的术语。

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

术语	描述
主站点（数据中心 A）	主站点部署了高可用性模式的 NetScaler Console 节点。
恢复站点（数据中心 B）	恢复站点部署了独立模式的灾难恢复节点。此节点处于只读模式，在主站点关闭之前无法运行。
灾难恢复节点	恢复节点是部署在恢复站点中的独立节点。如果主站点发生灾难且无法运行，此节点将投入运行（成为新的主节点）。

注意

主站点和 DR 站点通过端口 5454 和 22 相互通信，这些端口默认启用。

有关端口和协议详细信息的更多信息，请参阅 端口。

启用基本身份验证

必须临时启用基本身份验证，以便：

- 完成代理和灾难恢复节点的初始注册。
- 从 NetScaler GUI 启动许可证激活系统 (LAS) 签出。

注意

基本身份验证仅在初始注册时需要。

配置基本身份验证

1. 导航到 **设置 > 管理 > 系统配置 > 系统、时区、允许的 URL 和代理设置**。
2. 单击 **基本设置**。
3. 选择 **启用允许基本身份验证**。
4. 单击 **OK**。

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

注意

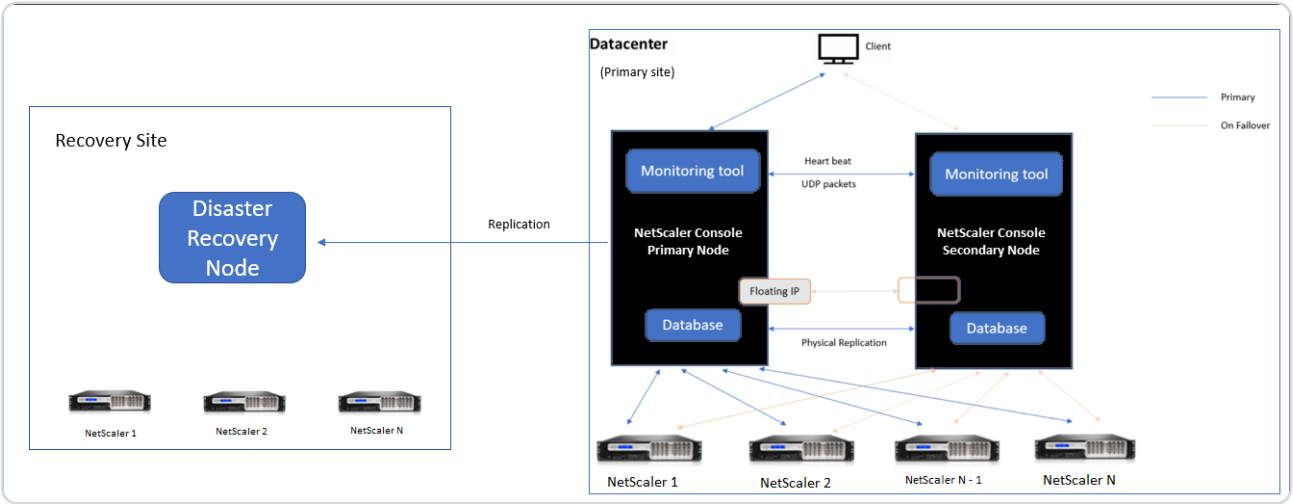
在成功配置 DR 站点之前启用基本身份验证选项；否则，将出现以下错误：

`Not valid username/password or incorrect host IP, or the host is unable to respond to the request.`.

灾难恢复工作流

下图显示了灾难恢复工作流程、灾难发生前的初始设置以及灾难发生后的工作流程。

灾难发生前的初始设置



该图显示了灾难发生前的灾难恢复设置。

主站点以高可用性模式部署了 NetScaler Console 节点。要了解更多信息，请参阅高可用性部署

恢复站点远程部署了一个独立的 NetScaler Console 灾难恢复节点。灾难恢复节点处于只读模式，并从主节点接收数据以创建数据备份。恢复站点中的 NetScaler 实例也会被发现，但没有流量流经它们。在备份过程中，所有数据、文件和配置都会从主节点复制到灾难恢复节点上。

先决条件

在设置灾难恢复节点之前，请注意以下先决条件：

- 要启用灾难恢复设置，主站点必须配置为高可用性模式的 NetScaler Console 节点。
- NetScaler Console HA 对（在主站点中）和独立节点（在 DR 站点中）必须具有相同的软件版本、内部版本和配置。

我们建议您将 CPU 优先级（在虚拟机属性中）设置为最高级别，以改善调度行为和网络延迟。

下表列出了配置灾难恢复节点的最低要求：

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

组件	要求
RAM	32 GB
虚拟 CPU	8 个 CPU
存储空间	我们建议在 NetScaler Console 部署中使用固态硬盘 (SSD) 技术。默认值为 120 GB。实际存储要求取决于 NetScaler Console 的大小估算。如果您的 NetScaler Console 存储要求超过 120 GB，则必须附加一个额外的磁盘。**注意** 您只能再添加一个磁盘。我们建议您在初始部署时估算存储并附加更多磁盘。有关详细信息，请参阅 如何将附加磁盘连接到 NetScaler Console。
虚拟网络接口	1
吞吐量	1 吉比特每秒 或 100 兆比特每秒
管理程序	**版本**
思杰 虚拟机监控程序	6.2 和 6.5
VMware ESXi 平台	5.5 和 6.0
微软 Hyper-V	2012 R2
Linux KVM 平台	乌班图和费多拉

首次灾难恢复设置

- 以高可用性模式部署 NetScaler Console
- 部署并注册 NetScaler Console 灾难恢复节点
- 从用户界面启用和禁用灾难恢复设置

以高可用性模式部署 NetScaler Console

要设置灾难恢复设置，请确保 NetScaler Console 以高可用性模式部署。有关以高可用性模式部署 NetScaler Console 的信息，请参阅高可用性部署

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

注意

- 以高可用性模式部署的 NetScaler Console 必须升级到 NetScaler Console 13.1 版本。
- 要将灾难恢复节点注册到主节点，**浮动 IP 地址是强制性的**。

使用 DR 控制台部署并注册 NetScaler Console 灾难恢复节点

要注册 NetScaler Console 灾难恢复节点：

1. 从 NetScaler 站点下载 `.xva` 镜像文件并将其导入到您的虚拟机管理程序中。
2. 在**控制台**选项卡中，使用初始网络配置来配置 NetScaler Console。

   注意

   灾难恢复节点可以位于不同的子网中。

   ```
   ------------------------------------------------------------------------
   Citrix ADM initial network configuration.
   This menu allows you to set and modify the initial IPv4 network addresses.
   The current value is displayed in brackets ([]).
   Selecting the listed number allows the address to be changed.
   ------------------------------------------------------------------------
         1. Citrix ADM Host Name [DR]:
         2. Citrix ADM IPv4 address [10.102.29.53]:
         3. Netmask [255.255.255.0]:
         4. Gateway IPv4 address [10.102.29.1]:
         5. DNS IPv4 Address [127.0.0.2]:
         6. Cancel and quit.
         7. Save and quit.

   Select a menu item from 1 to 7 [7]:
   ```

3. 初始网络配置完成后，系统会提示登录。使用以下凭据登录 – `nsrecover` / `nsroot`。

   重要

   注册期间请勿更改 DR 节点凭据 (`nsrecover` / `nsroot`)。成功注册 DR 节点后，您可以更改 DR 节点凭据。

4. 要部署灾难恢复节点，请键入 **/mps/deployment_type.py** 并按 Enter 键。将显示 NetScaler Console 部署配置菜单。

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

```
bash-3.2# /mps/deployment_type.py
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

5. 选择 **2** 以注册灾难恢复节点。

```
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 2
Selected Option      2. Remote Disaster Recovery Node.
```

6. 控制台会提示输入高可用性节点的浮动 IP 地址和密码。
7. 输入浮动 IP 地址和密码，将灾难恢复节点注册到主节点。

```
--------------------------------------------------------------------------------
    Backup node Configuration.

    Specify the IP address and the password of the Citrix ADM server.
    Type 0 anytime to cancel and quit.
    --------------------------------------------------------------------------
    Enter Citrix ADM Floating IP Address:10.102.29.97
    Enter password for Citrix ADM:
```

灾难恢复节点现已成功注册。

```
Stopping appd
Stopping nsulfd
Stopped nsulfd
Stopped appd
waiting for server to shut down.... done
server stopped
--------------------------------------------------------------------------
    Backup node Registration successful.
--------------------------------------------------------------------------
```

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

注意

- 灾难恢复节点没有 GUI。
- 注册成功后，登录服务器的默认管理员凭据为 `nsroot` / `nsroot`。

8. 如果要更改 DR 节点密码，请运行以下脚本：

```
/mps/change_freebsd_password.sh <username> <password>
```

示例：

```
/mps/change_freebsd_password.sh nsroot new_password
```

使用 NetScaler Console GUI 部署灾难恢复节点

使用 DR 控制台成功注册灾难恢复节点后，从 NetScaler Console GUI 部署 DR 节点。此步骤将启用 NetScaler Console 主站点的灾难恢复设置。

1. 导航到 **系统 \> 系统管理 \> 灾难恢复设置。**
2. 在“**灾难恢复**”页面上，选择“**部署 DR 节点**”。
3. 将显示一个确认对话框。单击“**是**”继续。

注意

系统备份所需的时间取决于数据大小和 WAN 链路速度。

在 NetScaler Console GUI 中成功部署 DR 节点后，您可以监视 DR 节点的数据库状态、内存、CPU 和磁盘使用情况。

要禁用灾难恢复设置，请选择 **移除 DR 节点**。将显示一个确认对话框。单击 **是** 继续。

要再次启用 DR 节点，请为高可用性对重新配置 DR 节点：

1. 使用虚拟机管理程序或 SSH 控制台登录到 DR 节点。
2. 请按照以下链接中的步骤配置 DR 节点：使用 DR 控制台部署和注册 NetScaler Console 灾难恢复节点。
3. 使用 NetScaler Console GUI 部署灾难恢复节点。

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

有关详细信息，请参阅常见问题解答。

重要提示

- 管理员有责任检测主站点是否发生灾难。
- 灾难恢复工作流由管理员在主站点发生故障后手动启动。
- 管理员必须通过在恢复站点的灾难恢复节点上运行恢复脚本来手动启动该过程。
- 如果升级主站点中的 HA 对，还必须手动升级 DR 站点中的独立节点。

灾难后的工作流

当主站点在灾难后发生故障时，必须按如下方式启动灾难恢复工作流：

1. 管理员识别出主站点已遭受灾难且无法运行。
2. 管理员启动恢复过程。
3. 管理员必须根据您的要求（在恢复站点）在灾难恢复节点上手动运行以下恢复脚本之一：

   - 在灾难恢复节点上配置 SNMP、Syslog 和分析：

     ```
     /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh
     ```

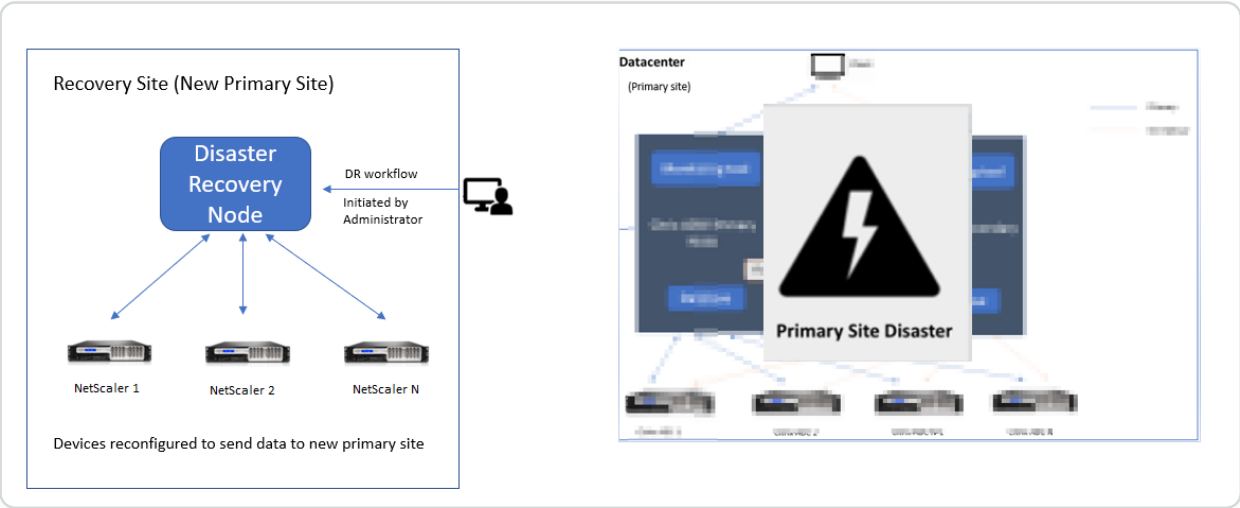
   - 还要将灾难恢复节点配置为许可证服务器：

     ```
     /mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh -reconfig-ls
     <IP-address-of-the-primary-site>
     ```

4. 在内部，NetScaler 实例会自动重新配置，以将数据发送到已成为新主站点的灾难恢复节点。

   下图显示了主站点遭受灾难后的灾难恢复工作流。

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



注意：

在灾难恢复站点启动脚本后，该灾难恢复站点将成为新的主站点。您还可以访问灾难恢复用户界面。

灾难恢复后

灾难发生后，管理员启动恢复脚本，灾难恢复站点将成为新的主站点。

如果您以后想将配置还原到原始站点，请参阅将配置还原到原始主站点。

重要

- 如果您安装了 NetScaler Console 12.1.49.x 或更早版本，您将获得 30 天的宽限期，在此期间可以联系 Citrix 在 NetScaler Console（在灾难恢复站点）上重新托管原始许可证。
- 对于 12.1.50.x 或更高版本，NetScaler Console 许可证会自动同步到灾难恢复站点（无需联系 Citrix 获取许可证）。
- 如果您已为实例应用了池化许可证，则版本为 **11.1 65.x 或更高版本**、**12.1 58.x 或更高版本**、**13.0 47.x 或更高版本**以及 NetScaler SDX **13.0 76.x 或更高版本**的 NetScaler 实例支持在灾难恢复站点自动更新许可证服务器。所有其他版本，您必须手动将实例重新配置到灾难恢复站点。

将配置恢复到原始主站点

灾难发生后，配置的灾难恢复 (DR) 节点将成为新的主站点，客户端流量将通过此节点。

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

灾难后的设置(/en-us/netscaler-application-delivery-management-software/media/disaster-recovery-node-active-console.png)

有关详细信息，请参阅灾难后的工作流程。

当您的原始主站点摆脱灾难，并且您决定将所有操作移回主站点时，请重新配置原始主站点以匹配 DR 节点的配置。

在开始之前，请确保主站点和 DR 站点都处于活动状态。

要将更改从 DR 站点恢复到原始主站点，请执行以下步骤：

1. 登录到原始主站点并运行以下命令：

   ```
   nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
   password> -L <primary-node-password> &
   ```

   此命令仅将 Syslog、SNMP 和 Analytics 配置到主站点。

   如果要将主站点配置为 NetScaler 实例的池化许可证服务器，请运行以下命令：

   ```
   nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
   password> -L <primary-node-password>  -O yes &
   ```

   `-O` 命令获取 DR 站点 IP 地址，并将主站点重新配置为池化许可证服务器。

2. 重新配置 DR 站点。请参阅部署灾难恢复设置。

恢复到原始主站点(/en-us/netscaler-application-delivery-management-software/media/revert-to-original-primary-site-console.png)

成功将配置从 DR 站点恢复到原始主站点后，客户端流量将通过 NetScaler Console 主节点。

为独立节点配置灾难恢复

您还可以为以独立模式部署的 NetScaler Console 配置灾难恢复。

下表描述了在 NetScaler Console 中配置灾难恢复时使用的术语。

术语	描述
主站点（数据中心 A）	主站点部署了独立模式的 NetScaler Console 节点。

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

术语	描述
恢复站点（数据中心 B）	恢复站点部署了一个独立模式的灾难恢复节点。此节点处于只读模式，并且在主站点发生故障之前不会运行。
灾难恢复节点	恢复节点是部署在恢复站点中的独立节点。如果主站点发生灾难且无法正常运行，此节点将投入运行（成为新的主节点）。

注意

主站点和灾难恢复站点通过端口 5454 和 22 进行通信，这些端口默认启用。

有关端口和协议的更多信息，请参阅 端口。

灾难恢复工作流

主站点部署了独立模式的 NetScaler Console 节点。

恢复站点远程部署了一个灾难恢复节点。灾难恢复节点处于只读模式，并从主节点接收数据以创建数据备份。恢复站点中的 NetScaler 实例也会被发现，但它们没有流量流经。在备份过程中，所有数据、文件和配置都会从主节点复制到灾难恢复节点。

先决条件

在设置灾难恢复节点之前，请注意以下先决条件：

- 要启用灾难恢复设置，主站点必须将 NetScaler Console 配置为独立模式。
- 独立的 NetScaler Console（在主站点中）和灾难恢复节点（在灾难恢复站点中）必须具有相同的软件版本、内部版本和配置。

建议您将 CPU 优先级（在虚拟机属性中）设置为最高级别，以改善调度行为和网络延迟。

下表列出了配置灾难恢复节点的最低要求：

组件	要求
内存	32 GB
虚拟 CPU	8 个 CPU

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

组件	要求
存储空间	建议为 NetScaler Console 部署使用固态硬盘 (SSD) 技术。默认值为 120 GB。实际存储要求取决于 NetScaler Console 的大小估算。如果您的 NetScaler Console 存储要求超过 120 GB，则必须附加一个额外的磁盘。**注意** 您只能再添加一个磁盘。建议您在初始部署时估算存储并附加更多磁盘。有关详细信息，请参阅 如何将附加磁盘连接到 NetScaler Console。
虚拟网络接口	1
吞吐量	1 千兆位/秒 或 100 兆位/秒
管理程序	**版本**
Citrix 管理程序	6.2 和 6.5
威睿 ESXi	5.5 和 6.0
微软 Hyper-V	2012 R2
Linux KVM 虚拟化	乌班图 和 费多拉

首次灾难恢复设置

- 部署 NetScaler Console
- 部署并注册 NetScaler Console 灾难恢复节点
- 从用户界面启用和禁用灾难恢复设置

部署 NetScaler Console

要设置灾难恢复设置，请确保 NetScaler Console 以独立模式部署。有关详细信息，请参阅 单服务器部署。

使用 DR 控制台部署并注册 NetScaler Console 灾难恢复节点

要注册 NetScaler Console 灾难恢复节点：

1. 从 NetScaler 站点下载 `.xva` 映像文件，并将其导入到您的虚拟机管理程序中。
2. 在“**控制台**”选项卡中，使用初始网络配置来配置 NetScaler Console。

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

注意

灾难恢复节点可以位于不同的子网中。

```
--------------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
--------------------------------------------------------------------------
      1. Citrix ADM Host Name [DR]:
      2. Citrix ADM IPv4 address [10.102.29.53]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

Select a menu item from 1 to 7 [7]:
```

3. 初始网络配置完成后，系统会提示登录。使用以下凭据登录 – `nsrecover` / `nsroot`。

重要

注册期间请勿更改 DR 节点凭据 (`nsrecover` / `nsroot`)。成功注册 DR 节点后，您可以更改 DR 节点凭据。

4. 要部署灾难恢复节点，请键入 **/mps/deployment_type.py** 并按 Enter 键。将显示 NetScaler Console 部署配置菜单。

```
bash-3.2# /mps/deployment_type.py
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

5. 选择 **2** 以注册灾难恢复节点。

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

```
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 2
Selected Option      2. Remote Disaster Recovery Node.
```

6. 控制台会提示输入独立节点的 IP 地址和密码。
7. 输入独立节点的 IP 地址和密码以注册灾难恢复节点。

   灾难恢复节点现已成功注册。

```
Stopping appd
Stopping nsulfd
Stopped nsulfd
Stopped appd
waiting for server to shut down.... done
server stopped
--------------------------------------------------------------------------
    Backup node Registration successful.
--------------------------------------------------------------------------
```

注意

- 灾难恢复节点没有 GUI。
- 注册成功后，登录服务器的默认管理员凭据为 `nsroot` / `nsroot`。

8. 如果要更改 DR 节点密码，请运行以下脚本：

```
/mps/change_freebsd_password.sh <username> <password>
```

示例：

```
/mps/change_freebsd_password.sh nsroot new_password
```

使用 NetScaler Console GUI 部署灾难恢复节点

在使用 DR 控制台成功注册灾难恢复节点后，从 NetScaler Console GUI 部署 DR 节点。此步骤将启用 NetScaler Console 主站点的灾难恢复设置。

1. 导航到 **系统 \> 系统管理 \> 灾难恢复设置**。

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

2. 在**灾难恢复**页面上，选择**部署 DR 节点**。
3. 将显示一个确认对话框。单击**是**继续。

> **注意**
>
> 系统备份所需的时间取决于数据大小和 WAN 链路速度。

在 NetScaler Console GUI 中成功部署 DR 节点后，您可以监控 DR 节点的数据库状态、内存、CPU 和磁盘使用情况。

要禁用灾难恢复设置，请选择**删除 DR 节点**。将显示一个确认对话框。单击**是**继续。

要再次启用 DR 节点，请为高可用性对重新配置 DR 节点：

1. 使用虚拟机管理程序或 SSH 控制台登录到 DR 节点。
2. 按照 使用 DR 控制台部署和注册 NetScaler Console 灾难恢复节点 中提供的步骤配置 DR 节点。
3. 使用 NetScaler Console GUI 部署灾难恢复节点。

有关更多信息，请参阅 常见问题。

> **重要**
>
> - 管理员有责任检测主站点是否发生了灾难。
> - 灾难恢复工作流在主站点发生故障后由管理员手动启动。
> - 管理员必须通过在恢复站点的灾难恢复节点上运行恢复脚本来手动启动该过程。
> - 如果您升级主站点中的独立节点，则还必须手动升级灾难恢复站点中的独立节点。

灾难发生后的工作流

当主站点在灾难发生后宕机时，必须按如下方式启动灾难恢复工作流：

1. 管理员确认主站点已遭受灾难且无法运行。
2. 管理员启动恢复过程。
3. 管理员必须根据您的要求（在恢复站点）在灾难恢复节点上手动运行以下恢复脚本之一：
    - 在灾难恢复节点上配置 SNMP、Syslog 和分析：

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

```
/mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh
```

- 将灾难恢复节点也配置为许可证服务器：

```
/mps/scripts/pgsql/pgsql\_restore\_remote\_backup.sh -reconfig-ls
<IP-address-of-the-primary-site>
```

4. 在内部，NetScaler 实例会自动重新配置，以将数据发送到已成为新主站点的灾难恢复节点。

注意：

在灾难恢复站点启动脚本后，灾难恢复站点现在成为新的主站点。您还可以访问灾难恢复用户界面。

灾难恢复后

灾难发生后，管理员启动恢复脚本，灾难恢复站点现在成为新的主站点。

如果您想稍后将配置还原到原始站点，请参阅 将配置还原到原始主站点。

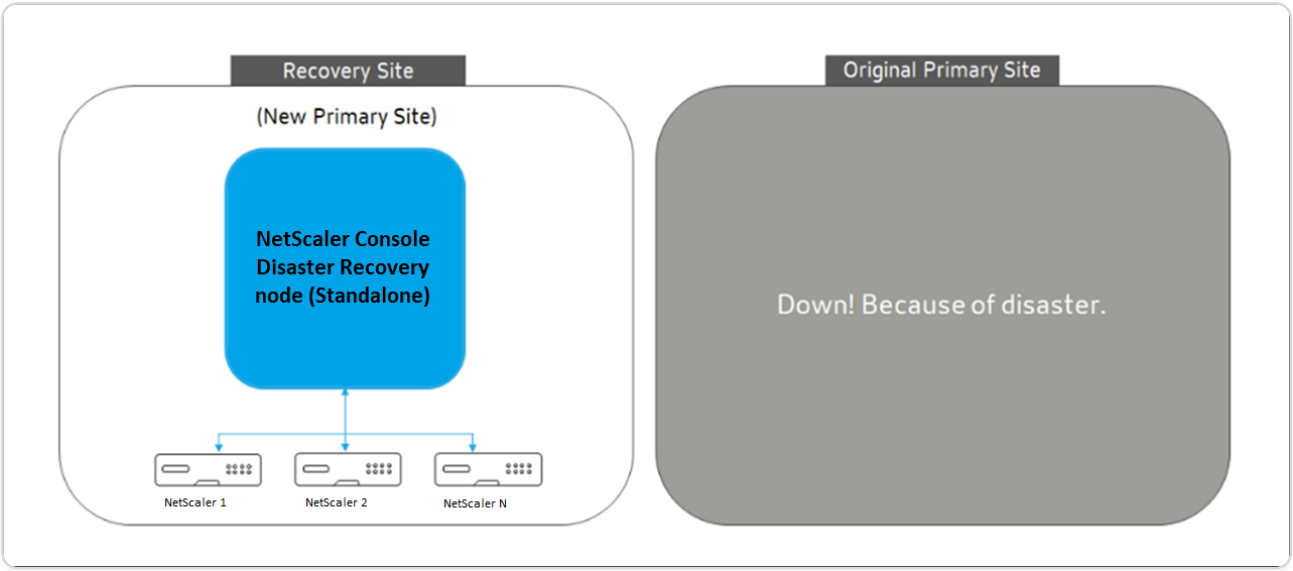
重要

- 如果您安装了 NetScaler Console 12.1.49.x 或更早版本，您将获得 30 天的宽限期，在此期间可以联系 Citrix 将原始许可证重新托管到 NetScaler Console（在灾难恢复站点）。
- 对于 12.1.50.x 或更高版本，NetScaler Console 许可证会自动同步到灾难恢复站点（无需联系 Citrix 获取许可证）。
- 如果您已为实例应用了池化许可证，则版本为 **11.1 65.x 或更高版本**、**12.1 58.x 或更高版本**、**13.0 47.x 或更高版本** 的 NetScaler 实例以及 **13.0 76.x 或更高版本** 的 NetScaler SDX 支持在灾难恢复站点自动更新许可证服务器。所有其他版本，您必须手动将实例重新配置到灾难恢复站点。

将配置还原到原始主站点

灾难发生后，配置的灾难恢复 (DR) 节点将成为新的主站点，客户端流量将通过此节点流经。

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



有关更多信息，请参阅 灾难后的工作流程。

当您的原始主站点摆脱灾难并且您决定将所有操作移回主站点时，请重新配置原始主站点以匹配灾难恢复节点的配置。

在开始之前，请确保主站点和灾难恢复站点都处于活动状态。

要将更改从灾难恢复站点还原到原始主站点，请执行以下步骤：

1. 登录到原始主站点并运行以下命令：

   ```
   nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
   password> -L <primary-node-password> &
   ```

   此命令仅将 Syslog、SNMP 和 Analytics 配置到主站点。

   如果您想将主站点配置为 NetScaler 实例的池化许可证服务器，请运行以下命令：

   ```
   nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
   password> -L <primary-node-password>  -O yes &
   ```

   `-O` 命令获取灾难恢复站点的 IP 地址，并将主站点重新配置为池化许可证服务器。

2. 重新配置灾难恢复站点。请参阅 部署灾难恢复设置。

成功将配置从灾难恢复站点恢复到原始主站点后，客户端流量将通过 NetScaler Console 主节点。

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

配置用于多站点部署的本地代理

在早期版本的 NetScaler Console 中，部署在远程数据中心的 NetScaler 实例可以从主数据中心运行的 NetScaler Console 进行管理和监控。NetScaler 实例直接将数据发送到主 NetScaler Console，这导致了 WAN 带宽的消耗。此外，分析数据的处理会占用主 NetScaler Console 的 CPU 和内存资源。

您的数据中心可以遍布全球。代理在以下场景中发挥着至关重要的作用：

- 在远程数据中心安装代理，以减少 WAN 带宽消耗。
- 限制直接向主 NetScaler Console 发送流量进行数据处理的实例数量。

注意

- 建议为远程数据中心中的实例安装代理，但并非强制要求。如有必要，用户可以直接将 NetScaler 实例添加到主 NetScaler Console。
- 如果您已为一个或多个远程数据中心安装了代理，则代理与主站点之间的通信通过浮动 IP 地址进行。有关更多信息，请参阅 端口。
- 您可以在一个或多个远程数据中心安装代理并将池化许可证应用于实例。在此场景中，主站点与一个或多个远程数据中心之间的通信通过浮动 IP 地址进行。
- NetScaler Console 本地代理不支持池化许可。

从 NetScaler Console 12.1 或更高版本开始，实例可以配置代理以与位于不同数据中心的主 NetScaler Console 进行通信。

代理作为主 NetScaler Console 与不同数据中心中发现的实例之间的中介。安装代理的好处如下：

- 实例配置为代理，以便将未处理的数据直接发送到代理，而不是主 NetScaler Console。代理执行第一级数据处理，并将压缩格式的处理数据发送到主 NetScaler Console 进行存储。
- 代理和实例位于同一数据中心，从而加快数据处理速度。
- 对代理进行集群可在代理故障转移时重新分配 NetScaler 实例。当站点中的一个代理发生故障时，来自 NetScaler 实例的流量将切换到同一站点中的另一个可用代理。

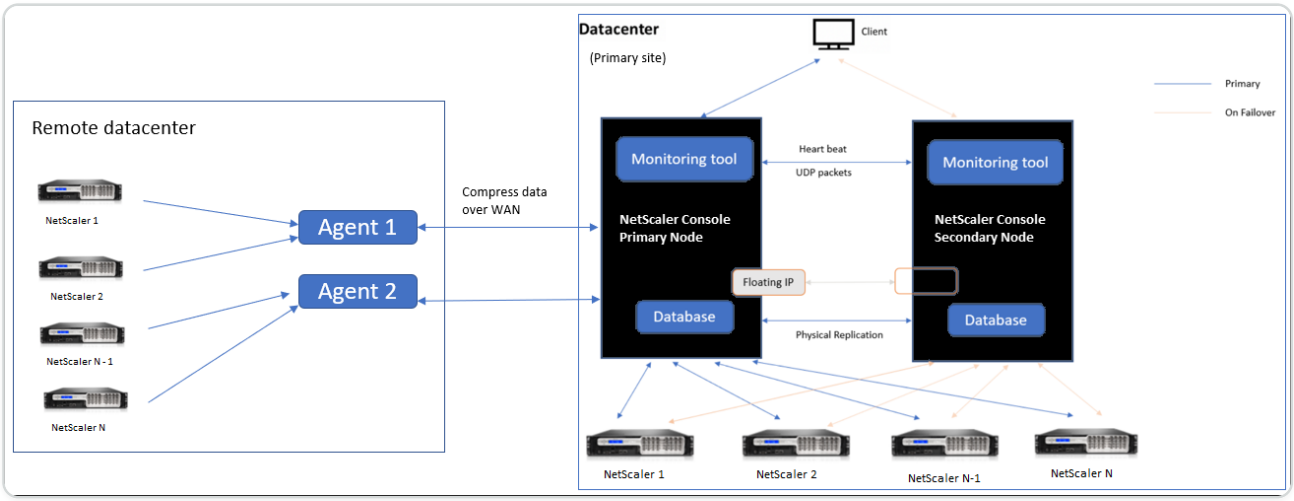
注意

每个站点要安装的代理数量取决于正在处理的流量。

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

架构

下图显示了两个数据中心中的 NetScaler 实例以及使用多站点基于代理的架构的 NetScaler Console 高可用性部署。



主站点部署了高可用性配置的 NetScaler Console 节点。主站点中的 NetScaler 实例直接注册到 NetScaler Console。

在辅助站点中，代理部署并注册到主站点中的 NetScaler Console 服务器。这些代理以集群方式工作，以在代理故障转移发生时处理连续的流量。辅助站点中的 NetScaler 实例通过位于该站点内的代理注册到主 NetScaler Console 服务器。实例直接将数据发送到代理，而不是主 NetScaler Console。代理处理从实例接收到的数据，并以压缩格式将其发送到主 NetScaler Console。代理通过安全通道与 NetScaler Console 服务器通信，并且通过该通道发送的数据经过压缩以提高带宽效率。

启用基本身份验证

必须暂时启用基本身份验证以：

- 完成代理和灾难恢复节点的初始注册。
- 从 NetScaler GUI 启动许可证激活系统 (LAS) 签出。

注意：

基本身份验证仅在初始注册时需要。

配置基本身份验证

1. 导航到 **设置 > 管理 > 系统配置 > 系统、时区、允许的 URL 和代理设置**。
2. 点击**基本设置**。

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

3. 选择**启用允许基本身份验证**。
4. 点击**确定**。

入门

- 在数据中心安装代理
  - 注册代理
  - 将代理关联到站点
- 添加 NetScaler 实例
  - 添加新实例
  - 更新现有实例

在数据中心安装代理

您可以安装和配置代理，以启用主 NetScaler Console 与另一个数据中心中托管的 NetScaler 实例之间的通信。

您可以在企业数据中心中的以下管理程序上安装代理：

- 思杰虚拟化管理程序™
- 威睿 ESXi
- 微软 Hyper-V
- Linux KVM 服务器

注意

多站点部署的本地代理仅支持 NetScaler Console 高可用性部署。

在开始安装代理之前，请确保您拥有虚拟机监控程序必须为每个代理提供的所需虚拟计算资源。

组件	要求
内存	32 GB
虚拟 CPU	8 个 CPU
存储空间	30 GB

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

组件	要求
虚拟网络接口	1
吞吐量	1 千兆位/秒

端口

为了通信目的，代理与 NetScaler Console 本地部署服务器之间必须打开以下端口。

类型	端口	详细信息	通信方向
TCP	8443、7443、443	用于代理与 NetScaler Console 本地部署服务器之间的出站和入站通信。	NetScaler 代理到 NetScaler Console

代理与 NetScaler 实例之间必须打开以下端口。

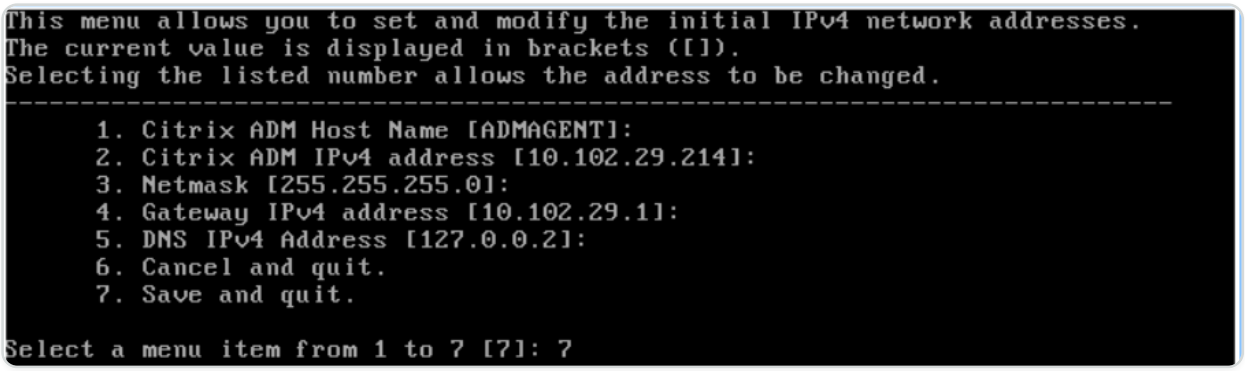
类型	端口	详情	通信方向
TCP	80	用于代理与 NetScaler 实例之间的 NITRO 通信。	NetScaler Console 到 NetScaler 以及 NetScaler 到 NetScaler Console
TCP	22	用于代理与 NetScaler 实例之间的 SSH 通信。用于高可用性模式下部署的 NetScaler Console 服务器之间的同步。	NetScaler Console 到 NetScaler 以及 NetScaler 代理到 NetScaler
UDP	4739	用于代理与 NetScaler 实例之间的 AppFlow 通信。	NetScaler 到 NetScaler Console 的连接
ICMP	无保留端口	用于检测 NetScaler Console 和 NetScaler 实例之间，或以高可用性模式部署的辅助	

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

类型	端口	详情	通信方向
		NetScaler Console 服务器之间的网络可达性。	
UDP	161, 162	用于从 NetScaler 实例接收 SNMP 事件到代理。	端口 161 - NetScaler Console 到 NetScaler
			端口 162 - NetScaler 到 NetScaler Console
UDP	514	用于从 NetScaler 实例接收 syslog 消息到代理。	奈思乐 至 奈思乐 控制台
TCP	5557	用于代理和 NetScaler 实例之间的 Logstream 通信。	奈思乐 至 奈思乐 控制台

注册代理

1. 使用从 NetScaler 站点下载的代理映像文件，并将其导入到您的虚拟机管理程序中。代理映像文件的命名模式如下：**MASAGENT-\<HYPERVISOR\>-\<Version.no\>.** 例如：**MASAGENT-XEN-13.0-xy.xva**
2. 在“**控制台**”选项卡中，使用初始网络配置来配置 NetScaler Console。
3. 输入 NetScaler Console 主机名、IPv4 地址和网关 IPv4 地址。选择选项 7 以保存并退出配置。



4. 注册成功后，控制台会提示登录。使用 *nsrecover/nsroot* 作为凭据。
5. 要注册代理，请输入 **/mps/register_agent_onprem.py**。NetScaler 代理注册凭据将显示，如以下图像所示。

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

6. 输入 NetScaler Console 浮动 IP 地址和用户凭据。

```
bash-3.2# /mps/register_agent_onprem.py

--------------------------------------------------------------------------------
----------------------------------------
Citrix ADM Agent Registration with Citrix ADM On-Prem Server. This menu allows y
ou to specify Citrix ADM Server IP Address and admin credentials.
If Citrix ADM is deployed in HA mode, it is advisable to register with Citrix AD
M floating IP Address.
--------------------------------------------------------------------------------
----------------------------------------
    Enter IP Address or URL:10.102.29.211
    Enter User Name:nsroot
    Enter Password:

Trying to register this agent with Citrix ADM  10.102.29.211
Dec  3 18:07:52 <auth.notice> ns date: date set by nsrecover
--------------------------------------------------------------------------
    Citrix ADM Agent Registration successful.
--------------------------------------------------------------------------
```

注册成功后，代理将重新启动以完成安装过程。

代理重新启动后，访问 NetScaler Console GUI，从主菜单转到“**基础结构 > 实例 > 代理**”页面以验证代理的状态。新添加的代理将显示为“**正常运行**”状态。

注意

NetScaler Console 显示代理的版本，并检查代理是否为最新版本。下载图标表示代理不是最新版本，需要升级。我们建议您将代理版本升级到 NetScaler Console 版本。

将代理附加到站点

1. 选择代理，然后单击“**附加站点**”。
2. 在“**附加站点**”页面中，从列表中选择一个站点，或使用加号 (+) 按钮创建一个站点。
3. 单击“**保存**”。

注意

- 默认情况下，所有新注册的代理都将添加到默认数据中心。
- 将代理与正确的站点关联非常重要。如果代理发生故障，分配给它的 NetScaler 实例将自动切换到同一站点中其他正常运行的代理。

代理操作

您可以在“**基础结构 > 代理 > 选择操作**”下对代理应用各种操作。

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

在“**选择操作**”下，您可以使用以下功能：

安装新证书：如果您需要不同的代理证书来满足您的安全要求，可以添加一个。

更改默认密码：为确保基础结构的安全，请更改代理的默认密码。

生成技术支持文件：为选定的 NetScaler 代理生成技术支持文件。您可以下载此文件并将其发送给 Citrix 技术支持进行调查和故障排除。

添加 NetScaler 实例

实例是您希望通过代理从 NetScaler Console 发现、管理和监控的 NetScaler 设备或虚拟设备。您可以将以下 NetScaler 设备和虚拟设备添加到 NetScaler Console 或代理中：

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler 网关
- Citrix SSL 正向代理

更多信息，请参阅将实例添加到 NetScaler Console。

将现有实例附加到代理

如果实例已添加到主 NetScaler Console，您可以通过编辑代理将其附加到代理。

1. 导航到**基础结构 > 实例**，然后选择实例类型。例如，NetScaler。
2. 单击**编辑**以编辑现有实例。
3. 单击以选择代理。
4. 在**代理**页面上，选择要与实例关联的代理，然后单击**确定**。

> **注意**
>
> 确保选择要与实例关联的**站点**。

访问实例的 GUI 以验证事件

添加实例并配置代理后，访问实例的 GUI 以检查是否配置了陷阱目标。

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

在 NetScaler Console 中，导航到**基础架构 > 实例**。在**实例**下，选择要访问的实例类型（例如，NetScaler VPX），然后单击特定实例的 IP 地址。

所选实例的 GUI 将显示在一个弹出窗口中。

默认情况下，代理在实例上配置为陷阱目标。要确认，请登录实例的 GUI 并检查陷阱目标。

重要

建议为远程数据中心中的 NetScaler 实例添加代理，但不是强制性的。

如果您想将实例直接添加到主 MAS，则在添加实例时不要选择**代理**。

NetScaler 代理故障转移

代理故障转移可能发生在具有两个或更多注册代理的站点中。当站点中的代理变为非活动状态（DOWN 状态）时，NetScaler Console 会将非活动代理的 NetScaler 实例重新分配给其他活动代理。

重要

- 确保您的帐户已启用**代理故障转移**功能。要启用此功能，请参阅启用或禁用 NetScaler Console 功能。
- 如果代理正在运行脚本，请确保该脚本存在于站点中的所有代理上。因此，更改后的代理可以在代理故障转移后运行该脚本。

要在 NetScaler Console GUI 中将站点附加到代理，请参阅将代理附加到站点。

要实现代理故障转移，请逐个选择 NetScaler 代理并将其附加到同一站点。

例如，两个代理 10.106.1xx.2x 和 10.106.1xx.3x 已在班加罗尔站点中附加并运行。如果其中一个代理变为非活动状态，NetScaler Console 会检测到它并将其状态显示为“关闭”。

当 NetScaler 代理在站点中变为非活动状态（关闭状态）时，NetScaler Console 会等待五分钟，直到代理变为活动状态（启动状态）。如果代理仍处于非活动状态，NetScaler Console 会自动将实例重新分配给同一站点中的可用代理。

NetScaler Console 每 30 分钟触发一次实例重新分配，以平衡站点中活动代理之间的负载。

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

配置代理不可达阈值和通知

如果代理在特定持续时间内处于关闭状态或无法访问，您可以通过电子邮件、Slack、PagerDuty 和 ServiceNow 获取代理状态通知。在 **Infrastructure > Instances > Agents** 中，单击 **Settings**，指定 5 到 60 分钟之间的持续时间，然后选择您希望接收通知的方式。

代理阈值通知(/en-us/netscaler-application-delivery-management-software/media/agent-threshold-notification.png)

NetScaler® Console 代理与 NetScaler Console 之间的安全通信

NetScaler Console 代理与 NetScaler Console 之间的安全通信适用于 14.1-34.x 或更高版本。您可以通过验证 Console 服务器 SSL 证书来启用此安全通信。以前，NetScaler Console 代理与 NetScaler Console 本地服务器之间的通信未验证 Console 服务器 SSL 证书，从而导致潜在的安全漏洞。

要启用此安全通信，请执行以下操作：

1. 确保 NetScaler Console 已配置 SSL 证书。
2. 登录到 NetScaler Console 代理。
3. 将 CA 根证书放置在 **/mpsconfig/console_onprem_cacert**。这用于验证服务器证书。CA 根证书的名称必须是 **cacert.pem**。
4. 通过运行以下命令配置安全通信。 **Configure_secure_communication_with_server.py**
5. 这将提示输入 NetScaler Console 服务器的 FQDN（完全限定域名）或 IP 地址。
6. 输入 FQDN 或 IP 地址以完成脚本执行。

   安全通信(/en-us/netscaler-application-delivery-management-software/media/secure-communication-mitm.png)
7. 脚本使用提供的 CA 根证书验证由 FQDN 或 IP 地址提供的服务器证书。如果证书验证通过，则启用安全通信。
8. 此脚本可以在代理注册到 NetScaler Console 之前或之后调用。

注意：

这仅适用于基于 VM 的代理。

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

在 Kubernetes 集群上将 NetScaler® 代理安装为微服务

如果您正在使用本地部署的 NetScaler Console，则出于一些特定的战略和技术原因，会使用容器代理。其中一些重要原因包括：

- **云原生工作负载的无缝管理** - 使用容器代理的主要原因是管理 NetScaler CPX（NetScaler 的容器化版本）。
- **本地化控制**：代理充当您的本地 Console 与在 Kubernetes 集群中运行的 NetScaler CPX 实例之间的许可代理。
- **简化连接（微服务架构）** - 如果您的 NetScaler Console 和 Kubernetes 集群位于不同的网络上，则容器代理充当安全的“集群内”网关。

注意：

- 您还可以配置本地代理，并在托管 Kubernetes 集群的网络上注册该代理。
- 从 NetScaler Console 14.1 build 60.x 版本开始，NetScaler Console 支持使用容器化控制台代理。使用容器化控制台代理可简化 Kubernetes 或 OpenShift 平台上托管实例的连接和监控。

入门

1. 在 NetScaler Console 中，导航到 **基础架构 > 实例 > 代理**。
2. 从 **选择操作** 列表中，选择 **下载代理微服务** 选项。
3. 在 **下载代理微服务** 页面中，指定以下参数：
   - **应用程序 ID** – 一个字符串 ID，用于定义 Kubernetes 集群中代理的服务，并将此代理与同一集群中的其他代理区分开来。
   - **密码** – 为 NetScaler CPX 指定一个密码，以便 NetScaler CPX 使用此密码通过代理加入 NetScaler Console。
   - **确认密码** – 指定相同的密码进行确认。

     注意：

     - 您不得使用默认密码 (`nsroot`)。
4. 单击“**下载 Yaml 文件**”。

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

在 Kubernetes 集群中安装 NetScaler 代理

在 Kubernetes 主节点中执行以下步骤：

1. 保存下载的 YAML 文件。
2. 运行以下命令：

   ```
   kubectl create -f <yaml file>
   ```

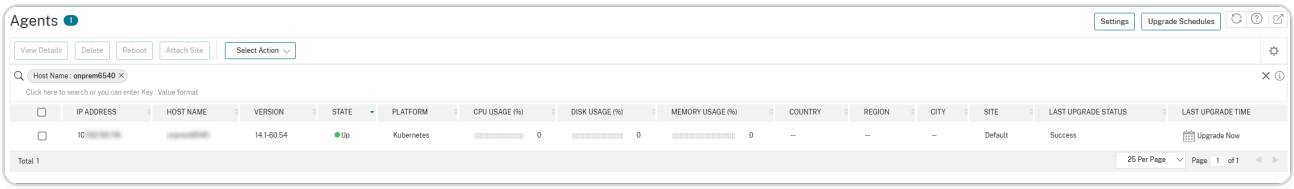
   示例：

   ```
   kubectl create -f onprem6540.yaml
   ```

代理已成功创建。

```
root@master:~# kubectl create -f onprem6540.yaml
clusterrole.rbac.authorization.k8s.io/onprem6540 created
serviceaccount/onprem6540 created
clusterrolebinding.rbac.authorization.k8s.io/onprem6540 created
deployment.apps/onprem6540-kad created
service/onprem6540-kad created
deployment.apps/onprem6540-redis created
service/onprem6540-redis created
deployment.apps/onprem6540-core created
service/onprem6540 created
deployment.apps/onprem6540-lic created
service/onprem6540-lic created
deployment.apps/onprem6540-sharding created
secret/onprem6540 created
configmap/onprem6540 created
horizontalpodautoscaler.autoscaling/admagent-hpa created
service/onprem6540-logstream created
root@master:~# kubectl get pods
NAME                                  READY   STATUS    RESTARTS   AGE
onprem6540-core-67f94c6967-b4hws      1/1     Running   0          17m
onprem6540-kad-775f64dc6-6vlct        1/1     Running   0          17m
onprem6540-lic-68fbdd466d-v2nvq       1/1     Running   0          17m
onprem6540-redis-56d8c4b89-bdbgp      1/1     Running   0          17m
onprem6540-sharding-5b6cbb55d6-n8rx2  1/1     Running   0          17m
root@master:~#
```

在 NetScaler Console 中，导航到“**基础结构 > 实例 > 代理**”以查看代理状态。



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

配置代理后，您可以添加 NetScaler CPX 实例并在服务图中查看分析。有关详细信息，请参阅：

- 将 NetScaler NetScaler CPX 实例添加到 NetScaler Console
- 设置服务图

为 NetScaler Console 本地部署安装 NetScaler Console 代理 OpenShift 操作器

如果您使用的是 NetScaler Console 本地部署，则使用容器代理有几个特定的战略和技术原因。其中一些重要原因包括：

- **云原生工作负载的无缝管理** - 使用容器代理的主要原因是管理 NetScaler CPX（NetScaler 的容器化版本）。
- **本地化控制** - 该代理充当您的 NetScaler Console 本地部署与在 Kubernetes 集群中运行的 NetScaler CPX 实例之间的许可代理。
- **简化连接（微服务架构）** - 如果您的 NetScaler Console 和 Kubernetes 集群位于不同的网络上，则容器代理充当安全的“集群内”网关。

注意：

NetScaler Console 代理支持从 NetScaler Console 本地部署 14.1.60.x 开始的 NetScaler Console 本地部署。

操作器是一种开源工具包，可让您以有效、自动化和可扩展的方式部署和管理 Kubernetes 应用程序。作为管理员，您可以使用 **NetScaler® ADM Agent Operator** 在 OpenShift 集群中部署代理。

注意：

在 OpenShift 集群中配置的代理默认情况下不会自动升级。

先决条件

在部署之前，请确保：

- 您拥有特权安全上下文约束来控制 Pod 的权限。对于代理，运行以下命令以获取服务帐户的特权安全上下文约束：

```
oc adm policy add-scc-to-user privileged -z adm-agent-serviceaccount
```

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

- 运行以下命令以创建代理登录密钥 (`loginsecret`)：

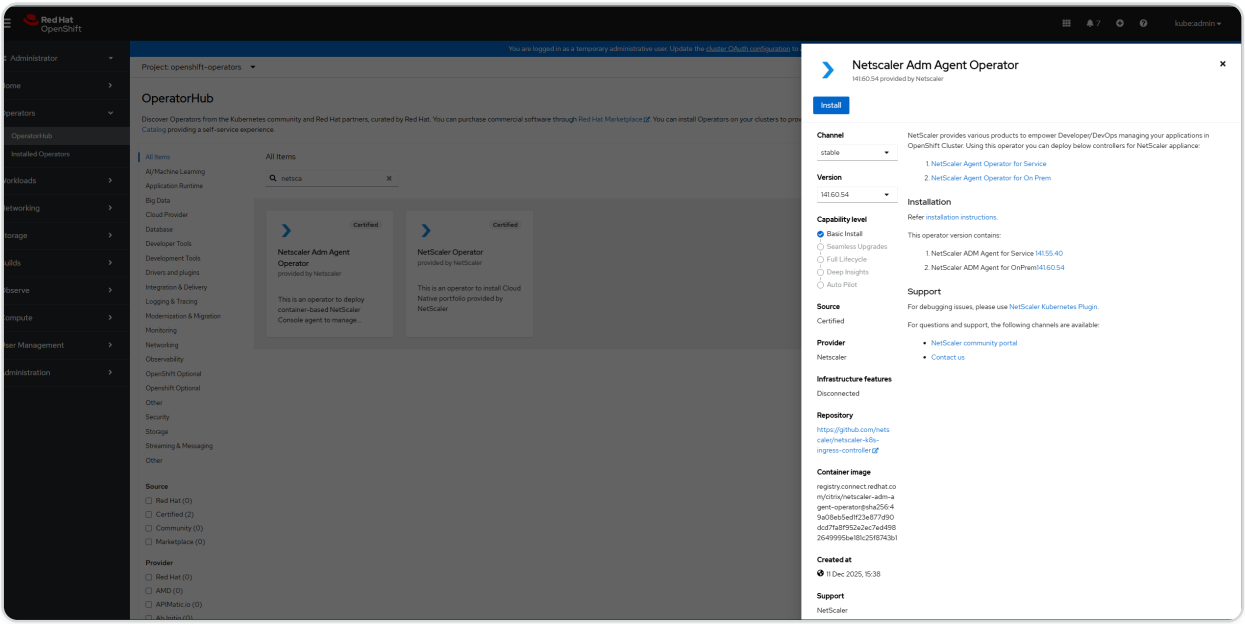
```
oc create secret generic admlogin --from-literal=username=nsroot --
from-literal=password=<NetScaler Console-agent-password> -n <namespace>
```

- 运行以下命令以创建 NetScaler Console 服务器的密钥 (`accessSecret`) 密钥：

```
oc create secret generic testonprem--from-literal=username=nsroot --
from-literal=password=< NetScaler Console password> -n <namespace>
```

安装代理操作员

1. 登录到 OpenShift 集群控制台。
2. 导航到 **Operators > OperatorHub**。
3. 在搜索栏中，提供代理名称并选择 **NetScaler ADM Agent Operator**，然后单击 **Install**。



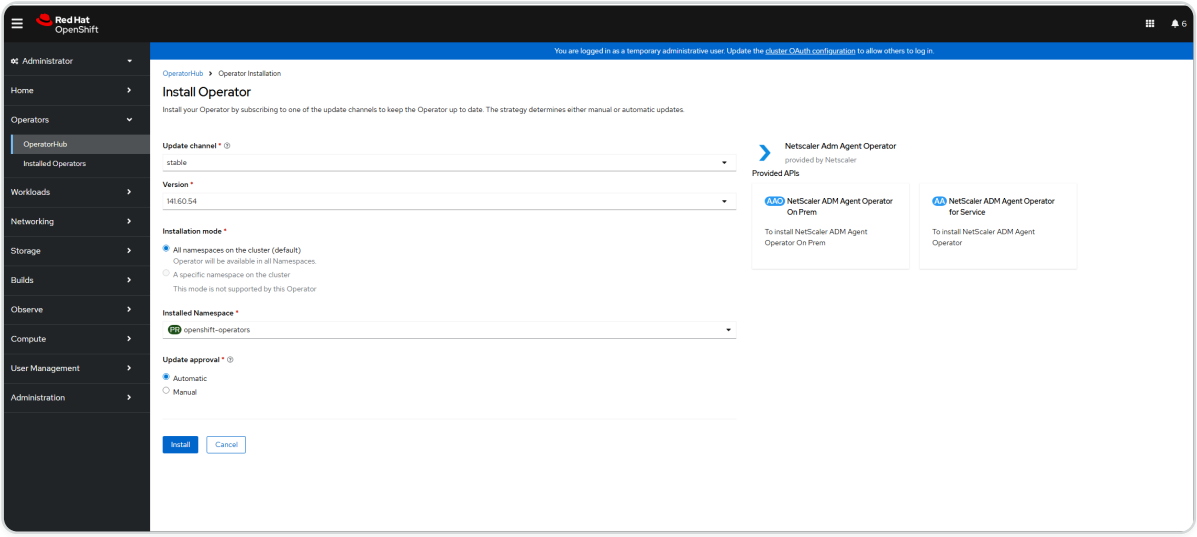
4. 在 **Install Operator** 页面中，您有两个选项：

   a. **集群上的所有命名空间（默认）** - 使代理操作员能够订阅集群中所有可用的命名空间，并允许您从集群上的任何命名空间启动代理操作员实例。

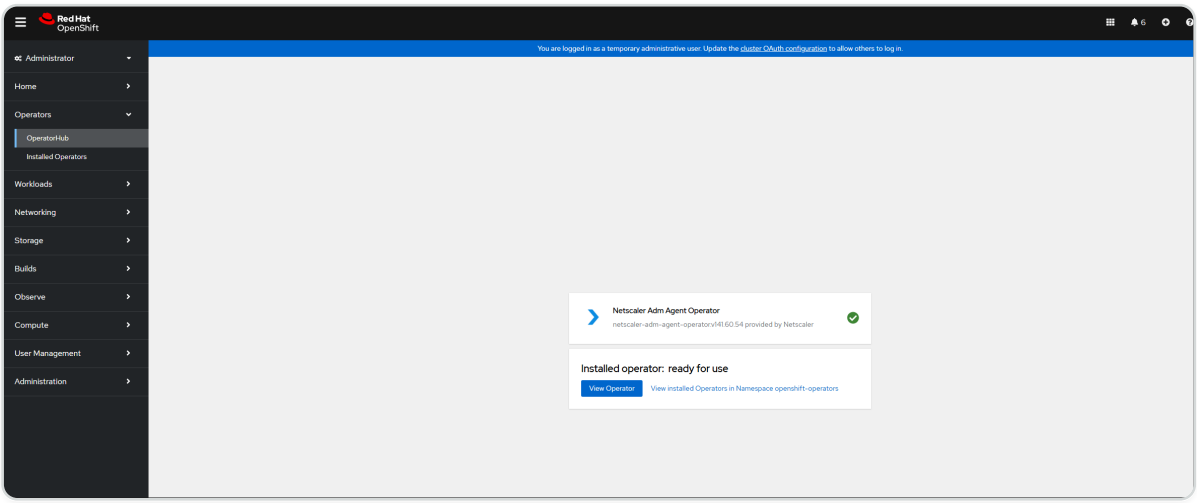
   b. **集群上的特定命名空间** - 使代理操作员能够订阅集群上选定的命名空间，并且您只能从选定的命名空间启动代理操作员实例。

   在此示例中，代理操作员被分配给名为 **Default** 的命名空间。在 **Update approval** 下选择 **Automatic**，然后单击 **Install**。

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

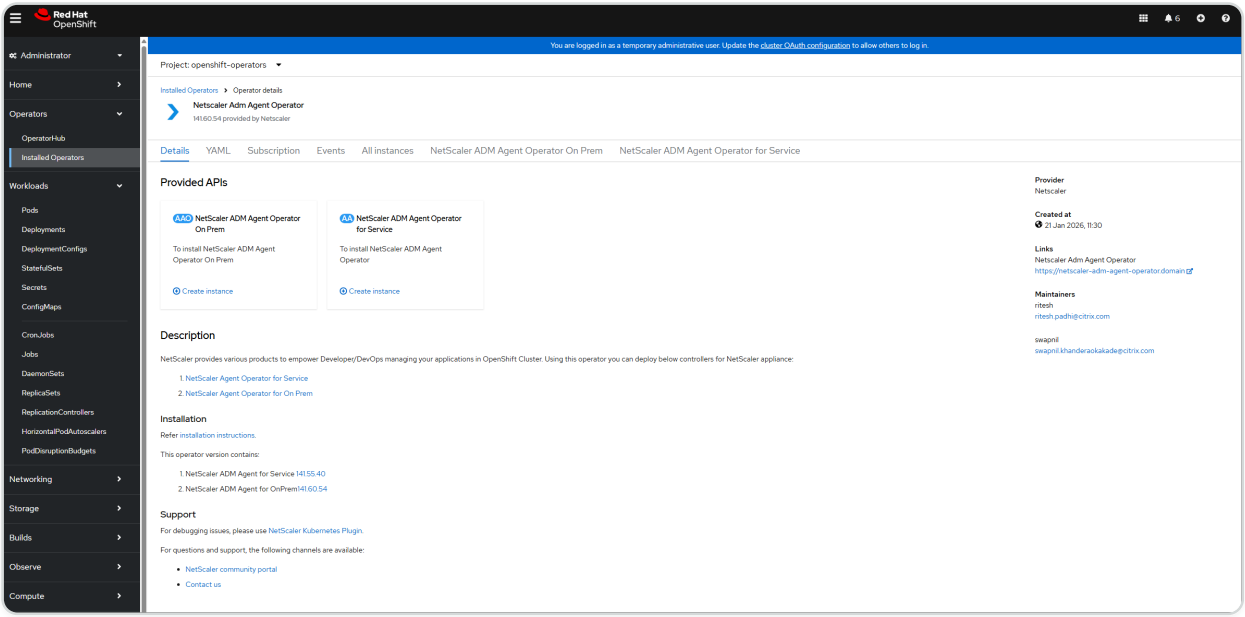


等待代理操作员成功订阅。



5. 导航到 **Workloads > Pods** 并验证 `netscaler-adm-agent-operator-controller` pod 正在运行。
6. 在 pod 启动并运行后，您应该在 **NetScaler ADM Agent Operator** 中看到两个控制台代理实例。单击 **NetScaler ADM Agent Operator On Prem** 以部署代理。

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



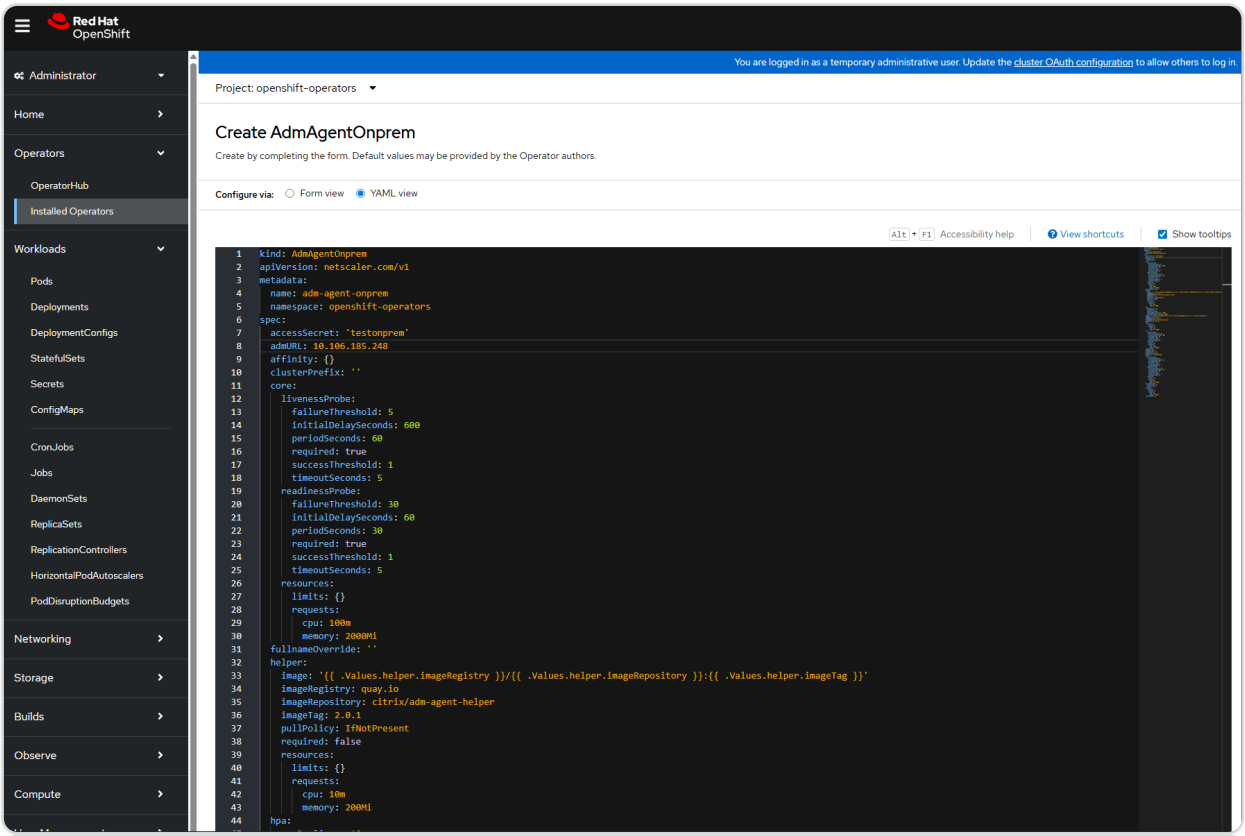
7. 选择 **YAML 视图** 以更新任何参数，然后点击 **创建**。

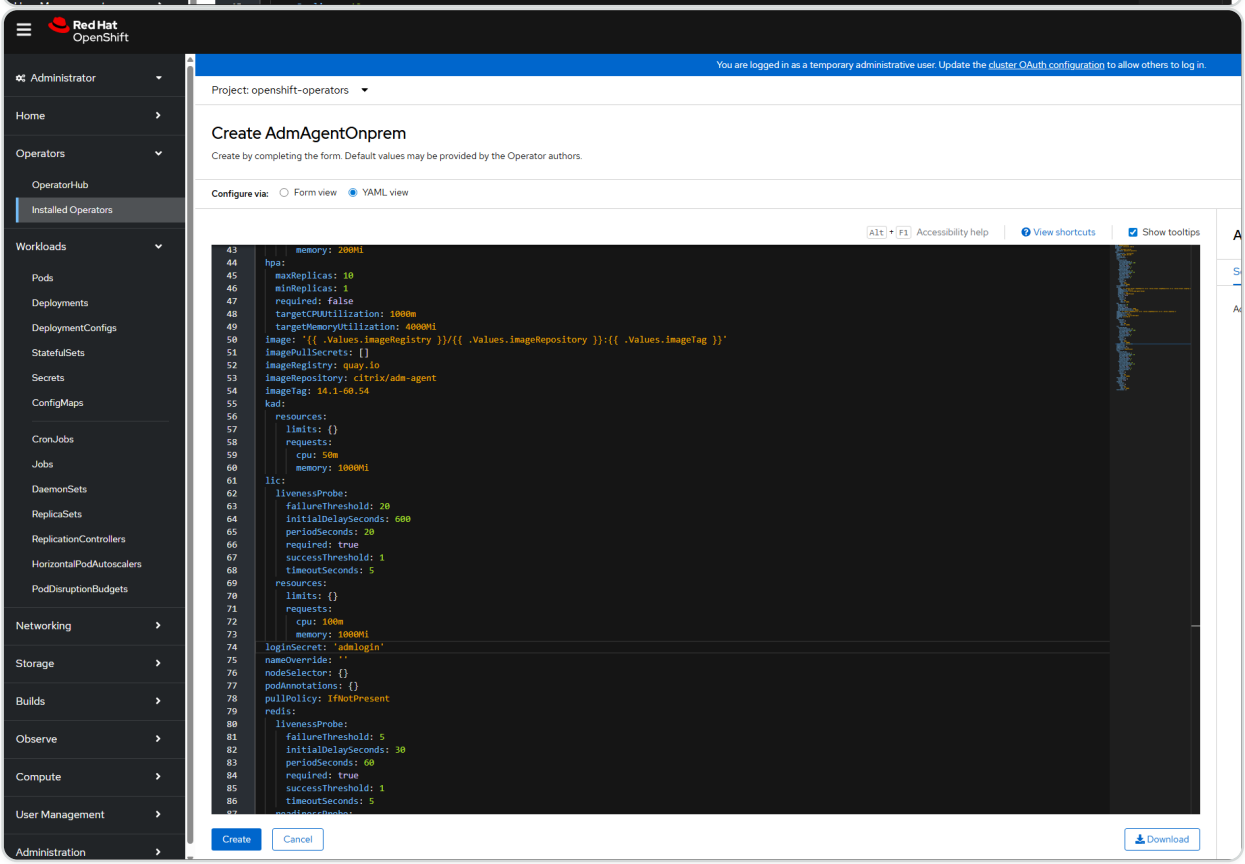
> **注意：**
>
> 确保每个 OpenShift 集群只有一个代理实例。

以下三个参数是强制性的：

- `accessSecret`：名为 `testonprem` 的 Secret 已创建。
- `AdmURL`：NetScaler Console IP 地址。
- `loginsecret`：名为 `admlogin` 的 Secret 已创建。

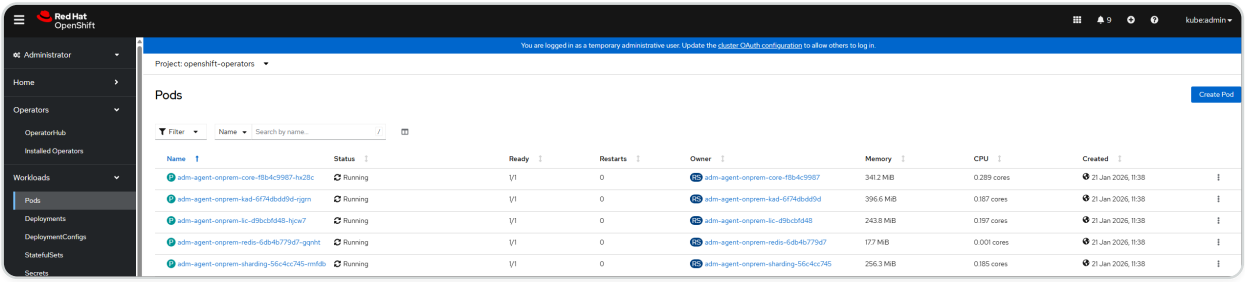
© 1997–2026 Citrix Systems, Inc. All rights reserved.





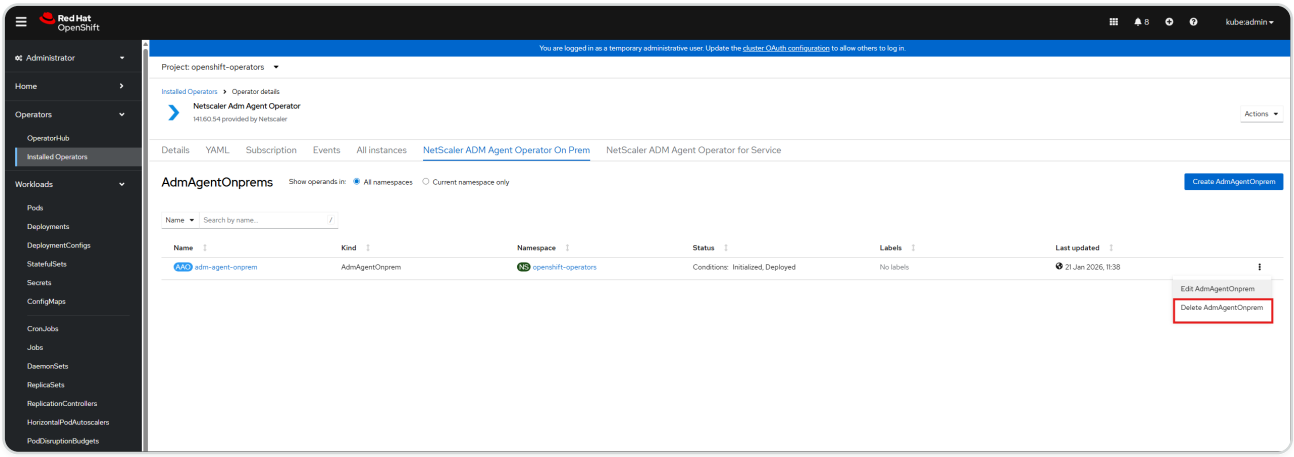
8. 导航到 **工作负载 > Pods** 并确保代理 Pod 正在运行。

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



删除代理实例

您可以通过导航到 **Operators > Installed Operators** 从集群中删除代理实例。在 **NetScaler ADM Agent Operator** 选项卡中，选择该实例，然后从列表中选择 **Delete AdmAgentOnPrems**。



卸载代理操作员

如果您想从集群中卸载代理操作员 Pod，请导航到 **Operators > Installed Operators**，然后从列表中选择 **Uninstall Operator**。

NetScaler 操作员卸载 ADM 代理（本地部署）(/en-us/netscaler-application-delivery-management-software/media/netscaler-agent-uninstall.png)

升级代理

注意：

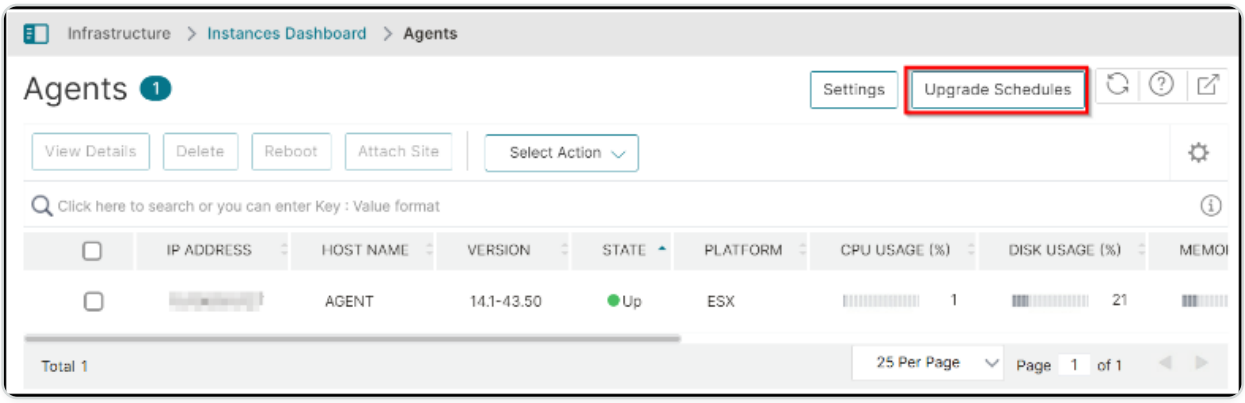
确保代理版本为 14.1-38.x 或更高版本。

从 14.1–43.50 开始，您可以通过 NetScaler Console GUI 升级 NetScaler 代理（14.1-38.x 或更高版本）。此增强功能消除了每个代理的手动升级工作流，使您能够在一个工作流中升级所有代理或安排在以后升级。

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

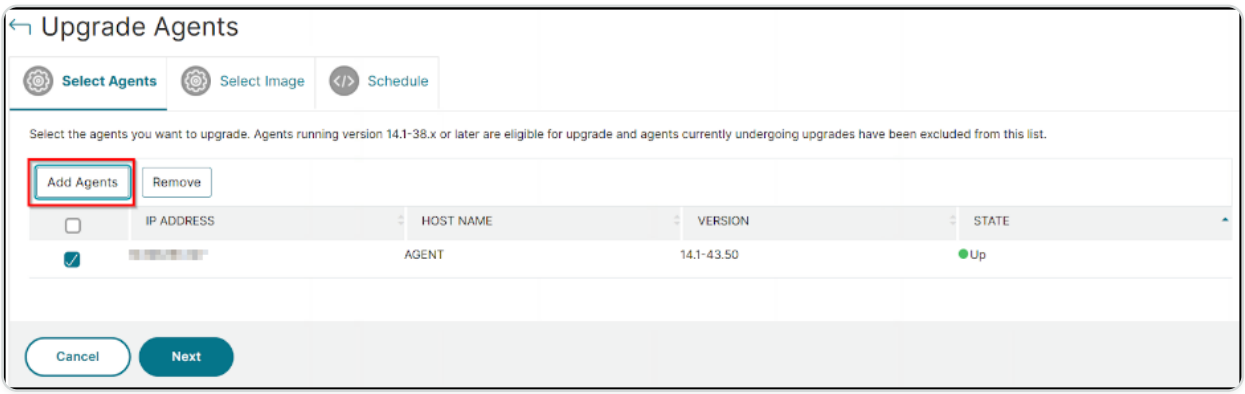
升级工作流

1. 导航到 **基础设施 > 实例 > 代理**。
2. 单击 **升级计划**。



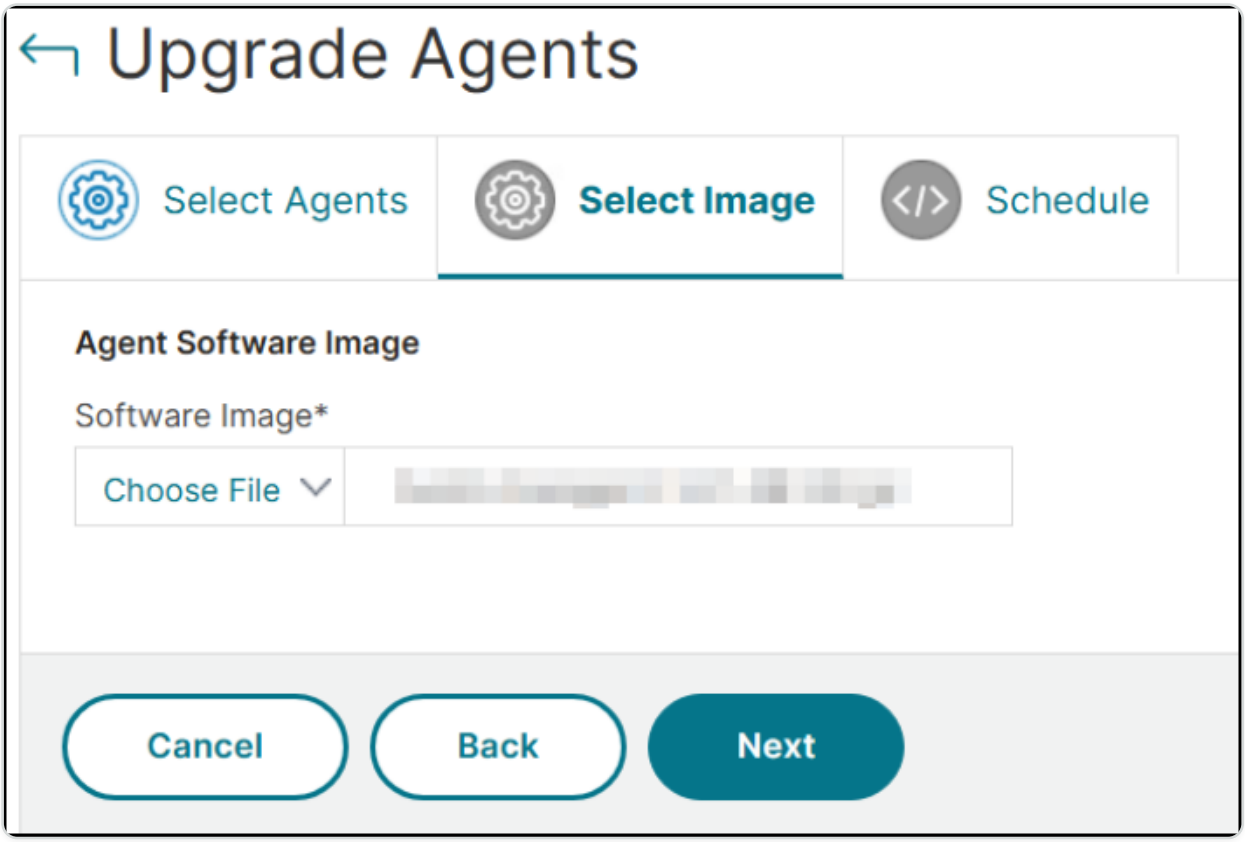
3. 在 **Upgrade Schedules** 页面中，单击 **Add**。
4. 单击 **Add Agents**，从列表中选择要升级的代理，然后单击 **Next**。

> **注意：**
>
> 仅显示运行版本 14.1-38.x 或更高版本的代理。

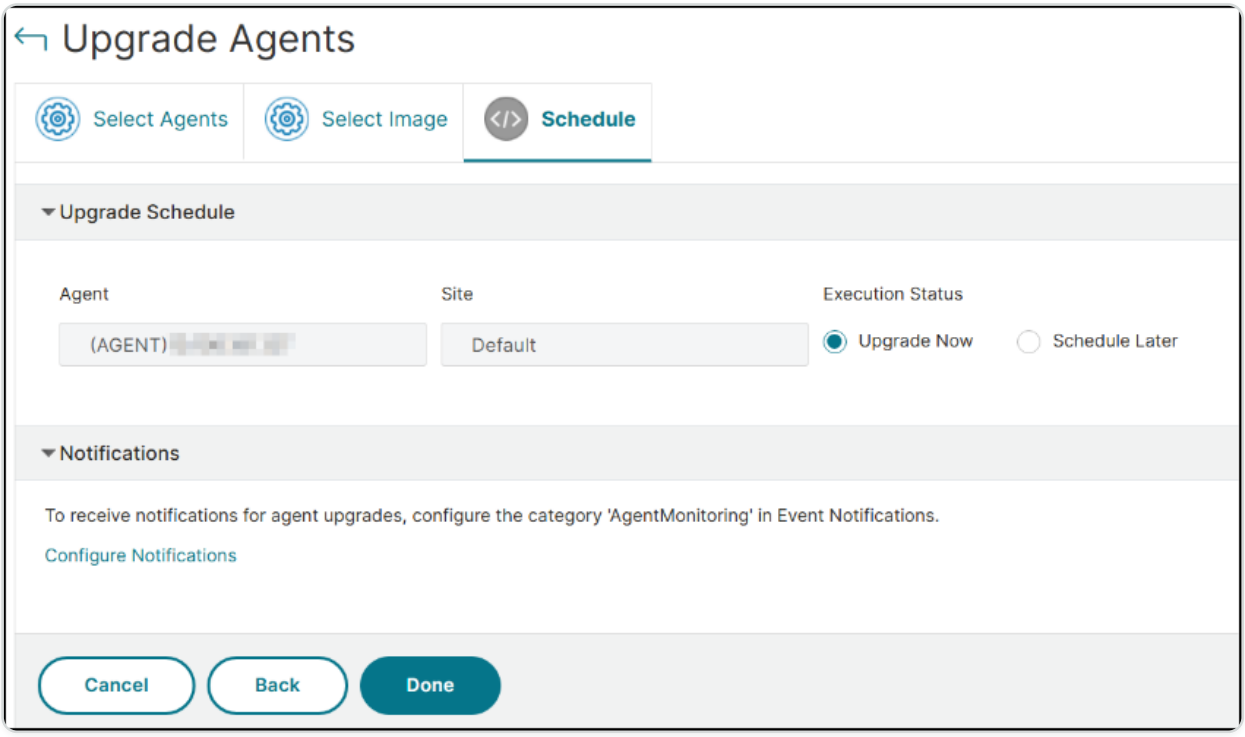


5. 在 **Select Image** 选项卡中，从本地或设备中选择一个映像 (.tgz)。您可以从本地计算机或设备上传映像。当您选择 **Appliance** 时，NetScaler Console GUI 会显示 `/var/mps/mas_agent_images` 中存在的映像。从列表中选择一个映像。

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

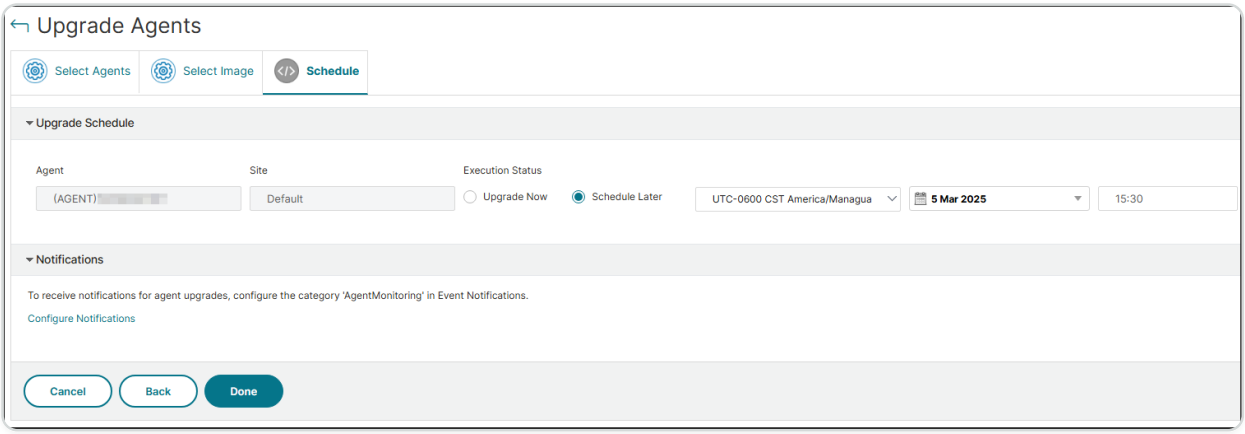


6. 选择映像后，单击“**下一步**”。
7. 在“**升级计划**”下，选择“**立即升级**”以立即升级。



如果要安排升级，请选择“**稍后安排**”，然后通过选择时区、日期和时间（24 小时制）来提供详细信息。

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



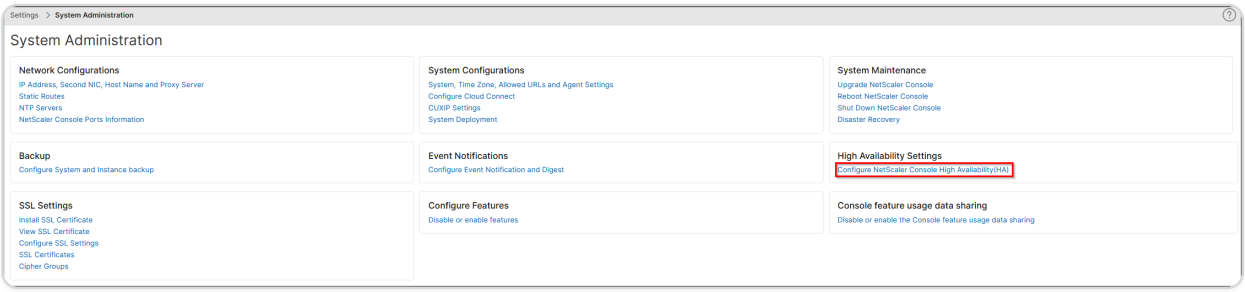
8. 如果您希望收到升级工作流的通知，请在“**通知**”下单击“**配置通知**”，选择类别 `AgentMonitoring`，然后选择您希望收到通知的通信选项（电子邮件、短信、Slack、PagerDuty 和 ServiceNow）。
9. 单击“**完成**”。

将 NetScaler Console 单服务器部署迁移到高可用性部署

您可以将 NetScaler Console 单服务器升级到由两台 NetScaler Console 服务器组成的高可用性部署。NetScaler Console 服务器的高可用性对处于主动-被动模式，两台服务器具有相同的配置。在这种主动-被动部署中，一台 NetScaler Console 服务器配置为主节点，另一台配置为辅助节点。如果主节点因任何原因发生故障，辅助节点将接管。有关详细信息，请参阅 配置高可用性部署。

要将 NetScaler Console 单服务器迁移到高可用性对，您必须：

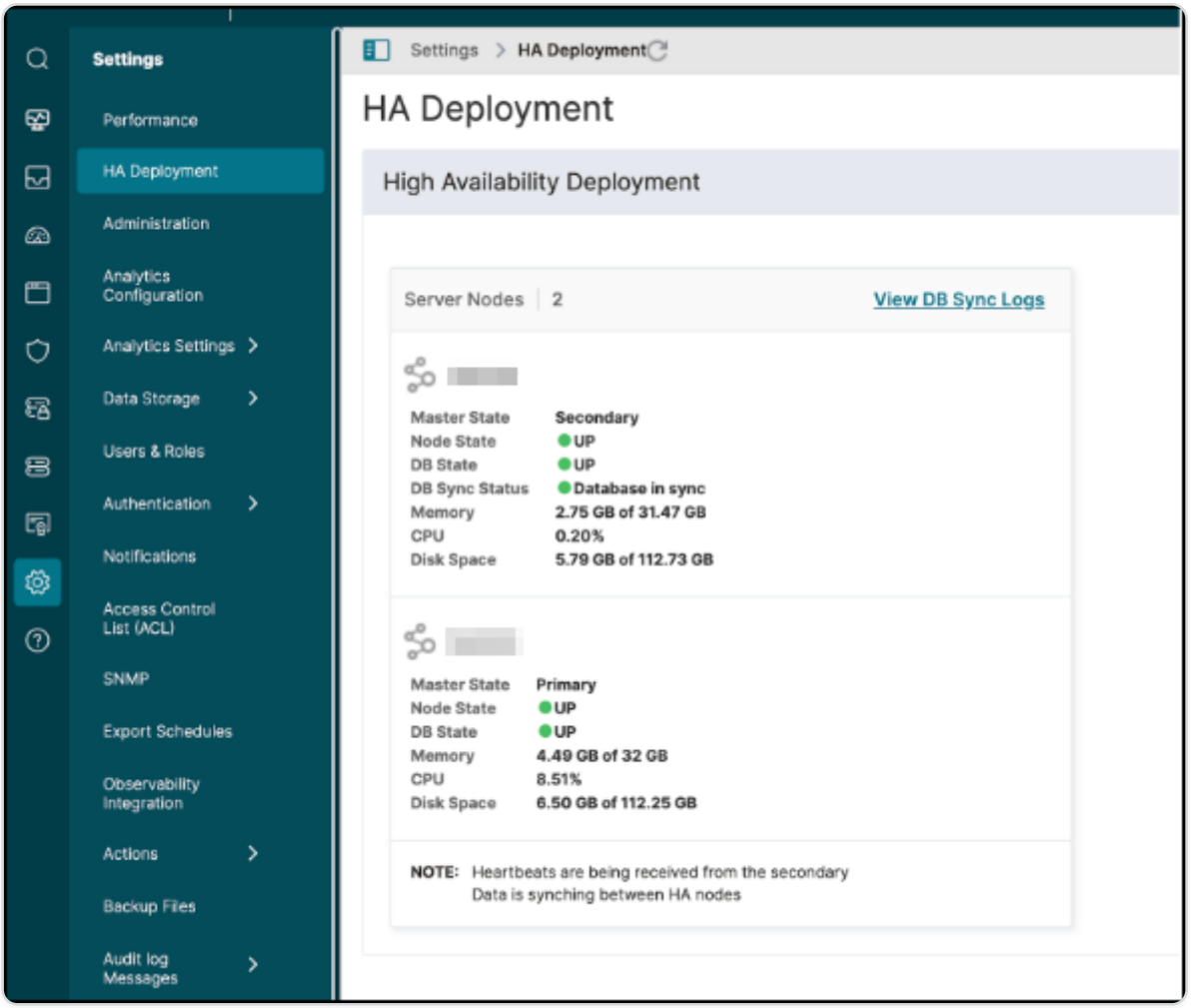
1. 登录到单个 NetScaler Console 服务器。
2. 导航到 **设置 > 管理**，然后在 **高可用性设置** 下单击 **配置 NetScaler® Console 高可用性 (HA)**。



3. 在 **配置 NetScaler Console 高可用性 (HA)** 页面中：
   a. 提供辅助 NetScaler Console 服务器 IP 地址。
   b. 指定辅助节点密码。
   c. 指定浮动 IP 地址。
   d. 单击 **配置**。

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

4. 在确认窗口中，单击 **是**。NetScaler Console 实例将重新启动以形成 HA 对。
5. HA 对配置完成后，登录到主 NetScaler Console 并导航到 **设置 > HA 部署** 以验证主节点和辅助节点。



从 NetScaler Insight Center 迁移到 NetScaler Console

您现在可以将 NetScaler Insight Center 部署迁移到 NetScaler Console，而不会丢失现有配置、设置或数据。借助 NetScaler Console，您不仅可以查看与应用程序关联的 NetScaler 实例生成的各种分析数据，还可以从一个统一的控制台管理、监视和排查整个全球应用程序交付基础架构。

注意

目前仅支持在 NetScaler® Insight Center 独立实例上进行迁移。

先决条件

在将 NetScaler Insight Center 虚拟设备迁移到 NetScaler Console 之前，请验证是否满足以下要求：

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

- 已安装 NetScaler Insight Center 11.1 Build 47.14 或更高版本。
- 您已下载 NetScaler Console 12.0 build 57.24 .tgz 映像文件。

> **注意**
>
> 您必须安装 NetScaler Console 12.0 build 57.24，然后升级到最新的 NetScaler Console 13.1 版本。有关详细信息，请参阅 升级。

- 您已下载 NetScaler Console 13.1 最新版本 .tgz 映像文件。

硬件要求

组件	要求
RAM	32 GB
虚拟 CPU	8 个 CPU
存储空间	120 GB
	注意：我们建议您使用 **500 GB** 以获得更好的性能。此外，Citrix 建议在 NetScaler Console 部署中使用固态硬盘 (SSD) 技术。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps 的网络速度
虚拟机管理程序要求	
思杰 Hypervisor	6.2、6.5
威睿 ESX	5.5、6.0
微软 Hyper-V	2012 R2
Linux 上的 KVM	乌班图, 费多拉

安装步骤

要将 NetScaler Insight Center 迁移到 NetScaler Console：

1. 登录到 NetScaler Insight Center 的 shell 提示符。

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

2. 将 NetScaler Console 12.0 build 57.24 下载到 */var/mps/mps_images* 文件夹。
3. 使用 **tar -zxvf build-mas-12.0-57.24.tgz** 命令解压 TGZ 文件。

```
bash-3.2# tar -zxvf build-mas-12.0.57.24.tgz
```

4. 使用 **./installmas** 命令安装 NetScaler Console。

```
bash-3.2# ./installmas
```

5. 安装 NetScaler Console 12.0 build 57.24 后，您需要通过执行上述步骤升级到最新的 NetScaler Console 13.1 build。

迁移后，在 NetScaler Insight Center 清单中发现的所有 NetScaler 实例都将显示在 NetScaler Console 的**基础架构 > 实例**部分。但是，首次使用时，您需要手动轮询在发现的设备中托管的虚拟服务器。

注意

在 NetScaler Console 中，默认情况下，管理和监控在发现的 NetScaler 实例中创建的两个虚拟服务器无需许可费用。要监控和管理两个以上的虚拟服务器，请安装所需的 NetScaler Console 许可证。有关更多详细信息，请参阅 NetScaler Console 许可。

将 NetScaler Console 与 Citrix Director 集成

Director 与 NetScaler Console 集成，用于网络分析和性能管理。

- 网络分析从 NetScaler Console 获取 HDX Insight 报告，并提供网络的应用程序和桌面视图。借助此功能，Director 可提供部署中 ICA 流量的高级分析视图。
- 性能管理提供历史数据保留和趋势报告。通过数据历史保留而非实时评估，您可以创建趋势报告，包括容量和运行状况趋势。

将 NetScaler Console 与 Director 集成后，HDX Insight 报告将在 Director 中为您提供以下信息：

- “趋势”页面中的“网络”选项卡显示了部署中应用程序、桌面和用户的延迟和带宽影响。
- “用户详细信息”页面显示特定用户会话的延迟和带宽信息。

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

先决条件

HDX Insight 到 NetScaler Console 迁移的硬件要求

组件	要求
内存	32 GB
虚拟 CPU	8
存储空间	500 GB。我们建议将固态硬盘 (SSD) 技术用于 NetScaler Console 部署。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps

最低要求

在配置网络集成之前，请确保创建具有 HDX™ Insights 访问权限的 RBAC 用户。

软件要求

在迁移到 NetScaler Console 虚拟设备之前，请验证是否满足以下要求：

- 已安装 Director 1811 版本
- 已安装 NetScaler HDX Insight 10.1 或更高版本
- HDX Insight 和 NetScaler Console 支持 Citrix VDA 7.0 及更高版本
- Citrix Workspace 支持 Citrix Virtual Apps and Desktops 7.0 及更高版本
- 确保 Mac 版 Citrix Workspace 11.8 及更高版本以及 Windows 版 Citrix Workspace 14.0 及更高版本可用，以显示准确的 ICA RTT 指标
- NetScaler Console 11.0 及更高版本已安装。有关如何安装 NetScaler Console 的更多信息，请参阅 部署 NetScaler Console。

限制

- 此功能的可用性取决于您组织的许可证和您的管理员权限。
- ICA 会话往返时间 (RTT) 可正确显示适用于 Windows 3.4 或更高版本的 Citrix Workspace 和适用于 Mac 11.8 或更高版本的 Citrix Workspace 的数据。对于这些 Workspace 的早期版本，数据无法正确显示。

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

- 在“趋势”视图中，不收集版本 7 之前的 VDA 的 HDX 连接登录数据。对于早期 VDA，图表数据显示为 0。
- 对于已具有存储空间小于 500 GB 的外部硬盘的部署，您无法添加另一个硬盘。

注意

- 有关 Director 的更多信息以及将 NetScaler Console 与 Director 集成的步骤，请参阅 `<https://docs.citrix.com/zh-cn/citrix-virtual-apps-desktops/director/install-and-configure/hdx-insight.html>`。
- 有关 HDX Insight 的更多信息，请参阅 `<http://docs.citrix.com/zh-cn/xenapp-and-xendesktop/7-11/director/hdx-insight.html>`。

将额外磁盘附加到 NetScaler Console

NetScaler Console 的存储要求根据您的 NetScaler Console 大小估算确定。默认情况下，NetScaler Console 提供 120 GB 的存储容量。如果您需要超过 120 GB 的存储空间来存储数据，可以附加一个额外磁盘。

注意：

- 估算存储要求并将额外磁盘附加到服务器。
- 对于 NetScaler Console 单服务器部署，除了默认磁盘之外，您只能向服务器附加一个磁盘。
- 对于 NetScaler Console 高可用性部署，您必须向每个节点附加一个额外磁盘。两个磁盘的大小必须相同。
- 如果存在容量较低的现有外部磁盘，您必须在附加新磁盘之前将其移除。
- 我们建议使用固态硬盘 (SSD) 技术用于 NetScaler Console 部署。

本文档解释了以下关于附加额外新磁盘、创建分区以及调整附加磁盘大小的场景：

1. 在独立 NetScaler Console 中附加额外磁盘
2. 启动磁盘分区工具
3. 在新附加磁盘中创建分区
4. 调整现有附加磁盘中的分区大小

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

5. 移除附加磁盘中的分区

在独立 NetScaler Console 中附加额外磁盘

1. 关闭 NetScaler Console 虚拟机。
2. 在管理程序中，将所需大小的额外磁盘附加到 NetScaler Console 虚拟机。

   新附加的较大磁盘存储数据库数据和 NetScaler Console 日志文件。现有的 120 GB 默认磁盘现在用于存储核心文件、操作系统日志文件等。
3. 启动 NetScaler Console 虚拟机。

启动磁盘分区工具

NetScaler Console 现在提供了一个新的命令行工具：**NetScaler Console 磁盘分区工具**。

1. 使用该工具，您可以在新添加的额外磁盘中创建分区。
2. 您还可以使用该工具调整现有额外磁盘的大小。但现有外部磁盘不得大于 2 TB。

   注意：

   - 将现有磁盘大小调整到 2 TB 以上可能会导致数据丢失。这是因为平台存在已知限制。
   - 要创建大于 2 TB 的存储容量，您必须删除现有分区并使用此新工具创建分区。

3. 使用此新工具，您可以显式地对磁盘执行任何分区操作。该工具为您提供了对磁盘和相关数据的清晰可见性和控制。

   注意：

   您只能在已附加到 NetScaler Console 服务器的额外磁盘上使用此工具。您不能使用此工具在主（默认）磁盘中创建分区。

要启动磁盘分区工具：

1. 使用 SSH 客户端（例如 PuTTY）打开与 NetScaler Console 的 SSH 连接。
2. 使用 `nsrecover/nsroot` 凭据登录到 NetScaler Console。
3. 切换到 shell 提示符并键入：

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

```
/mps/DiskPartitionTool.py
```

```
bash-3.2# /mps/DiskPartitionTool.py

-------------------------------------
MAS/SVM Disk Partition Tool (DPT) 1.0
-------------------------------------
Welcome to MAS/SVM DPT! Type 'help' or '?' to view a list of commands.

(dpt):
```

注意：

对于高可用性部署中的 NetScaler Console，您必须在两个节点中启动该工具，并在将磁盘附加到相应的虚拟机后创建或调整分区大小。

在新的附加磁盘中创建分区

每当添加新的辅助磁盘时，都会使用 **create** 命令来创建分区。您也可以在使用“remove”命令删除现有分区后，使用此命令在现有辅助磁盘上创建分区。

```
(dpt): ?create
Creates a new partition on the attached disk. A swap partition of size 32GB is also created automatically.

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

注意：

使用磁盘分区工具创建分区时，没有 2 TB 的大小限制。该工具可以创建大于 2 TB 的分区。当您对磁盘进行分区时，会自动添加一个大小为 32 GB 的交换分区。然后，主分区将使用磁盘上所有剩余空间。

命令运行后，将创建一个 GUID 分区表 (GPT) 分区方案。同时还会创建一个 32 GB 的交换分区和数据分区以使用剩余空间。然后，将在主分区上创建一个新的文件系统。

注意：

此过程可能需要几秒钟，您不得中断此过程。

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

```
(dpt): create

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
Creating GPT partition scheme...
da1 created

Creating partition 1 using (456287933) blocks. Leaving aside 32G for swap...
da1p1 added

Creating partition 2 for swap using remaining 32G...
da1p2 added

Formatting the new partition. This may take some time (~20 seconds). Please be patient and don't interrup the process...
```

创建命令完成后，虚拟机将自动重启，以便挂载新分区。

```
Create Done.
VM has to be rebooted for the new partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

重启后，新分区将挂载到 /var/mps。

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0        456046  374346     72580    84%    /
devfs                1       1         0   100%    /dev
procfs               4       4         0   100%    /proc
fdescfs              1       1         0   100%    /dev/fd
/dev/da0s1a    1623950  284466   1209568    19%    /flash
/dev/da0s1e  116073918 2812298 103975708     3%    /var
/dev/da1p1   495168802   43854 455511444     0%    /var/mps
```

添加的交换分区在“create”命令的输出中显示为交换空间。

```
CPU:  0.0% user,  0.0% nice,  0.0% system,  0.7% interrupt, 99.3% idle
Mem: 89M Active, 21M Inact, 123M Wired, 16M Cache, 74M Buf, 6965M Free
Swap: 37G Total, 37G Free
```

注意：

创建分区后，该工具会重启虚拟机。

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

调整现有附加磁盘中的分区大小

您可以使用 **resize** 命令调整附加（辅助）磁盘的大小。您可以调整具有 `master boot record (MBR)` 或 GPT 方案的磁盘大小。磁盘大小必须小于 2 TB。

注意：

- `resize` 命令旨在在不丢失任何现有数据的情况下运行。但我们建议您在调整大小之前将此磁盘中的关键数据备份到外部存储。在调整大小操作期间磁盘数据可能损坏的情况下，数据备份会很有帮助。
- 在调整分区大小时，请确保以 100 GB 的增量增加磁盘空间。这种增量增加可确保您无需更频繁地调整大小。

```
(dpt): ?resize
Resizes existing partition on attached disk to utilize all space available. Pre-conditions are:
1. Secondary disk exists and capcity of disk < 2TB
2. A single partition exists on secondary disk and there is atleast 100GB to gain by resizing

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

在您同意调整大小后，`resize` 命令会检查所有先决条件，如果所有先决条件都满足，则会继续执行。它会停止访问磁盘的进程，其中包括 NetScaler Console 子系统、PostgreSQL DB 进程和 NetScaler Console 监视器进程。进程停止后，磁盘将被卸载以准备进行大小调整。调整大小通过扩展分区以占用所有可用空间，然后扩展文件系统来完成。如果磁盘上存在交换分区，则在调整大小后会将其删除并在磁盘末尾重新创建。交换分区在文档的“**Create** 命令”部分中讨论。

注意：

“扩展文件系统”过程可能需要一些时间才能完成，请注意不要在进行过程中中断该过程。调整分区大小后，该工具会重新启动虚拟机。

```
(dpt): resize

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to resize (Y/N): y
```

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

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/da1p2
Deleting swap partition: da1p2
Resizing partition da1p1...
da1p1 resized

Adding a swap partition da1p2...
da1p2 added

Formatting the newly added portions of the partition. This may take some time (~10 seconds). Please be patient and don't
 interrup the process...
```

调整大小过程中的所有中间步骤（停止应用程序、调整磁盘大小、扩展文件系统）都会显示在控制台上。过程完成后，将显示以下消息。

```
Resize Done.
VM has to be rebooted for the resized partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

重启后，可以使用 `df` 命令观察到大小的增加。以下是增加大小前后的详细信息：

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374864     72062    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1662048 105125958     2%    /var
/dev/da1s1a   152329216 3082226 137060654     2%    /var/mps
```

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374838     72088    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1666800 105121206     2%    /var
/dev/da1s1a   304651668 3137954 277141582     1%    /var/mps
```

移除附加磁盘中的分区

辅助磁盘上的现有分区最大可调整为 2 TB。出现此问题是因为分区存在已知限制。如果您需要大于 2 TB 的磁盘，请附加一个新磁盘并使用磁盘分区工具对其进行分区。您也可以使用 `remove` 命令移除现有分区，然后创建一个新分区。

注意：

移除现有分区会删除所有现有数据。因此，在使用此命令之前，必须将所有关键数据备份到外部存储。

```
(dpt): ?remove
Removes existing partition from attached disk.

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

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

运行“remove”命令会要求您确认，一旦确认，它将停止所有使用辅助磁盘的进程（例如 NetScaler Console 子系统、PostgreSQL 进程和 NetScaler Console 监视器）。如果存在交换分区并且该分区上启用了交换，则会禁用交换。

```
(dpt): remove

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

当您输入“y”时，该命令会卸载磁盘并删除磁盘上的所有分区。

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to remove existing partitions.
Disabling swap on partition: /dev/da1p2
Removing all partitions from: da1
Remove Done.
Rebooting VM now...
```

注意：

删除分区后，该工具会重新启动虚拟机。

重新启动虚拟机

创建或调整分区大小，或创建交换文件后，请重新启动虚拟机。更改仅在重新启动后生效。为此，工具中提供了 **reboot** 命令。

```
(dpt): ?reboot
Reboot the VM. Note: VM has to be rebooted after new partition is created, existing one is resized or swap file is creat
ed.
The VM is rebooted automatically after these operations. If the automatic reboot does not happen, then this command can
be used to reboot the VM.
```

系统会提示您进行确认，确认后，所有进程（例如 NetScaler Console 子系统、PostgreSQL 进程和 NetScaler Console 监视器）都将停止。然后，虚拟机将重新启动。

```
(dpt): reboot
Are you sure you want to reboot the VM (Y/N): y
```

```
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

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

创建磁盘数据备份文件

注意：

创建备份文件需要磁盘空间。在运行备份命令之前，请确保有足够的磁盘空间（50% 或更多）。

在调整或删除分区之前备份 NetScaler Console 数据：

1. 停止 NetScaler Console。

```
/mps/masd stop
```

2. 停止 PostgreSQL。

```
su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
```

3. 停止 NetScaler Console 监控。

```
/mps/scripts/stop_mas_monit.sh
```

4. 创建一个 tarball。

```
cd /var

tar cvfz /var/mps/mps_backup.tgz mps
```

注意：

此操作所需时间取决于要备份的数据大小。

5. 生成校验和。

```
md5 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
```

6. 将 tarball 和校验和文件复制到远程服务器。
7. 验证复制的 tarball 的正确性。生成传输文件的校验和，并与源校验和进行比较。

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

8. 从 NetScaler Console 虚拟机中删除 tarball。

```
cd /var/mps/

rm mps_backup.tgz  mps_backup_checksum
```

附加命令

除了前面列出的命令之外，您还可以在该工具中使用以下命令：

帮助命令：

要列出支持的命令，请键入 **help** 或 **?** 并按 Enter 键。要获取每个命令的进一步帮助，请按 **help** 或 **?**，后跟命令名称，然后按 **Enter** 键。

```
(dpt): help

DPT Commands
------------
create  create_swapfile  exit  help  info  reboot  remove  resize

(dpt):
```

信息命令：

如果磁盘存在，**info** 命令将提供有关已连接辅助磁盘的信息。该命令提供设备名称、分区方案、人类可读格式的大小以及磁盘块的数量。该方案可以是 MBR 或 GPT。MBR 方案表示磁盘是使用早期版本的 NetScaler Console 进行分区的。基于 MBR/GPT 的分区可以调整大小，但不能超过 2 TB。GPT 分区方案表示磁盘是使用 NetScaler Console 12.1 或更高版本进行分区的。

注意：

GPT 分区在创建时可以大于 2 TB。但是，在创建较小大小的磁盘后，您无法将磁盘大小调整为大于 2 TB。此问题是平台的已知限制。

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

```
(dpt): ?info
Provides information about attached disk (if found).
(dpt): info
--------------
Disk: da1
Scheme: MBR
Size: (150G)
Blocks: 314572737
--------------
(dpt):
```

Create_swapfile 命令：

NetScaler Console 主磁盘上的默认交换分区为 4 GB，因此默认交换空间为 4 GB。对于 NetScaler Console 的默认内存配置（2 GB），此交换空间是足够的。但是，当您以更高的内存配置运行 NetScaler Console 时，您需要在磁盘上分配更多的交换空间。

注意：

交换分区通常是一个专用分区，在安装操作系统期间在硬盘驱动器 (HDD) 上创建。此类分区也称为交换空间。交换分区用于模拟额外主内存的虚拟内存。

在早期版本的 NetScaler Console 中添加的辅助磁盘默认情况下没有创建交换分区。“create_swapfile”命令适用于使用没有交换分区的旧版 NetScaler Console 创建的辅助磁盘。该命令检查以下内容：

- 辅助磁盘的存在
- 磁盘是否已挂载
- 磁盘大小（至少 500 GB）
- 交换文件是否存在

`create_swapfile` 命令仅在内存大于或等于 16 GB 时有用，而不是在内存不足时。因此，此命令在继续创建交换文件之前也会检查内存。

```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

Creating swapfile is a time consuming operation and can take ~5 minutes to complete. Once started the operation should n
ot be interrupted.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

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

如果所有条件都满足，并且用户同意继续，则会在辅助磁盘上创建一个 32 GB 的交换文件。交换文件创建过程需要几分钟才能完成，请注意不要在进行过程中中断该过程。成功完成后，将重新启动以使交换文件生效。

创建交换文件命令](/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-22.png)

重启后，可以使用 top 命令观察到交换空间的增加。

创建交换文件命令 2(/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-23.png)

退出命令：

要退出该工具，请键入 exit 并按 **Enter** 键。

退出命令(/en-us/netscaler-application-delivery-management-software/media/nmas-disk-partitioning-tool-24.png)

将附加磁盘连接到高可用性部署中的 NetScaler Console

假设您已在高可用性设置中配置了一对 NetScaler Console 服务器，但没有辅助磁盘。此外，假设您已添加了 2 个或更多 NetScaler 实例，并检查并确保所有进程都在运行。您可能希望在此设置中为虚拟机添加辅助磁盘。在高可用性设置中，您必须按照此任务中的详细说明为两个节点添加附加磁盘：

1. 关闭辅助节点。
2. 通过管理程序添加磁盘。

   注意：

   确保不要扩展辅助节点主磁盘。

3. 启动辅助节点。
4. 在辅助节点上运行分区工具。
5. 磁盘添加后，辅助节点会重新启动。
6. 辅助节点重新启动后将其关闭。
7. 关闭主节点。
8. 通过虚拟机管理程序添加磁盘。

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

> **注意：**
>
> 确保不要扩展主节点主磁盘。

9. 启动主节点。
10. 在主节点上运行分区工具。
11. 磁盘添加后，主节点会重新启动。
12. 主节点启动并运行后，启动辅助节点。
13. 确保辅助节点已启动并运行，并且数据库已同步。
14. 确认所有数据仍然存在。

要增加两个节点的 RAM 容量：

1. 关闭 Console_Secondary 并根据需要增加 RAM 大小。不要重新启动节点。
2. 关闭 Console_Primary 并根据需要增加 RAM 大小。

   确保您在两个节点上平等地增加 RAM 大小。例如，如果您将主节点上的 RAM 大小增加到 16 GB，则辅助节点也应如此。
3. 重新启动 Console_Primary。
4. 在 Console_Primary 重新启动后，检查它是否是主节点。
5. 启动 Console_Secondary 节点。重新启动后，确保它已作为辅助节点启动并且数据库同步正常工作。
6. 确认所有数据仍然存在。

> **注意：**
>
> 添加辅助磁盘后，主节点需要一些时间才能启动。此外，将辅助磁盘添加到两个节点并增加 RAM 容量的整个过程需要两个节点停机一段时间。在规划此维护活动时，请考虑此停机时间。

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

通过 NetScaler Console 进行 NetScaler MPX™ 磁盘加密

注意：

- 磁盘加密仅在 NetScaler MPX 9100 实例上受支持。
- NetScaler MPX 9100 实例的磁盘加密只能在独立 NetScaler Console 中启用。
- 从版本 14.1-56.x 开始，在 May 20, 2025 之后制造的 NetScaler MPX 9100、16000 和 MPX 15000-50G 实例上支持磁盘加密。

磁盘加密对于保护存储磁盘上存储的敏感数据至关重要。它确保即使物理存储设备遭到破坏，数据也无法访问。对于 NetScaler MPX，磁盘加密提供了额外的安全层，特别是对于 `/var/core`、`/var/crash`、`/var/log`、`/var/nslog`、`/flash/nsconfig`、`/var/nstrace` 和 `/var/temp` 等关键目录。

磁盘加密的一些优点包括：

- **静态数据保护**：防止系统关闭时未经授权访问敏感数据。
- **合规性**：有助于满足数据安全的法规和合规性要求。
- **降低物理盗窃风险**：确保被盗或放错位置的存储设备上的敏感和专有数据无法被访问。
- **安全启动过程**：在启动期间需要经过身份验证的凭据，确保只有授权用户才能访问系统。
- **增强关键数据的安全性**：保护日志、配置和崩溃数据免受未经授权的访问。

NetScaler MPX 9100 上的磁盘加密仅在 **May 20, 2025** 之后发布的 14.1-47.x 版本中受支持，并且可以通过运行 14.1-47.x 版本的 NetScaler Console 启用。每个 NetScaler MPX 实例的磁盘加密都需要一个由硬件安全模块 (HSM) 服务器（即 Thales CipherTrust Manager）管理的密钥。NetScaler MPX 实例使用 NetScaler Console 从 HSM 服务器获取密钥。

NetScaler MPX 9100、16000 和 MPX 15000-50G 上的磁盘加密仅在 **May 20, 2025** 之前发布的 14.1-56.x 版本中受支持，并且可以通过运行 14.1-56.x 版本的 NetScaler Console 启用。要启用此功能，请参阅 通过 NetScaler Console 进行实例磁盘加密。

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

注意：

NetScaler Console 支持 Thales CipherTrust Manager 作为 HSM 服务器。

为了成功加密，您必须(#add-the-instance-serial-number-in-the-hsm-thales-ciphertrust-manager-server)。添加 NetScaler MPX 实例序列号后，NetScaler Console 会使用该实例序列号从 HSM 服务器获取密钥。

磁盘加密完成后：

- 如果 NetScaler MPX 实例磁盘被移除，数据将无法访问。
- 如果您重新启动 NetScaler MPX 实例，只有在 NetScaler Console 使用其序列号从 HSM 服务器对 NetScaler MPX 实例进行身份验证后，重新启动才能成功。

先决条件

确保：

- 对于 9100，NetScaler MPX 实例运行的是版本 14.1-47.x，并且在运行版本 14.1-47.x 的本地 NetScaler Console 上进行管理。

  注意：

  NetScaler Console 服务不支持磁盘加密。

- 您已在 HSM (Thales CipherTrust Manager) 服务器中添加了 NetScaler MPX 实例序列号，以便 NetScaler Console 在使用其序列号对实例进行身份验证后共享密钥。
- NetScaler MPX 实例已通过 NetScaler Console 备份。有关详细信息，请参阅(/zh-cn/netscaler-application-delivery-management-software/current-release/analytics/security/backup-restore-netscaler-instances.html)。
- 对于 MPX 16000 和 MPX 15000-50G，本地 NetScaler Console 的版本为 14.1 build 56.x。

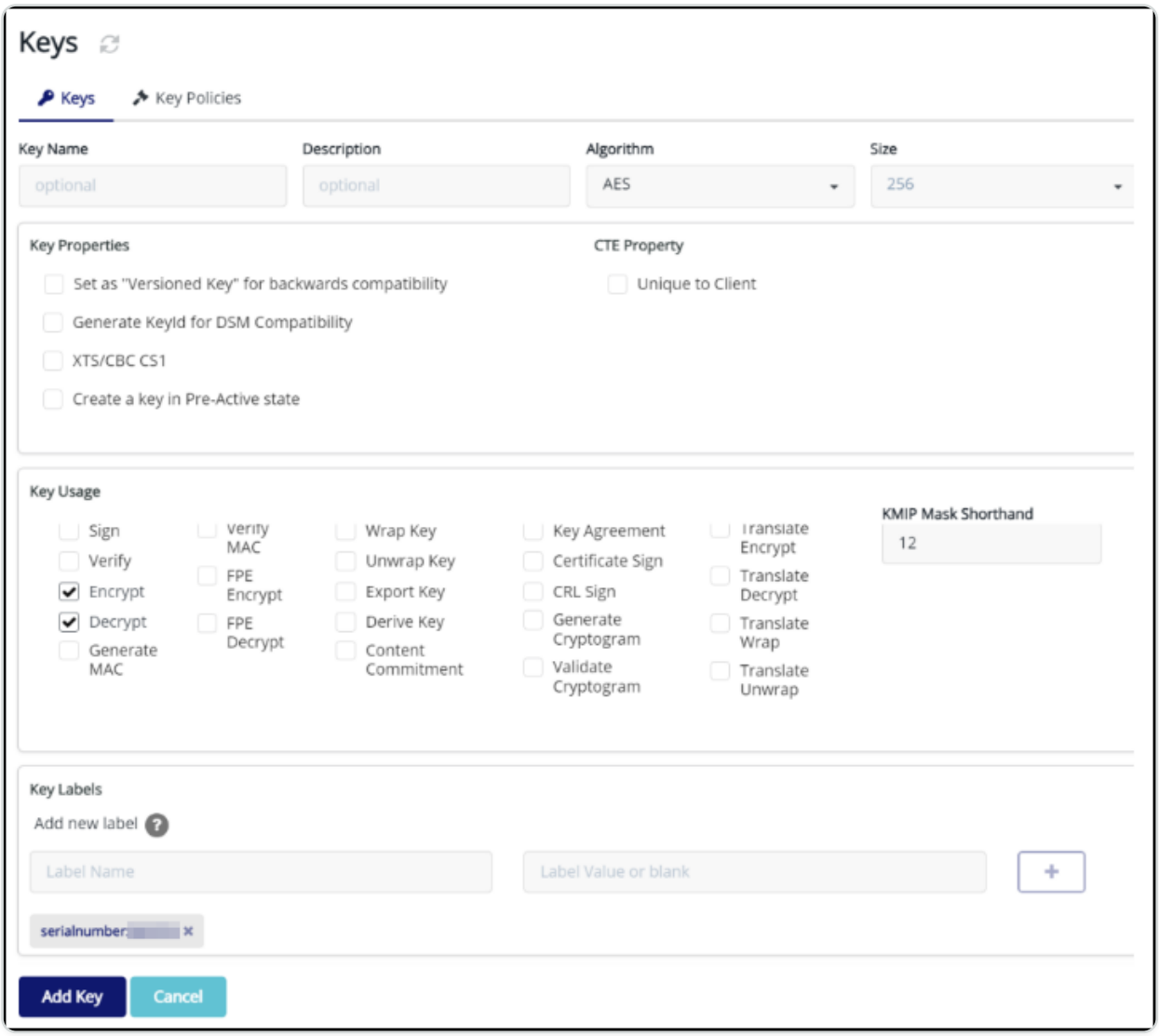
在 HSM (Thales CipherTrust Manager) 服务器中添加实例序列号

在加密 NetScaler MPX 实例之前，您必须在 HSM 服务器中添加 NetScaler MPX 实例序列号。

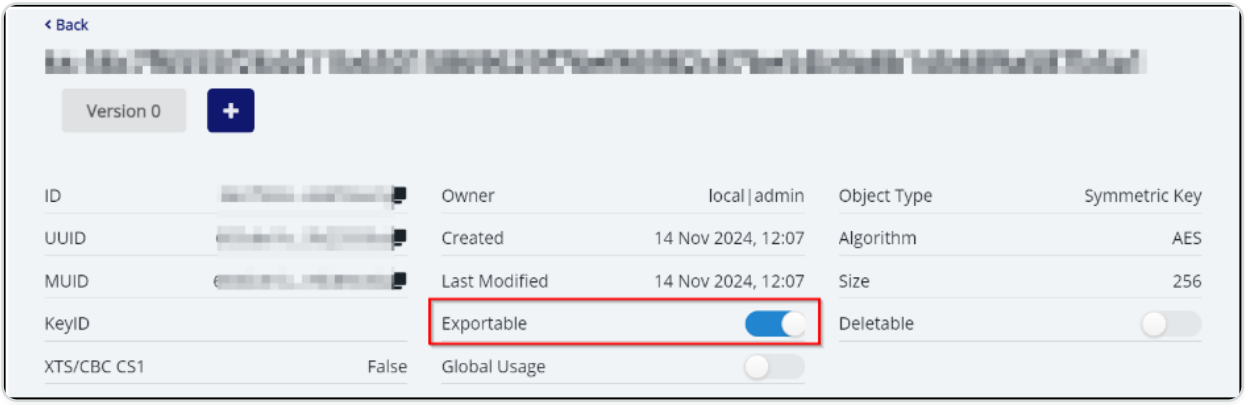
1. 登录 Thales CipherTrust Manager 服务器。

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

2. 在左侧窗格中，选择 **Keys**，然后单击 **Add Key**。
3. 在 **Key Labels** 下，添加一个名为 `serialnumber` 的标签，在 **Label Value** 文本框中指定实例序列号，单击 **+** 按钮添加密钥详细信息，然后单击 **Add Key**。



4. 在密钥详细信息页面中，您必须为此密钥启用 Exportable 切换。



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

注意：

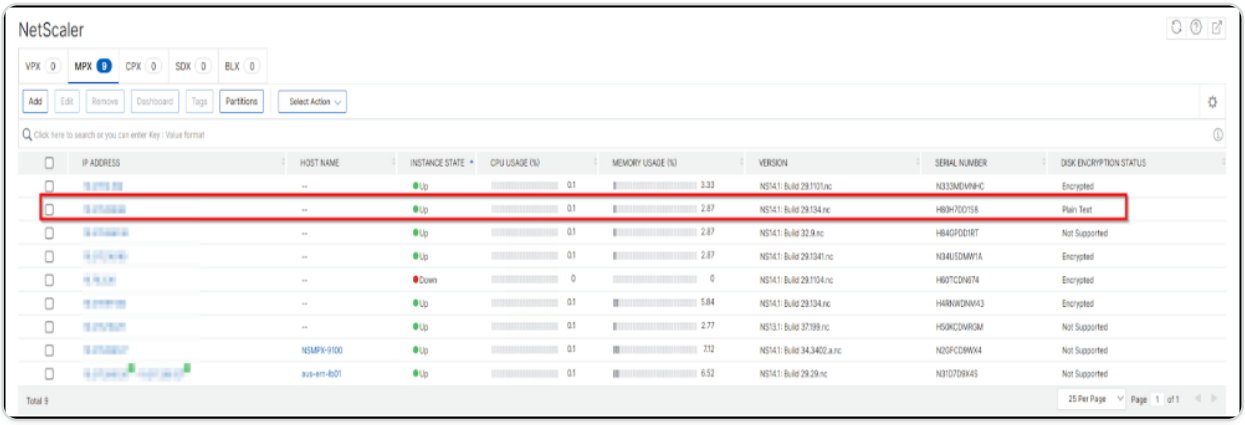
- 支持的最大密钥大小为 511 字节。例如：支持 AES-128 和 AES-256。不支持 512 到 4096 之间的 RSA 密钥。
- 建议您仅使用支持的密钥大小。如果配置了不支持的密钥大小，NetScaler® 实例将失败。
- 确保指定正确的序列号。如果序列号不匹配，加密过程将不会启动。
- 建议您从 NetScaler Console 复制实例序列号。在 NetScaler Console GUI 中，导航到 **Infrastructure > Instance > MPX**，选择 NetScaler MPX 实例，然后从 **Select Action** 列表中单击 **Get Serial Number**。

通过 NetScaler Console 进行实例磁盘加密

在开始磁盘加密之前，请确保通过 NetScaler Console 备份 MPX 实例。有关详细信息，请参阅 配置实例备份。

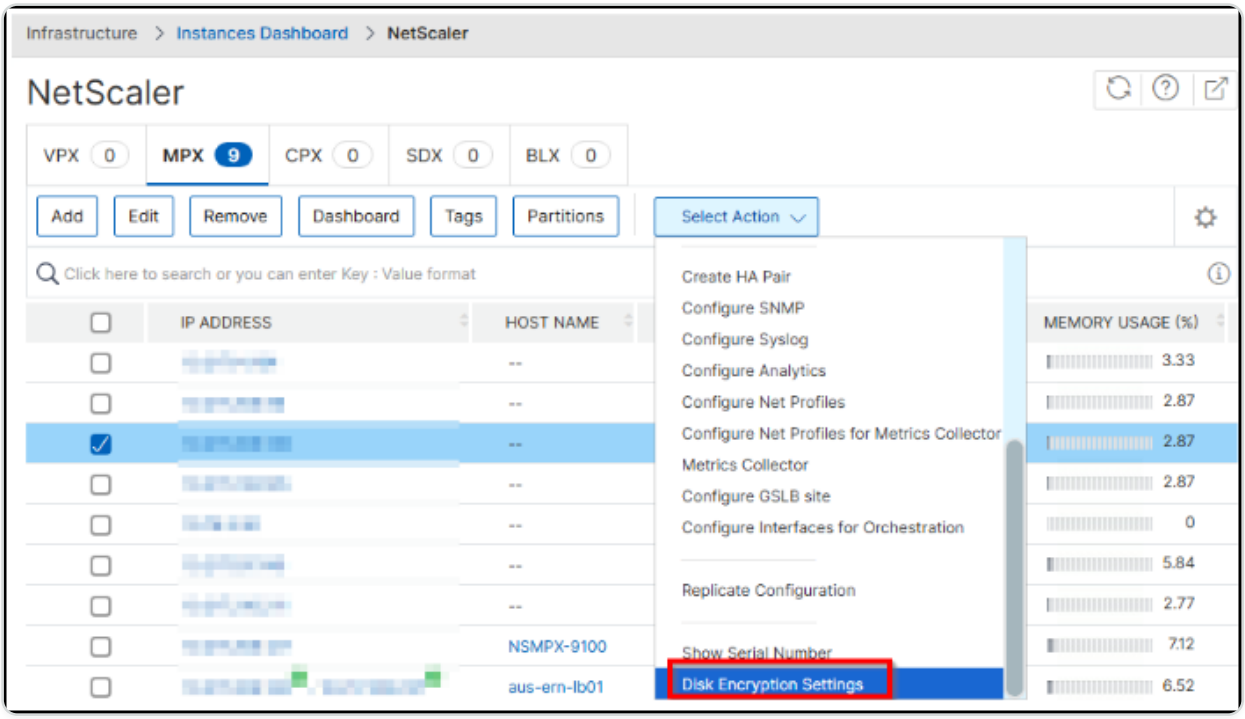
备份后：

1. 导航到 **基础设施 > 实例 > NetScaler**。
2. 在 **NetScaler MPX** 选项卡中，您可以看到托管实例的详细信息。您要加密的实例在 **磁盘加密状态** 下显示 **纯文本**。



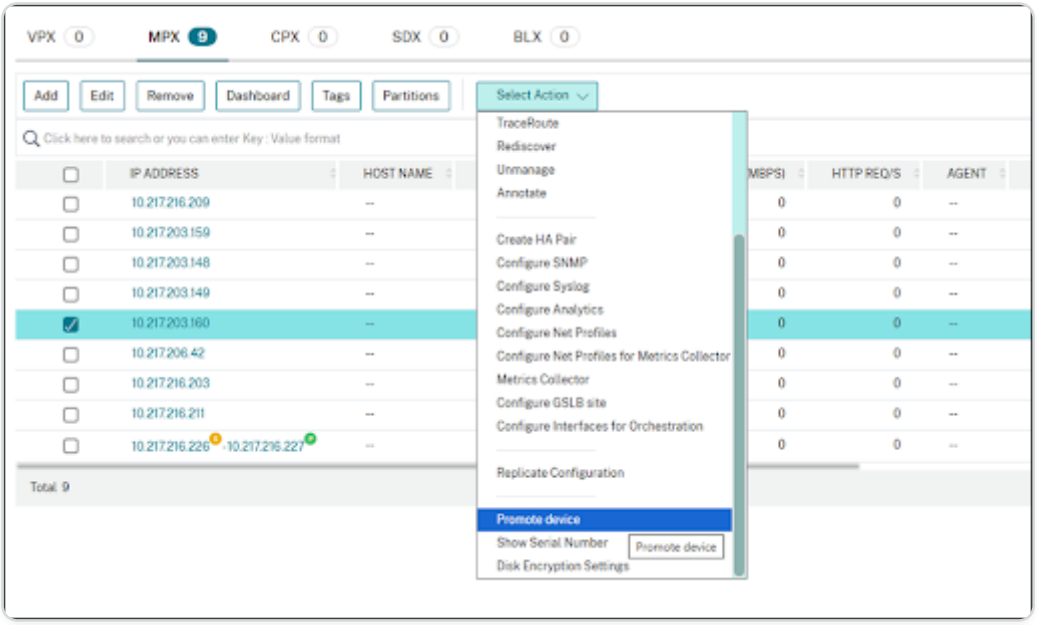
3. 从 **选择操作** 列表中，单击 **磁盘加密设置**。

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



4. 从 **选择操作** 列表中，单击 **提升设备**。

> **注意：**
>
> 选择 **提升设备** 选项是强制性的，以便激活磁盘加密功能，特别是对于在 May 20, 2025 之前制造的 MPX 设备。请预留大约 30 分钟，让 MPX 设备完成转换为启用磁盘加密的设备。



5. 在 **磁盘加密设置** 页面中：

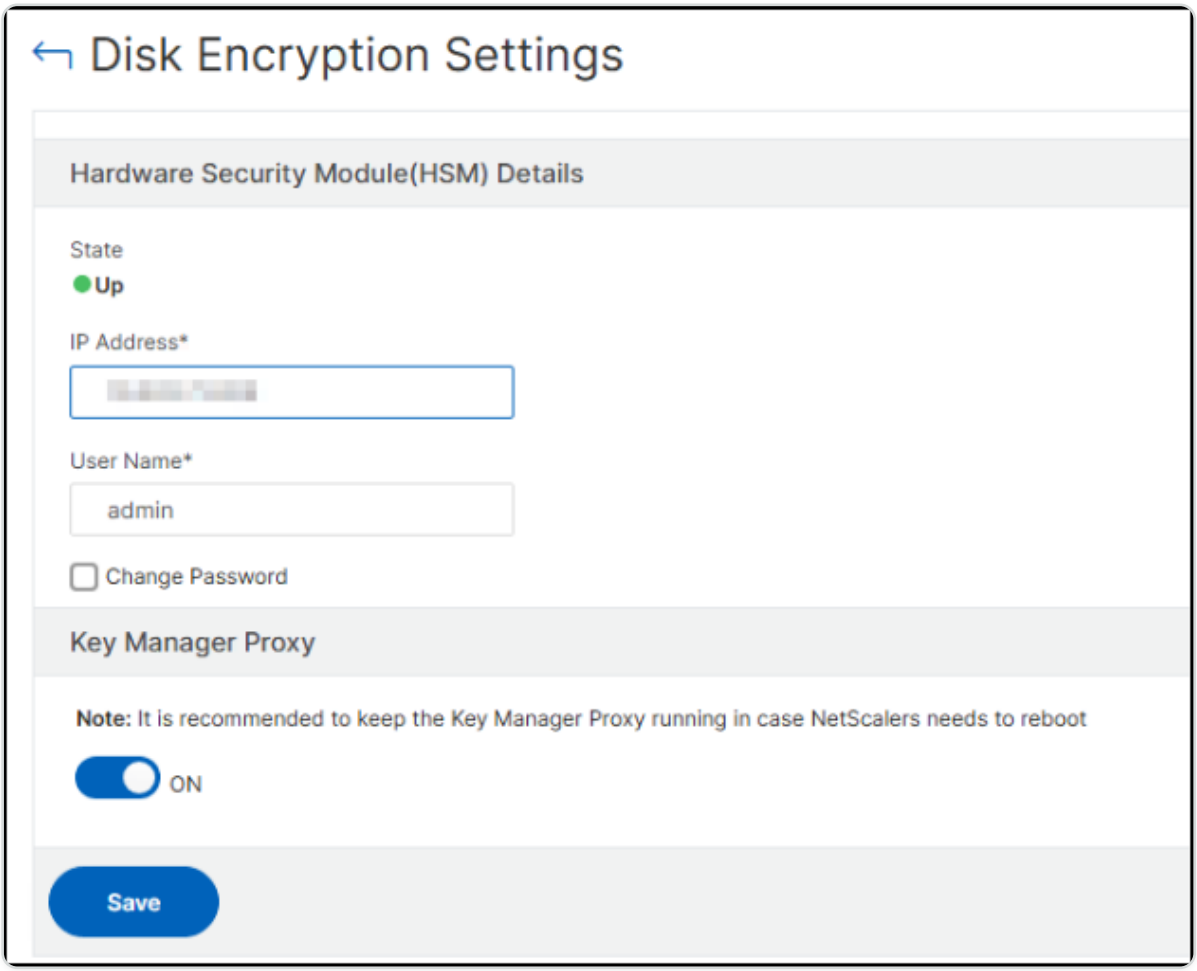
© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 指定 HSM 服务器的 IP 地址、用户名和密码，NetScaler Console 可以通过序列号从中获取加密密钥。

b. 启用 **密钥管理器代理**。您必须启用此选项才能继续磁盘加密过程。

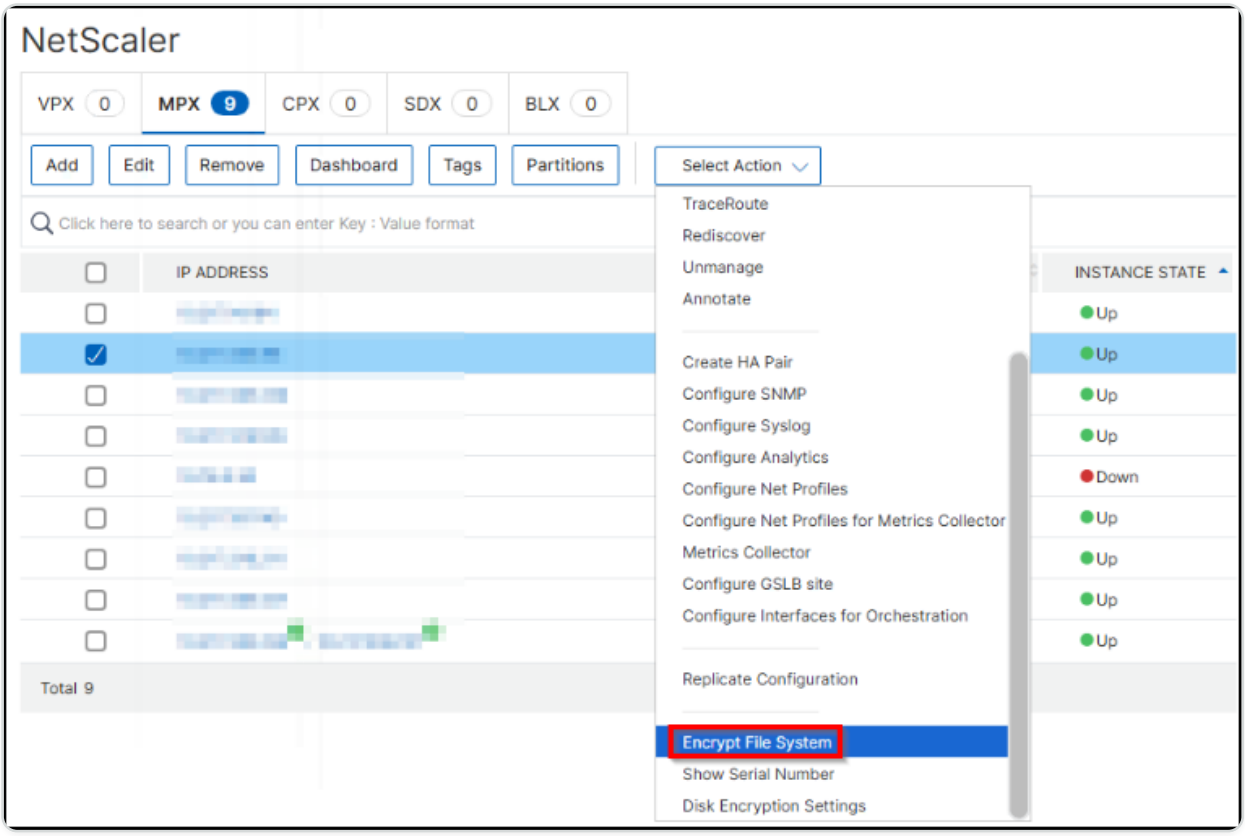
> **注意：**
>
> 即使加密完成后，也要确保 **密钥管理器代理** 始终处于启用状态。如果禁用此选项，加密实例将无法在某些情况下成功重新启动，例如在升级实例或强制重新启动实例之后。

c. 单击 **保存**。



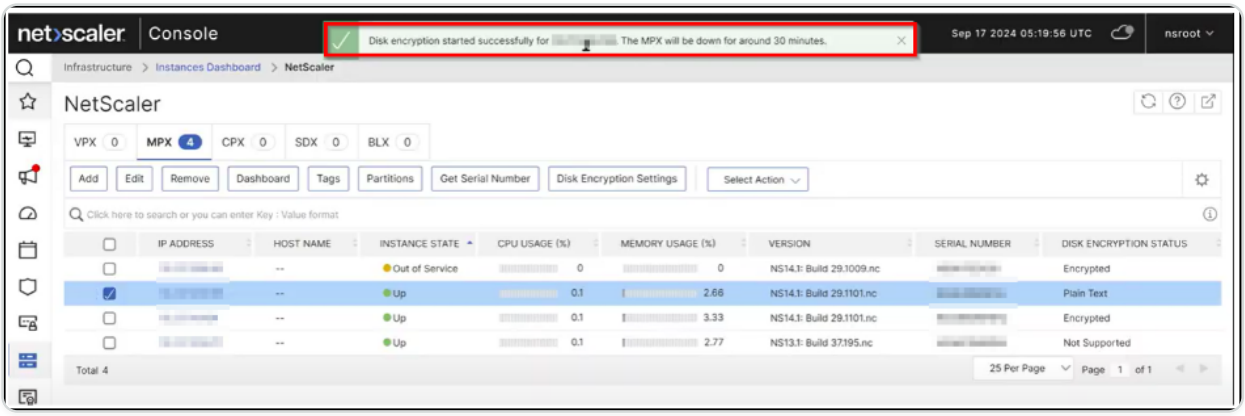
6. 选择实例，然后从**选择操作**列表中，单击**加密文件系统**。

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

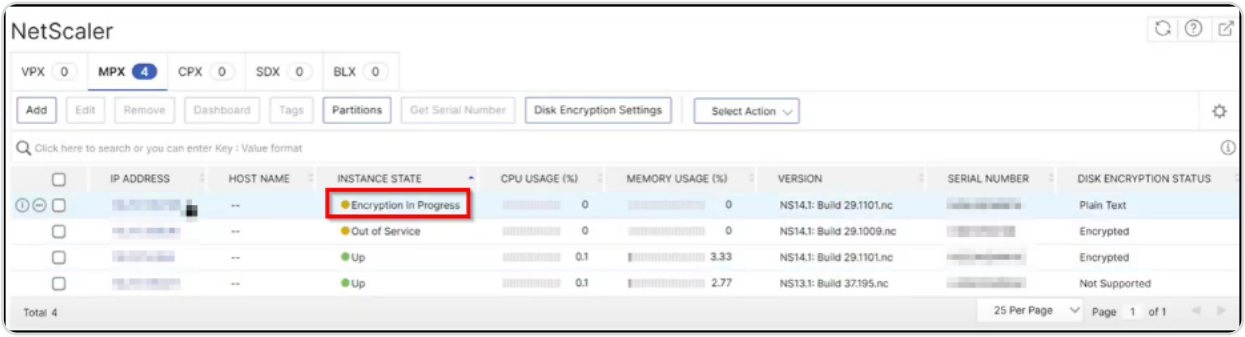


出现确认窗口。单击**是**以继续。

7. NetScaler Console 中出现确认消息，指出加密已启动，并且实例将在大约 30 分钟内处于**关闭**状态。



实例状态显示为**加密进行中**。



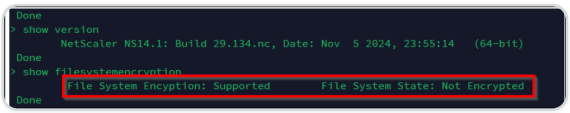
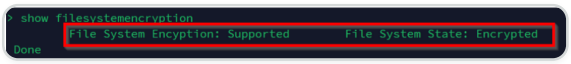
© 1997–2026 Citrix Systems, Inc. All rights reserved.

加密后验证

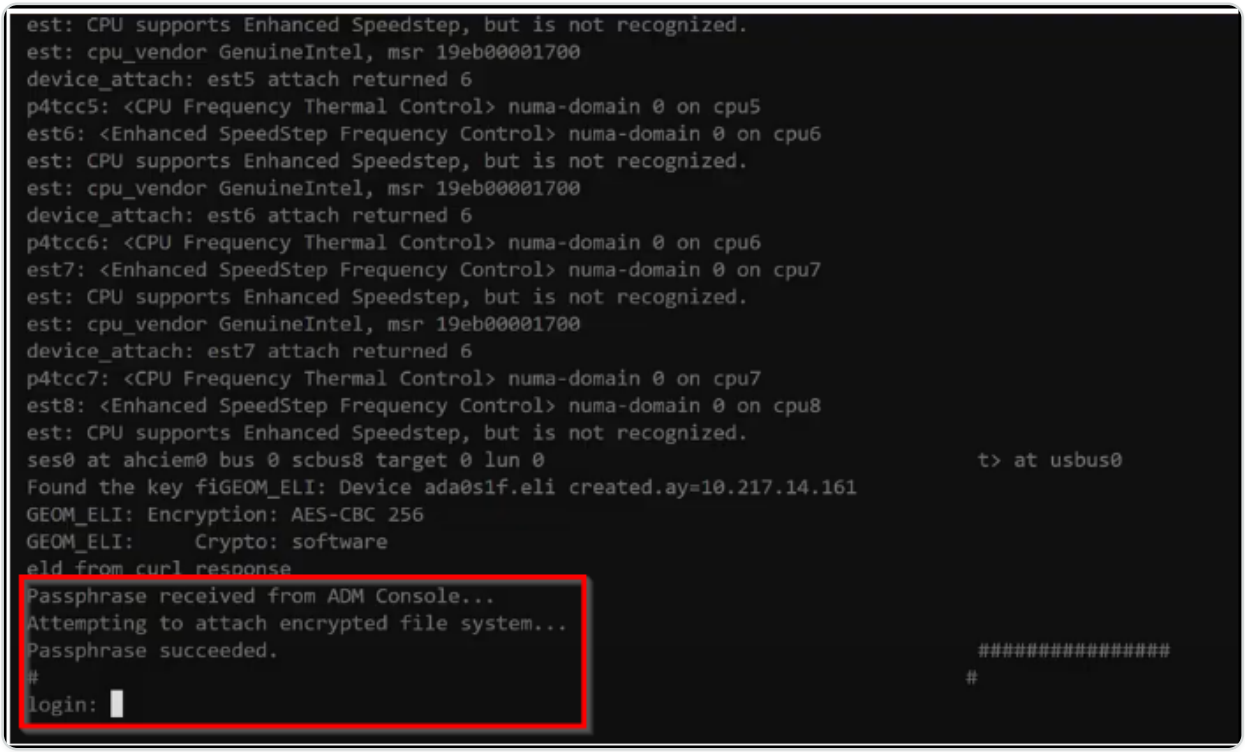
实例加密在大约 30 分钟内完成。加密完成后：

- 您可以使用 SSH 客户端登录到 NetScaler MPX 实例，然后通过以下命令验证加密是否成功：

  `show filesystemencryption`

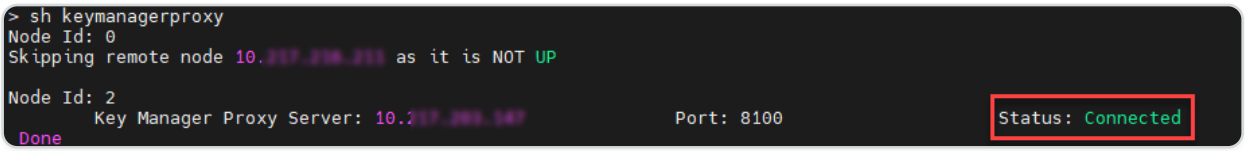
加密前	加密后
	

- 您可以重新启动 NetScaler MPX 实例，并验证加密后重新启动是否完成，如以下示例所示：



- 您可以使用以下命令验证 **Key Manager Proxy** 是否已成功配置并可从 NetScaler 访问：

  `show keymanagerproxy`



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

注意：

加密后，NetScaler Console 使用 `mpx_disk_encryption_default_profile` 访问 NetScaler MPX 实例。`mpx_disk_encryption_default_profile` 具有默认凭据 (`nsroot` / `nsroot`)。

加密后恢复 NetScaler MPX 实例

如果您在备份前更改了默认密码 (nsroot)，请确保加密后，备份期间使用的配置文件在 NetScaler Console 中可用。

加密后 NetScaler MPX™ HA 对的行为

主节点和辅助节点必须具有相同的加密状态。如果主节点和辅助节点的加密状态不匹配，则两个节点之间的同步将被禁用。使用 SSH 客户端登录到主 NetScaler® MPX 实例，并使用以下命令验证两个节点是否显示相同的加密状态：

```
sh ha node
```

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

```
> sh ha node
1)      Node ID:      0
        IP:   10.146.116.21 (VPX16-INTRAPRO-CB)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: ON
        INC State: DISABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 1/1 1/2 1/3 1/5 LA/2
        Disabled Interfaces : None
        HA MON ON Interfaces : 1/1 1/2 1/5
        HA HEARTBEAT OFF Interfaces : 1/3
        Interfaces on which heartbeats are not seen : None
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 8:23:53:54 (days:hrs:min:sec)
2)      Node ID:      1
        IP:   10.146.116.22
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: DISABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 1/1 1/2 1/3 1/5 LA/2
        Disabled Interfaces : None
        HA MON ON Interfaces : 1/1 1/2 1/3 1/5 LA/2
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/3
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT

Local node information:
        Critical Interfaces: 1/1 1/2 1/5
 Done
```

如果两个节点的加密状态不同：

- 当存在磁盘加密不匹配时，将显示以下输出：

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

```
> sh ha node
1)      Node ID:      0
        IP:  10.217.216.223
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: AUTO DISABLED (Disk Encryption Mismatch)
        Propagation: AUTO DISABLED (Disk Encryption Mismatch)
        Enabled Interfaces : 0/1 25/8 25/7 25/6 25/5 25/4 25/3 25/2 25/1
        Disabled Interfaces : None
        HA MON ON Interfaces : 0/1
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 25/8 25/7 25/6 25/5 25/4 25/3 25/2 25/1
        Interfaces causing Partial Failure: None
        SSL Card Status: UP
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:11:52 (days:hrs:min:sec)
2)      Node ID:      1
        IP:   10.146.116.21
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: AUTO DISABLED (Disk Encryption Mismatch)
        Propagation: AUTO DISABLED (Disk Encryption Mismatch)
        Enabled Interfaces : UNKNOWN
        Disabled Interfaces : UNKNOWN
        HA MON ON Interfaces : UNKNOWN
        HA HEARTBEAT OFF Interfaces : UNKNOWN
        Interfaces on which heartbeats are not seen : UNKNOWN
        Interfaces causing Partial Failure: UNKNOWN
        SSL Card Status: UNKNOWN

Local node information:
        Critical Interfaces: 0/1
 Done
>
```

- 启用 HA 同步、启用 HA 属性和强制 HA 同步时，会出现磁盘加密不匹配错误：
  - `set ha node -haprop enabled`

    ```
    > set ha node -haprop enabled
    ERROR: Disk Encryption mismatch between HA Nodes. [Prop and sync not allowed]
    ```

  - `set ha node -hasync enabled`

    ```
    > set ha node -hasync enabled
    ERROR: Disk Encryption mismatch between HA Nodes. [Prop and sync not allowed]
    ```

  - `force ha sync`

    ```
    > force ha sync
    ERROR: Disk Encryption mismatch between HA Nodes.
    ```

NetScaler MPX™ 群集加密后的行为

为了成功形成群集，所有节点必须具有相同的加密状态。如果任何节点的加密状态不匹配：

- 不匹配节点的健康状态显示为 **NOT UP**，且该节点不提供流量。

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

```
> sh cluster instance
1) Cluster ID: 1
        Dead Interval: 3 secs
        Hello Interval: 200 msecs
        Preemption: DISABLED
        Propagation: AUTO DISABLED (Disk Encryption Mismatch)
        Quorum Type: MAJORITY
        INC State: DISABLED
        Process Local: DISABLED
        Retain Connections: NO
        Heterogeneous: NO
        Backplane based view: DISABLED
        Cluster sync strict mode: DISABLED
        DFD Retain L2 Params: DISABLED
        Cluster Proxy Arp Status: ENABLED
        Secure Heartbeats: DISABLED
        Cluster Status: ENABLED(admin), ENABLED(operational), UP

        WARNING(s):
                (1) - There are no spotted SNIPs configured on the cluster. Spotted SNIPs can help improve cluster performance.
                (2) - Disk encryption mismatch detected. Please refer show filesystemencryption

        Member Nodes:
        Node ID     Node IP            Health     Admin State  Operational State
        -------     -------            ------     -----------  -----------------
1)      0           [redacted]195*     UP         ACTIVE       ACTIVE(Configuration Coordinator)
2)      1           [redacted]26       NOT UP     ACTIVE       INACTIVE
```

- 群集中不匹配节点的同步已禁用。

```
> sh cluster node
1) Node ID: 0
        IP:                     [redacted]*
        Backplane:              0/25/1
        Health:                 UP
        Admin State:            ACTIVE
        Operational State:      ACTIVE(Configuration Coordinator)
        Sync State:             ENABLED
        Priority:               31
        Tunnel Mode:            NONE
        Node Group:             DEFAULT_NG
2) Node ID: 1
        IP:                     [redacted]
        Backplane:              1/25/1
        Health:                 NOT UP
                                Reason(s):
                                Cluster health is not up due to config sync is in progress
                                The node is not in sync with the cluster configurations as sync is disabled on this node
        Admin State:            ACTIVE
        Operational State:      INACTIVE
        Sync State:             DISABLED
        Priority:               31
        Tunnel Mode:            NONE
        Node Group:             DEFAULT_NG
 Done
```

- 无法将节点添加到群集。出现加入命令失败消息：

```
> join cluster -clip [redacted] -password [redacted]
ERROR: [Cluster disk encryption mismatch between Configuration Coordinator and local node]
> shell
```

- 群集命令传播已禁用。

```
> add vlan 10
ERROR: Command propagation disabled. [Disk encryption mismatch]
> vtysh
ns#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ns(config)#hostname rama
% Propagation of command to cluster disabled [Disk encryption mismatch]
```

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

NetScaler Console 云连接

NetScaler Console 云连接通过 Citrix Cloud™ 从本地 NetScaler Console 到 NetScaler Console 服务建立安全的出站连接，以在本地 NetScaler Console 上启用云交付功能。

您可以配置云连接以在本地 NetScaler Console 中使用以下功能：

- **基于 LAS 的许可（权利交付）** - 当在本地 NetScaler Console 上启用 Cloud Connect 并且部署正在运行 LAS 兼容版本时，LAS 会自动启用。许可权利会自动检索和续订。有关详细信息，请参阅 许可证激活服务。
- **资产交付** - 资产交付为内置 WAF 配置文件提供加密签名更新和加密架构更新，这些配置文件旨在保护传入的身份验证、授权、审计、VPN 和 GUI 组件请求。默认情况下，当云连接启用时，资产交付也会启用，如果需要，管理员可以禁用。有关详细信息，请参阅 Web App Firewall 对 VPN 虚拟服务器和身份验证虚拟服务器的保护。
- **升级建议** - 要在本地 NetScaler Console 上使用升级建议，必须启用云连接。启用云连接后，NetScaler Console 可以检索最新的内部版本信息，并将其与受管 NetScaler 实例的内部版本进行比较，从而帮助识别本地 NetScaler Console 上 NetScaler 实例的 EOL、EOM 和运行旧版本内部版本的实例。默认情况下，当云连接启用时，升级建议也会启用。如果需要，管理员可以禁用它。有关详细信息，请参阅 升级建议。
- **ServiceNow 集成** - 此集成使用 Citrix ITSM 连接器在 NetScaler Console 和 ServiceNow 实例之间进行通信。NetScaler Console 与 ServiceNow 的集成使用 ITSM 适配器服务进行基于令牌的身份验证。有关详细信息，请参阅 将 NetScaler Console 与 ServiceNow 实例集成。

先决条件

在配置云连接之前，请确保满足以下先决条件：

- 确保有互联网连接，或者在本地 NetScaler Console 中配置了代理服务器，以便访问 Citrix Cloud。
- 用于访问 NetScaler Console 以进行云连接配置的笔记本电脑或机器在初始设置期间必须具有互联网连接。有关详细信息，请参阅 常见问题。
- 确保 NetScaler Console 服务帐户可用。
    - 步骤 1：创建 Citrix Cloud 帐户或使用现有 Citrix Cloud 帐户登录。有关如何创建 Citrix Cloud 帐户的详细信息，请参阅 创建 Citrix Cloud 帐户。

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

- 步骤 2：通过管理 NetScaler Console 服务来创建 NetScaler Console 服务租户。有关如何管理 NetScaler Console 服务的详细信息，请参阅 入门。

- 确保您已允许访问以下端点 URL：

服务	政府云的 URL	亚太地区、欧盟和美国地区的 URL	日本的 URL	为什么需要它？
信任服务	`*.citrixnetworkapi.us`	-	-	用于在本地 NetScaler Console 和 Citrix Cloud 服务之间建立信任。
	`trust.citrixnetworkapi.us`	`trust.citrixnetworkapi.net`	`trust.citrixnetworkapi.jp`	
服务 URL	`*.agent.adm.cloud.us`	`*.agent.adm.cloud.com`	`*.agent.adm.citrixcloud.jp`	这些是用于 Cloud Connect 操作的 NetScaler Console 服务端点。本地部署的 NetScaler Console 会向这些端点发起出站通信，以实现云交付功能。
	`*.adm.cloud.us`	`*.adm.cloud.com`	`*.citrixnetworkapi.jp`	
	`adm.cloud.us`	`adm.cloud.com`	`*.adm.citrixcloud.jp`	
	-	`netscalermas.cloud.com`	`adm.citrixcloud.jp`	用于获取客户详细信息，例如端点、POP 名称。

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

服务	政府云的 URL	亚太地区、欧盟和美国地区的 URL	日本的 URL	为什么需要它？
Citrix Cloud™ 连接性	`citrix.cloud.us`	`Citrix.cloud.com`	`citrix.citrixcloud.jp`	Cloud Connect 入门期间进行身份验证和租户选择所需。
	`accounts.cloud.us`	`Accounts.cloud.com`	`accounts.citrixcloud.jp`	

- 确保您从访问 NetScaler Console 本地 GUI 的浏览器中禁用弹出窗口阻止程序。
- (仅适用于政府云) 在 NetScaler Console 本地版上执行以下步骤，以连接到政府云区域端点。
  - 在 NetScaler Console 本地版的 shell 中，运行以下命令：

```
cd /mps/python/util/



python consoleService.py --region gov
```

注意：

这些命令会重新启动 NetScaler Console 进程。

- (仅适用于日本云用户) 在 NetScaler Console 本地版上执行以下步骤，以连接到日本区域端点。
  - 在 NetScaler Console 本地版的 shell 中，运行以下命令：

```
cd /mps/python/util/



python consoleService.py --region japan
```

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

> **注意：**
>
> 该命令会重新启动 NetScaler Console 进程。

- 配置以下端口：

```
-  443 (NetScaler Console on-prem/proxy to Cloud)

-  80 (NetScaler Console on-prem to proxy)
```

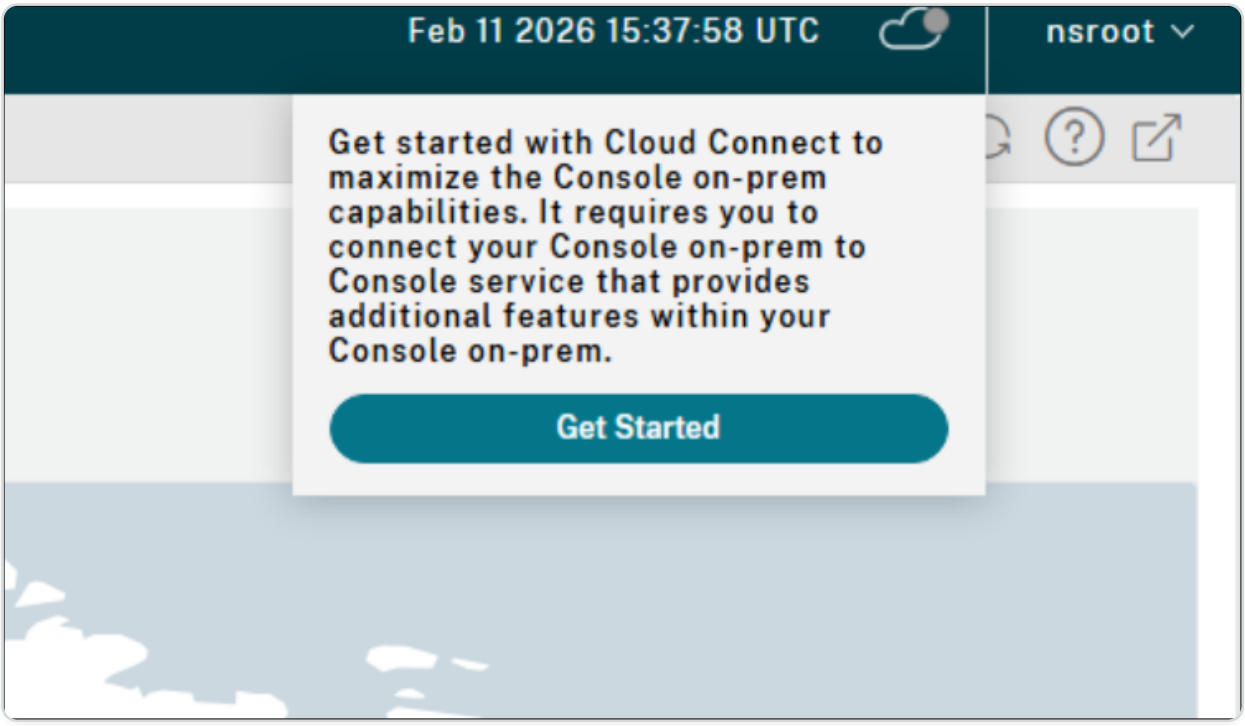
- 禁用用于配置 Cloud Connect 的 NetScaler Console GUI 主机的浏览器弹出窗口阻止程序。

配置云连接

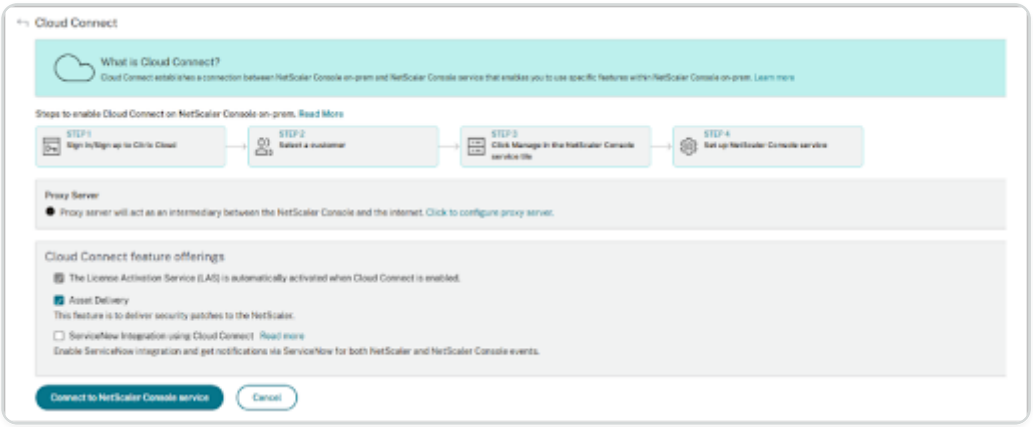
工作流 1 – 新用户（无 Citrix Cloud 帐户且无 NetScaler Console 服务租户）

1. 创建 Citrix Cloud 帐户。有关详细信息，请参阅 创建 Citrix Cloud 帐户。
2. 登录 Citrix Cloud 帐户，然后单击 **NetScaler Console 服务**磁贴。成功登录后，页面将重定向到 NetScaler Console 服务租户创建步骤。
   a. 选择一个适合您业务需求的**区域**，然后点击**完成**。
   b. 选择一个**角色**并完成设置。有关更多信息，请参阅入门。
3. 登录到本地NetScaler Console，点击**云**图标 > **开始**。

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



4. 点击**连接到NetScaler Console服务**。



   a. 登录到您的Citrix Cloud帐户。

   b. 选择您的帐户名称以完成登录。

   c. 您将看到“登录成功”消息。

Cloud Connect 配置已完成，Cloud Connect 显示**已连接**状态。您可以从**Cloud Connect**配置页面进一步启用集成，例如**ServiceNow**。

工作流 2 – Citrix Cloud 帐户存在但 NetScaler Console 服务租户不存在

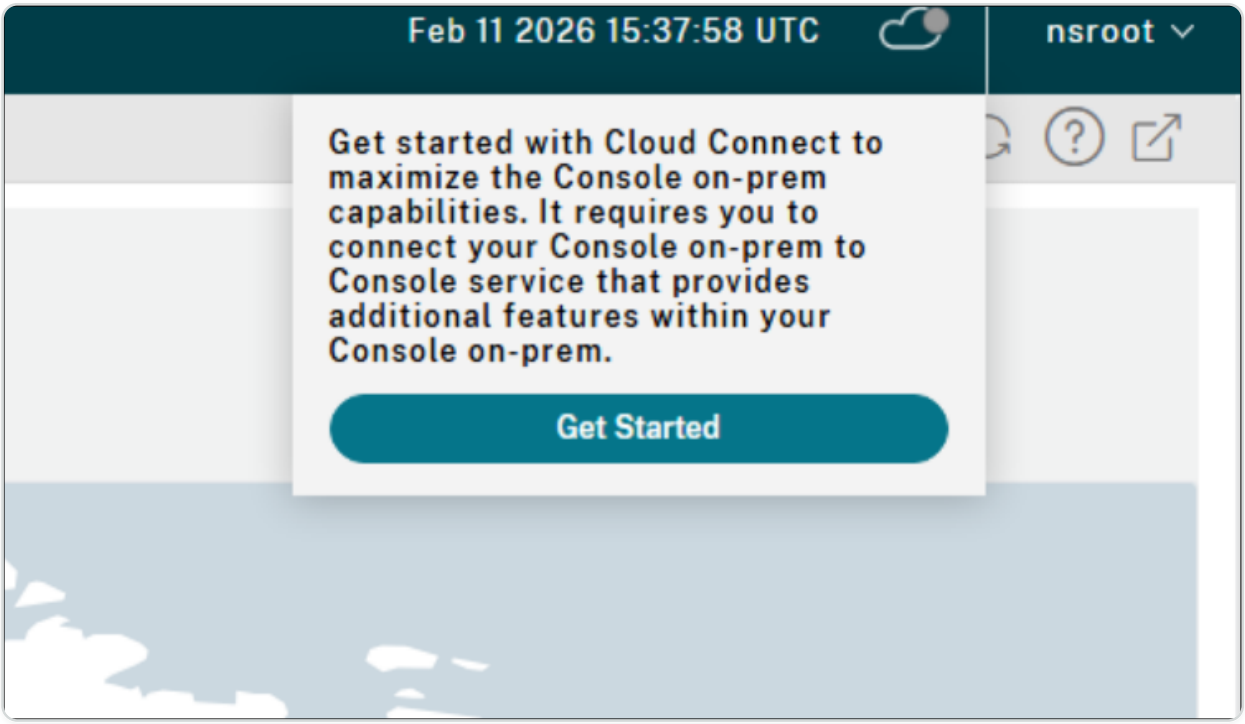
1. 登录到 Citrix Cloud 帐户并点击**NetScaler Console 服务**磁贴。成功登录后，页面将重定向到 NetScaler Console 服务租户创建步骤。

   a. 选择一个适合您业务需求的**区域**，然后点击**完成**。

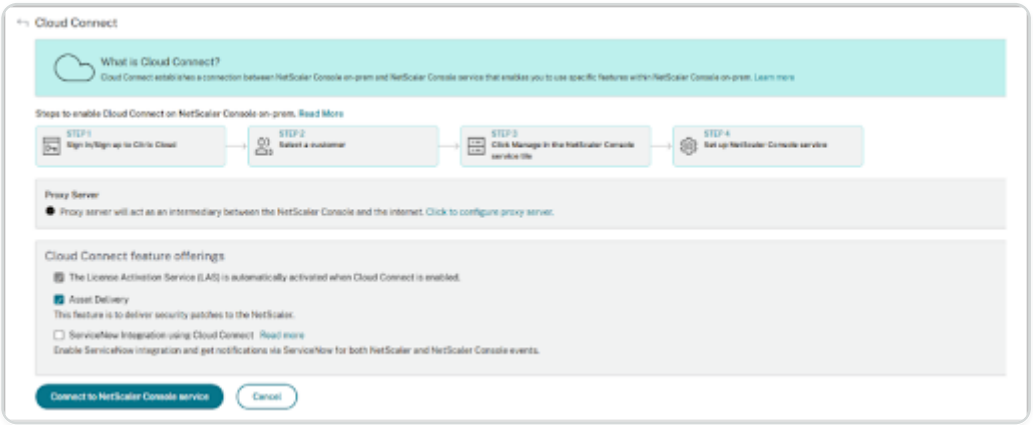
   b. 选择一个**角色**并完成设置。有关更多信息，请参阅入门。

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

2. 在 NetScaler Console 中，点击**云**图标 > **开始**。



3. 单击**连接到 NetScaler Console 服务**。



   a. 登录到您的 Citrix Cloud 帐户。

   b. 选择您的帐户名称以完成登录。

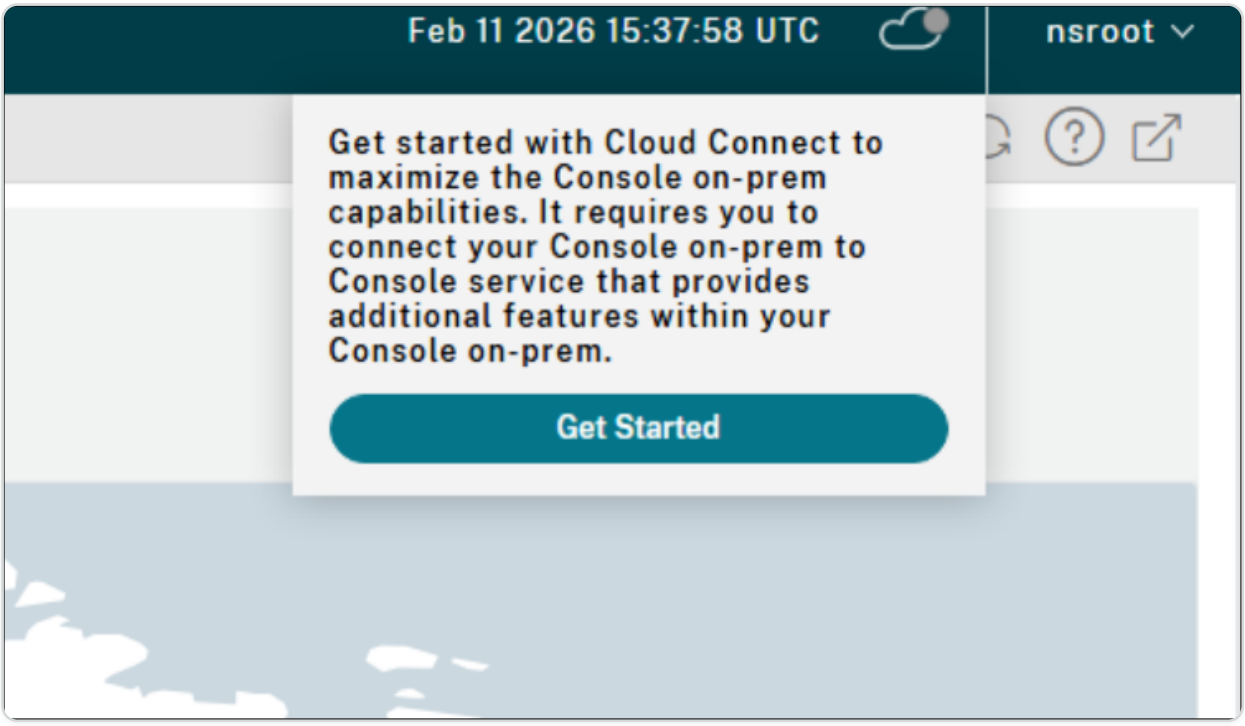
   c. 您将看到“登录成功”消息。

Cloud Connect 配置完成，Cloud Connect 显示**已连接**状态。您可以从 **Cloud Connect** 配置页面进一步启用集成，例如 **ServiceNow**。

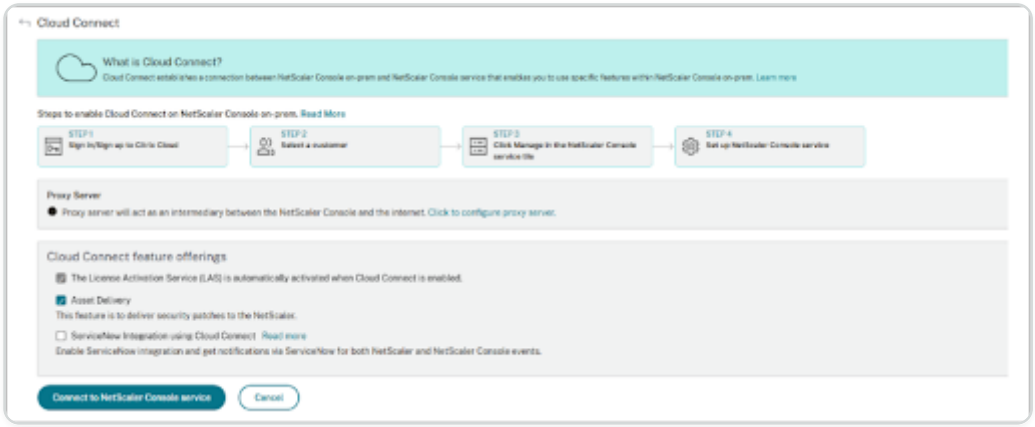
工作流 3 - Citrix Cloud 帐户和 NetScaler Console 服务租户已存在

1. 在 NetScaler Console 中，单击**云**图标 > **开始**。

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



2. 单击**连接到 NetScaler Console 服务**。



   a. 登录到您的 Citrix Cloud 帐户。

   b. 选择您的帐户名称以完成登录。

   c. 您将看到“登录成功”消息。

Cloud Connect 配置已完成，Cloud Connect 显示**已连接**状态。您可以从 **Cloud Connect** 配置页面进一步启用集成，例如 **ServiceNow**。

Cloud Connect 的代理配置支持

Cloud Connect 支持未经身份验证和已通过身份验证的代理服务器。代理服务器配置是可选的。

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

注意：

- 从 NetScaler Console 14.1-66.x 版本开始，Cloud Connect 支持显式代理部署的 SSL 拦截。上传代理的 CA 证书以建立受信任的通信。有关使用 SSL 检查管理启用代理的配置的证书的信息，请参阅管理 CA 证书。
- 支持基本身份验证类型。
- 支持以下代理配置类型：
  - 显式正向代理（非拦截）
  - 显式 SSL 拦截代理
  - 透明 SSL 拦截代理

  有关代理配置类型的更多信息，请参阅代理配置支持。
- 确保代理已配置为允许 WebSocket 连接，因为 Cloud Connect 在某些服务操作中需要 WebSocket 通信。

1. 在 Cloud Connect 配置页面上，单击**单击以配置代理服务器**。

2. 启用代理并输入 IP/FQDN 和端口。
3. 如果需要，添加一个 `Username` 和 `Password`。

   连接 NetScaler Console 服务(/en-us/netscaler-application-delivery-management-software/media/proxy-server-configuration-fields.png)

Cloud Connect 状态和刷新行为

云连接状态

Cloud Connect 状态反映了本地部署的 NetScaler Console 与 Citrix Cloud 之间连接的当前运行状况。支持的状态包括：

- **已连接** – 连接正常且运行良好。
- **已断开连接** – 连接已主动断开。
- **待定** – Cloud Connect 正在建立中。

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

- **错误** – Cloud Connect 连接检测到问题。

刷新 Cloud Connect 状态

Cloud Connect 状态每六小时自动刷新一次。管理员还可以使用**刷新 Cloud Connect 状态**来触发即时状态更新。

刷新操作会验证所需云服务 URL 的可访问性。

注意：

从 NetScaler Console 14.1-73.x 版本开始，刷新功能已与**检查连接**合并。

云连接诊断

“**检查连接**”诊断工具可帮助管理员排查本地 NetScaler Console 与 NetScaler Console 服务之间的连接问题。

“**检查连接**”工具执行以下检查：

- 检查所有必需的 Cloud Connect 服务端点的可达性。
- 验证通过配置的代理设置（如果适用）的连接。
- **WebSocket 连接验证：** 验证 Cloud Connect 用于与云服务保持持久连接的 WebSocket 通信。在 NetScaler Console 14.1-72.x 及更早版本中，此检查是刷新操作的一部分。
- **虚拟文件上传和下载验证：** 验证所有 Cloud Connect 功能（例如基于 LAS 的许可）的端到端通信。在 NetScaler Console 14.1-72.x 及更早版本中，此检查是刷新操作的一部分。

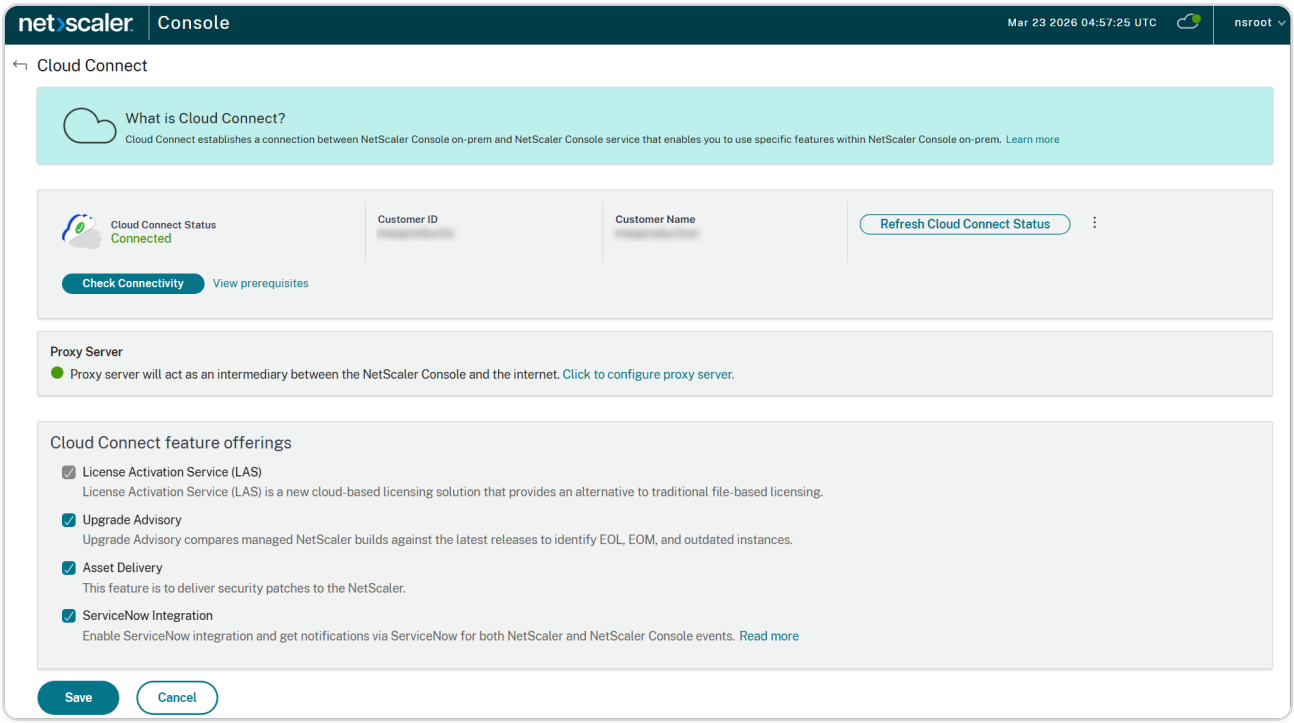
诊断结果包括以下信息：

- 每个服务 URL 显示为“可达”或“不可达”。
- 任何故障都会直接在 UI 中显示，并附带描述性错误消息。

解决网络或代理问题后，管理员必须执行以下操作：

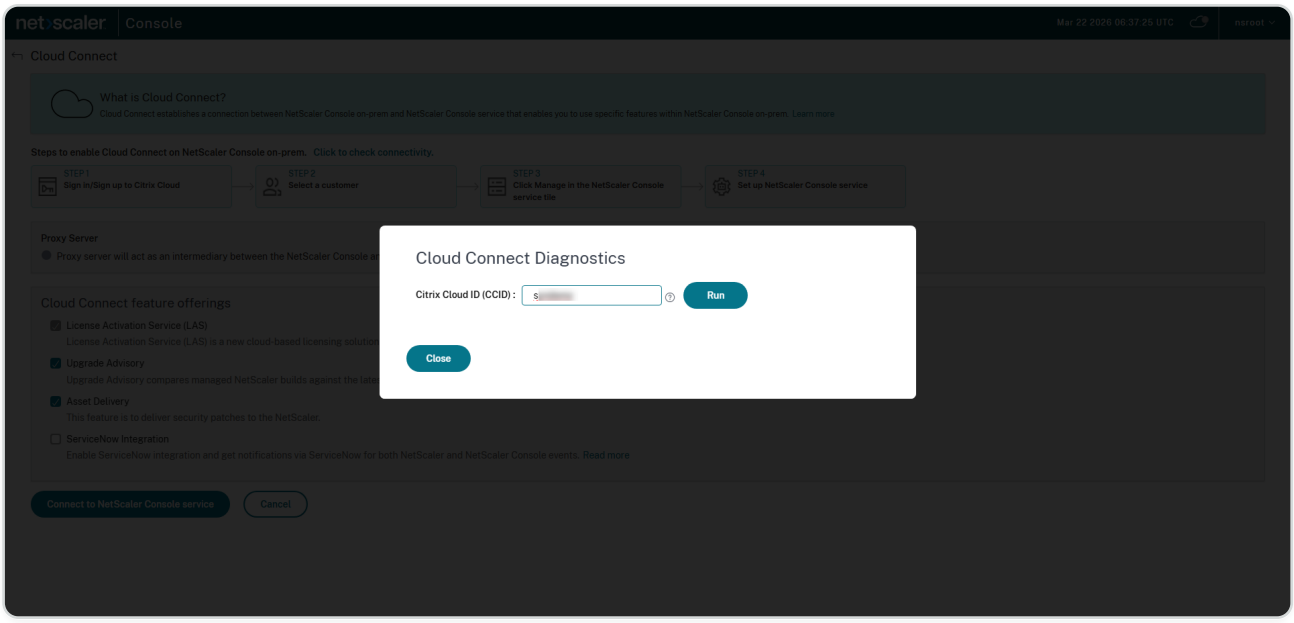
- 重新运行**检查连接**。
- 使用**刷新 Cloud Connect 状态**来更新整体连接状态。

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



即使 Cloud Connect 尚未完全建立或连接，您也可以通过输入 CCID 来运行**检查连接**。此步骤有助于在连接到 Cloud Connect 之前确认所有先决条件均已满足。

单击**检查连接**，通过输入 CCID 来验证与您的 CCID 的连接，并确保即使在 Cloud Connect 完全建立之前，所有先决条件都已满足。



单击**查看先决条件**以查看 Cloud Connect 的所有先决条件。

Cloud Connect - 查看先决条件(/en-us/netscaler-application-delivery-management-software/media/cloud-connect-prerequisite-list.png)

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

错误处理和消息传递

根据诊断和代理验证，可能会出现以下错误：

- **SSL 证书验证失败** – 表示缺少或无效的代理 CA 证书。当使用 SSL 拦截代理且代理 CA 证书未上传到 Console 时，会发生此错误。

  Cloud Connect - SSL 证书验证失败(/en-us/netscaler-application-delivery-management-software/media/cloud-connect-ssl-certificate-failure.png)

- **所需服务 URL 不可达** – 表示代理配置未正常运行，或者网络上不允许所需的 URL。

  Cloud Connect - 代理配置失败(/en-us/netscaler-application-delivery-management-software/media/cloud-connect-proxy-failure.png)

Cloud Connect 状态通知

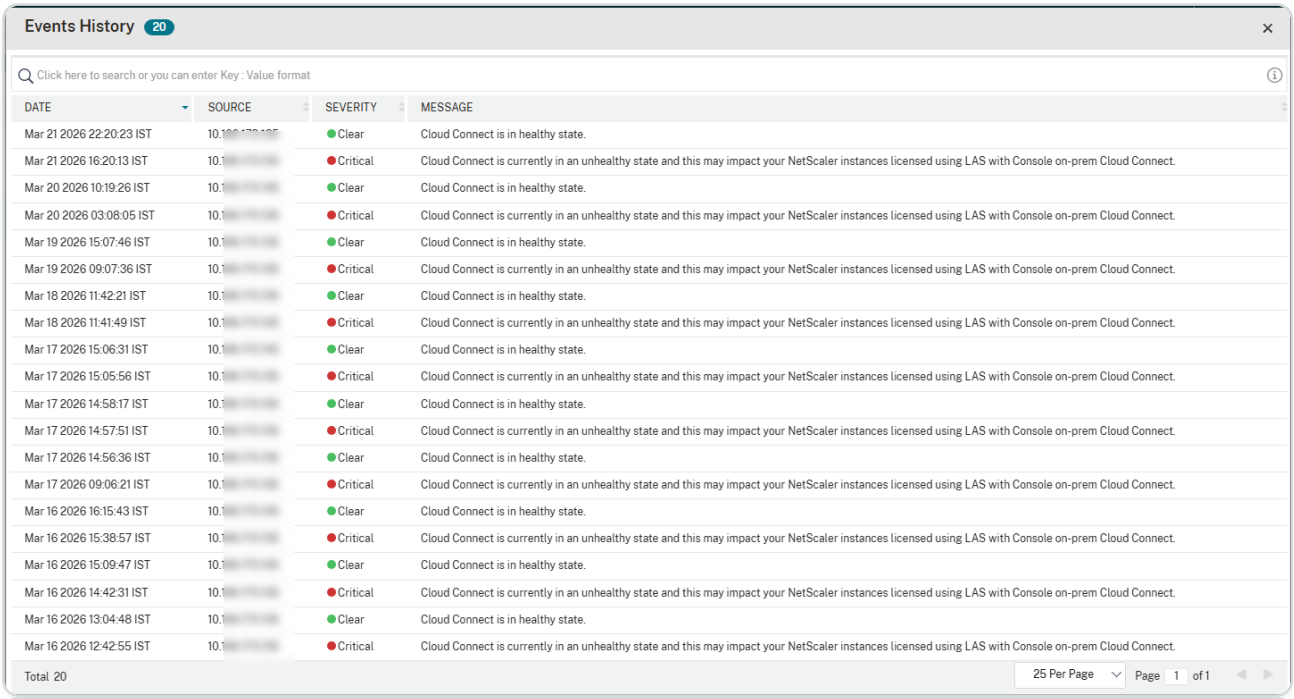
NetScaler Console 生成通知，以告知管理员 Cloud Connect 状态的变化。这些通知会提醒管理员 Cloud Connect 连接问题，这些问题可能会影响 Cloud Connect 依赖的功能，例如升级建议、资产交付、基于遥测的服务和集成。

当本地 NetScaler Console 和 Citrix Cloud 之间的连接状态发生变化时，会触发 Cloud Connect 通知，包括：

- 当 Cloud Connect 从“已连接”转换为“已断开连接”或“错误”时
- 当 Cloud Connect 从“已断开连接”或“错误”转换回“已连接”时

您还可以在**设置 > 系统事件**下查看 Cloud Connect 状态事件。

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

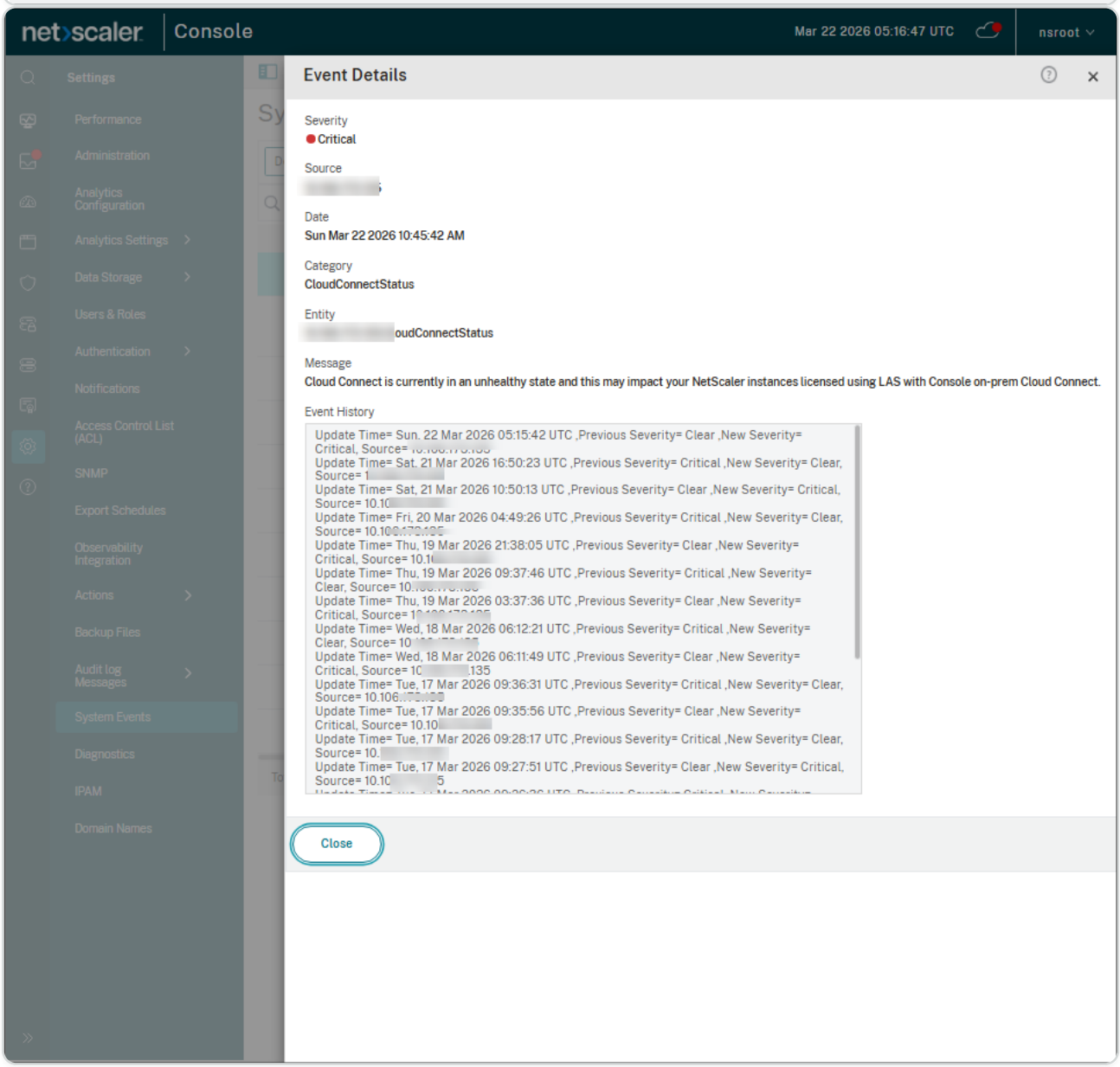


Events History 20

Click here to search or you can enter Key : Value format

DATE	SOURCE	SEVERITY	MESSAGE
Mar 21 2026 22:20:23 IST	10.1[illegible]	Clear	Cloud Connect is in healthy state.
Mar 21 2026 16:20:13 IST	10.1[illegible]	Critical	Cloud Connect is currently in an unhealthy state and this may impact your NetScaler instances licensed using LAS with Console on-prem Cloud Connect.
Mar 20 2026 10:19:26 IST	10.1[illegible]	Clear	Cloud Connect is in healthy state.
Mar 20 2026 03:08:05 IST	10.1[illegible]	Critical	Cloud Connect is currently in an unhealthy state and this may impact your NetScaler instances licensed using LAS with Console on-prem Cloud Connect.
Mar 19 2026 15:07:46 IST	10.1[illegible]	Clear	Cloud Connect is in healthy state.
Mar 19 2026 09:07:36 IST	10.1[illegible]	Critical	Cloud Connect is currently in an unhealthy state and this may impact your NetScaler instances licensed using LAS with Console on-prem Cloud Connect.
Mar 18 2026 11:42:21 IST	10.1[illegible]	Clear	Cloud Connect is in healthy state.
Mar 18 2026 11:41:49 IST	10.1[illegible]	Critical	Cloud Connect is currently in an unhealthy state and this may impact your NetScaler instances licensed using LAS with Console on-prem Cloud Connect.
Mar 17 2026 15:06:31 IST	10.1[illegible]	Clear	Cloud Connect is in healthy state.
Mar 17 2026 15:05:56 IST	10.1[illegible]	Critical	Cloud Connect is currently in an unhealthy state and this may impact your NetScaler instances licensed using LAS with Console on-prem Cloud Connect.
Mar 17 2026 14:58:17 IST	10.1[illegible]	Clear	Cloud Connect is in healthy state.
Mar 17 2026 14:57:51 IST	10.1[illegible]	Critical	Cloud Connect is currently in an unhealthy state and this may impact your NetScaler instances licensed using LAS with Console on-prem Cloud Connect.
Mar 17 2026 14:56:36 IST	10.1[illegible]	Clear	Cloud Connect is in healthy state.
Mar 17 2026 09:06:21 IST	10.1[illegible]	Critical	Cloud Connect is currently in an unhealthy state and this may impact your NetScaler instances licensed using LAS with Console on-prem Cloud Connect.
Mar 16 2026 16:15:43 IST	10.1[illegible]	Clear	Cloud Connect is in healthy state.
Mar 16 2026 15:38:57 IST	10.1[illegible]	Critical	Cloud Connect is currently in an unhealthy state and this may impact your NetScaler instances licensed using LAS with Console on-prem Cloud Connect.
Mar 16 2026 15:09:47 IST	10.1[illegible]	Clear	Cloud Connect is in healthy state.
Mar 16 2026 14:42:31 IST	10.1[illegible]	Critical	Cloud Connect is currently in an unhealthy state and this may impact your NetScaler instances licensed using LAS with Console on-prem Cloud Connect.
Mar 16 2026 13:04:48 IST	10.1[illegible]	Clear	Cloud Connect is in healthy state.
Mar 16 2026 12:42:55 IST	10.1[illegible]	Critical	Cloud Connect is currently in an unhealthy state and this may impact your NetScaler instances licensed using LAS with Console on-prem Cloud Connect.

Total 20 | 25 Per Page | Page 1 of 1



net›scaler | Console | Mar 22 2026 05:16:47 UTC | nsroot

Settings
Performance
Administration
Analytics Configuration
Analytics Settings
Data Storage
Users & Roles
Authentication
Notifications
Access Control List (ACL)
SNMP
Export Schedules
Observability Integration
Actions
Backup Files
Audit log Messages
System Events
Diagnostics
IPAM
Domain Names

Event Details

Severity
Critical

Source
[illegible]

Date
Sun Mar 22 2026 10:45:42 AM

Category
CloudConnectStatus

Entity
[illegible]oudConnectStatus

Message
Cloud Connect is currently in an unhealthy state and this may impact your NetScaler instances licensed using LAS with Console on-prem Cloud Connect.

Event History

Update Time= Sun, 22 Mar 2026 05:15:42 UTC ,Previous Severity= Clear ,New Severity= Critical, Source= [illegible]
Update Time= Sat, 21 Mar 2026 16:50:23 UTC ,Previous Severity= Critical ,New Severity= Clear, Source= 1[illegible]
Update Time= Sat, 21 Mar 2026 10:50:13 UTC ,Previous Severity= Clear ,New Severity= Critical, Source= 10.10[illegible]
Update Time= Fri, 20 Mar 2026 04:49:26 UTC ,Previous Severity= Critical ,New Severity= Clear, Source= 10.10[illegible]
Update Time= Thu, 19 Mar 2026 21:38:05 UTC ,Previous Severity= Clear ,New Severity= Critical, Source= 10.1[illegible]
Update Time= Thu, 19 Mar 2026 09:37:46 UTC ,Previous Severity= Critical ,New Severity= Clear, Source= 10.[illegible]
Update Time= Thu, 19 Mar 2026 03:37:36 UTC ,Previous Severity= Clear ,New Severity= Critical, Source= 1[illegible]
Update Time= Wed, 18 Mar 2026 06:12:21 UTC ,Previous Severity= Critical ,New Severity= Clear, Source= 10[illegible]
Update Time= Wed, 18 Mar 2026 06:11:49 UTC ,Previous Severity= Clear ,New Severity= Critical, Source= 10[illegible].135
Update Time= Tue, 17 Mar 2026 09:36:31 UTC ,Previous Severity= Critical ,New Severity= Clear, Source= 10.106.[illegible]
Update Time= Tue, 17 Mar 2026 09:35:56 UTC ,Previous Severity= Clear ,New Severity= Critical, Source= 10.10[illegible]
Update Time= Tue, 17 Mar 2026 09:28:17 UTC ,Previous Severity= Critical ,New Severity= Clear, Source= 10.[illegible]
Update Time= Tue, 17 Mar 2026 09:27:51 UTC ,Previous Severity= Clear ,New Severity= Critical, Source= 10.10[illegible]5

Close

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

通知频率

如果 Cloud Connect 保持 `Disconnected` 或 `Error` 状态，则每六小时发送一次通知。当 Cloud Connect 连接恢复时，将发送一条通知以指示恢复。

通知渠道

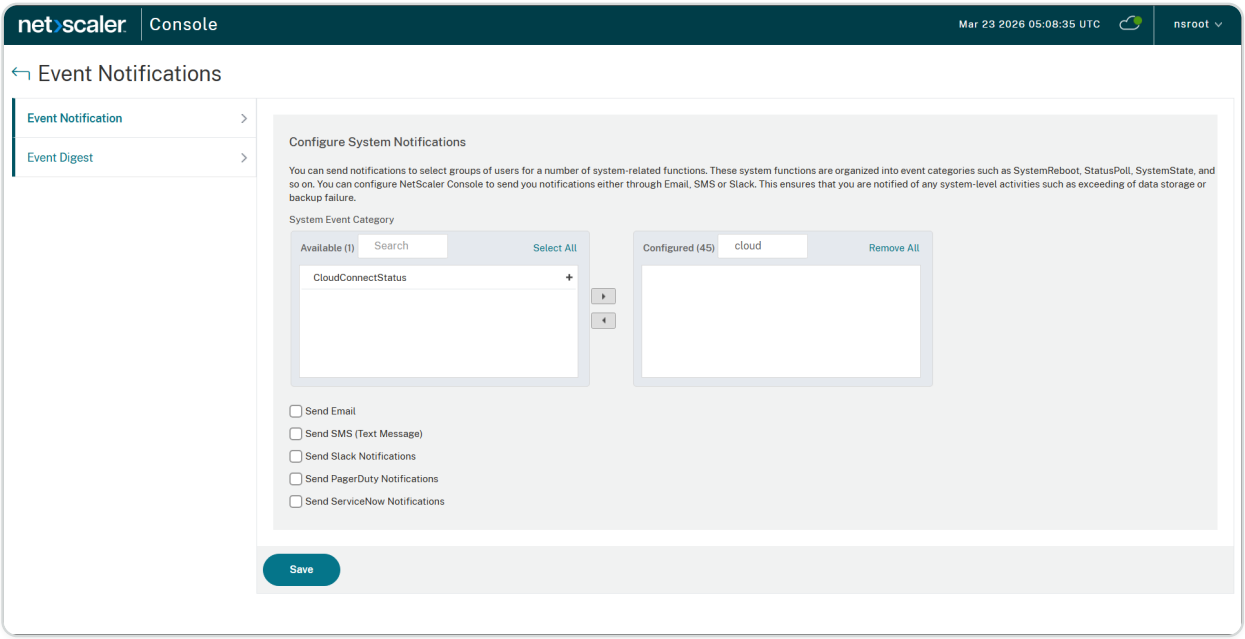
Cloud Connect 通知通过标准的 NetScaler Console 通知框架传递，可以使用“**系统事件通知**”进行配置。支持的通知渠道包括：

- 电子邮件
- 斯莱克
- PagerDuty
- ServiceNow

管理通知

Cloud Connect 状态通知默认启用。如有必要，您可以禁用电子邮件通知。要禁用电子邮件通知：

1. 导航到“**设置 > 管理 > 配置事件通知和摘要**”。
2. 在“**事件通知 > 配置系统通知**”下，搜索“**CloudConnectStatus**”。
3. 删除“**CloudConnectStatus**”系统事件类别，然后单击“**保存**”。



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

通过 Cloud Connect 收集的数据

重要提示：

Cloud Connect 不是 NetScaler 遥测程序的通道。遥测数据是使用自动启用的通道收集的。有关遥测相关信息，请参阅 NetScaler 遥测程序。

当在本地 NetScaler Console 上启用 Cloud Connect 且您使用的是 LAS 兼容版本时，LAS 会自动启用。有关作为 LAS 相关工作流一部分收集的信息的详细信息，请参阅 许可证激活服务。

Cloud Connect 连接问题故障排除

- 问题：登录时弹出窗口被阻止

  解决方案：禁用浏览器弹出窗口阻止程序并重试 Cloud Connect 入门。

- 问题：端点被阻止

  解决方案：验证 Download/Trust/Service 和 Citrix Cloud 域（或日本区域等效项）的允许列表。

- 问题：LAS 宽限期警告

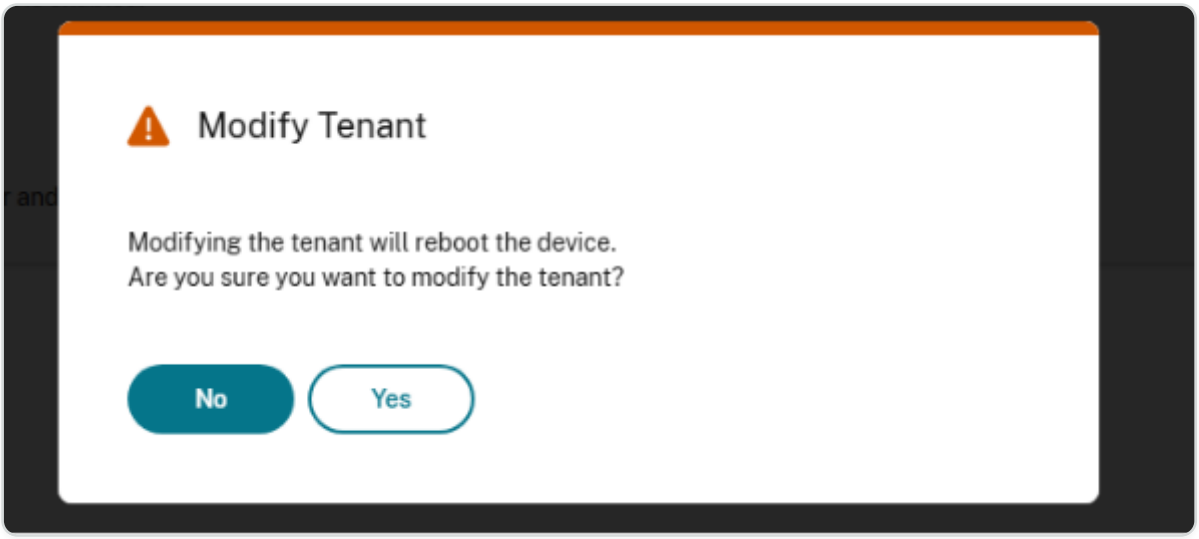
  确保本地 NetScaler Console 可以访问 Citrix Cloud（直接或通过代理）。授权 blob 会自动刷新；重复失败会触发宽限期和警报。

其他选项

启用 Cloud Connect 后，您可以使用以下选项：

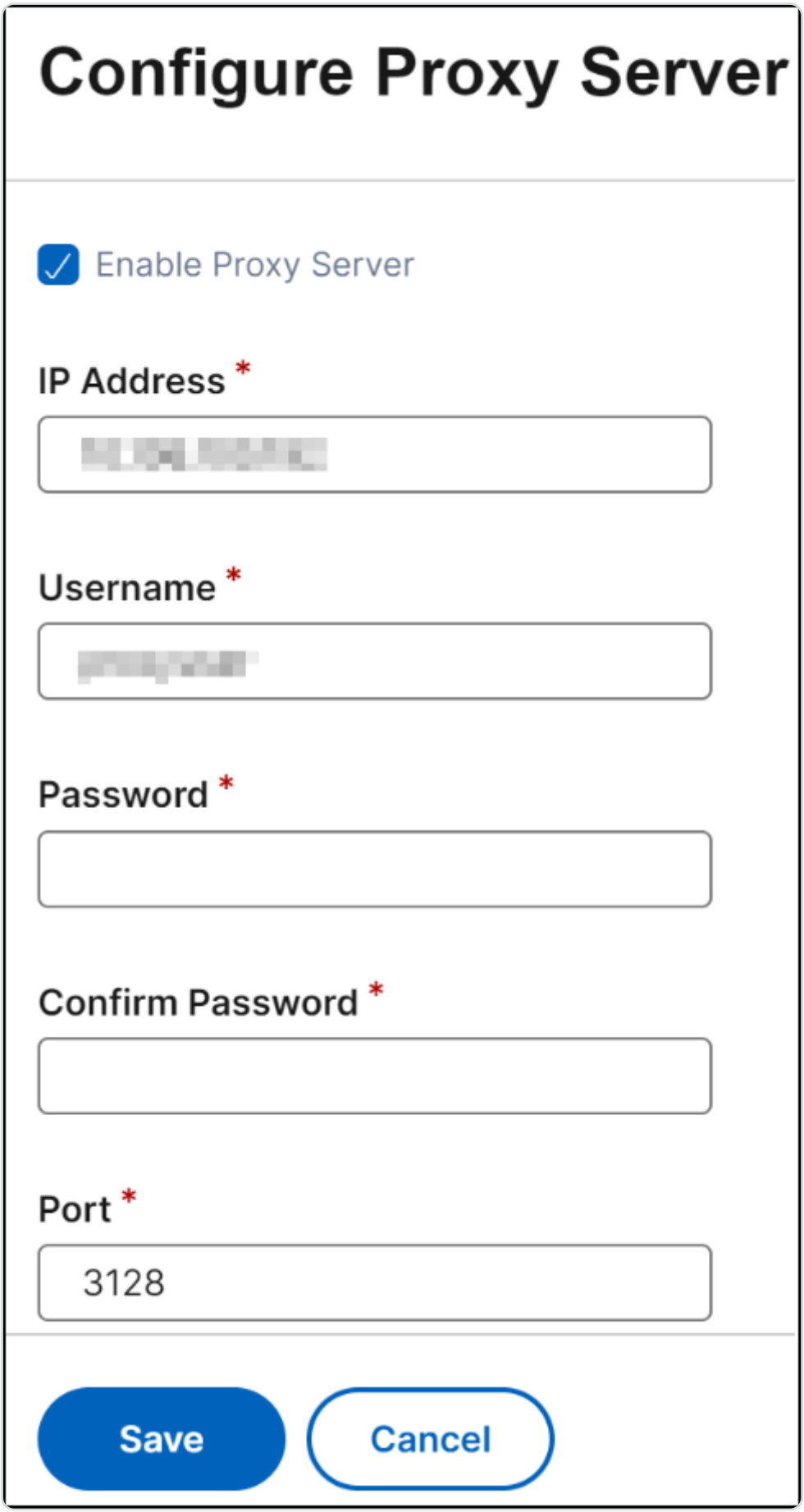
- **修改租户** - 使您能够更改现有租户。当您单击“**修改租户**”时，您将被重定向到一个新选项卡，并且必须登录 Citrix Cloud。成功登录后，您可以选择不同的租户。

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



- **修改代理** - 允许您在本地 NetScaler Console 中配置代理设置。当 NetScaler Console 无法通过管理网络直接访问互联网时，需要执行此操作。从列表中单击“**修改代理**”，更新详细信息，然后单击“**保存**”。

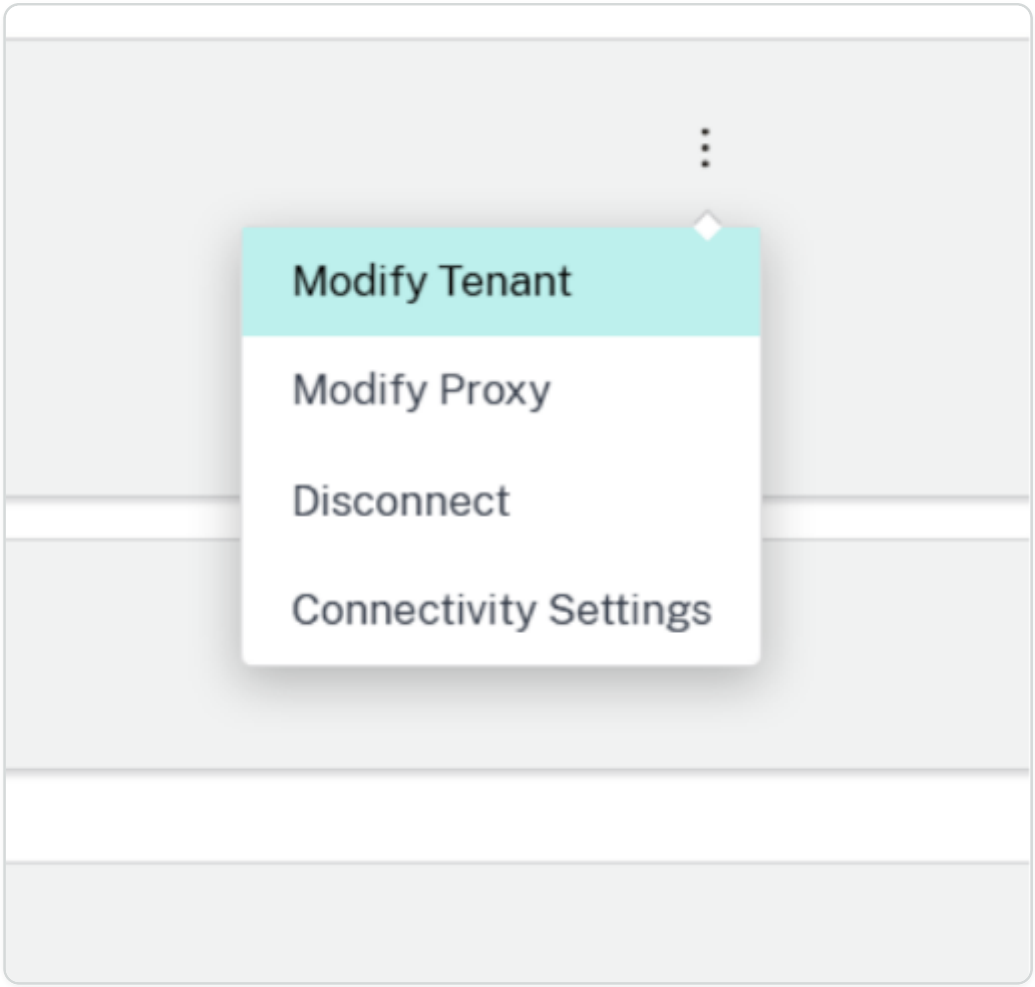
© 1997–2026 Citrix Systems, Inc. All rights reserved.



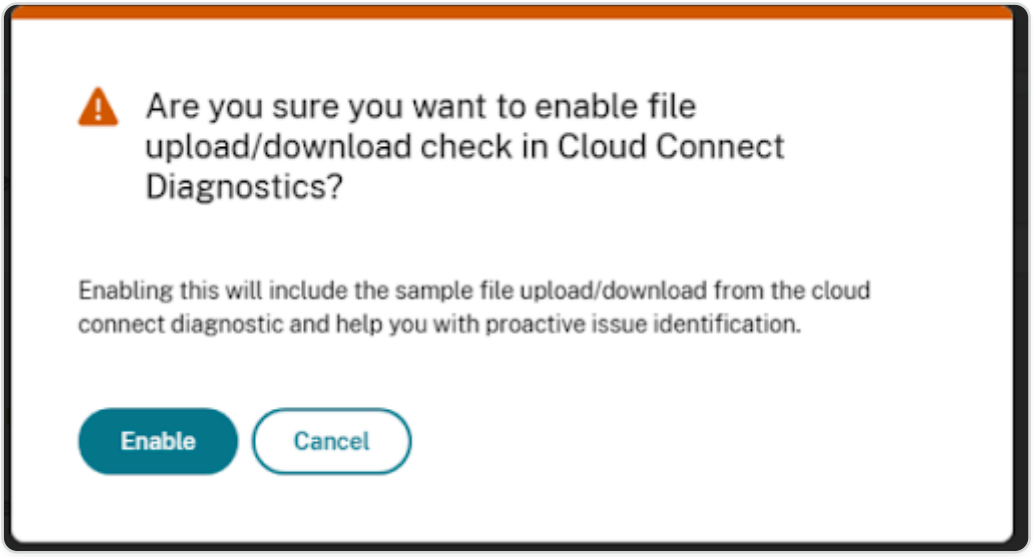
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **断开连接** - 禁用 Cloud Connect 功能。如果选择禁用，作为 Cloud Connect 一部分启用的所有功能都将停止工作。

  要禁用，请从列表中单击“**断开连接**”。



- **连接设置** - 禁用此设置会关闭示例文件上传和下载验证检查。因此，可能无法主动检测到可能影响 LAS 许可等功能的问题。



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

特定版本的功能行为

下表提供了不同本地 NetScaler Console 版本中通过 Cloud Connect 可用的功能：

版本	CLOUD CONNECT 中可用的功能	所需操作	通过 CLOUD CONNECT 收集数据
14.1-66.x 及更高版本	基于 LAS 的许可	配置云连接	否
	ServiceNow 集成		
	资产交付		
	升级建议		
14.1-56.x 及更高版本	基于 LAS 的许可	配置 云连接	否
	ServiceNow 集成		
	资产交付		
14.1-51.x 及更高版本	基于 LAS 的许可	配置 云连接	否
	ServiceNow 集成		
14.1-25.x 及更高版本	ServiceNow 集成	配置 Cloud Connect 并启用 ServiceNow 集成。	否
介于 14.1-8.x 和 14.1-21.x 之间	安全通告和 ServiceNow 集成	配置 Cloud Connect 并启用该功能	是。配置 Cloud Connect 后。有关更多信息，请参阅 Cloud Connect 的数据治理
14.1-4.x 或更早版本	不适用	不适用	不适用

常见问题

1. 必须添加到笔记本电脑允许列表中的确切 URL 是什么？

   为确保正常连接，请根据您的 NetScaler Console 服务帐户环境，将以下 URL 添加到浏览器的允许列表：

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

- 商业云
  - 信任服务
  - 思杰云
  - Citrix Cloud 帐户
- 日本云
  - 信任服务
  - 思杰云
  - Citrix Cloud 帐户
- 政府云
  - 信任服务
  - 思杰云

2. Cloud Connect 是否将配置推送到我的 NetScaler 实例？

   否。Cloud Connect 不会将配置推送到 NetScaler 实例；它只为本地 NetScaler Console 启用云交付服务，并促进许可证或资产交付。

3. 思杰云是否有任何入站连接到我的环境？

   否。Cloud Connect 使用从本地 NetScaler Console 发起的仅出站通信。

4. 是否需要将 NetScaler 实例迁移到 NetScaler Console 服务？

   否。您无需将实例迁移到 NetScaler Console 服务即可使用 Cloud Connect 功能。

5. 支持哪些代理身份验证类型？

   Cloud Connect 可以通过代理使用。我们支持基本身份验证或无身份验证代理集成。

6. 安全建议是否仍通过 Cloud Connect 启用？

   仅在特定的旧版 14.1 版本（8.x 到 21.x）上。在更高版本中，Cloud Connect 主要启用本主题中描述的功能。从版本 14.1-25.x 开始，安全建议可以通过自动启用通道使用。有关详细信息，请参阅 自动遥测数据收集模式。

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

配置

您只能通过使用 GUI 访问 NetScaler Console 服务器。您必须访问 GUI 才能添加实例、管理和监控您的实例和应用程序、查看分析以及配置 NetScaler Console 服务器。

您的工作站必须安装受支持的 Web 浏览器才能访问配置实用程序和控制板。

支持以下浏览器。

WEB 浏览器	版本
IE浏览器	11.0 及更高版本
谷歌浏览器	Chrome 19 及更高版本
Safari 浏览器	Safari 5.1.1 及更高版本
火狐浏览器	Firefox 3.6.25 及更高版本

要访问 NetScaler Console GUI：

使用管理员凭据登录到 NetScaler Console。

登录到 NetScaler Console 后，您需要执行以下操作才能开始：

- 将实例添加到 NetScaler Console。如果您想管理和监视这些实例，则必须将实例添加到 NetScaler Console 服务器。
- 在虚拟服务器上启用分析。要查看应用程序流量的分析数据，您必须在接收特定应用程序流量的虚拟服务器上启用分析功能。
- 在 NetScaler Console 上配置 NTP 服务器。您必须在 NetScaler Console 中配置网络时间协议 (NTP) 服务器，以使其时钟与 NTP 服务器同步。
- 配置系统设置以优化 NetScaler Console 性能。在开始使用 NetScaler Console 管理和监视实例和应用程序之前，建议您配置一些系统设置，以确保 NetScaler Console 服务器的最佳性能。

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

将实例添加到 NetScaler Console

实例是您希望从 NetScaler Console 发现、管理和监控的 NetScaler 设备或虚拟设备。如果您想管理和监控这些实例，则必须将实例添加到 NetScaler Console 服务器。您可以将以下 NetScaler 设备和虚拟设备添加到 NetScaler Console：

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler 网关

您可以在首次设置 NetScaler Console 服务器时或之后添加实例。然后，您必须指定 NetScaler Console 可用于访问实例的实例配置文件。

注意：

- NetScaler Console 使用 NetScaler 实例的 NetScaler IP (NSIP) 地址进行通信。有关 NetScaler 实例和 NetScaler Console 之间必须打开的端口的信息，请参阅 端口。
- 要了解 NetScaler Console 如何发现实例，请参阅 发现实例。

如何创建 NetScaler 配置文件

NetScaler 配置文件包括用于将实例添加到 NetScaler Console 的凭据、端口和身份验证类型。对于每种实例类型，都有一个默认配置文件可用。例如，`nsroot` 是 NetScaler 实例的默认配置文件。默认配置文件是使用默认 NetScaler 管理员凭据定义的。如果您更改了实例的默认管理员凭据，则可以为这些实例定义自定义实例配置文件。如果在发现实例后更改了实例的凭据，则必须编辑实例配置文件或创建配置文件，然后重新发现实例。

您可以从**实例**页面或在添加或更改实例时创建 NetScaler 配置文件。

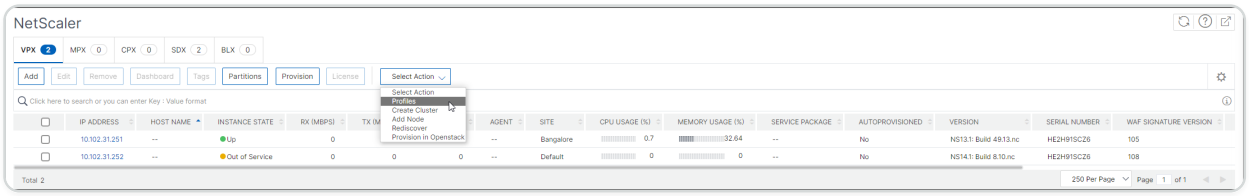
注意：

确保使用超级管理员帐户创建实例配置文件。

从“实例”页面创建 NetScaler 配置文件：

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

1. 导航到 **基础结构 > 实例**。
2. 选择一个实例。例如，NetScaler。
3. 在 NetScaler 页面上，在 **选择操作** 下选择 **配置文件**。



4. 在 **管理员配置文件** 页面上，选择 **添加**。

5. 在 **创建 NetScaler 配置文件** 页面上，执行以下操作：

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

Create NetScaler Profile

Profile Name*

profileName

User Name*

username

Password*

••••••••••••

SSH Port

22

HTTP Port

80

HTTPS Port

443

☑ Use global settings for NetScaler communication

SNMP

Version

○ v2 ◉ v3

Security Name*

security

Security Level*

NoAuthNoPriv

Timeout Settings

Maximum waiting time to reboot NetScaler.

Timeout (in Seconds)

1800

Create Close

a. **配置文件名称**：为 NetScaler 实例指定配置文件名称。

b. **用户名**：指定用于登录 NetScaler 实例的用户名。

c. **密码**：指定用于登录 NetScaler 实例的密码。

d. **SSH 端口**：指定 NetScaler Console 与 NetScaler 实例之间 SSH 通信的端口。

e. **HTTP 端口**：指定 NetScaler Console 与 NetScaler 实例之间 HTTP 通信的端口。

> **注意：**
>
> 默认 HTTP 端口为 80。您还可以指定可能已在 NetScaler CPX 实例中配置的非默认或自定义 HTTP 端口。自定义 HTTP 端口只能用于 NetScaler Console 与 NetScaler CPX 之间的通信。

f. **HTTPS 端口**：指定 NetScaler Console 与 NetScaler 实例之间 HTTPS 通信的端口。

> **注意：**
>
> 默认 HTTPS 端口为 443。您还可以指定可能已在 NetScaler CPX 实例中配置的非默认或自定义 HTTPS 端口。自定义 HTTPS 端口只能用于 NetScaler Console 与 NetScaler CPX 之间的通信。

g. **使用 NetScaler 通信的全局设置**：如果要使用系统设置进行 NetScaler Console 与 NetScaler 实例之间的通信，请选择此选项；否则，请选择 HTTP 或 HTTPS。

h. **SNMP 版本**：选择 **SNMPv2** 或 **SNMPv3**，然后执行以下操作：

   i. 如果选择 SNMPv2，请指定用于身份验证的**社区**名称。

   ii. 如果选择 SNMPv3，请指定**安全名称**和**安全级别**。根据安全级别，选择**身份验证类型**和**隐私类型**。

   > **注意：**
   >
   > 对于 NetScaler SDX，仅支持 **SNMPv2**。

i. **超时设置**：指定 NetScaler Console 在重启后向 NetScaler 实例发送连接请求之前必须等待的时间。

j. 选择**创建**。

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

将 NetScaler 实例添加到 NetScaler Console

您可以首次设置 NetScaler Console 服务器时添加实例，也可以稍后添加。

要添加实例，您必须指定每个 NetScaler 实例的主机名或 IP 地址，或者指定一个 IP 地址范围。

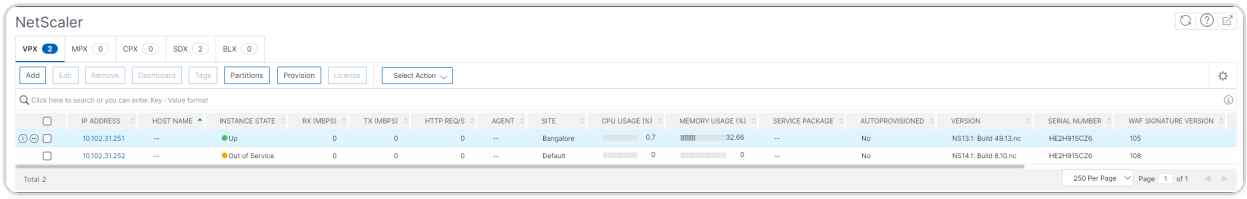
注意：

- 要添加在群集中配置的 NetScaler 实例，您必须指定群集 IP 地址或群集设置中的任何一个独立节点。但是，在 NetScaler Console 上，群集仅由群集 IP 地址表示。
- 对于设置为 HA 对的 NetScaler 实例，当您添加一个实例时，对中的另一个实例会自动添加。

当您从配置了代理的远程数据添加实例时，流量源通过该代理。

将实例添加到 NetScaler Console：

1. 使用管理员凭据登录到 NetScaler Console。
2. 导航到 **Infrastructure > Instances > NetScaler**。选择要添加的实例类型（例如，NetScaler VPX），然后单击 **Add**。



3. 选择以下选项之一：
   - **输入设备 IP 地址** - 对于 NetScaler 实例，请指定以下项之一：
     - 主机名
     - 每个 NetScaler 实例的 IP 地址或 NAT IP
     - IP 地址范围

     例如，输入一个或多个主机名、IP 地址或 NAT IP，和/或一个 IP 地址范围（例如，10.10.20.10-10.10.20.45），使用逗号分隔。用于发现 NAT HA 实例的输入格式为 `10.10.20.10#10.10.20.32`（两个 NetScaler HA 实例的 NAT IP 地址）。

     如果要使用 SNIP 发现 NetScaler HA 对，请确保已启用独立网络配置 (INC) 模式。并且，请按以下格式指定 SNIP 地址：

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

```
<SNIP of primary instance>#<SNIP of secondary instance>
```

- **从文件导入** - 从本地系统上传一个文本文件，其中包含要添加的所有实例的 IP 地址。

4. 从“**配置文件名称**”中，选择相应的实例配置文件，或通过单击“+”图标创建配置文件。
5. 从“**站点**”中，选择要添加实例的位置，或通过单击“**+**”图标创建位置。
6. 单击“**确定**”开始将实例添加到 NetScaler Console 的过程。

注意：

如果要重新发现实例，请导航到“**基础结构 > 实例 > NetScaler**”。选择实例类型（例如，VPX）并选择要重新发现的实例，然后从“**选择操作**”列表中单击“**重新发现**”。

将 NetScaler CPX 实例添加到 NetScaler Console

NetScaler Console 已得到增强，以支持 CPX 功能中已实现的改进。现在，通过为 CPX 提供 IP 地址以及设备配置文件，可以在 NetScaler Console 中添加 NetScaler CPX 实例。添加 CPX 实例的过程现在类似于在 NetScaler Console 中添加其他 NetScaler 类型（例如 VPX 或 MPX）的过程。此外，NetScaler Console 中 CPX 的注册也得到了增强。当 CPX 启动时，NetScaler Console 会自动发现并注册 CPX 实例。CPX 实例不再通过 Docker 主机发现。

1. 导航到“**基础结构 > 实例 > NetScaler**”，然后单击“**CPX**”。
2. 单击“**添加**”以在 NetScaler Console 中添加新的 CPX 实例。
3. “**添加 NetScaler CPX**”页面打开。输入以下参数的值：

   a. 您可以通过提供 CPX 实例的可访问 IP 地址或托管 CPX 实例的 Docker 容器的 IP 地址来添加 CPX 实例。

   b. 选择 CPX 实例的配置文件。

   c. 选择要部署实例的站点。

   d. 选择代理。

   e. 您可以选择为实例输入键值对。添加键值对可让您以后轻松搜索实例。

   添加 NetScaler CPX(/en-us/netscaler-application-delivery-management-software/media/add-cpx-instances.png)

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

注意：

对于 NetScaler CPX 实例，在创建 CPX 实例配置文件时，必须指定主机的 **HTTP**、**HTTPS**、**SSH** 和 **SNMP** 端口详细信息。您还可以在“**起始端口**”和“**端口数量**”字段中指定主机发布的端口范围。

4. 单击“**确定**”。

在 NetScaler Console 中添加独立 NetScaler BLX 实例

独立 NetScaler BLX 实例是在专用主机 Linux 服务器上运行的单个实例。

1. 导航到“**基础架构 > 实例 > NetScaler**”。
2. 在“**BLX**”选项卡中，单击“**添加**”。
3. 从“**实例类型**”列表中选择“**独立**”选项。
4. 在“**IP 地址**”字段中，指定 BLX 实例的 IP 地址。
5. 在“**主机 IP 地址**”字段中，指定托管 BLX 实例的 Linux 服务器的 IP 地址。
6. 在“**配置文件名称**”列表中，为 BLX 实例选择相应的配置文件，或创建配置文件。

   要创建配置文件，请点击 **添加**。

   重要提示：

   请确保您已在配置文件中指定了正确的 Linux 服务器主机用户名和密码。

7. 在 **站点** 列表中，选择要添加实例的站点。

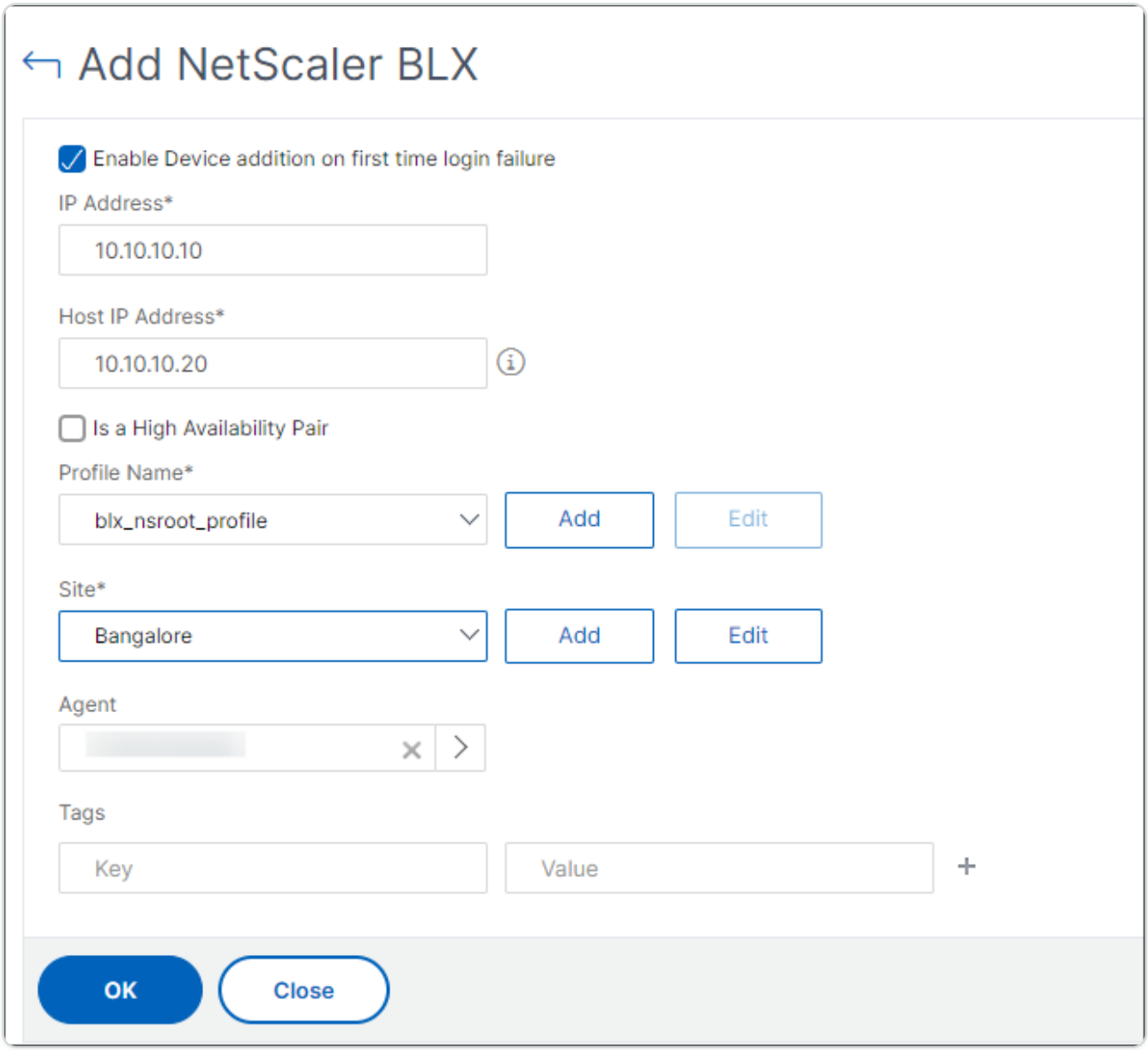
   如果要添加站点，请点击 **添加**。

8. 在 **代理** 列表中，选择要关联实例的 NetScaler 代理。

   如果您的 NetScaler Console 上只配置了一个代理，则默认选择该代理。

9. 点击 **确定**。

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



在 NetScaler Console 中添加高可用性 NetScaler BLX 实例

高可用性 NetScaler BLX 实例运行在不同的主机 Linux 服务器上。一台 Linux 服务器不能托管多个 BLX 实例。

1. 在 **BLX** 选项卡中，点击 **添加**。
2. 从 **实例类型** 列表中选择 **高可用性** 选项。
3. 在 **IP 地址** 字段中，指定 BLX 实例的 IP 地址。
4. 在 **主机 IP 地址** 字段中，指定托管 BLX 实例的 Linux 服务器的 IP 地址。
5. 在“**对等 IP 地址**”字段中，指定对等 BLX 实例的 IP 地址。
6. 在“**对等主机 IP 地址**”字段中，指定托管对等 BLX 实例的 Linux 服务器的 IP 地址。
7. 在“**配置文件名称**”列表中，选择适用于 BLX 实例的配置文件，或创建配置文件。

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

要创建配置文件，请单击“**添加**”。

> **重要提示：**
>
> 确保在配置文件中指定 Linux 服务器的正确主机用户名和密码。

8. 在“**站点**”列表中，选择要添加实例的站点。

   如果要添加站点，请单击“**添加**”。

9. 在“**代理**”列表中，选择要将实例关联到的 NetScaler 代理。

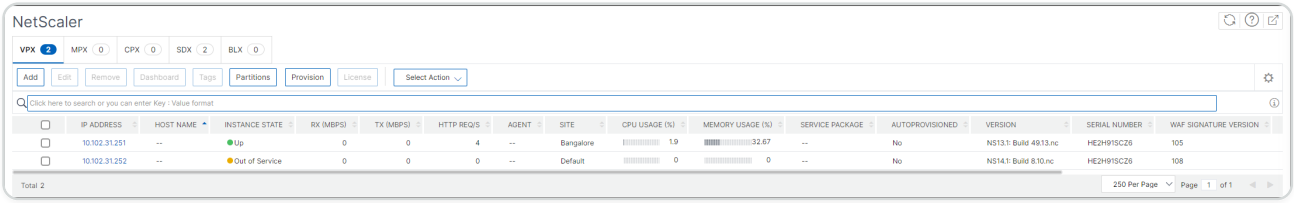
   如果您的 NetScaler Console 上只配置了一个代理，则默认选择该代理。

10. 单击“**确定**”。

将 NetScaler BLX 高可用性实例添加到 NetScaler Console(/en-us/netscaler-application-delivery-management-software/media/add-blx-ha-instance.png)

从 NetScaler Console 访问实例 GUI

1. 导航到“**基础结构 > 实例** > **NetScaler**”。
2. 选择要访问的实例类型（例如，VPX、MPX、CPX、SDX 或 BLX）。
3. 单击所需的 NetScaler IP 地址或主机名。



所选实例的 GUI 将在弹出窗口中显示。

将部署在云中的 NetScaler VPX 实例添加到 NetScaler Console

您可以使用 NetScaler Console 管理和监控部署在 Amazon Web Services (AWS)、Microsoft Azure 或 Google Cloud 等公有云上的 NetScaler VPX 实例。您需要在 NetScaler Console 与部署在公有云上的 NetScaler VPX 实例之间建立第 3 层连接。要建立第 3 层连接，您可以使用 Direct Connect to AWS、Azure 中的 VPN 或 Equinix 等第三方连接器。

以下示例拓扑使用 Citrix CloudBridge Connector 在 NetScaler Console 与部署在云中的 NetScaler VPX 实例之间建立第 3 层连接。

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

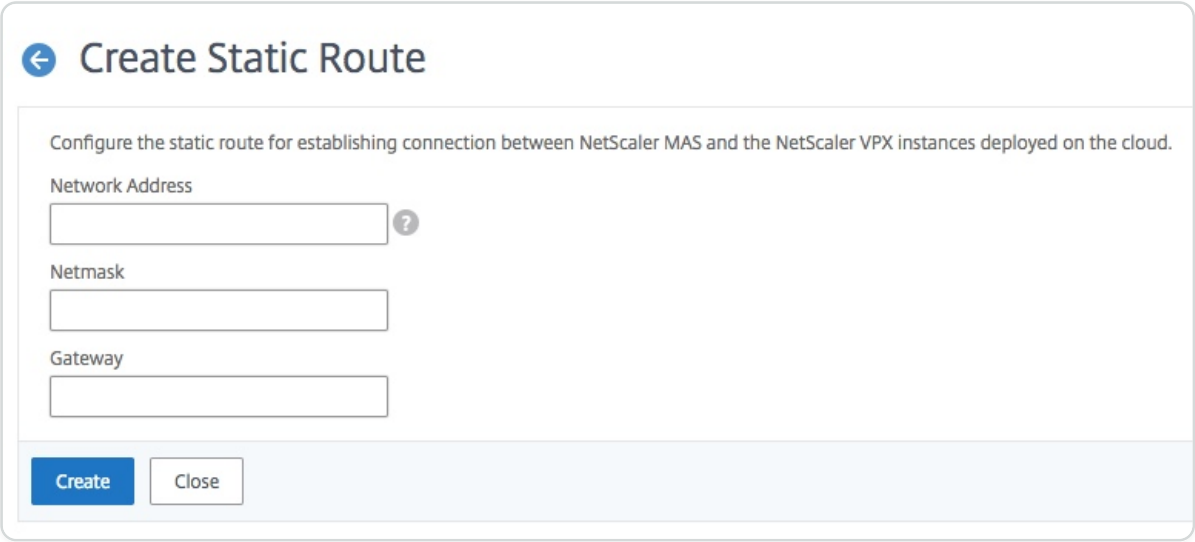
Citrix CloudBridge 连接器(/en-us/netscaler-application-delivery-management-software/media/cb-dc-dc-console.png)

在数据中心 DC 中的 NetScaler 设备 NS_Appliance-DC 与公有云中的 NetScaler 虚拟设备 (VPX) NS_VPX_CBC 之间建立 Citrix CloudBridge Connector 隧道。NS_Appliance-DC 和 NS_VPX_CBC 启用 NetScaler Console 与部署在公有云中的 NetScaler VPX 实例 NS_VPX_1 之间的通信。建立通信后，您可以在 NetScaler Console 中发现 NS_VPX_1。

配置此拓扑：

1. 在公有云中安装、配置和启动 NetScaler VPX 实例。
   - 有关说明，请参阅 在 AWS 上安装 NetScaler VPX。
   - 有关说明，请参阅 在 Microsoft Azure 上安装 NetScaler VPX。
   - 有关说明，请参阅 在 Google Cloud 上安装 NetScaler VPX。
2. 在数据中心的虚拟化平台上部署和配置 NetScaler 物理设备，或预配和配置 NetScaler 虚拟设备 (VPX)。
   - 有关说明，请参阅 在 Citrix Hypervisor 上安装 NetScaler VPX 实例。
   - 有关说明，请参阅 在 VMware ESXi 上安装 Citrix 虚拟设备。
   - 有关说明，请参阅 在 Microsoft Hyper-V 上安装 NetScaler 虚拟设备。
3. 配置数据中心与公有云之间的 Citrix CloudBridge Connector。有关说明，请参阅 配置 Citrix CloudBridge Connector。
4. 配置静态路由，用于在 NetScaler Console 与部署在云中的 NetScaler VPX 实例之间建立连接，如下所示：
   a. 登录到 NetScaler Console。
   b. 导航到 **系统 \> 静态路由**，然后单击**添加**。

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



c. 在**网络地址**字段中，输入您希望通过连接器从 NetScaler Console 建立静态路由的网络的地址。

d. 在**子网掩码**字段中，输入网络的子网掩码。

e. 在**网关**字段中，输入网关的地址。

5. 通过指定公有云中 NetScaler VPX 实例的 IP 地址范围，将 NetScaler VPX 云实例添加到 NetScaler Console。有关详细说明，请参阅将实例添加到 NetScaler Console。

配置分析

- 适用于 14.1-17.x 及更早版本(/zh-cn/netscaler-application-delivery-management-software/current-release/configure/enable-analytics-on-virtual-servers.html)
- 适用于 14.1-21.x 或更高版本(/zh-cn/netscaler-application-delivery-management-software/current-release/configure/enable-analytics-for-flexed-license.html)

管理许可并在虚拟服务器上启用分析

注意

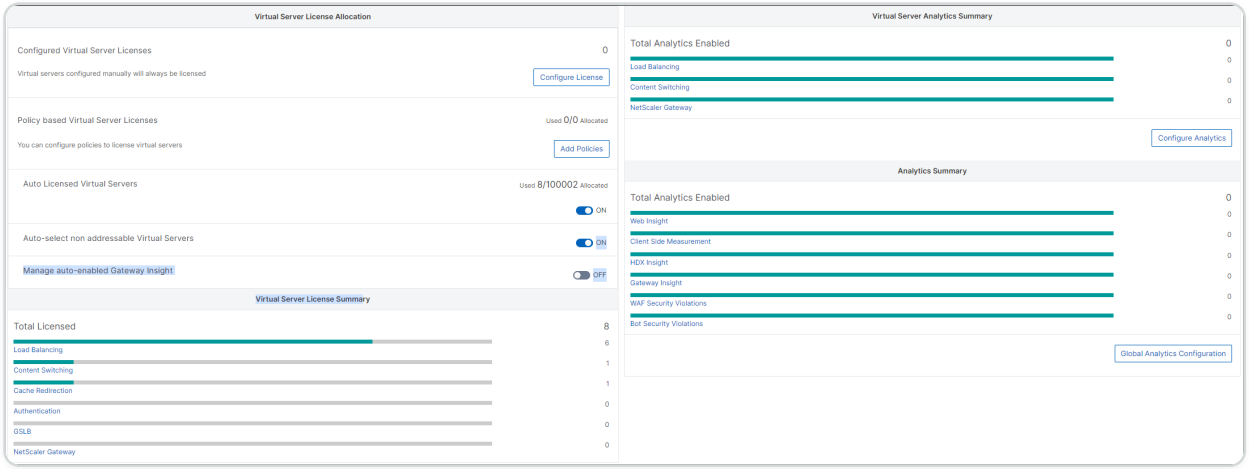
- 默认情况下，**自动许可虚拟服务器**选项处于启用状态。您必须确保拥有足够的许可证来许可虚拟服务器。如果您的许可证数量有限，并且只想根据需要许可选择性虚拟服务器，请禁用**自动许可虚拟服务器**选项。导航到**设置 > 许可与分析配置**，并在**虚拟服务器许可证分配**下禁用**自动许可虚拟服务器**选项。

启用分析的过程已简化。您可以在单个工作流程中许可虚拟服务器并启用分析。

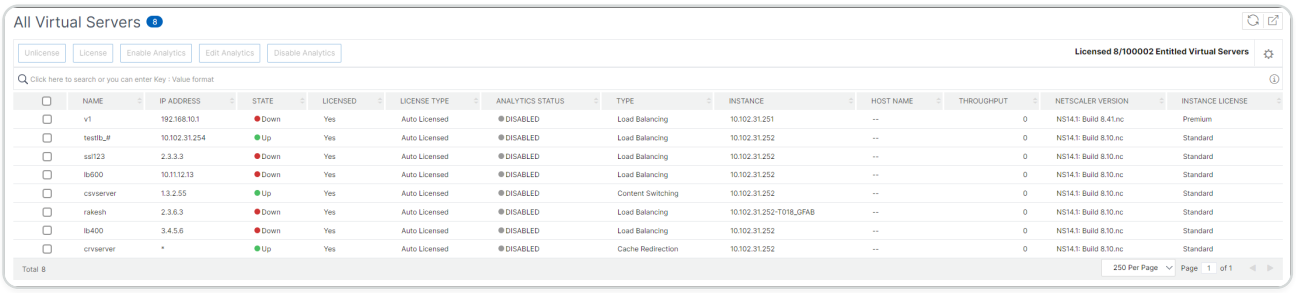
© 1997–2026 Citrix Systems, Inc. All rights reserved.

导航到**设置 > 许可与分析配置**以：

- 查看**虚拟服务器许可证摘要**
- 查看**虚拟服务器分析摘要**



当您单击**配置许可证**或**配置分析**时，将显示**所有虚拟服务器**页面。



在**所有虚拟服务器**页面上，您可以：

- 为未许可的虚拟服务器应用许可证
- 为已许可的虚拟服务器移除许可证
- 在已许可的虚拟服务器上启用分析
- 编辑分析
- 禁用分析

注意

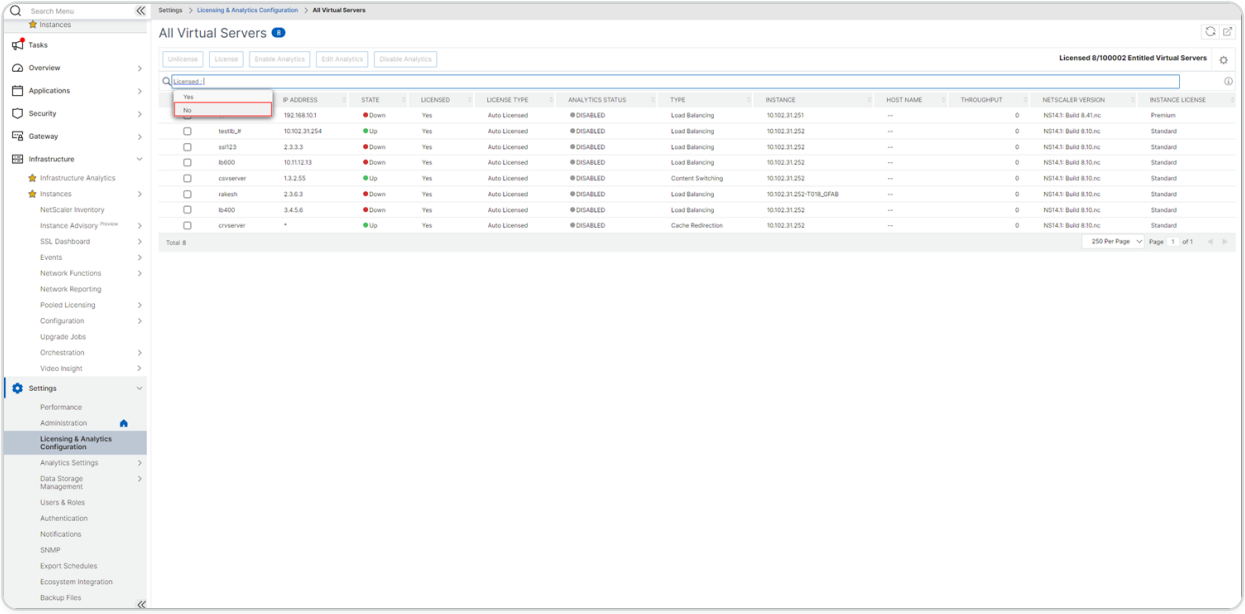
支持启用分析的虚拟服务器包括负载均衡、内容交换和 NetScaler Gateway。

管理虚拟服务器上的许可

要许可虚拟服务器，请在“**所有虚拟服务器**”页面中执行以下操作：

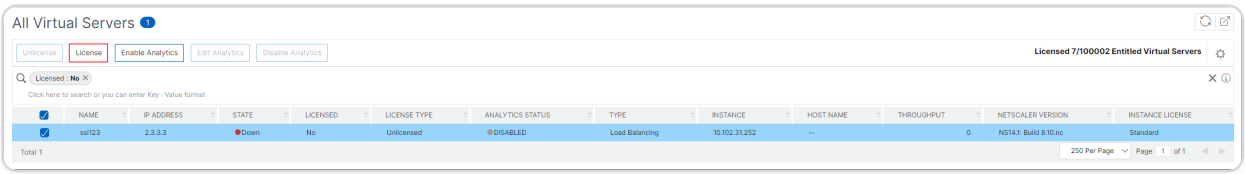
1. 单击搜索栏，选择“**已许可**”，然后选择“**否**”。

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



筛选器现已应用，仅显示未许可的虚拟服务器。

2. 选择虚拟服务器，然后单击“**许可**”。



要取消许可虚拟服务器，请在“**所有虚拟服务器**”页面中执行以下操作：

1. 单击搜索栏，选择“**已许可**”，然后选择“**是**”。
2. 选择虚拟服务器，然后单击“**取消许可**”。

启用分析

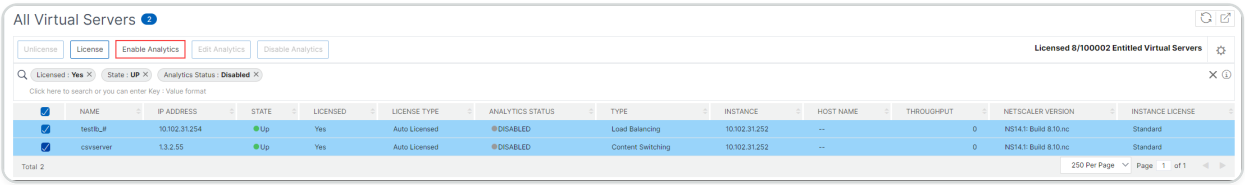
以下是为虚拟服务器启用分析的先决条件：

- 确保虚拟服务器已**获得许可**
- 确保分析状态为**已禁用**
- 确保虚拟服务器处于**UP**状态

您可以筛选结果以识别先决条件中提到的虚拟服务器。

1. 单击搜索栏并选择**状态**，然后选择**UP**。
2. 单击搜索栏并选择**已获得许可**，然后选择**是**。
3. 单击搜索栏并选择**分析状态**，然后选择**已禁用**。
4. 应用筛选器后，选择虚拟服务器，然后单击**启用分析**。

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



注意

或者，您可以为特定实例启用分析：

a. 导航到**基础架构 > 实例 > NetScaler**，然后选择实例类型。例如，VPX。

b. 选择实例，然后从**选择操作**列表中选择**配置分析**

c. 在“在虚拟服务器上配置分析”页面上，选择虚拟服务器，然后单击**启用分析**。

5. 在**启用分析**窗口中：

a. 选择洞察类型（Web Insight 或 WAF 安全违规）

b. 选择 **Logstream** 作为传输模式

注意

对于 NetScaler 12.0 或更早版本，**IPFIX** 是传输模式的默认选项。对于 NetScaler 12.0 或更高版本，您可以选择 **Logstream** 或 **IPFIX** 作为传输模式。

有关 IPFIX 和 Logstream 的更多信息，请参阅 Logstream 概述。

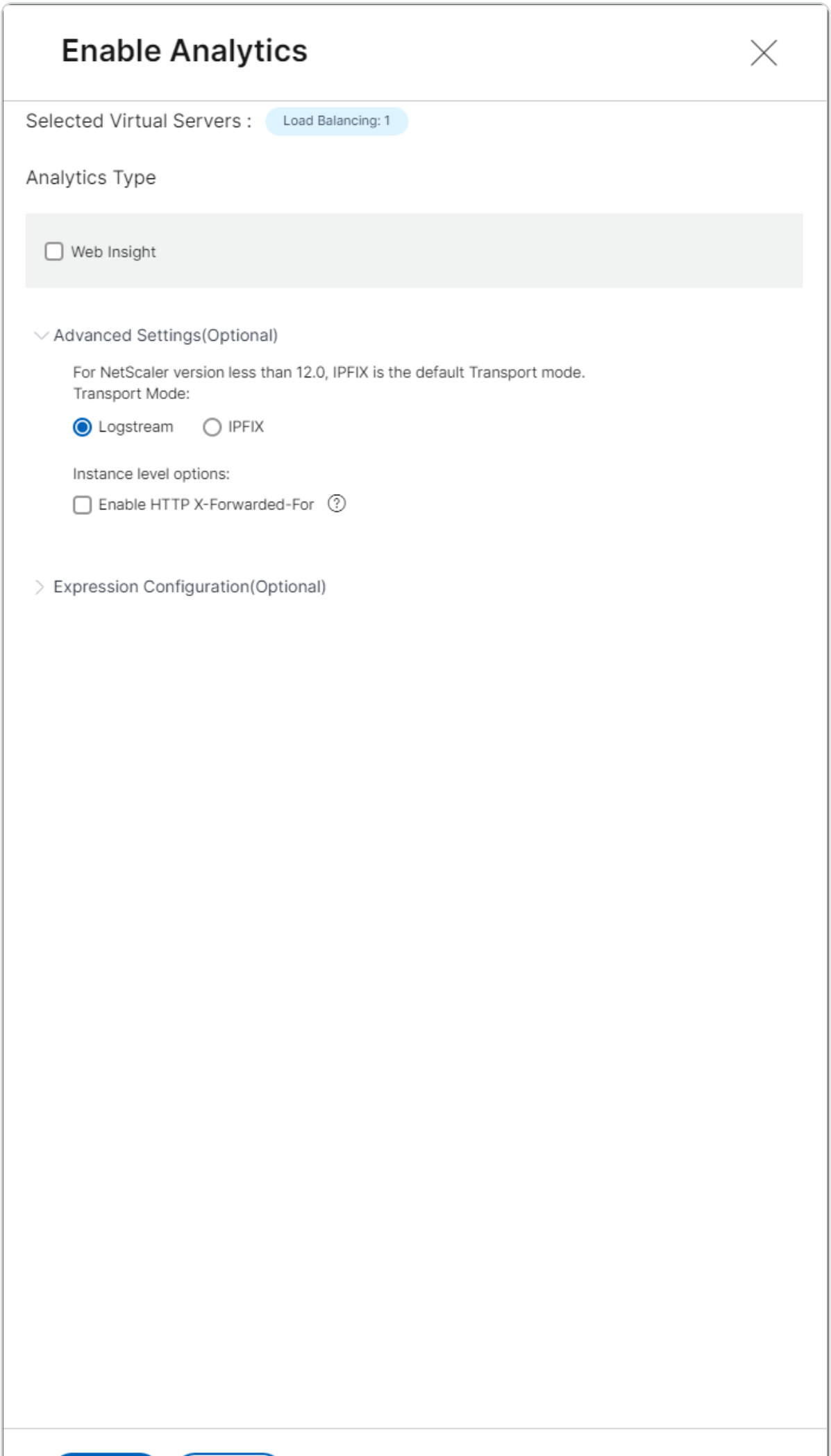
c. 在 **实例级别选项** 下：

- **启用 HTTP X-Forwarded-For** - 选择此选项可通过 HTTP 代理或负载均衡器识别客户端与应用程序之间连接的 IP 地址。
- **NetScaler Gateway** - 选择此选项可查看 NetScaler Gateway 的分析数据。

d. 表达式默认为 true

e. 单击 **确定**

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


Enable Analytics
Selected Virtual Servers :
Load Balancing: 1
Analytics Type
Web Insight
Advanced Settings(Optional)
For NetScaler version less than 12.0, IPFIX is the default Transport mode.
Transport Mode:
Logstream
IPFIX
Instance level options:
Enable HTTP X-Forwarded-For
Expression Configuration(Optional)

注意

- 如果您选择未获得许可的虚拟服务器，则 NetScaler Console 会首先许可这些虚拟服务器，然后启用分析功能
- 对于管理分区，仅支持 **Web Insight**
- 对于缓存重定向、身份验证和 GSLB 等虚拟服务器，您无法启用分析功能。将显示错误消息。

单击“**确定**”后，NetScaler Console 会处理以在选定的虚拟服务器上启用分析功能。

注意

NetScaler Console 对 Logstream 使用 NetScaler SNIP，对 IPFIX 使用 NSIP。如果在 NetScaler 代理和 NetScaler 实例之间启用了防火墙，请确保打开以下端口，以使 NetScaler Console 能够收集 AppFlow 流量：

传输模式	源 IP	类型	端口
IPFIX	NSIP	UDP	4739
日志流	SNIP	TCP	5557

编辑分析

要在虚拟服务器上编辑分析，请执行以下操作：

1. 选择虚拟服务器

   注意

   > 或者，您也可以编辑特定实例的分析：

   a. 导航到 **Infrastructure > Instances > NetScaler**，然后选择实例类型。例如，VPX。

   b. 选择实例，然后单击 **Edit Analytics**。

2. 单击 **编辑分析**
3. 在 **Edit Analytics Configuration** 窗口中编辑要应用的参数

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

4. 单击 **OK**。

禁用分析

要在选定的虚拟服务器上禁用分析，请执行以下操作：

1. 选择虚拟服务器
2. 单击 **禁用分析**

NetScaler Console 会禁用选定虚拟服务器上的分析

下表描述了 NetScaler Console 支持 IPFIX 和 Logstream 作为传输模式的功能：

功能	IPFIX	日志流
Web 洞察	•	•
WAF 安全违规	•	•
网关洞察	•	•
HDX 洞察	•	•
SSL 洞察	不支持	•
CR 洞察	•	•
IP 信誉	•	•
AppFirewall	•	•
客户端测量	•	•
Syslog/审计日志	•	•

全局配置分析功能

除了现有的启用分析功能流程外，您还可以使用单一面板工作流来配置以下分析功能：

- 所有现有的许可虚拟服务器
- 后续的许可虚拟服务器

配置后，此功能无需手动在现有和后续虚拟服务器上启用分析功能。

注意事项：

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

在配置分析功能之前，您必须了解 NetScaler Console 的以下行为：

- 首次配置此功能时，您必须确保满足本文档中提及的先决条件。
- 稍后修改分析设置。

  假设您首次配置分析设置时选择了 Web Insight、HDX™ Insight 和 Gateway Insight。如果您稍后想修改分析设置并取消选择 Gateway Insight，则这些更改不会影响已启用分析功能的虚拟服务器。
- 已启用分析功能的虚拟服务器。

  假设您有 10 个已授权的虚拟服务器，其中两个已启用分析功能。在这种情况下，此功能仅为剩余的八个虚拟服务器启用分析功能。
- 手动禁用分析功能的虚拟服务器。

  假设您有 10 个已授权的虚拟服务器，并且您已手动为其中两个虚拟服务器禁用了分析功能。在这种情况下，此功能仅为剩余的八个虚拟服务器启用分析功能，并跳过手动禁用分析功能的虚拟服务器。
- **Bot 安全违规**和 **WAF 安全违规**选项仅在高级授权的虚拟服务器中受支持。如果虚拟服务器未获得高级授权，则不会启用 **Bot 安全违规**和 **WAF 安全违规**。

先决条件

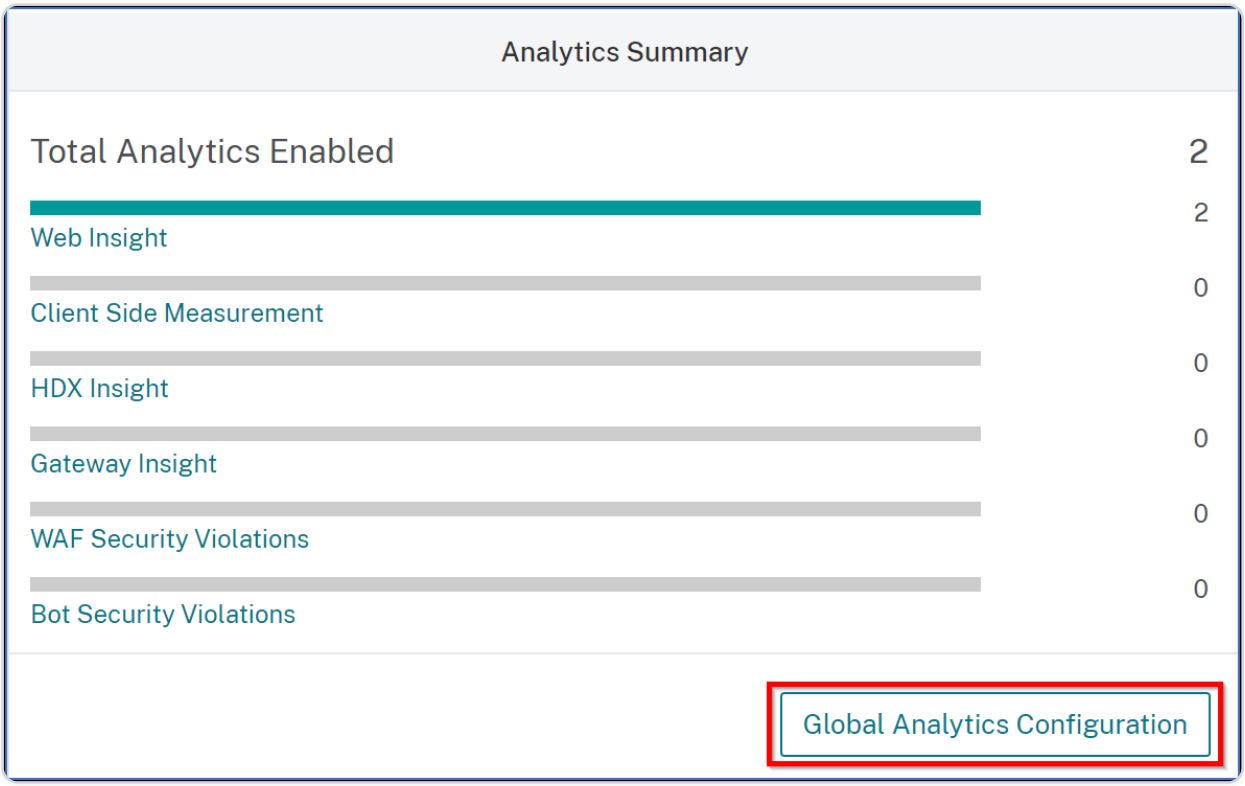
确保：

- 所有现有虚拟服务器均已获得授权。
- 启用自动授权选项以授权所有后续虚拟服务器。导航到 **设置 > 授权和分析配置**，然后在 **虚拟服务器许可证分配**下，打开 **自动授权虚拟服务器**选项。

启用分析

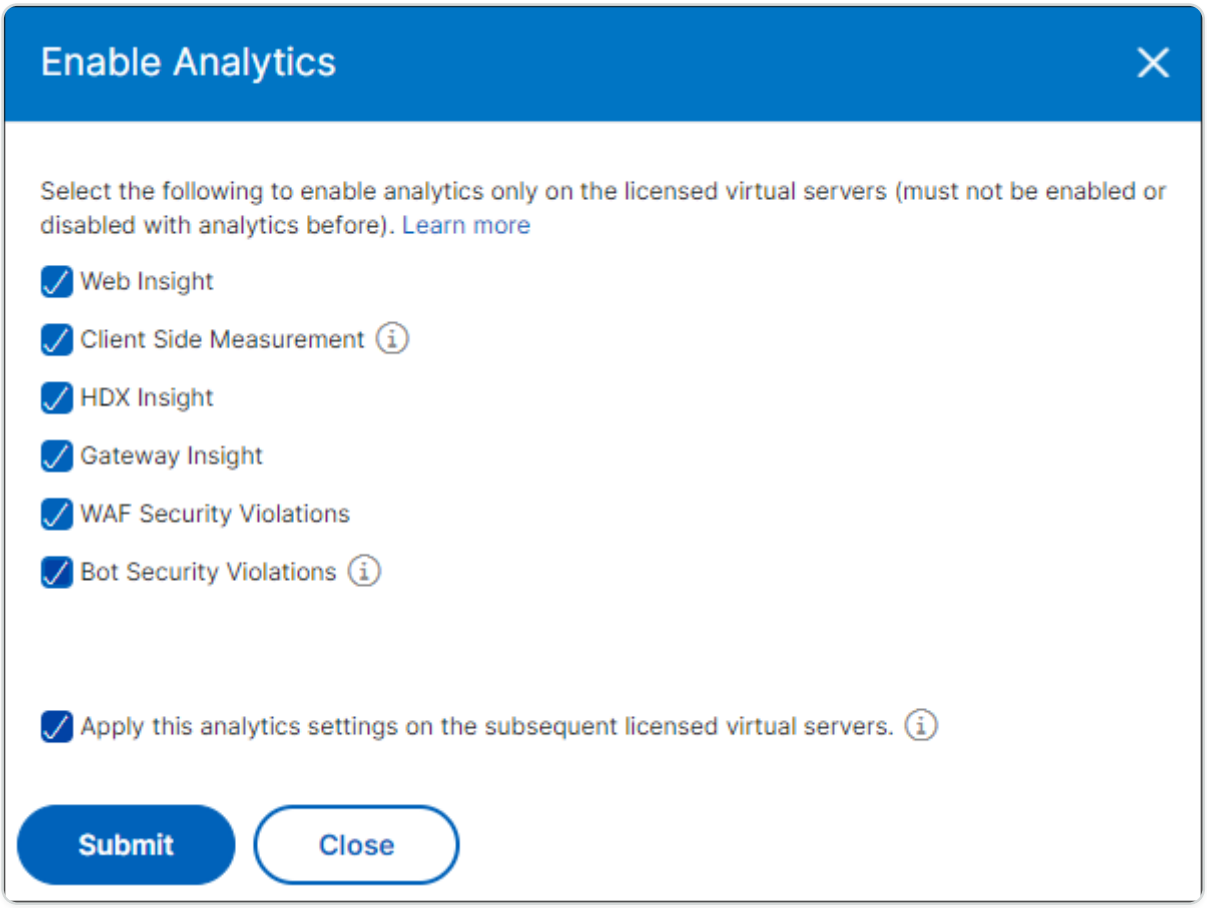
1. 导航到 **设置 > 授权和分析配置**。
2. 在 **分析摘要**下，单击 **全局分析配置**。

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



3. 选择您要在虚拟服务器上启用分析功能的分析功能。
4. 要在后续虚拟服务器上启用分析功能，请选中 **将此分析设置应用于后续授权的虚拟服务器**复选框。
5. 单击 **提交**。

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



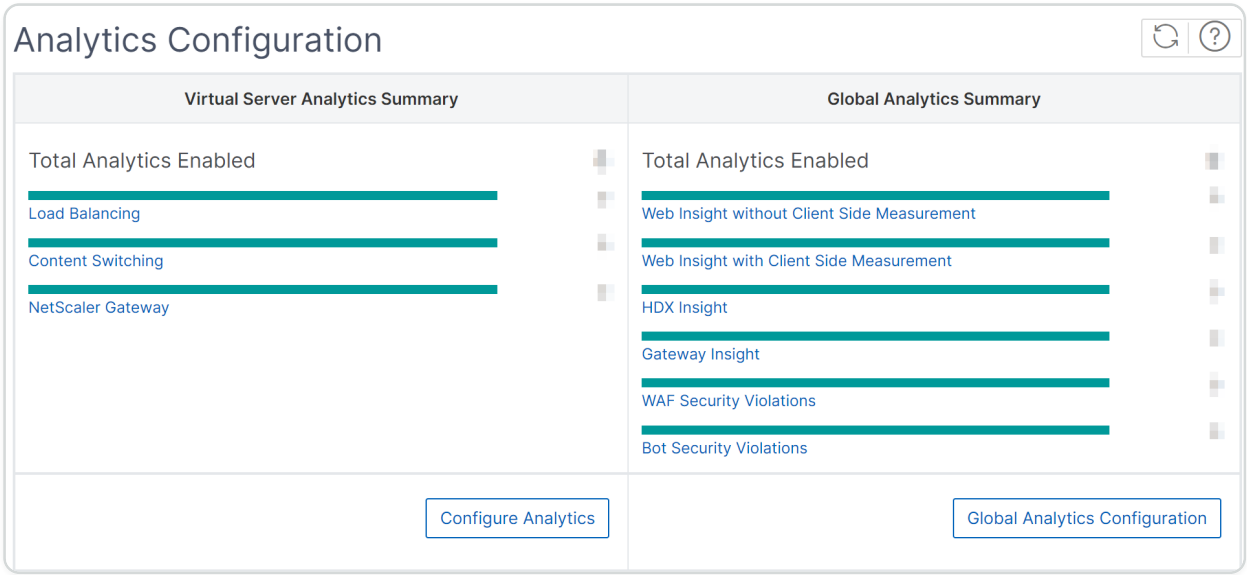
在虚拟服务器上配置分析

启用分析的先决条件是虚拟服务器必须获得许可。如果您使用弹性许可证，所有现有虚拟服务器和后续虚拟服务器都将自动获得许可。您可以继续配置分析。

您可以通过两种方式配置分析。导航到 **设置 > 分析配置** 以查看：

- **虚拟服务器分析摘要** - 使您能够在现有虚拟服务器上配置分析。
- **全局分析摘要** - 使您能够在现有和后续虚拟服务器上配置分析。

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



在现有虚拟服务器上配置分析

注意：

确保您要启用分析的虚拟服务器处于 **UP** 状态。

1. 在 **虚拟服务器分析摘要** 下，单击 **配置分析**。

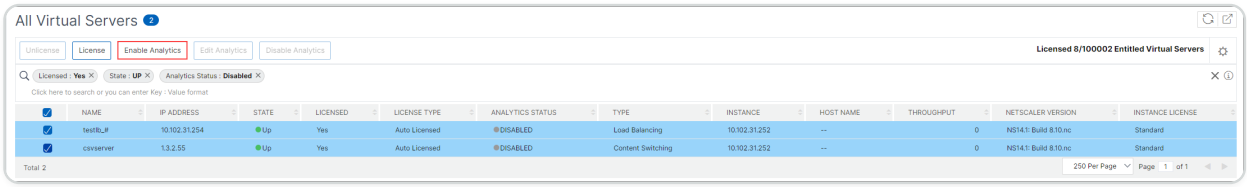
   将显示 **所有虚拟服务器** 页面。您可以：

   - 启用分析
   - 编辑分析
   - 禁用分析

   注意：

   支持启用分析的虚拟服务器包括负载平衡、内容切换和 NetScaler Gateway。

2. 选择虚拟服务器，然后单击**启用分析**。



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

注意

或者，您可以为实例启用分析：

a. 导航到**基础架构 > 实例 > NetScaler**，然后选择实例类型。例如，VPX。

b. 选择实例，然后从**选择操作**列表中选择**配置分析**

c. 在“在虚拟服务器上配置分析”页面上，选择虚拟服务器，然后单击**启用分析**。

3. 在**启用分析**窗口中：

a. 选择洞察类型。

b. 选择 **Logstream** 作为传输模式。

注意：

对于 NetScaler 12.0 或更早版本，**IPFIX** 是传输模式的默认选项。对于 NetScaler 12.0 或更高版本，您可以选择 **Logstream** 或 **IPFIX** 作为传输模式。

有关 IPFIX 和 Logstream 的更多信息，请参阅Logstream 概述。

c. 在**实例级别选项**下：

- **启用 HTTP X-Forwarded-For** - 选择此选项可通过 HTTP 代理或负载均衡器识别客户端与应用程序之间连接的 IP 地址。
- **自定义标头** - 定义自定义标头，例如 X-Real-IP、X-Client-IP 或任何其他自定义标头，以获取实际客户端 IP 地址而非代理 IP 地址。确保托管的 NetScaler 实例为 14.1–38.24 或更高版本。
- **NetScaler Gateway** - 选择此选项可查看 NetScaler Gateway 的分析数据。

d. 表达式默认为 true。

e. 单击“**确定**”。

注意：

- 对于管理分区，仅支持 **Web Insight**。
- 对于缓存重定向、身份验证和 GSLB 等虚拟服务器，您无法启用分析。系统将显示错误消息。

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

单击“**确定**”后，NetScaler Console 将处理以在选定的虚拟服务器上启用分析。

注意

NetScaler Console 将 NetScaler SNIP 用于 Logstream，将 NSIP 用于 IPFIX。如果在 NetScaler 代理和 NetScaler 实例之间启用了防火墙，请确保打开以下端口以使 NetScaler Console 能够收集 AppFlow 流量：

传输模式	源 IP	类型	端口
IPFIX	NSIP	UDP	4739
日志流	SNIP	TCP	5557

编辑分析

要在虚拟服务器上编辑分析，请执行以下操作：

1. 选择虚拟服务器。

   注意：

   或者，您也可以编辑实例的分析：

   a. 导航到 **Infrastructure > Instances > NetScaler**，然后选择实例类型。例如，VPX。
   b. 选择实例，然后单击 **Edit Analytics**。

2. 单击 **编辑分析**
3. 在 **编辑分析配置** 窗口中编辑您要应用的参数。
4. 单击 **确定**。

禁用分析

要在选定的虚拟服务器上禁用分析：

1. 选择虚拟服务器。
2. 单击 **禁用分析**。

NetScaler Console 禁用选定虚拟服务器上的分析。

下表描述了 NetScaler Console 支持 IPFIX 和 Logstream 作为传输模式的功能：

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

功能	IPFIX	日志流
Web 洞察	•	•
WAF 安全违规	•	•
网关洞察	•	•
HDX 洞察	•	•
SSL 洞察	不支持	•
CR 洞察	•	•
IP 信誉	•	•
AppFirewall	•	•
客户端测量	•	•
Syslog/审计日志	•	•

配置全局分析

您可以通过创建自定义策略或全局策略来启用全局分析。

注意：

- 您最多只能创建 10 个策略。这些策略可以是九个自定义策略和一个全局策略的组合，也可以是 10 个自定义策略。
- 如果您同时拥有自定义策略和全局策略，则这两个策略中选择的洞察将应用于虚拟服务器。如果您想删除任何洞察，则必须手动删除它们。

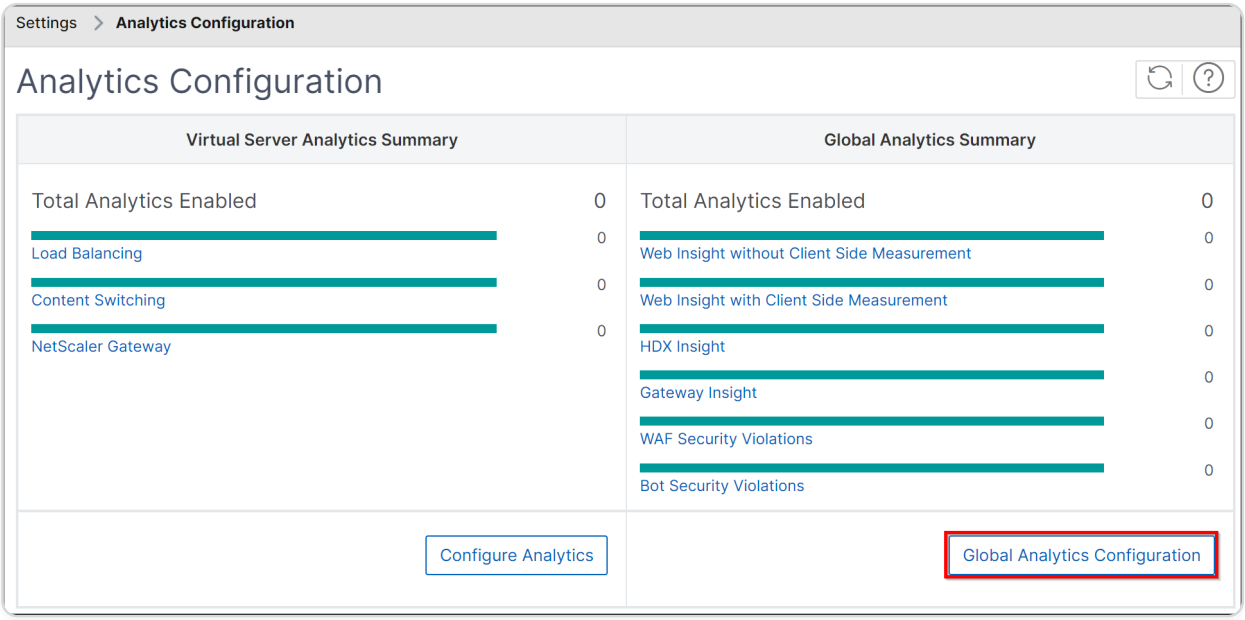
自定义策略

使用自定义策略，您可以控制只需要特定洞察的实例或虚拟服务器。您可能通过 NetScaler Console 中管理的各种 NetScaler 实例配置了数百个虚拟服务器。在某些情况下，您可能只想将选择性洞察（例如，Bot 安全违规和 WAF 安全违规）应用于部分虚拟服务器或实例。对于此类情况，您可以配置自定义策略，选择特定的分析功能，并将其应用于相关的实例和虚拟服务器。

要配置自定义策略：

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

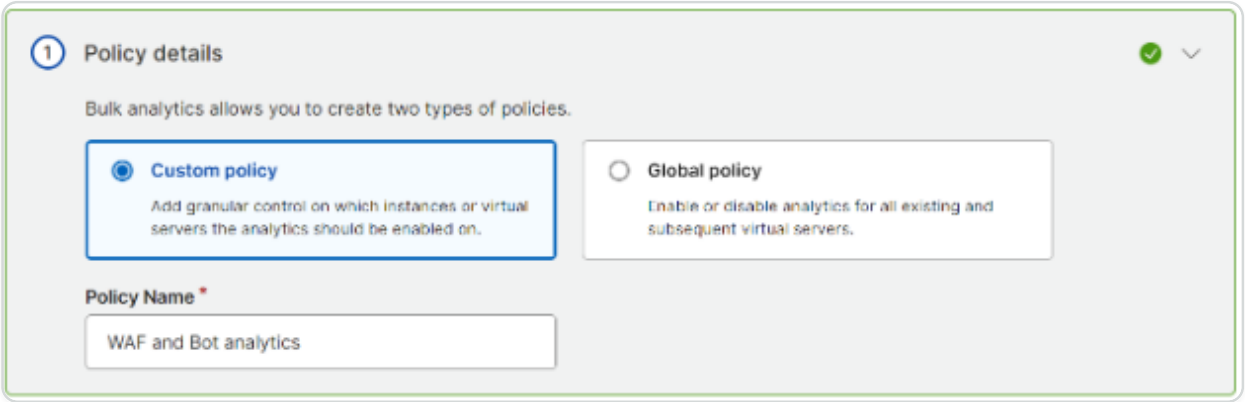
1. 在 **全局分析摘要** 下，单击 **全局分析配置**。



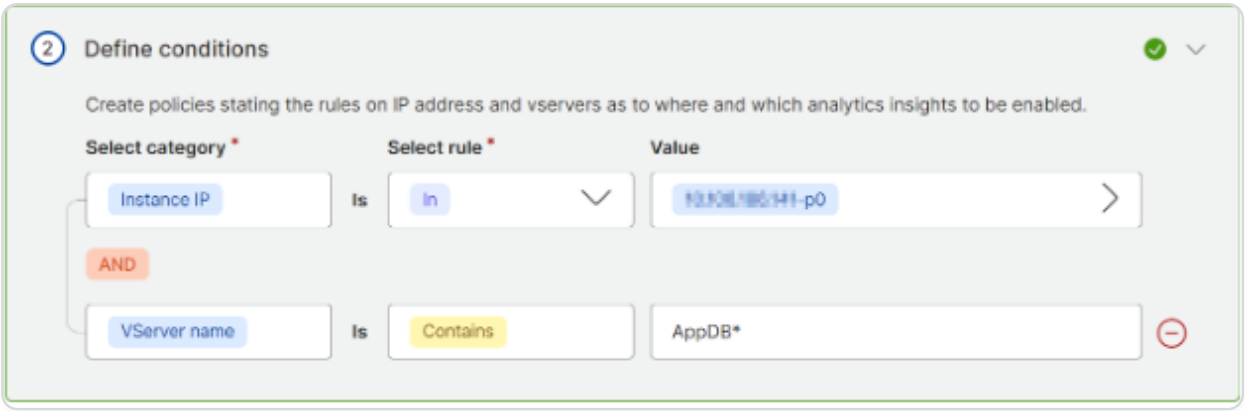
2. 在 **策略详细信息** 下，选择 **自定义策略** 并指定您选择的策略名称。

注意：

您以后无法编辑策略名称。



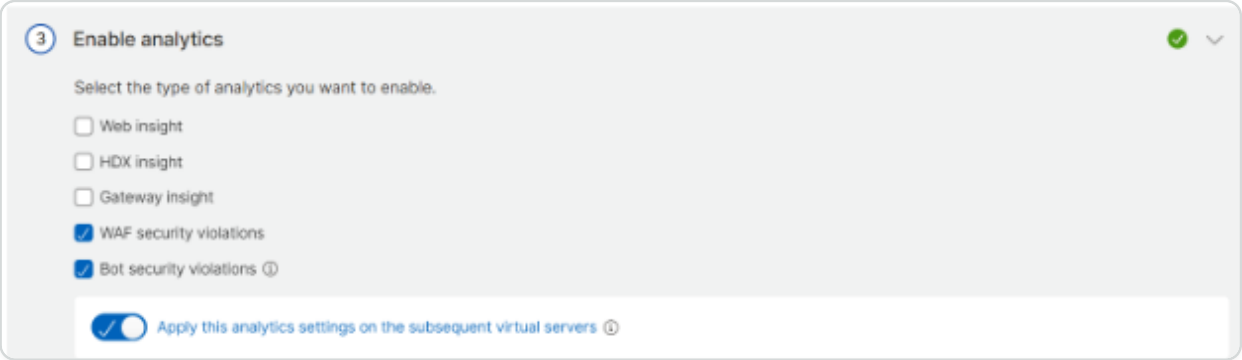
3. 在 **定义条件** 下，通过选择实例 IP 集或特定实例或虚拟服务器名称或两者来创建条件。



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

4. 在 **启用分析** 下，选择分析功能类型。

> **注意：**
>
> 如果您启用**将此分析设置应用于后续虚拟服务器**，则分析将根据定义的分析功能应用于后续虚拟服务器。



5. 单击**保存**。

注意事项：

- 如果您通过删除现有洞察并添加另一个洞察来修改策略，则更新后的策略将应用新的洞察。如果要删除任何洞察，必须手动删除已配置的洞察。

  假设您已创建包含 HDX 洞察和 Web 洞察的自定义策略。如果您更新策略以删除 HDX 洞察并添加 Bot 安全违规，则虚拟服务器/实例将更新为 HDX 洞察、Web 洞察和 Bot 安全违规。如果要删除 HDX 洞察，必须使用 编辑分析 选项手动删除。

- 如果您删除现有策略并通过添加相同的实例或虚拟服务器来创建另一个策略，则相同的逻辑也适用。

全局策略

使用全局策略，您可以在已发现的虚拟服务器和后续虚拟服务器上启用分析。要创建全局策略：

1. 在**全局分析摘要**下，单击**全局分析配置**。
2. 在**策略详细信息**下，选择**全局策略**。
3. 在**启用分析**下，选择分析功能类型。

> **注意：**
>
> 如果您启用**将此分析设置应用于后续虚拟服务器**，则分析将根据定义的类别应用于后续虚拟服务器。

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

4. 单击**保存**。

配置后，分析功能将在已发现和后续的虚拟服务器上启用。

注意事项

- 假设您首次通过选择 **Web Insight**、**HDX™ Insight** 和 **Gateway Insight** 配置了全局策略。如果您稍后再次更改分析设置并取消选择 **Gateway Insight**，则这些更改不会影响已启用分析功能的虚拟服务器。您必须手动从虚拟服务器中移除 Gateway Insight。
- 假设您有 10 个虚拟服务器，其中两个已使用“**配置分析**”选项启用了分析功能。在这种情况下，当您配置全局策略时，分析功能仅应用于剩余的八个虚拟服务器。
- 假设您有 10 个虚拟服务器，并且您已手动为其中两个虚拟服务器禁用了分析功能。在这种情况下，当您配置全局策略时，分析功能仅应用于剩余的八个虚拟服务器，并跳过已手动禁用分析功能的虚拟服务器。

迁移分析

从 **14.1-43.x** 版本开始，当您在虚拟服务器上启用分析功能时，分析功能将通过基于配置文件的配置应用。以前，分析功能是通过 AppFlow 策略配置的。基于配置文件的配置具有以下优点：

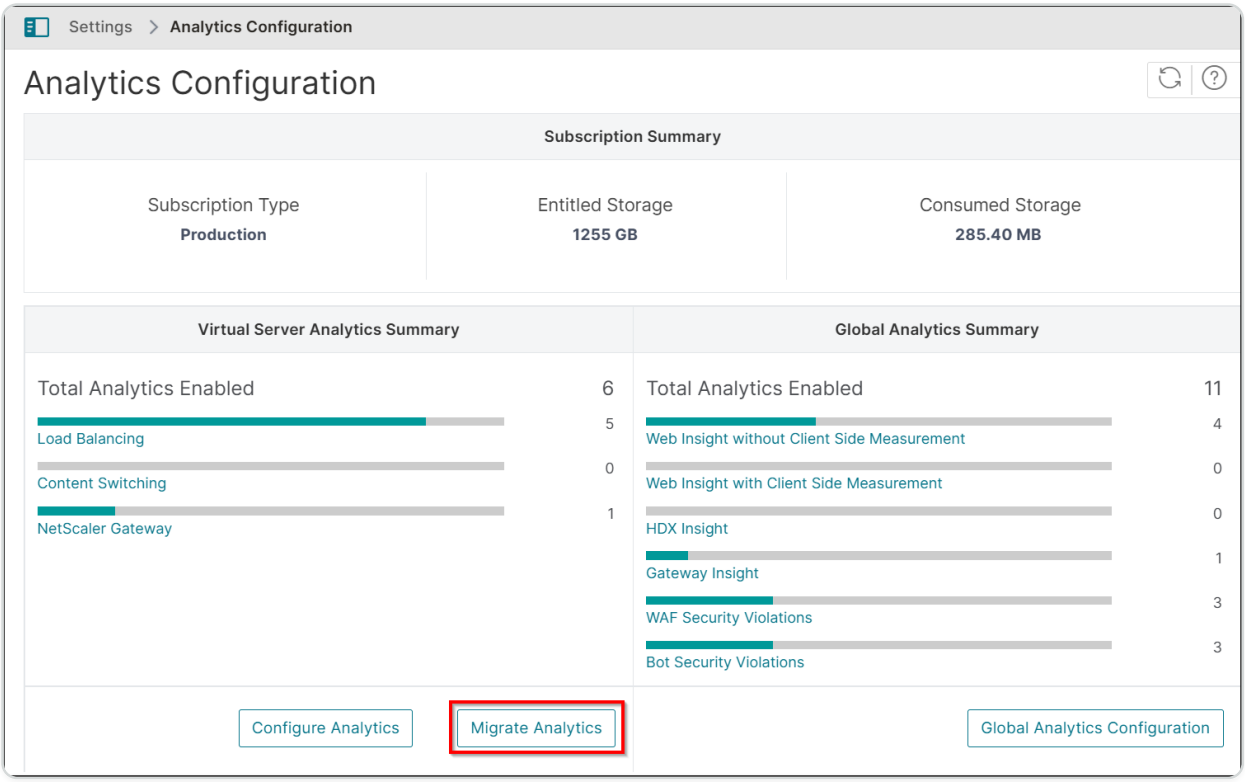
- 提高了性能和灵活性
- 更轻松的配置和管理

注意：

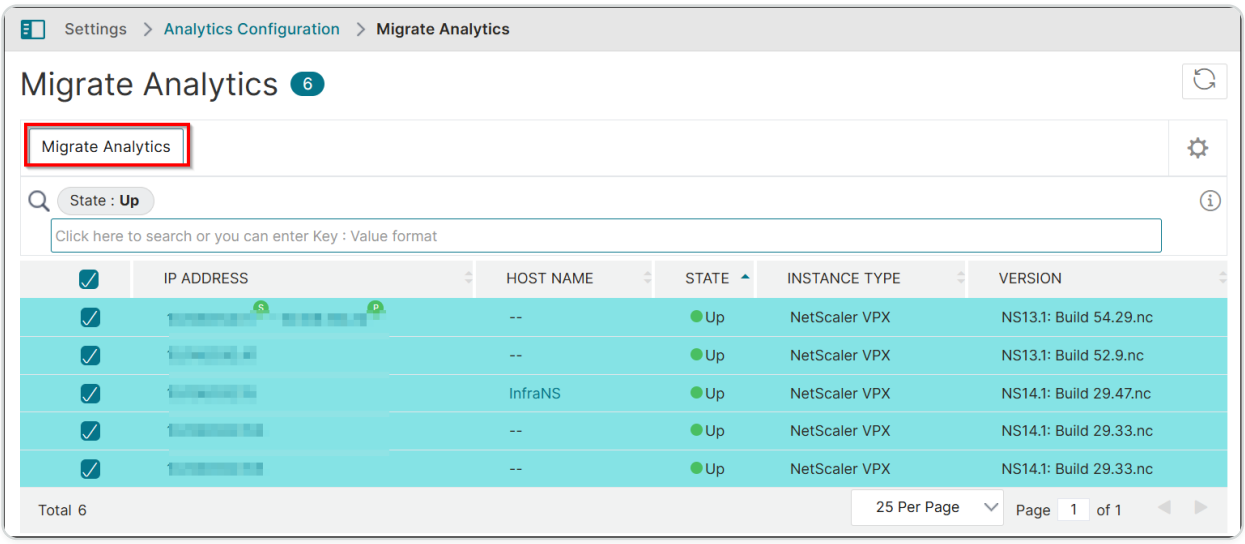
与分析配置相关的增强功能仅通过基于配置文件的配置支持。我们建议您将所有已启用分析功能的现有虚拟服务器迁移到基于配置文件的配置。

1. 导航到“**设置 > 分析配置**”，然后选择“**迁移分析**”。

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



2. 在“**迁移分析**”页面中，您可以查看通过 AppFlow® 策略配置了一个或多个虚拟服务器的实例。



出现一个确认窗口。点击 **是** 以完成迁移。

为托管的 NetScaler 实例分配网络配置文件

当您在 NetScaler Console 中为虚拟服务器启用分析或指标收集器时，来自 NetScaler 的 AppFlow 或指标数据将通过 NetScaler 子网 IP 地址 (SNIP) 导出到 NetScaler Console。在某些情况下，SNIP 可能会因网络中的防火墙而被阻止。在这种情况下，您可能需要使用与 SNIP 不同的 IP 地址。有关网络配置文件的更多信息，请参阅 为后端通信使用指定的源 IP。

您可以通过 NetScaler Console 为 NetScaler 实例分配网络配置文件，以便将 AppFlow 数据从 NetScaler 导出到 NetScaler Console。

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

先决条件

确保：

- NetScaler 实例版本为 **13.0-48.4 或更高版本**。
- 网络配置文件已在 NetScaler 实例中配置。

要在 NetScaler Console 中分配网络配置文件，请执行以下操作：

1. 导航到 **基础结构 > 实例 > NetScaler**。
2. 选择实例，然后从 **选择操作** 列表中：
   - 单击 **配置网络配置文件** 为 AppFlow 分配网络配置文件。
   - 单击 **为指标收集器配置网络配置文件** 为指标收集器分配网络配置文件。
3. 从列表中选择一个网络配置文件，然后单击 **应用**。

注意：

- 对于 AppFlow，请确保在为实例分配网络配置文件之前禁用所有虚拟服务器的分析功能。
- 对于 Metrics Collector，请确保在为实例分配网络配置文件之前，禁用所有虚拟服务器的指标。

配置 NTP 服务器

您可以在 NetScaler Console 中配置网络时间协议 (NTP) 服务器，以使其时钟与 NTP 服务器同步。配置 NTP 服务器可确保 NetScaler Console 时钟与网络上的其他服务器具有相同的日期和时间设置。

在 NetScaler Console 上配置 NTP 服务器：

1. 在 NetScaler Console GUI 中，导航到 **Settings（设置）> Administration（管理）**。在 **System Administration（系统管理）**页面上的 **Network Configurations（网络配置）**下，单击 **NTP Servers（NTP 服务器）**。然后单击 **Add（添加）**。
2. 在 **Create NTP Server（创建 NTP 服务器）**页面上，输入以下详细信息：
   - **Server Name/IP Address（服务器名称/IP 地址）** – 输入 NTP 服务器的域名或 IP 地址。添加 NTP 服务器后，名称或 IP 地址无法更改。

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

- **Minimum Poll Interval（最小轮询间隔）** – 指定传输的 NTP 消息之间的时间间隔的最小值，以 2 的幂次方秒为单位。例如，如果希望最小轮询间隔为 64 秒（可表示为 2\^6），则输入 6
- **Maximum Poll Interval（最大轮询间隔）** – 指定传输的 NTP 消息之间的时间间隔的最大值，以 2 的幂次方秒为单位。例如，如果希望最大轮询间隔为 256 秒（可表示为 2\^8），则输入 8。
- **Key Identifier（密钥标识符）** - 输入可用于与 NTP 服务器进行对称密钥身份验证的密钥标识符。如果选择 Autokey，请勿添加密钥标识符。要查找密钥标识符，请参阅 NTP 服务器的文档。
- **Autokey** - 如果要使用公钥身份验证与 NTP 服务器进行身份验证，请选择 **Autokey**。如果要添加密钥标识符，请勿选择此项。
- **Preferred（首选）** – 如果要将此 NTP 服务器指定为时钟同步的首选服务器，请选择此选项。这仅适用于配置了多个服务器的情况。

3. 单击 **Create（创建）**。

在 NetScaler Console 上启用 NTP 同步：

1. 导航到 **NTP Servers（NTP 服务器）**主页。
2. 单击 **NTP Synchronization（NTP 同步）**并选中 **Enable NTP Synchronization（启用 NTP 同步）**复选框。
3. 单击 **确定**。

   出现一个确认窗口以重新启动 NetScaler Console。单击 **是** 以继续。

配置系统设置

在开始使用 NetScaler Console 管理和监控实例和应用程序之前，建议您配置一些系统设置，以确保 NetScaler Console 服务器的最佳性能。

配置系统警报

配置系统警报以确保您了解任何严重或主要系统问题。例如，您可能希望在 CPU 使用率高或服务器多次登录失败时收到通知。对于某些警报类别，例如 cpuUsageHigh 或 memoryUsageHigh，您可以设置阈值并为每个类别定义严重性（例如“严重”或“主要”）。对于某些类别，例如 inventoryFailed 或 loginFailure，您只能定义严重性。当警报类别（例如 memoryUsageHigh）的阈值被突破或发生与警报类别（例如 loginFailure）对应的事件时，系统会记录一条消息，您可以将该消息视为 syslog 消息进行查看。

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

配置系统警报：

1. 导航到 **Settings > SNMP**（设置 > SNMP），然后单击右上角的 **Alarms**（警报）选项卡。
2. 选择要配置的警报，然后单击 **Edit**（编辑）。
3. 在 **Configure Alarm**（配置警报）页面上，选择警报严重性，然后设置阈值。
4. 要查看已突破阈值或已发生事件的警报，请导航到 **Settings > Auditing**（设置 > 审计），然后单击 **Syslog Messages**（Syslog 消息）。

配置系统通知

您可以向选定的用户组发送各种系统相关功能的通知。您可以在 NetScaler Console 中设置通知服务器，并且可以配置电子邮件和短消息服务 (SMS) 网关服务器，以向用户发送电子邮件和文本通知。设置通知可确保您收到任何系统级活动的通知，例如用户登录或系统重启。

配置系统通知：

1. 导航到 **Settings > Administration**（设置 > 管理）。在 **System Administration**（系统管理）页面中，在 **Event Notifications**（事件通知）下，单击 **Configure Event Notification and Digest > Event Notification**（配置事件通知和摘要 > 事件通知）。
2. 在 **Configure System Notification Settings**（配置系统通知设置）页面上，选择 NetScaler Console 生成的事件类别或类别。
3. 然后，配置电子邮件服务器或 SMS 服务器，以通过电子邮件、SMS 或两者接收通知。

配置系统备份设置

NetScaler Console 每天 00:30 自动备份系统。默认情况下，它保存三个备份文件。您可能希望保留更多系统备份。您还可以加密备份文件。您还可以选择将备份保存到外部服务器。

配置系统备份设置：

1. 导航到 **设置 > 管理**。
2. 在 **备份** 下，单击 **配置系统和实例备份**。
3. 单击 **系统**，然后在 **配置系统备份设置** 页面上，指定所需值。

配置实例备份设置

如果您备份 NetScaler 实例的当前状态，则可以在实例变得不稳定时使用备份文件来恢复稳定性。在执行升级之前，这样做尤其重要。默认情况下，每 12 小时进行一次备份，并在系统中保留三个备份文件。

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

配置实例备份设置：

1. 导航到 **设置 > 管理**。
2. 在 **备份** 下，单击 **配置系统和实例备份**。
3. 在 **配置实例备份设置** 下，单击 **实例**，并指定所需值。

启用基本身份验证

必须临时启用基本身份验证以：

- 完成代理和灾难恢复节点的初始注册。
- 从 NetScaler GUI 启动许可证激活系统 (LAS) 结账。

注意：

仅在初始注册时需要基本身份验证。

配置基本身份验证

1. 导航到 **设置 > 管理 > 系统配置 > 系统、时区、允许的 URL 和代理设置**。
2. 单击 **基本设置**。
3. 选择 **启用允许基本身份验证**。
4. 单击 **确定**。

启用或禁用 NetScaler Console 功能

作为管理员，您可以在 **设置 > 管理 > 可配置功能** 页面中启用或禁用以下功能：

- **代理故障转移** - 代理故障转移可能发生在具有两个或更多活动代理的站点上。当站点中的代理变为非活动状态（DOWN 状态）时，NetScaler Console 服务会将非活动代理的 NetScaler 实例重新分配给其他活动代理。有关详细信息，请参阅为多站点部署配置本地代理。
- **实体轮询网络功能** - 实体是附加到 NetScaler 实例的策略、虚拟服务器、服务或操作。默认情况下，NetScaler Console 每 60 分钟自动轮询一次配置的网络功能实体。有关详细信息，请参阅轮询概述。
- **实例备份** - 备份 NetScaler 实例的当前状态，然后使用备份文件将 NetScaler 实例恢复到相同状态。有关详细信息，请参阅备份和恢复 NetScaler 实例。
- **实例配置审计** - 监视托管 NetScaler 实例的配置更改，排查配置错误，并恢复未保存的配置。

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

- **实例事件** - 事件表示托管 NetScaler 实例上发生的事件或错误。NetScaler Console 中收到的事件显示在 **事件摘要** 页面（**基础架构 > 事件**）上，所有活动事件显示在事件消息页面（**基础架构 > 事件 > 事件消息**）中。有关详细信息，请参阅事件。
- **实例网络报告** - 您可以在全局级别为实例生成报告。此外，还可以为虚拟服务器和网络接口等实体生成报告。有关详细信息，请参阅网络报告。
- **实例 SSL 证书** - NetScaler Console 提供所有托管 NetScaler 实例上安装的 SSL 证书的集中视图。有关详细信息，请参阅SSL 控制板。
- **实例 Syslog** - 如果您已将设备配置为将所有 syslog 消息重定向到 NetScaler Console，则可以监视 NetScaler 实例上生成的 syslog 事件。

要启用某个功能，请执行以下步骤：

1. 从列表中选择要启用的功能。
2. 单击“**启用**”。

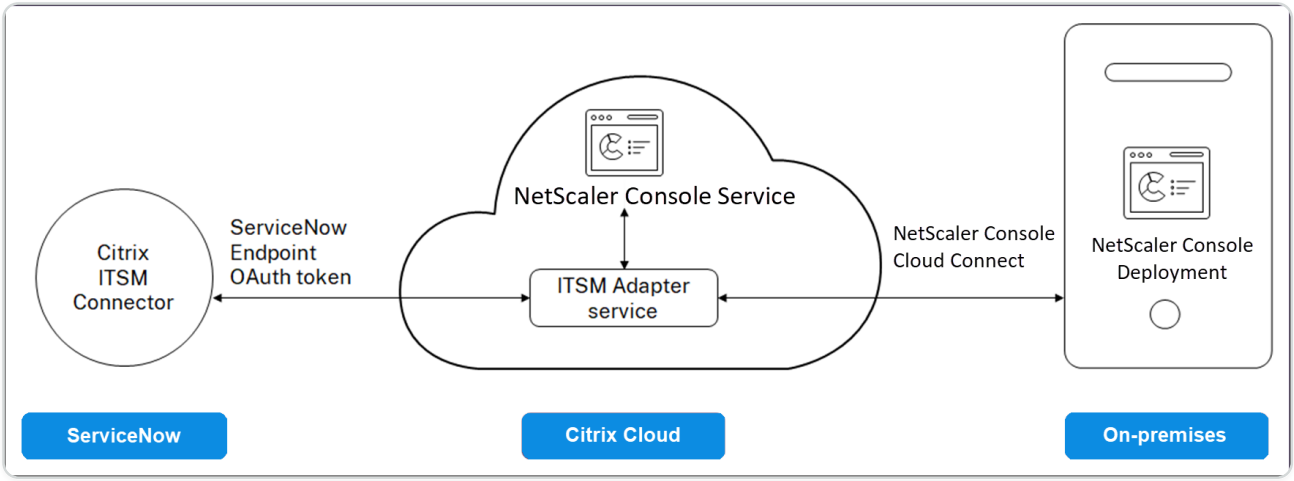
重要提示

如果某个功能被禁用，用户将无法执行与该功能相关的操作。

将 NetScaler Console 与 ServiceNow 实例集成

当您想要为 NetScaler 和 NetScaler Console 事件启用 ServiceNow 通知时，请将 NetScaler Console 与 ServiceNow 实例集成。此集成使用 Citrix ITSM 连接器在 NetScaler Console 和 ServiceNow 实例之间进行通信。

NetScaler Console 与 ServiceNow 的集成使用 ITSM Adapter 服务进行基于令牌的身份验证。为此，它会在 ServiceNow 中创建一个端点实例。有关更多信息，请参阅 ITSM Adapter 的工作原理。



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

要将您的 NetScaler Console 本地部署与 ITSM 适配器连接，请确保您已配置 Cloud Connect。有关更多信息，请参阅 Cloud Connect。

对于 NetScaler Console 版本 14.1-4.x 或更早版本与 ServiceNow 的集成，请务必配置客户身份。有关更多信息，请参阅 配置客户身份。

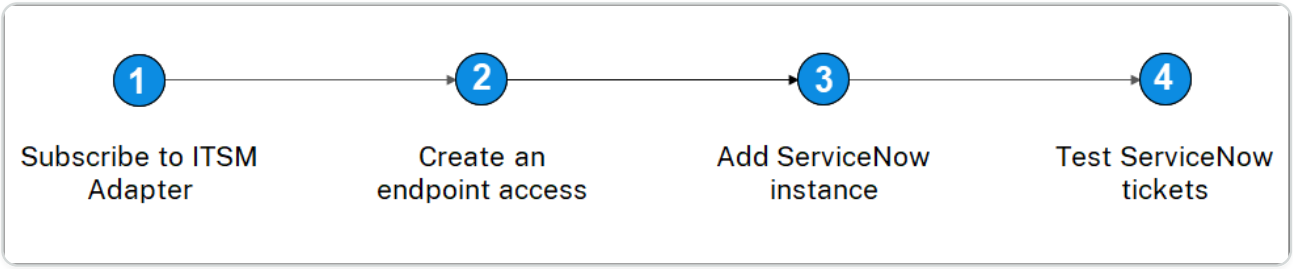
先决条件

在将 NetScaler Console 与 ServiceNow 集成之前，请确保以下事项：

1. 注册 Citrix Cloud。确保您有权管理 Citrix Cloud 管理员。有关更多信息，请参阅 管理 Citrix Cloud 管理员。

如何将 NetScaler Console 与 ServiceNow 集成?

执行以下步骤，使用 ITSM 连接器将 NetScaler Console 与 ServiceNow 集成：

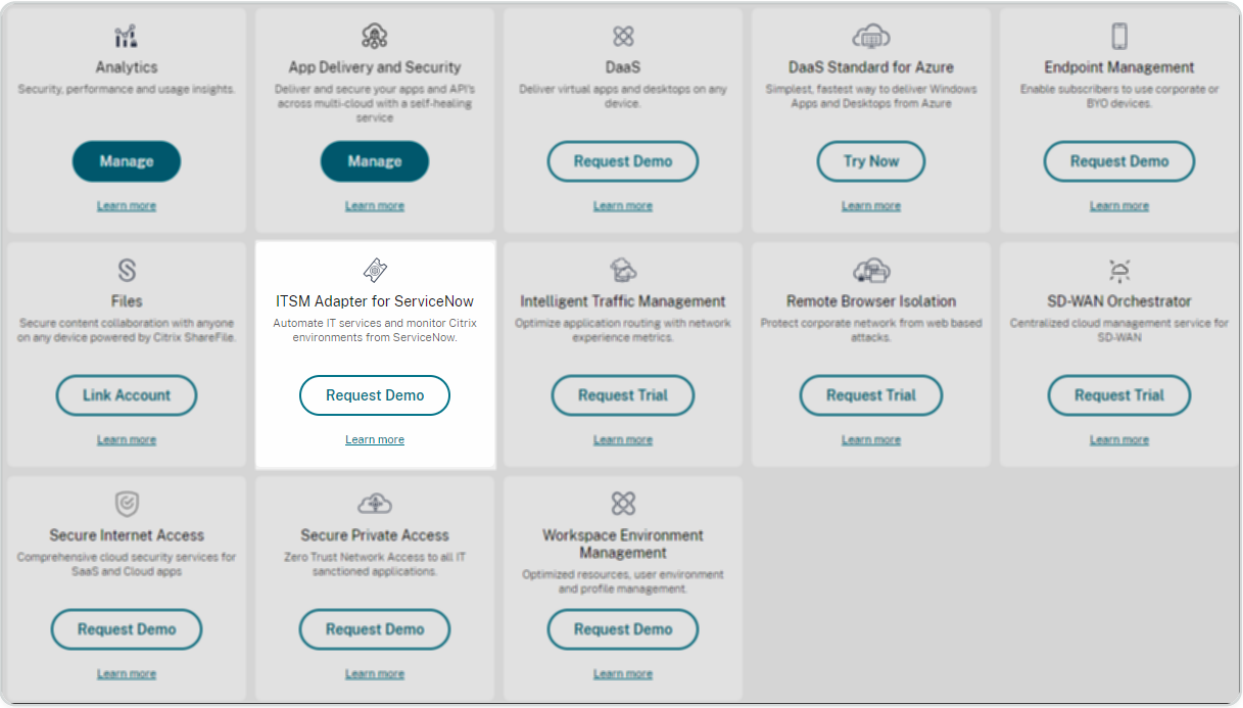


1. 订阅 Citrix Cloud™ 中的 ITSM Adapter 服务。
2. 在 ServiceNow 实例中创建端点访问。
3. 添加 ServiceNow 实例。
4. 在 NetScaler Console 中测试 ServiceNow 票证的自动生成(#step-4---test-auto-generation-of-servicenow-tickets-in-adm)。

步骤 1 - 在 Citrix Cloud 中订阅 ITSM Adapter 服务

1. 在 **ITSM Adapter** 磁贴上，单击 **Request Trial**。

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

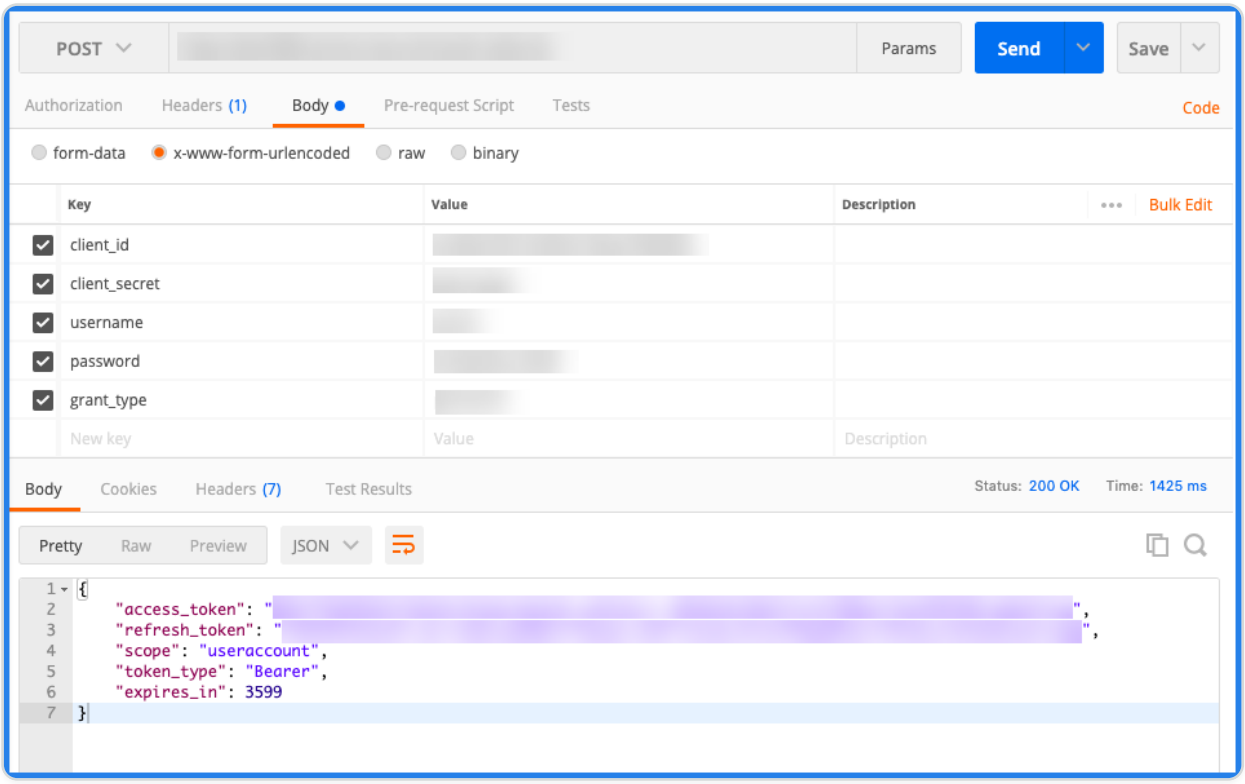


2. 导航到 **身份访问和管理** > **API 访问**，并记下 **客户端 ID** 和 **客户端密钥** 信息。

步骤 2 - 在 ServiceNow 实例中创建端点访问

1. 使用管理员凭据登录到您的 ServiceNow 实例。
2. 转到 ServiceNow 商店。下载并安装 **Citrix ITSM connector**。
3. 在 **Citrix ITSM Connector** 窗格上，选择 **Home**，然后单击 **Authenticate**。键入您从 Citrix Cloud 中记下的客户端 ID 和密钥。
4. 测试连接。
5. 保存配置。ServiceNow 会显示一条确认消息，指示连接处于活动状态。
6. 创建端点以访问 ServiceNow 实例。请参阅 为客户端创建访问实例的端点。
7. 使用客户端 ID 和客户端密钥获取访问令牌和刷新令牌。请参阅 OAuth 令牌。

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



步骤 3 - 添加 ServiceNow 实例

1. 在“**管理**”选项卡中，选择“添加 ServiceNow 实例”。
2. 指定“**实例名称**”、“**客户端 ID**”、“**客户端密钥**”、“**刷新令牌**”和“**访问令牌**”。
3. 单击“**测试**”。

   在 ITSM 适配器上注册 ServiceNow 实例(/en-us/netscaler-application-delivery-management-software/media/register-servicenow-itsm-instance.png)

   ServiceNow 实例现已连接到 ITSM 适配器服务。
4. 成功测试连接后，单击“**保存**”以添加 ServiceNow 实例。

步骤 4 - 在 NetScaler Console 中测试 ServiceNow 票证的自动生成

1. 登录到 NetScaler Console。
2. 导航到“**帐户 > 通知**”，然后选择“**ServiceNow**”。
3. 从列表中选择 ServiceNow 配置文件。
4. 单击“**测试**”以自动生成 ServiceNow 票证并验证配置。

   如果要在 NetScaler Console GUI 中查看 ServiceNow 票证，请选择“**ServiceNow 票证**”。

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

在 NetScaler Console 中设置 ServiceNow 通知

在 ITSM 适配器上注册 ServiceNow 实例后，您可以在 NetScaler Console GUI 中为以下事件设置 ServiceNow 通知：

重要

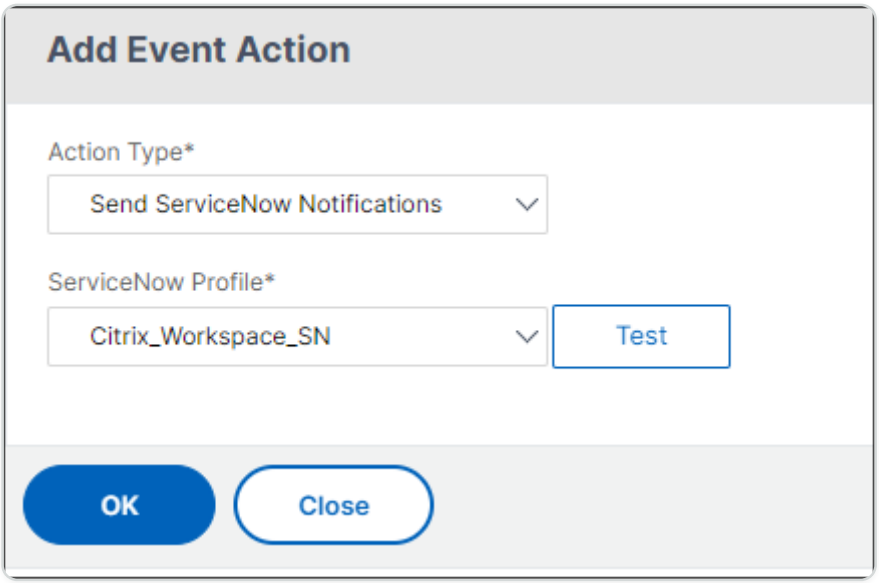
此功能在 ServiceNow Cloud 上受支持。

- **NetScaler 事件**：NetScaler Console 可以为选定托管 NetScaler 实例中的选定 NetScaler 事件生成 ServiceNow 事件。

  要为托管实例中的 NetScaler 事件发送 ServiceNow 通知，您必须配置事件规则并将规则操作指定为 **发送 ServiceNow 通知**。

  通过导航到 **基础架构 > 事件 > 规则** 在 NetScaler Console 上创建事件规则。有关更多信息，请参阅发送 ServiceNow 通知。

- **应用程序分析**：NetScaler Console 可以为超出指定阈值的应用程序生成 ServiceNow 事件。



  在此示例中，当应用程序的应用程序分数低于 90 时，将生成 ServiceNow 事件。

- **SSL 证书和 NetScaler Console 许可证事件**：NetScaler Console 可以为 SSL 证书过期和 NetScaler Console 许可证过期事件生成 ServiceNow 事件。

  要发送 SSL 证书过期通知，请参阅SSL 证书过期。

  要发送 NetScaler Console 许可证过期通知，请参阅NetScaler Console 许可证过期。

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

导出或计划导出报告

在 NetScaler Console 中，您可以导出针对所选 NetScaler Console 功能的全面报告。此报告为您提供了实例、分区和相应详细信息之间的映射关系概述。

NetScaler Console 在各个 NetScaler Console 功能下显示特定功能的计划导出报告，您可以查看、编辑或删除这些报告。例如，要查看 NetScaler 实例的导出报告，请导航到 **Network > Instances > NetScaler** 并单击导出图标。您可以将这些报告导出为 PDF、JPEG、PNG 和 CSV 文件格式。

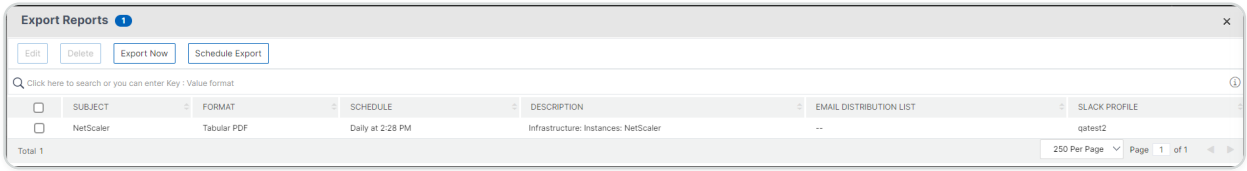
在“**导出报告**”中，您可以执行以下操作：

- 将报告导出到本地计算机
- 计划导出报告
- 查看、编辑或删除计划的导出报告

导出报告

要将报告从 NetScaler Console 导出到本地计算机，请执行以下步骤：

1. 单击页面右上角的导出图标。
2. 选择“**立即导出**”。
3. 选择以下导出选项之一：
   - **快照** - 此选项将 NetScaler Console 报告导出为快照。
   - **表格** - 此选项以表格格式导出 NetScaler Console 报告。您还可以选择以表格格式导出多少数据记录



4. 选择您要将报告保存到本地计算机的文件格式。
5. 单击“**导出**”。

计划导出报告

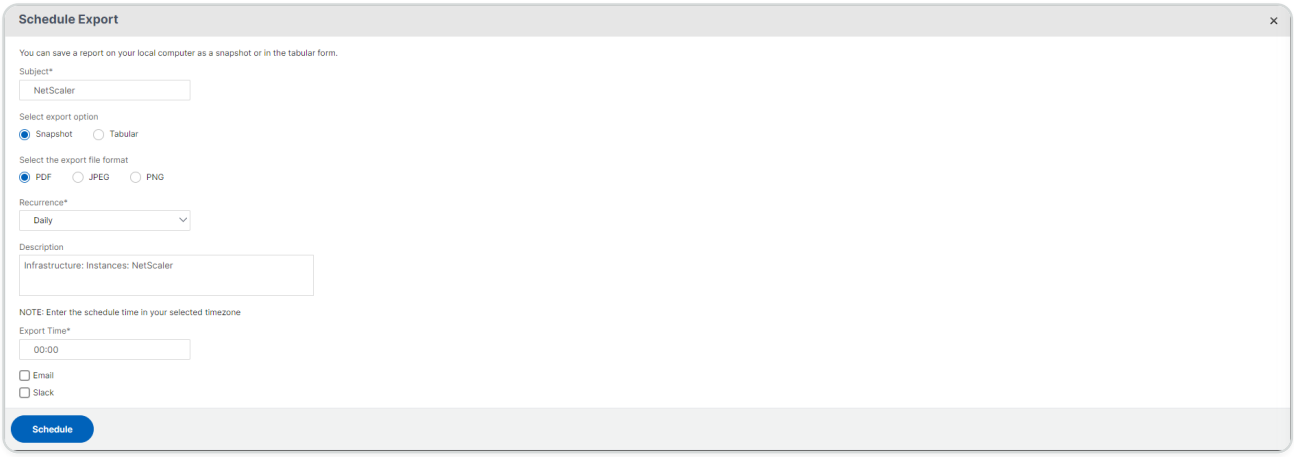
要定期计划导出报告，请指定重复间隔。NetScaler Console 会将导出的报告发送到配置的电子邮件或 Slack 配置文件。

1. 单击页面右上角的导出图标。
2. 选择“**计划导出**”并指定以下内容：

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

- “**主题**” - 默认情况下，此字段会自动填充所选功能名称。但是，您可以将其重写为有意义的标题。
- “**导出选项**” - 以快照或表格格式导出 NetScaler Console 报告。您还可以选择以表格格式导出多少数据记录。
- “**格式**” - 选择您希望在配置的电子邮件或 Slack 配置文件上接收报告的文件格式。
- “**重复**” - 从列表中选择“**每日**”、“**每周**”或“**每月**”。
- “**描述**” - 为报告指定有意义的描述。
- “**导出时间**” - 指定您希望导出报告的时间。
- “**电子邮件**” - 选中此复选框并从列表框中选择配置文件。如果要添加配置文件，请单击“**添加**”。
- “**Slack**” - 选中此复选框并从列表框中选择配置文件。如果要添加配置文件，请单击“**添加**”。

3. 单击“**计划**”。



查看和编辑计划导出的报告

要查看导出报告，请执行以下操作：

1. 单击页面右上角的导出图标。

   “**导出报告**”页面显示所有特定于功能的导出报告。

2. 选择要编辑的报告，然后单击**编辑**。

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

升级

每个 NetScaler Console 版本都提供新增和更新的功能，并增强了功能。建议您将 NetScaler Console 升级到最新版本，以利用新功能和错误修复。每个版本发布时，发行说明 中都包含增强功能、已知问题和错误修复的完整列表。在开始升级之前，了解许可框架和可使用的许可证类型也很重要。有关 NetScaler Console 许可信息，请参阅 许可。

升级前

从 NetScaler Console 下载页面下载升级包，并按照本文中的说明将系统升级到最新的 14.1 版本。升级过程开始后，NetScaler Console 将重新启动，现有连接将终止并在升级完成后重新连接。现有配置将保留，但 NetScaler Console 在升级完成之前不会处理任何数据。

重要

NetScaler Console 的版本和内部版本号应**等于或高于**您的 NetScaler 版本和内部版本号。例如，如果您已安装 NetScaler Console 12.1 Build 50.39，请确保您已安装 NetScaler 12.1 Build 50.28/50.31 或更早版本。

升级到 14.1 之前需要注意的事项：

- 如果您从版本 11.1 或版本 12.0 56.x 及更早版本升级，请执行以下步骤：
  a. 从现有版本升级到 12.0 build 57.24。
  b. 升级到版本 12.1 的最新内部版本。
  c. 升级到版本 13.1。
  d. 升级到版本 14.1。
- 如果您从 12.0 build 57.24 及更高版本升级，请首先升级到 12.1，然后升级到 13.1，最后升级到 14.1。
- 如果您从 12.1 升级，则必须首先升级到 13.0 64.xx，然后直接升级到 14.1
- 如果您从低于 13.0 64.xx 的版本升级，为了获得更好的用户体验，请首先升级到 13.0 64.xx，然后升级到 14.1。
- 要从版本 13.1 升级到版本 14.1，请首先升级到版本 13.1 的最新版本，然后再升级到版本 14.1。

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

- 成功升级到 14.1 并登录 GUI 后，如果您使用的是默认密码，系统会建议您更改密码。

升级到 14.1-xx.xx 及更高版本之前需要注意的重要事项

将 NetScaler Console 升级到版本 14.1-xx.xx 时，您的 NetScaler Console 数据库也会迁移。发生此数据迁移是因为 NetScaler Console 现在使用 PostgreSQL 10.11 版。

注意：

不支持降级 NetScaler Console。请勿尝试降级。

建议的预防措施：

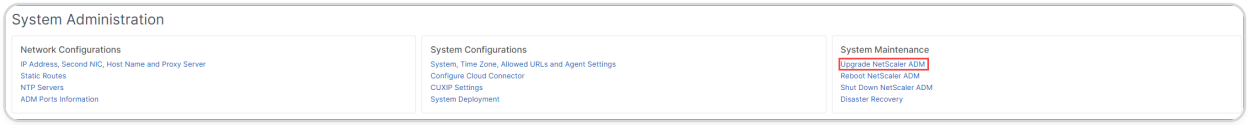
- 如果您要升级到 14.1-xx.xx 及更高版本，请为每次升级拍摄 NetScaler Console 服务器的快照。
- 升级前备份 NetScaler Console 服务器。
- 升级后，您可能需要重新建立 NetScaler Console 服务器与托管实例之间的连接。确认提示会警告您，如果继续操作，连接可能会失败。
- 对于高可用性设置中的 NetScaler Console 服务器，升级时请勿对任一节点进行任何配置更改。

警告：

在升级过程成功完成之前，请勿刷新浏览器。请查看 GUI 以了解升级完成的大致时间。

将单个 NetScaler Console 服务器升级到 14.1-xx.xx

1. 使用管理员凭据登录 NetScaler Console。
2. 导航到 **设置** \> **管理**。在 **系统维护** 下，单击 **升级 NetScaler Console**。



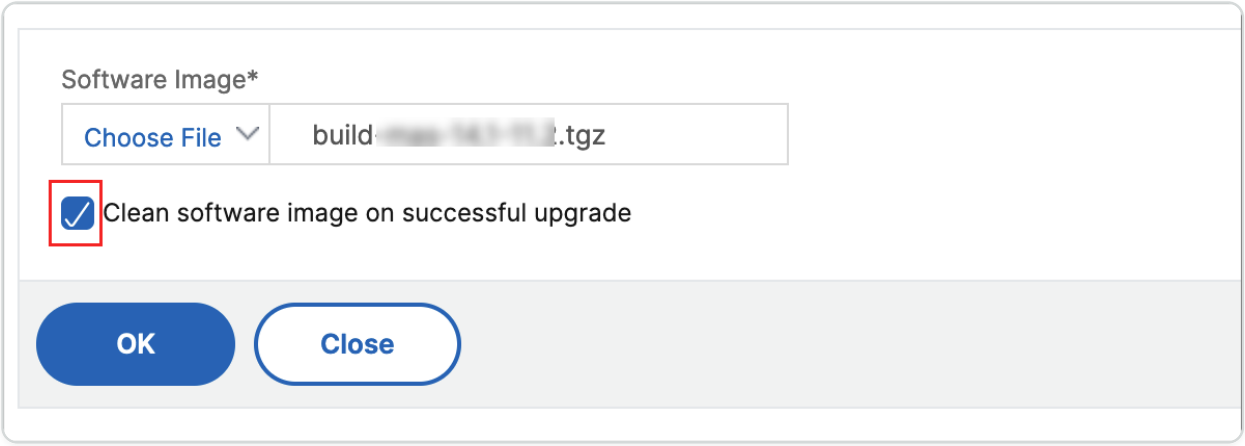
3. 在 **升级 NetScaler Console** 页面上，选中 **成功升级后清理软件映像** 复选框，以在升级后删除映像文件。选择此选项会在升级时自动删除 NetScaler Console 映像文件。

注意：

此选项默认处于选中状态。如果您在开始升级过程之前未选中此复选框，则必须手动删除映像。

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

4. 然后，您可以通过选择 **本地**（您的本地计算机）或 **设备** 来上传新的映像文件。构建文件必须存在于 NetScaler Console 虚拟设备上。



5. 单击 **确定**。 将显示“确认”对话框。单击 **是**。

   升级过程开始。

配置迁移后，您可以登录 NetScaler Console GUI。登录后，历史数据将在后台开始迁移，同时您可以继续在 NetScaler Console 上工作。

在历史数据迁移期间，某些旧数据可能不可用。迁移数据库所需的时间取决于数据大小和表的数量。

您可以使用 NetScaler Console GUI 监控数据库迁移。单击 **查看升级进度**，将显示 **数据库迁移状态**。

将高可用性对升级到 14.1 版本

对于处于高可用性模式的 NetScaler Console 服务器，您可以通过访问活动节点或浮动 IP 地址进行升级。一旦您在任一服务器中启动升级过程，两个 NetScaler Console 服务器都将自动升级到最新版本。

升级 NetScaler Console 灾难恢复部署

注意：

- 确保 HA 对和灾难恢复节点的密码相同。
- 仅在升级独立节点或 HA 节点后才升级灾难恢复节点。如果您在升级主节点或 HA 节点之前升级灾难恢复节点，可能会出现数据库同步问题。

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

升级 NetScaler Console 灾难恢复部署是一个两步过程：

- 升级主站点中配置为高可用性模式的 NetScaler Console 节点。之后，您必须升级灾难恢复节点。
- 在升级灾难恢复节点之前，请确保您已升级部署在高可用性模式下的 NetScaler Console 服务器。

升级 NetScaler Console 灾难恢复节点

1. 从 NetScaler 站点下载 NetScaler Console 升级映像文件。
2. 使用 `nsrecover` 凭据将此文件上传到灾难恢复节点。
3. 使用 `nsrecover` 凭据登录到灾难恢复节点。
4. 导航到放置映像文件的文件夹并解压缩该文件。
5. 运行以下脚本：

   ./安装mas

   ```
   bash-3.2# ./installmas
   ```

升级多站点部署的本地代理

升级 NetScaler 代理部署是一个三步过程。 在升级本地代理之前，请确保已完成以下任务：

1. 升级以高可用性部署的 NetScaler Console 服务器。
2. 升级 NetScaler Console 灾难恢复节点。

   有关详细信息，请参阅 升级 NetScaler Console 灾难恢复部署。

升级本地代理

1. 从 NetScaler 站点下载 NetScaler 代理升级映像文件。
2. 使用 `nsrecover` 凭据将此文件上传到代理节点。
3. 确保下载正确的代理升级映像。
4. 使用 `nsrecover` 凭据登录到本地代理。
5. 导航到放置映像文件的文件夹并解压缩该文件。

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

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 30 08:50:48 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-masagent-12.1-502.109.tgz
```

6. 运行以下脚本：

   `./installmasagent`

```
bash-3.2# ./installmasagent
```

向 NetScaler Console 服务器添加额外磁盘

如果您的 NetScaler Console 存储需求超出默认磁盘空间 (120 GB)，您可以附加一个额外磁盘。您可以在单服务器部署和高可用性部署中附加更多磁盘。

当您从版本 12.1–13.10 升级 NetScaler Console 时，您在早期版本中在附加磁盘上创建的分区保持不变。这些分区不会被删除或调整大小。

在升级后的版本中，附加更多磁盘的步骤保持不变。您现在可以使用 NetScaler Console 中新的磁盘分区工具在新添加的磁盘中创建分区。您还可以使用该工具调整现有更多磁盘中的分区大小。有关如何附加更多磁盘以及使用新的磁盘分区工具的更多信息，请参阅 如何将额外磁盘附加到 NetScaler Console。

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

认证

用户可以通过 NetScaler Console 内部认证、外部认证服务器认证，或者两者兼有。如果使用本地认证，用户必须存在于 NetScaler Console 安全数据库中。如果用户通过外部认证，则用户的“外部名称”必须与在认证服务器上注册的外部用户身份匹配，具体取决于所选的认证协议。

NetScaler Console 支持通过 RADIUS、LDAP 和 TACACS 服务器进行外部认证。这种统一支持提供了一个通用接口，用于认证和授权所有访问系统的本地和外部认证、授权和记账服务器用户。无论用户使用何种实际协议与系统通信，NetScaler Console 都可以认证用户。当用户尝试访问配置为外部认证的 NetScaler Console 实施时，请求的应用程序服务器会将用户名和密码发送到 RADIUS、LDAP 或 TACACS 服务器进行认证。如果认证成功，用户将被授予访问 NetScaler Console 的权限。

外部认证服务器

NetScaler Console 将所有认证、授权和审计服务请求发送到远程 RADIUS、LDAP 或 TACACS 服务器。远程认证、授权和审计服务器接收请求，验证请求，并向 NetScaler Console 发送响应。当配置为使用远程 RADIUS、TACACS 或 LDAP 服务器进行认证时，NetScaler Console 将成为 RADIUS、TACACS 或 LDAP 客户端。在任何这些配置中，认证记录都存储在远程主机服务器数据库中。帐户名、分配的权限和时间记账记录也存储在每个用户的认证、授权和审计服务器上。

此外，您可以使用 NetScaler Console 的内部数据库进行本地用户认证。您可以在数据库中为用户及其密码和默认角色创建条目。您还可以选择特定认证类型的认证顺序。服务器组中的服务器列表是一个有序列表。列表中的第一个服务器始终被使用，除非它不可用，在这种情况下将使用列表中的下一个服务器。您可以将服务器配置为将内部数据库作为已配置的认证、授权和审计服务器列表的备用认证备份。

您可以在 NetScaler Console 中配置和添加以下服务器：

- LDAP 认证服务器
- RADIUS 认证服务器
- TACACS 认证服务器
- 启用外部认证服务器和回退选项
- 支持 LDAP、RADIUS 和 TACACS 的双因素认证 (2FA)

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

在 NetScaler Console 中认证用户

您可以通过两种方式在 NetScaler Console 中认证用户：

- 在 NetScaler Console 中配置的本地用户

  本地用户身份验证(/en-us/netscaler-application-delivery-management-software/media/auth-local-users-console.png)

  配置完成后，以下是本地服务器中用户身份验证的工作流程。

  本地用户身份验证(/en-us/netscaler-application-delivery-management-software/media/auth-local-users1-console.png)

  1 – 用户登录到 NetScaler Console

  2 – NetScaler Console 提示用户输入凭据进行身份验证，并检查凭据是否与 NetScaler Console 数据库中的凭据匹配。

- 使用外部身份验证服务器

  外部用户身份验证(/en-us/netscaler-application-delivery-management-software/media/auth-external-console.png)

  配置完成后，以下是外部身份验证、授权和审计服务器中用户身份验证的工作流程：

  外部用户身份验证(/en-us/netscaler-application-delivery-management-software/media/auth-external1-console.png)

  1 – 用户连接到 NetScaler Console

  2 – NetScaler Console 提示用户输入凭据

  3 – NetScaler Console 使用外部身份验证、授权和审计服务器验证用户凭据。如果验证成功，用户可以继续登录

添加 LDAP 身份验证服务器

当您将 LDAP 协议与 RADIUS 和 TACAS 身份验证服务器集成时，您可以使用 NetScaler Console 从分布式目录搜索和验证用户凭据。

1. 导航到 **设置 > 身份验证**。
2. 选择 **LDAP** 选项卡，然后单击 **添加**。
3. 在 **创建 LDAP 服务器** 页面上，指定以下参数：

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

a. **名称** – 指定 LDAP 服务器名称

b. **服务器名称/IP 地址** – 指定 LDAP IP 地址或服务器名称

c. **安全类型** – 系统与 LDAP 服务器之间所需的通信类型。从列表中选择。如果纯文本通信不足，您可以通过选择传输层安全 (TLS) 或 SSL 来选择加密通信。

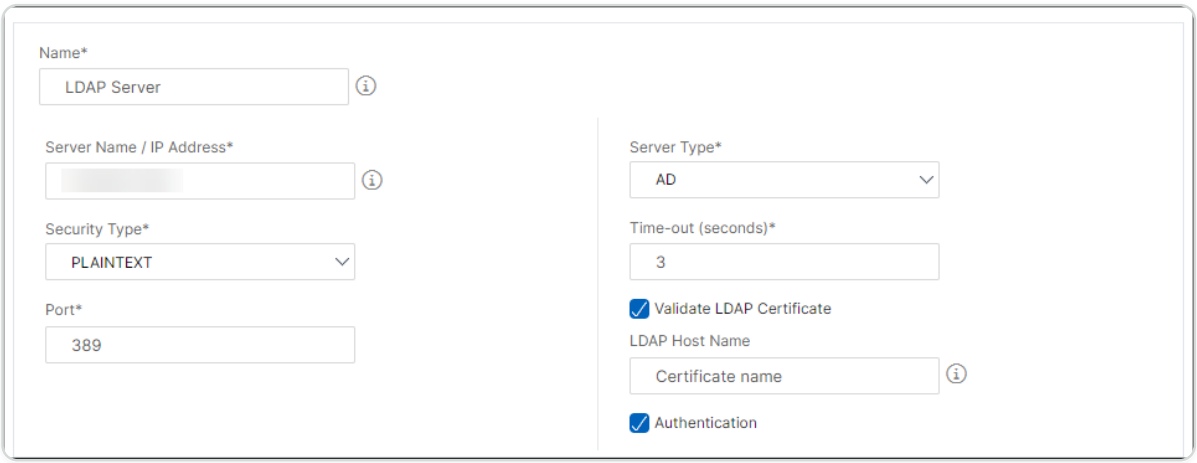
d. **端口** – 默认情况下，端口 389 用于纯文本。您也可以为 SSL/TLS 指定端口 636。

e. **服务器类型** – 选择 Active Directory (AD) 或 Novell Directory Service (NDS) 作为 LDAP 服务器类型。

f. **超时（秒）** – NetScaler Console 系统等待 LDAP 服务器响应的秒数。

g. **LDAP 主机名** – 选中“验证 LDAP 证书”复选框并指定要在证书上输入的主机名。

清除 **身份验证** 选项并指定 SSH 公钥。通过基于密钥的身份验证，您现在可以通过 SSH 获取存储在 LDAP 服务器用户对象上的公钥列表。



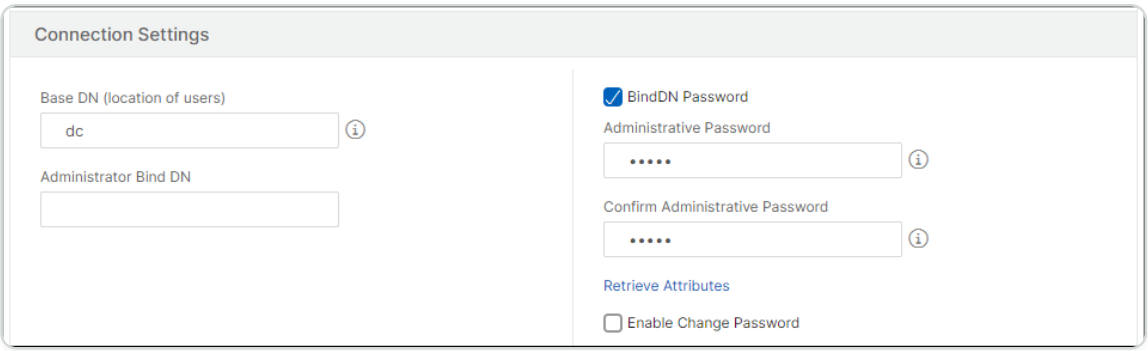
在连接设置下，指定以下参数：

i. **基本 DN** – LDAP 服务器开始搜索的基节点

ii. **管理员绑定 DN** – 用于绑定到 LDAP 服务器的用户名。例如，admin@aaa.local。

iii. **绑定 DN 密码** – 选择此选项以提供用于身份验证的密码

iv. **启用更改密码** – 选择此选项以启用密码更改



在**其他设置**下，指定以下参数

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

i. **服务器登录名属性** – 系统用于查询外部 LDAP 服务器或 Active Directory 的名称属性。从列表中选择 **samAccountname**。

ii. **搜索筛选器** – 根据 LDAP 服务器中配置的搜索筛选器，为外部用户配置双因素身份验证。例如，vpnallowed=true 与 ldaploginame `samaccount` 和用户提供的用户名 bob 将生成一个 LDAP 搜索字符串：`&(vpnallowed=true)(samaccount=bob)`。

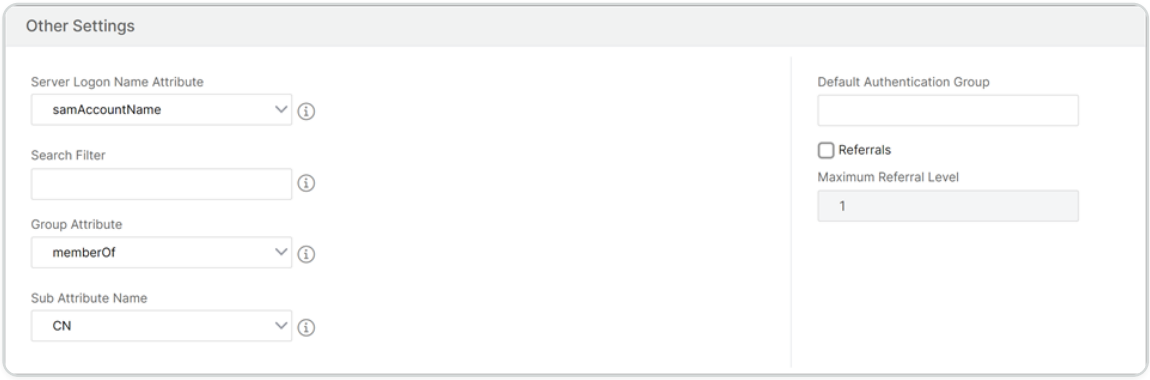
注意

> 默认情况下，搜索筛选器中的值用括号括起来。

iii. **组属性** – 从列表中选择 memberOf。

iv. **子属性名称** – 用于从 LDAP 服务器提取组的子属性名称。

v. **默认身份验证组** – 除了提取的组之外，身份验证成功时选择的默认组。



4. 单击**创建**。

LDAP 服务器现已配置。

注意

> 如果用户是 Active Directory 组成员，则 NetScaler Console 上的组和用户名称必须与 Active Directory 组成员的名称相同。

5. 启用外部身份验证服务器。

有关启用外部身份验证服务器的更多信息，请参阅启用外部身份验证服务器和回退选项。

添加 RADIUS 身份验证服务器

1. 导航到 **设置 > 身份验证**。

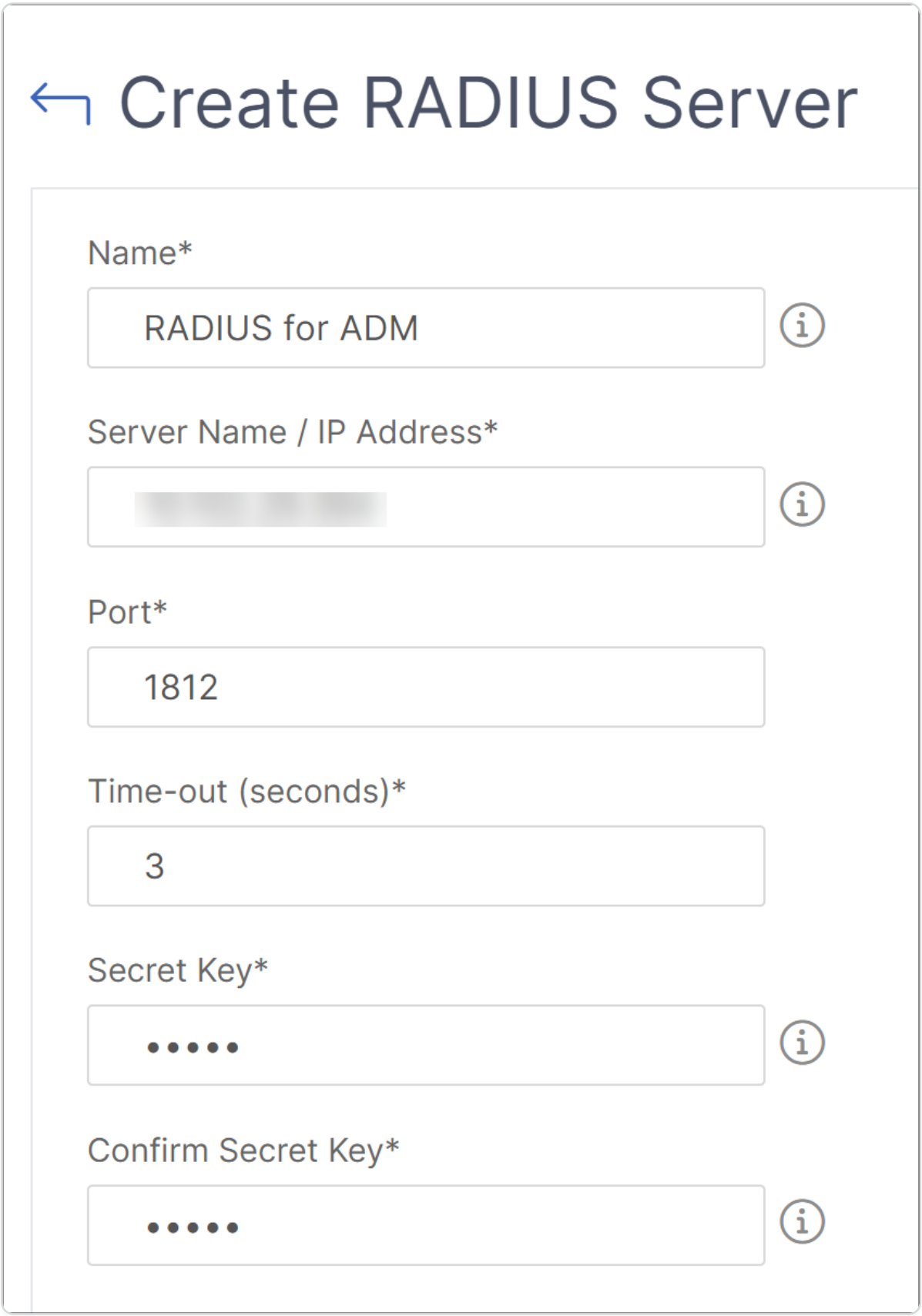
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 选择 **RADIUS** 选项卡，然后单击 **添加**。

   在 **创建 RADIUS 服务器** 页面上，指定以下参数：

   a. **名称** – 指定 RADIUS 服务器名称
   b. **服务器名称/IP 地址** – 指定 RADIUS 服务器 IP 地址
   c. **端口** – 指定 RADIUS 服务器托管的端口号。默认端口为 1812
   d. **超时（秒）** – NetScaler Console 系统等待 RADIUS 服务器响应的秒数
   e. **密钥** – 指定用于身份验证的 RADIUS 密钥
   f. **确认密钥** – 再次指定密钥以进行确认

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



在 **详细信息** 下，指定以下参数：

i. **NAS ID** – 指定要发送到 RADIUS 服务器的标识符 ID

ii. **组供应商标识符** – 指定用于 RADIUS 组提取的供应商 ID

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

iii. **组前缀** - 在 RADIUS 属性中，用于 RADIUS 组提取的组名前面的字符串

iv. **组属性类型** – 指定 RADIUS 组提取的属性类型

v. **组分隔符** – 用于分隔 RADIUS 属性中组名称的字符串，用于 RADIUS 组提取

vi. **IP 地址供应商标识符** – RADIUS 中的供应商 ID 表示内网 IP。值为 0 表示该属性未进行供应商编码

vii. **密码供应商标识符** – RADIUS 响应中的供应商 ID 密码，用于提取用户密码

viii. **IP 地址属性类型** – RADIUS 响应的远程 IP 地址属性

ix. **密码属性类型** – RADIUS 响应的密码属性

x. **密码编码** – 从列表中选择 pap、chap、mschapv1 或 mschapv2。这表示密码应如何在从系统传输到 RADIUS 服务器的 RADIUS 数据包中进行编码。

xi. **默认身份验证组** – 除了提取的组之外，身份验证成功时选择的默认组

如果您希望设备使用 RADIUS 服务器记录审计信息，请选择“记账”。

3. 单击“**创建**”。

RADIUS 服务器现已配置完成。

4. 启用外部身份验证服务器。

有关启用外部身份验证服务器的更多信息，请参阅启用外部身份验证服务器和回退选项。

添加 TACACS 身份验证服务器

1. 导航到 **设置 > 身份验证**。
2. 选择 **TACACS** 选项卡，然后单击 **添加**。
3. 在 **创建 TACACS** 页面上，指定以下参数：

a. **名称** – 指定 TACACS 服务器名称

b. **IP 地址** – 指定 TACACS IP 地址

c. **端口** – 指定托管 TACACS 服务器的端口号。默认端口为 49

d. **超时（秒）** – NetScaler Console 系统等待 LDAP 服务器响应的时间（以秒为单位）

e. **TACACS 密钥** – 指定用于身份验证的 TACACS 密钥

f. **确认 TACACS 密钥** – 再次指定 TACACS 密钥以进行确认

g. **组属性名称** – 指定组名称

如果您希望设备使用 TACACS 服务器记录审计信息，请选择 **记账**。

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

4. 单击 **创建**。

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

Create TACACS Server

Name*

TACACS for ADM

IP Address*

Port*

49

Time-out (seconds)*

3

TACACS Key*

•••••

Confirm TACACS Key*

•••••

Group Attribute Name

☑ Accounting

5. 启用外部身份验证服务器。

   有关启用外部身份验证服务器的更多信息，请参阅启用外部身份验证服务器和回退选项。

NetScaler Console 中的用户

您可以在 NetScaler Console 上本地创建用户帐户，以补充身份验证服务器上的用户。例如，您可能希望为临时用户（如顾问或访客）创建本地用户帐户，而无需在身份验证服务器上为这些用户创建条目。

有关配置用户的更多信息，请参阅 配置用户。

注意

> 如果用户位于 Active Directory 中，请确保 NetScaler Console 中的组名与外部服务器上 Active Directory 组的组名相同。

NetScaler Console 中的用户组

NetScaler Console 允许您通过创建组并将用户添加到组来对用户进行身份验证和授权。一个组可以拥有“管理员”或“只读”权限，该组中的所有用户都将获得相同的权限。

在 NetScaler Console 中：

- 组被定义为具有相似权限的用户集合
- 一个组可以有一个或多个角色
- 用户被定义为可以根据分配的权限拥有访问权限的实体
- 一个用户可以属于一个或多个组

您可以在 NetScaler Console 中创建本地组，并对组中的用户使用本地身份验证。如果您使用外部服务器进行身份验证，请在 NetScaler Console 上配置组以匹配内部网络中身份验证服务器上配置的组。当用户登录并进行身份验证时，如果组名与身份验证服务器上的组匹配，则用户将继承 NetScaler Console 上该组的设置。 如果您使用本地身份验证，请创建用户并将其添加到 NetScaler Console 上配置的组中。然后，用户将继承这些组的设置。

有关配置组和分配组权限的更多信息，请参阅 配置组。

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

提取身份验证服务器组

注意

从 **NetScaler Console 13.0** 开始支持 TACACS 服务器提取。

NetScaler Console 使您能够：

- 提取用户在外部身份验证服务器上所属的组列表。
- 将它们分配给与外部服务器上配置的组匹配的组设置。

优点：

- 您无需在 NetScaler Console 中创建用户，因为它们在外部服务器上进行管理。
- NetScaler Console 通过分配组权限来授权用户访问特定的负载均衡器虚拟服务器以及系统上的特定应用程序。

启用外部身份验证服务器和回退选项

回退选项允许在外部服务器身份验证失败时，由本地身份验证接管。在 NetScaler Console 和外部身份验证服务器上都配置的用户可以登录 NetScaler Console，即使配置的外部身份验证服务器已关闭或不可访问。为确保回退身份验证正常工作：

- 如果外部服务器已关闭或不可访问，非 nsroot 用户必须能够访问 NetScaler Console
- 您必须至少添加一个外部服务器

NetScaler Console 还支持统一的身份验证、授权和记账 (AAA) 协议系统（LDAP、RADIUS 和 TACACS）以及本地身份验证。这种统一支持提供了一个通用接口，用于对访问系统的所有用户和外部 AAA 客户端进行身份验证和授权。

NetScaler Console 无论用户使用何种实际协议与系统通信，都可以对其进行身份验证。 级联外部身份验证服务器为外部用户的身份验证和授权提供了一个持续不失败的过程。如果第一个身份验证服务器上的身份验证失败，NetScaler Console 会尝试使用第二个外部身份验证服务器对用户进行身份验证，依此类推。要启用级联身份验证，您必须在 NetScaler Console 中添加外部身份验证服务器。您可以添加任何类型的受支持外部身份验证服务器（RADIUS、LDAP 和 TACACS）。

例如，假设您要添加四个外部身份验证服务器，并配置了两个 RADIUS 服务器、一个 LDAP 服务器和一个 TACACS 服务器。NetScaler Console 会根据配置尝试与外部服务器进行身份验证。在此示例场景中，NetScaler Console 尝试：

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

- 连接到第一个 RADIUS 服务器
- 如果第一个 RADIUS 服务器的身份验证失败，则连接到第二个 RADIUS 服务器
- 如果两个 RADIUS 服务器的身份验证都失败，则连接到 LDAP 服务器
- 如果两个 RADIUS 服务器和 LDAP 服务器的身份验证都失败，则连接到 TACACS 服务器。

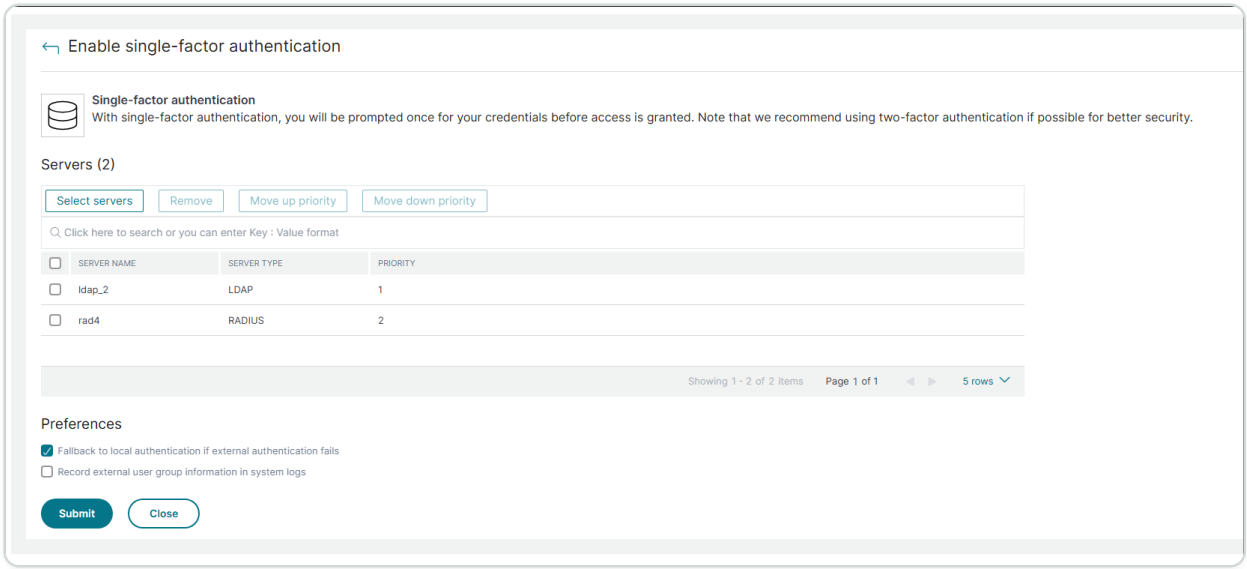
注意

> 您可以在 NetScaler Console 中配置多达 32 个外部身份验证服务器。

配置回退和级联外部服务器

1. 导航到 **设置 > 身份验证 > 身份验证设置**。
2. 在**身份验证设置**页面上，在**外部服务器身份验证**下，点击**启用单因素身份验证**。
3. 在**启用单因素身份验证**页面上，点击**选择服务器**。选择一个或多个身份验证服务器，然后点击**添加**。
4. 如果您希望在外部身份验证失败时由本地身份验证接管，请选择**如果外部身份验证失败，则回退到本地身份验证**。
5. 如果您希望在系统审计日志中捕获外部用户组信息，请选择**在系统日志中记录外部用户组信息**。
6. 点击**提交**以关闭页面。

   所选服务器显示在**身份验证设置**页面上。



您还可以使用服务器名称旁边的图标在列表中向上或向下移动服务器，从而指定身份验证顺序。

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

LDAP、RADIUS 和 TACACS 支持双因素认证 (2FA)

多因素认证是当今安全领域的最佳实践，大多数组织要求网络设备至少具备两个认证因素才能满足合规标准。双因素认证是一种安全机制，产品通过该机制在两个级别对用户进行身份验证。只有在两个级别都成功验证后，才授予访问权限。

从 NetScaler Console 14.1-43.x 及更高版本开始，NetScaler Console 本地部署支持双因素认证 (2FA)。您可以将 LDAP、RADIUS 和 TACACS 用作 NetScaler Console 本地部署的认证因素。

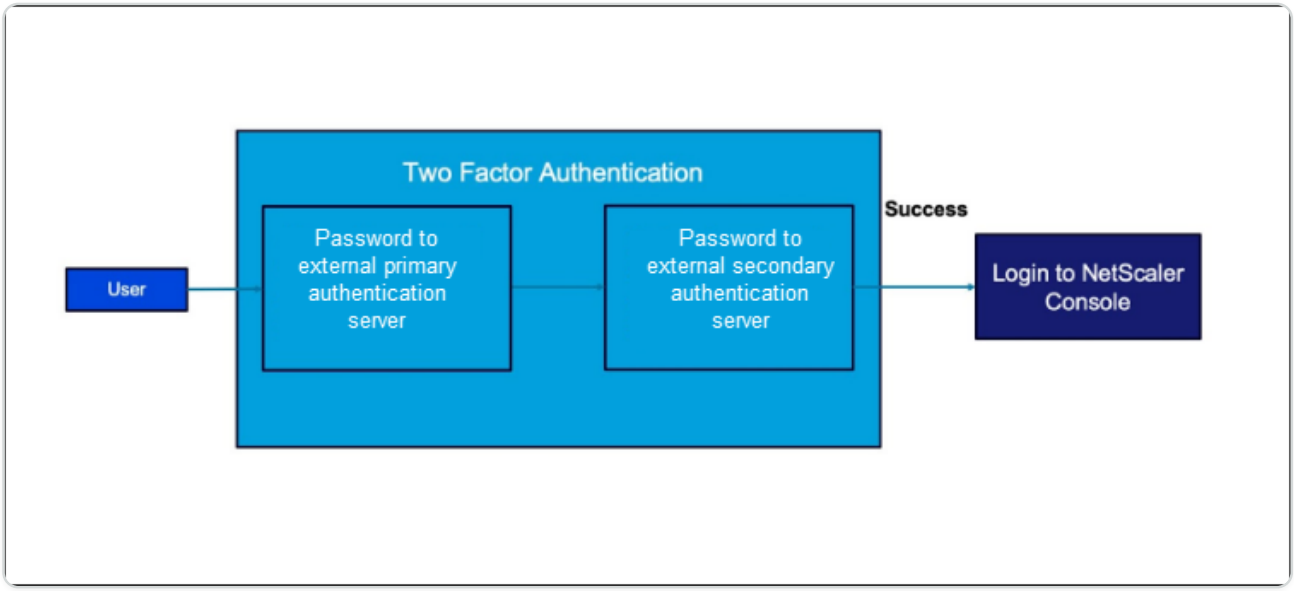
注意：

双因素认证支持仅适用于外部服务器认证。

当用户尝试登录启用了双因素认证的 NetScaler Console 时，系统会提示用户输入初始外部认证的用户名和密码。初始认证成功后，系统会提示用户进行第二级认证。

只有在两个密码都成功验证后，用户才能完全通过身份验证。如果认证失败，系统会向用户显示失败原因。

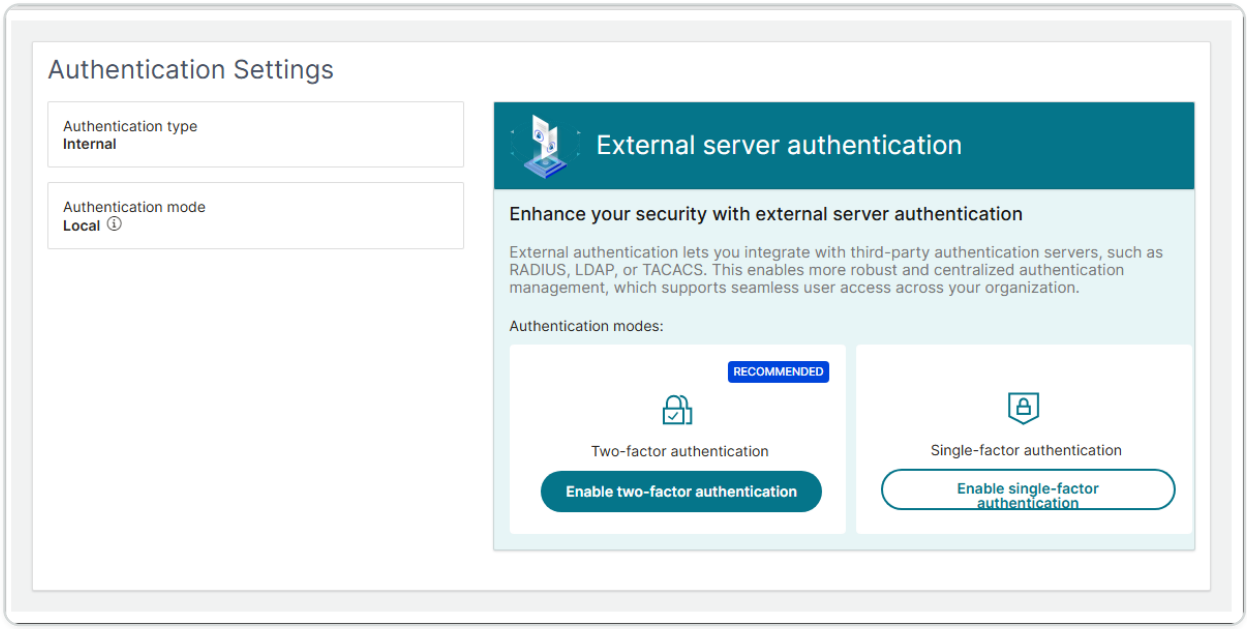
如果用户在本地进行身份验证，则必须在 NetScaler Console 数据库中创建用户配置文件。如果用户在外部进行身份验证，则用户名和密码必须与外部身份验证服务器中注册的用户身份匹配。



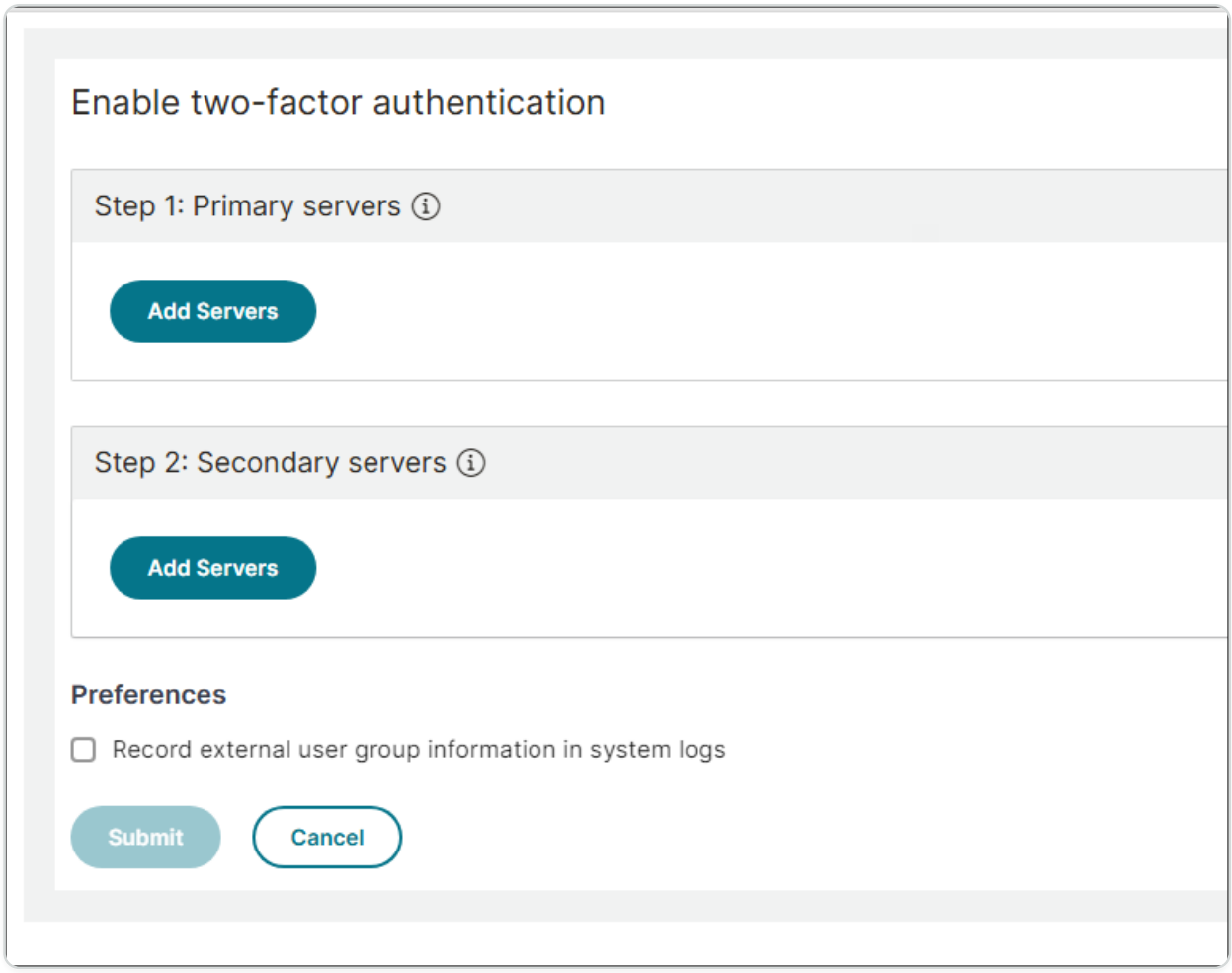
配置双因素认证

1. 登录 NetScaler Console 本地部署，然后导航到 **Settings > Authentication > Authentication Settings**。

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

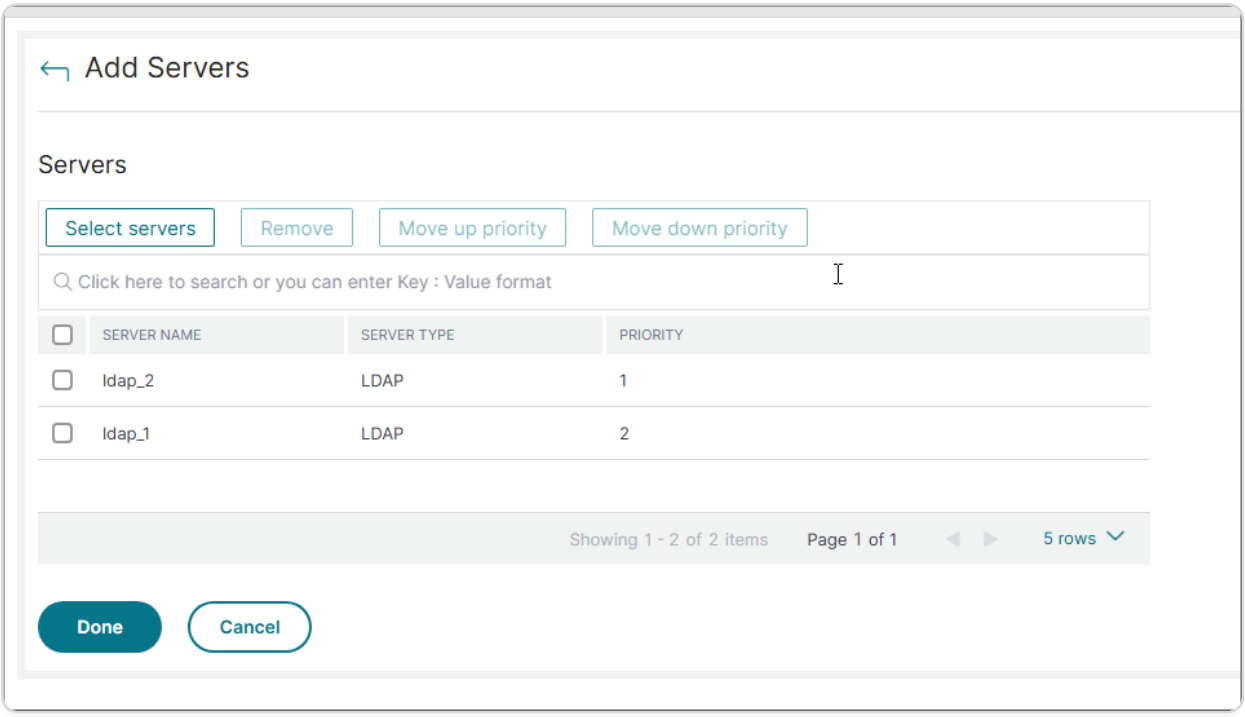


2. 在“**外部服务器认证**”部分，点击“**认证模式**”下的“**启用双因素认证**”。
3. 在“**启用双因素认证**”页面上，在“**步骤 1: 主服务器**”下，点击“**添加服务器**”。

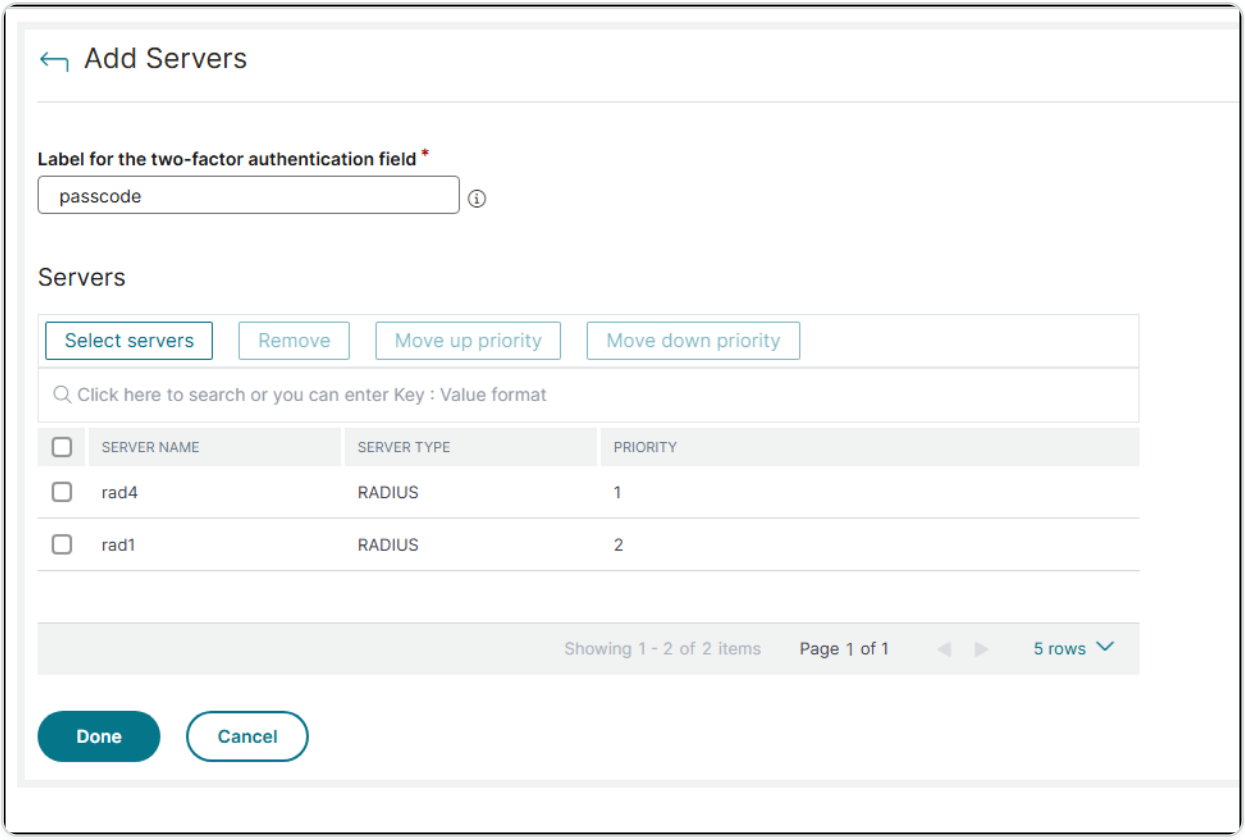


4. 点击 **Select Servers** 并选择所需的服务器。点击 **Add**，然后点击 **Done**。

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



5. 在“**启用双因素身份验证**”页面上，在“**步骤 2：辅助服务器**”下，单击“**添加服务器**”。
6. 在“**双因素身份验证字段的标签**”中，输入一个标签，该标签将用于对配置为第二因素身份验证的服务器进行身份验证。
7. 单击“**选择服务器**”并选择所需的服务器。单击“**添加**”，然后单击“**完成**”。

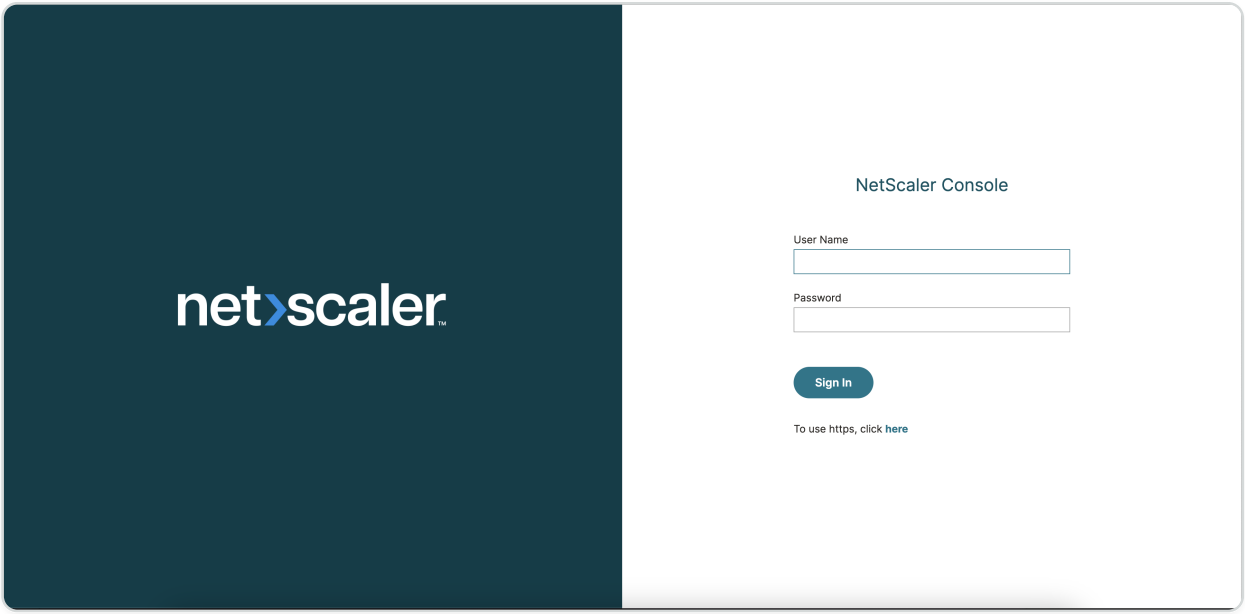


8. 单击“**提交**”。

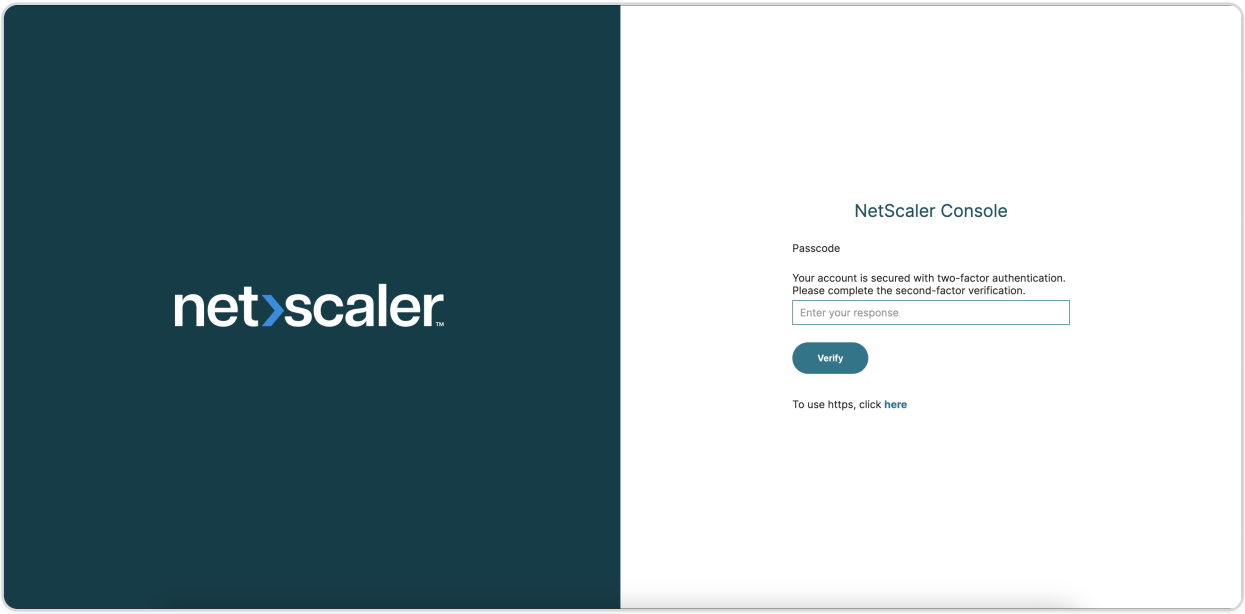
© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用双因素身份验证访问 NetScaler® Console

1. 在 Web 浏览器中，键入 NetScaler Console 的 IP 地址。登录页面随即出现。

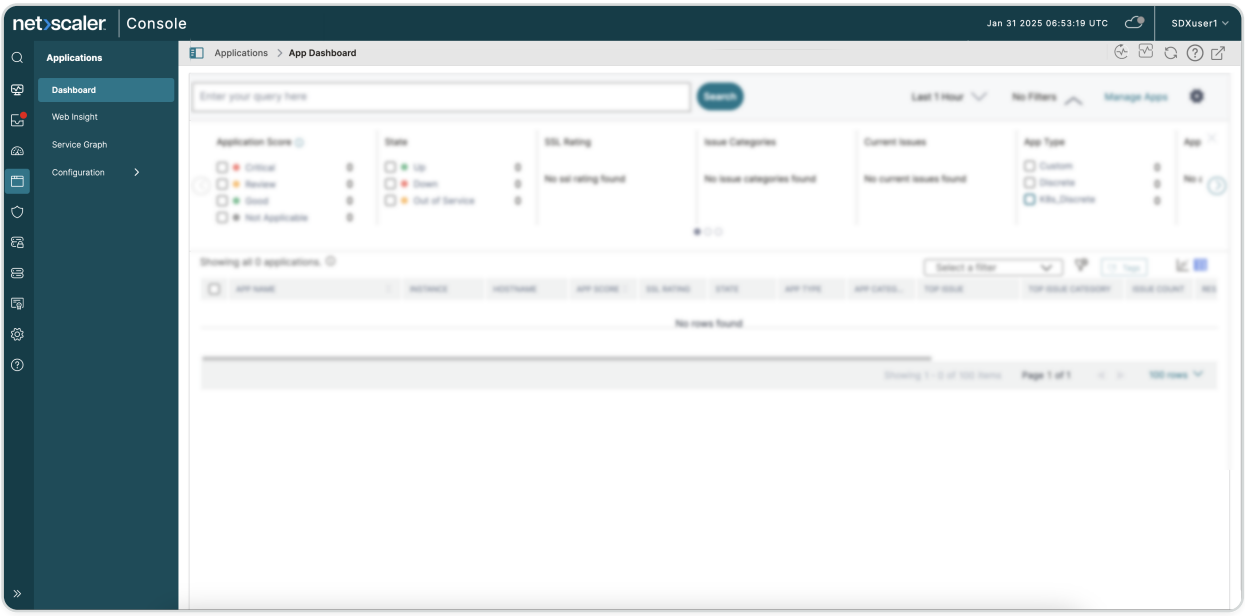


2. 在“**用户名**”和“**密码**”字段中输入用户名和密码。此步骤是第一因素身份验证。
3. 成功完成第一因素身份验证后，系统会提示用户进行第二因素身份验证。输入为第二因素身份验证配置的标签。



4. 成功完成第二因素身份验证后，用户将登录到 NetScaler Console GUI。

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



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

访问控制

身份验证是一个过程，通过该过程您可以验证某人是否是其所声称的身份。要执行身份验证，用户必须已在可由身份验证机制查询的系统中创建帐户，或者必须在首次身份验证过程中创建帐户。NetScaler 提供了一种对本地用户和外部用户进行身份验证的方法。虽然本地用户在内部进行身份验证，但 NetScaler Console 支持使用 RADIUS、LDAP 和 TACACS 协议进行外部身份验证。当用户尝试访问配置为外部身份验证的 NetScaler Console 时，请求的应用程序服务器会将用户名和密码发送到 RADIUS、LDAP 或 TACACS 服务器进行身份验证。身份验证成功后，将使用所需的协议在 NetScaler Console 上识别用户。

访问控制是强制执行特定资源所需安全性的过程。它是一种安全技术，可用于规范谁可以在计算环境中查看或使用资源。访问控制的目的是限制计算机系统的合法用户可以执行的操作。访问控制限制了用户可以直接执行的操作，以及代表用户运行的程序被允许执行的操作。通过这种方式，访问控制旨在防止可能导致安全漏洞的活动。访问控制假定在通过参考监视器强制执行访问控制之前，用户的身份验证已成功验证。NetScaler Console 允许细粒度的基于角色的访问控制 (RBAC)，管理员可以根据企业内各个用户的角色向用户提供访问权限。NetScaler Console 中的 RBAC 是通过创建访问策略、角色、组和用户来实现的。

基于角色的访问控制

NetScaler Console 提供细粒度、基于角色的访问控制 (RBAC)，您可以通过它根据企业内各个用户的角色授予访问权限。在此上下文中，访问是指执行特定任务的能力，例如查看、创建、修改或删除文件。角色是根据企业内用户的权限和职责定义的。例如，一个用户可能被允许执行所有网络操作，而另一个用户可以观察应用程序中的流量并帮助创建配置模板。

角色由策略决定。创建策略后，您可以创建角色，将每个角色绑定到一个或多个策略，并将角色分配给用户。您还可以将角色分配给用户组。

组是具有共同权限的用户集合。例如，管理特定数据中心的用户可以被分配到一个组。角色是根据特定条件授予用户或组的身份。在 NetScaler Console 中，创建角色和策略是 NetScaler 中 RBAC 功能特有的。随着企业需求的变化，可以轻松创建、更改或停用角色和策略，而无需单独更新每个用户的权限。

角色可以是基于功能的，也可以是基于资源的。例如，考虑 SSL/安全管理员和应用程序管理员。SSL/安全管理员必须对 SSL 证书管理和监控功能拥有完全访问权限，但对系统管理操作必须拥有只读访问权限。应用程序管理员必须只能访问范围内的资源。

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

示例：

Chris 是 NetScaler 团队负责人，也是其组织中 NetScaler Console 的超级管理员。Chris 创建了三个管理员角色：安全管理员、应用程序管理员和网络管理员。

安全管理员 David 必须对 SSL 证书管理和监控拥有完全访问权限，但对系统管理操作也必须拥有只读访问权限。

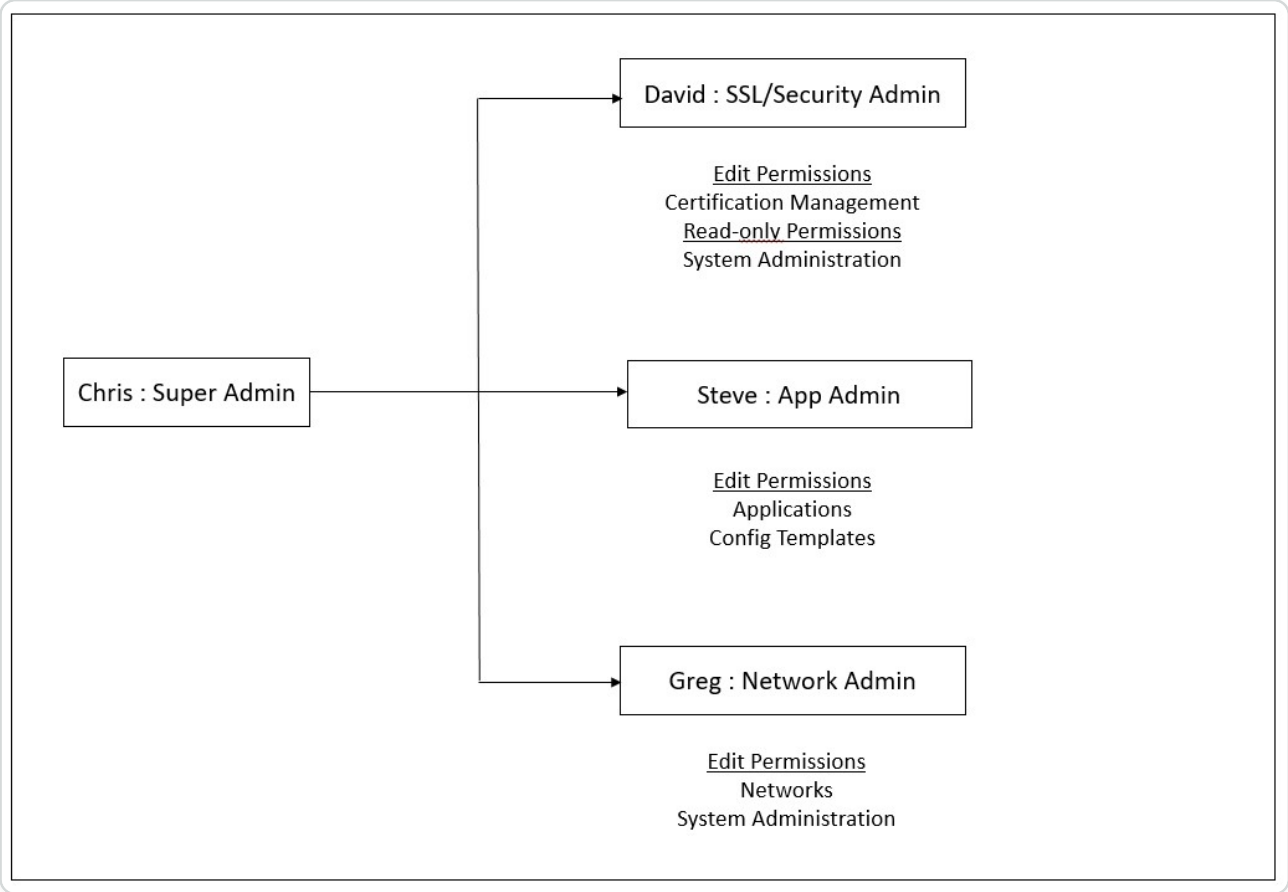
应用程序管理员 Steve 只需要访问特定的应用程序和特定的配置模板。

网络管理员 Greg 需要访问系统和网络管理。

Chris 还必须为所有用户提供 RBAC，无论他们是本地用户还是外部用户。

NetScaler Console 用户可以进行本地身份验证，也可以通过外部服务器（RADIUS/LDAP/TACACS）进行身份验证。RBAC 设置必须适用于所有用户，无论采用何种身份验证方法。

下图显示了管理员和其他用户拥有的权限及其在组织中的角色。



限制

RBAC 不完全支持以下 NetScaler Console 功能：

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

- **分析** - 分析模块中不完全支持 RBAC。RBAC 支持仅限于实例级别，不适用于 Web Insight、SSL Insight、Gateway Insight、HDX™ Insight 和 WAF 安全违规分析模块中的应用程序级别。例如：

示例 1：基于实例的 RBAC (支持)

被分配了少量实例的管理员只能在 **Web Insight** \> **实例** 下看到这些实例，并且只能在 **Web Insight** \> **应用程序** 下看到相应的虚拟服务器，因为 RBAC 在实例级别受支持。

示例 2：基于应用程序的 RBAC (不支持)

被分配了少量应用程序的管理员可以在 **Web Insight** \> **应用程序** 下看到所有虚拟服务器，但无法访问它们，因为 RBAC 在应用程序级别不受支持。

- **编排** - 编排不支持 RBAC。

配置访问策略

访问策略定义权限。策略可以应用于单个用户或组，也可以应用于多个用户和多个组。NetScaler Console 提供四种预定义访问策略：

1. **adminpolicy**。授予访问所有 NetScaler Console 功能的权限。用户拥有查看和编辑权限，可以查看所有 NetScaler Console 内容，并可以执行所有编辑操作。也就是说，用户可以对资源执行添加、修改和删除操作。
2. **readonlypolicy**。授予只读权限。用户可以查看 NetScaler Console 上的所有内容，但无权执行任何操作。
3. **appAdminPolicy**。授予访问 NetScaler Console 中应用程序功能的管理权限。绑定到此策略的用户可以添加、修改和删除自定义应用程序，并可以启用或禁用服务、服务组以及各种虚拟服务器，例如内容交换、缓存重定向和 HAProxy 虚拟服务器。
4. **appReadOnlyPolicy**。授予应用程序功能的只读权限。绑定到此策略的用户可以查看应用程序，但不能执行任何添加、修改、删除、启用或禁用操作。

注意：

预定义策略无法编辑。

您还可以创建自己的（用户定义的）策略。

创建用户定义访问策略：

1. 在 NetScaler Console 中，导航到 **设置 > 用户和角色 > 访问策略**。

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

2. 单击 **添加**。
3. 在 **策略名称** 字段中，输入策略名称，并在 **策略描述** 字段中输入描述。

   权限 部分列出了所有 NetScaler Console 功能，并提供了指定只读、启用-禁用或编辑访问的选项。
4. 单击 (+) 图标可将每个功能组展开为多个功能。

   a. 勾选功能名称旁边的权限复选框，以授予用户权限。

      - **查看：** 此选项允许用户在 NetScaler Console 中查看该功能。
      - **启用-禁用：** 此选项仅适用于允许在 NetScaler Console 上执行启用或禁用操作的**网络功能**。用户可以启用或禁用该功能。此外，用户还可以执行**立即轮询**操作。

        当您向用户授予**启用-禁用**权限时，**查看**权限也会被授予。您不能取消选择此选项。
      - **编辑：** 此选项授予用户完全访问权限。用户可以修改该功能及其功能。

        如果您授予**编辑**权限，则**查看**和**启用-禁用**权限都会被授予。您不能取消选择自动选定的选项。

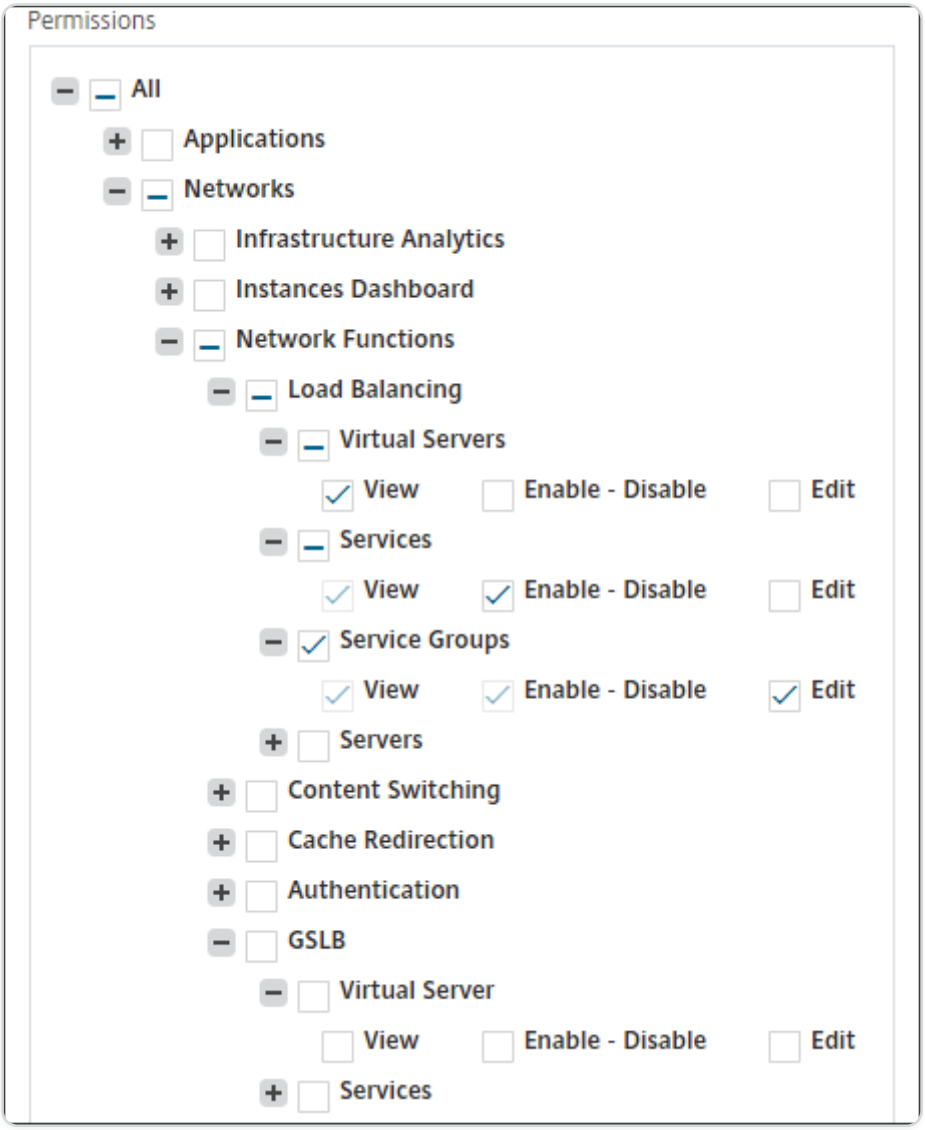
   如果您勾选功能复选框，它将选择该功能的所有权限。

注意：

展开“负载平衡”和“GSLB”以查看更多配置选项。

在下图中，“负载平衡”功能的配置选项具有不同的权限：

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



已向用户授予**虚拟服务器**功能的**查看**权限。用户可以在 NetScaler Console 中查看负载平衡虚拟服务器。要查看虚拟服务器，请导航到**基础结构 > 网络功能 > 负载平衡**并选择**虚拟服务器**选项卡。

已向用户授予**服务**功能的**启用-禁用**权限。此权限还授予**查看**权限。用户可以启用或禁用绑定到负载平衡虚拟服务器的服务。此外，用户还可以对服务执行**立即轮询**操作。要启用或禁用服务，请导航到**基础结构 > 网络功能 > 负载平衡**并选择**服务**选项卡。

注意：

如果用户具有**启用-禁用**权限，则在以下页面中对服务的启用或禁用操作将受到限制：

a. 导航到 **基础设施 > 网络功能**。

b. 选择一个虚拟服务器，然后单击**配置**。

c. 选择**负载均衡虚拟服务器服务绑定**页面。 如果选择**启用**或**禁用**，此页面将显示错误消息。

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

编辑权限授予用户以使用**服务组**功能。此权限授予完全访问权限，其中包含**查看**和**启用-禁用**权限。用户可以修改绑定到负载均衡虚拟服务器的服务组。要编辑服务组，请导航到 **Infrastructure > Network Functions > Load Balancing**，然后选择**服务组**选项卡。

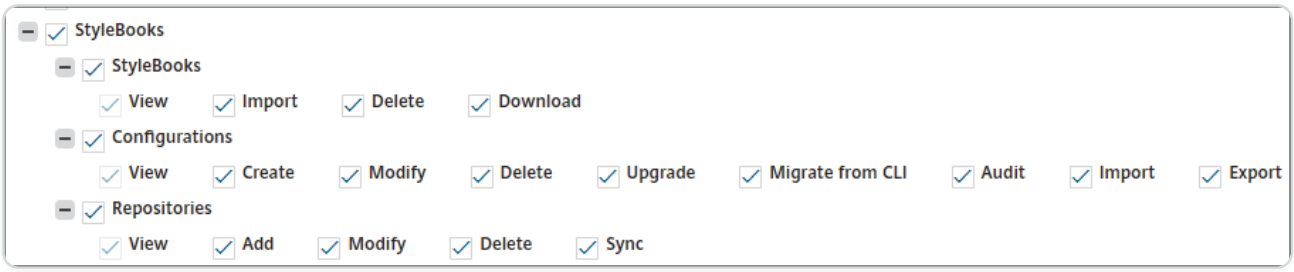
5. 单击**创建**。

授予用户 StyleBook 权限

您可以创建访问策略以授予 StyleBook 权限，例如导入、删除、下载等。

注意：

授予其他 StyleBook 权限时，将自动启用“查看”权限。



配置组

在 NetScaler Console 中，一个组可以同时拥有功能级别和资源级别的访问权限。例如，一个用户组可能只能访问选定的 NetScaler 实例；另一个组只能访问选定的几个应用程序，依此类推。

创建组时，您可以为组分配角色、为组提供应用程序级访问权限，并将用户分配给该组。该组中的所有用户在 NetScaler Console 中都被分配相同的访问权限。

您可以在 NetScaler Console 中在网络功能实体的单个级别管理用户访问。您可以在实体级别动态地为用户或组分配特定权限。

NetScaler Console 将虚拟服务器、服务、服务组和服务器视为网络功能实体。

- **虚拟服务器（应用程序）** - 负载平衡 (lb)、GSLB、上下文切换 (CS)、缓存重定向 (CR)、身份验证 (`Auth`) 和 NetScaler Gateway (VPN)
- **服务** - 负载平衡和 GSLB 服务
- **服务组** - 负载平衡和 GSLB 服务组
- **服务器** - 负载平衡服务器

创建用户组

1. 在 NetScaler Console 中，导航到 **设置 > 用户和角色 > 组**。

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

2. 单击 **添加**。

   将显示 **创建系统组** 页面。

3. 在 **组名称** 字段中，输入组的名称。允许的最大长度为 64 个字符。
4. 在 **组描述** 字段中，输入组的描述。提供良好的组描述有助于您在以后更好地理解组的角色和功能。
5. 在“**角色**”部分，将一个或多个角色添加或移动到“**已配置**”列表。

   注意：

   在“**可用**”列表下，您可以单击“**新建**”或“**编辑**”来创建或修改角色。或者，您可以导航到“**设置 > 用户和角色 > 用户**”来创建或修改用户。

6. 选择“**配置用户会话超时**”以配置用户保持活动状态的时间段。

   启用后，指定以下参数：

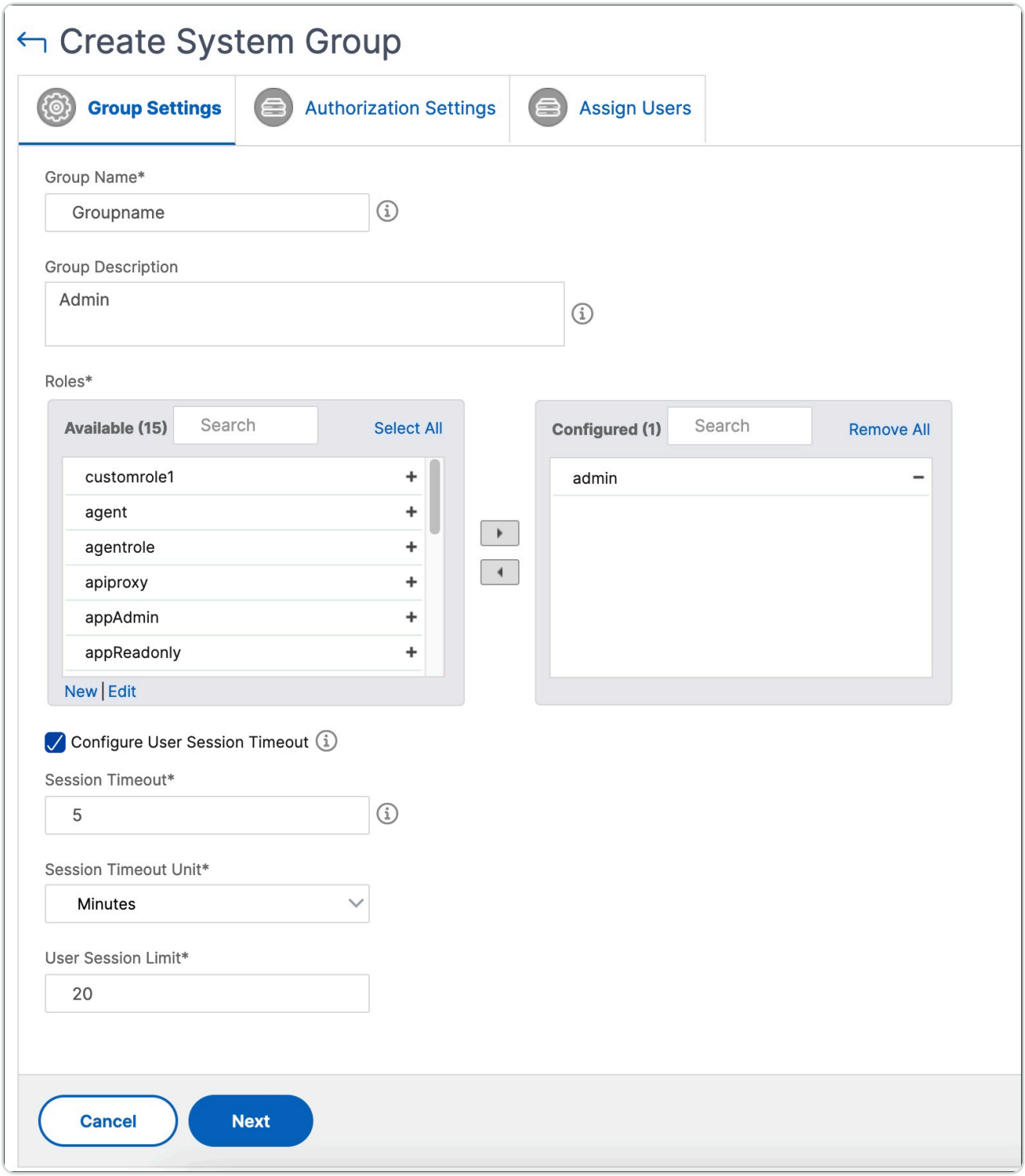
   - “**会话超时**”：输入用户会话必须保持活动状态的时间段。默认值为 15。
   - “**会话超时单位**”：从列表中选择超时单位，以分钟或小时为单位。默认值为分钟。

7. 在“**用户会话限制**”字段中，输入每个用户允许的最大会话数。

注意：

您最多可以配置 40 个用户会话。默认情况下，您被分配 20 个用户会话。但是，如果您属于管理员和只读用户组，您默认被分配 40 个用户会话，并且此值无法更改。

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



1. 单击“**下一步**”。在“**授权设置**”选项卡上，您可以为以下资源提供授权设置：

   - 自动扩缩组
   - 实例
   - 应用程序
   - 配置模板
   - StyleBooks

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

- 配置包
- 域名

授权设置中的类别(/en-us/netscaler-application-delivery-management-software/media/categories-authorization-settings.png)

您可能希望从用户可以访问的类别中选择特定资源。

自动扩缩组：

如果您想选择用户可以查看或管理的特定自动扩缩组，请执行以下步骤：

a. 清除**所有自动扩缩组**复选框，然后单击**添加自动扩缩组**。
b. 从列表中选择所需的自动扩缩组，然后单击**确定**。

实例：

如果您想选择用户可以查看或管理的特定实例，请执行以下步骤：

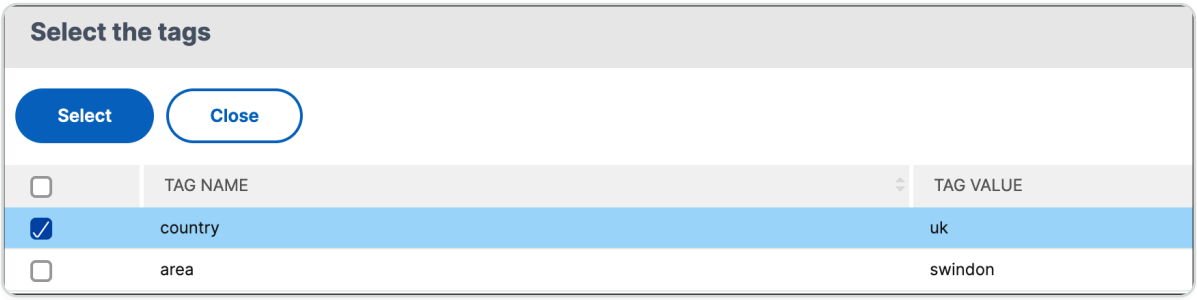
a. 清除**所有实例**复选框，然后单击**选择实例**。
b. 从列表中选择所需的实例，然后单击**确定**。

   选择实例(/en-us/netscaler-application-delivery-management-software/media/selecting-instances.png)

标签:

要根据关联标签授权用户查看或管理特定实例，请执行以下操作：

a. 清除“**所有实例**”复选框，然后单击“**选择标签**”。
b. 从列表中选择所需的标签，然后单击“**确定**”。



稍后，当您将更多实例与所选标签关联时，授权用户将自动获得对新实例的访问权限。

有关标签以及如何将标签关联到实例的更多信息，请参阅如何创建标签并将其分配给实例。

应用程序:

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

“**选择应用程序**”列表允许您授予用户对所需应用程序的访问权限。

您可以授予对应用程序的访问权限，而无需选择其实例。当您授予用户对某个应用程序的访问权限时，无论实例选择如何，用户都只能访问该应用程序。

以下选项可用：

- **所有应用程序：**此选项默认处于选中状态。它会添加 NetScaler Console 中存在的所有应用程序。
- **所选实例的所有应用程序：**仅当您从“**所有实例**”类别中选择实例时，此选项才会出现。它会添加所选实例上存在的所有应用程序。
- **特定应用程序：**此选项允许您添加希望用户访问的所需应用程序。单击“**添加应用程序**”并从列表中选择所需的应用程序。
- **选择单个实体类型：**此选项允许您选择特定类型的网络功能实体和相应的实体。

  您可以添加单个实体，也可以选择所需实体类型下的所有实体，以授予用户访问权限。

  “**也应用于绑定实体**”选项授权绑定到所选实体类型的实体。例如，如果您选择一个应用程序并选择“**也应用于绑定实体**”，NetScaler Console 将授权绑定到所选应用程序的所有实体。

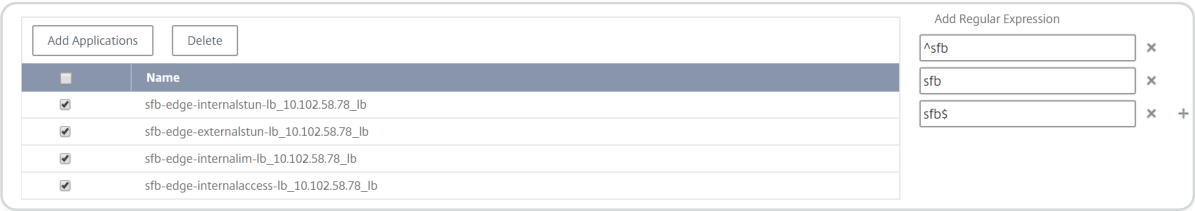
  注意：

  要授权绑定实体，请仅选择一个实体类型。

您可以使用正则表达式搜索并添加符合正则表达式条件的网络功能实体到组中。指定的正则表达式将保留在 NetScaler Console 中。要添加正则表达式，请执行以下步骤：

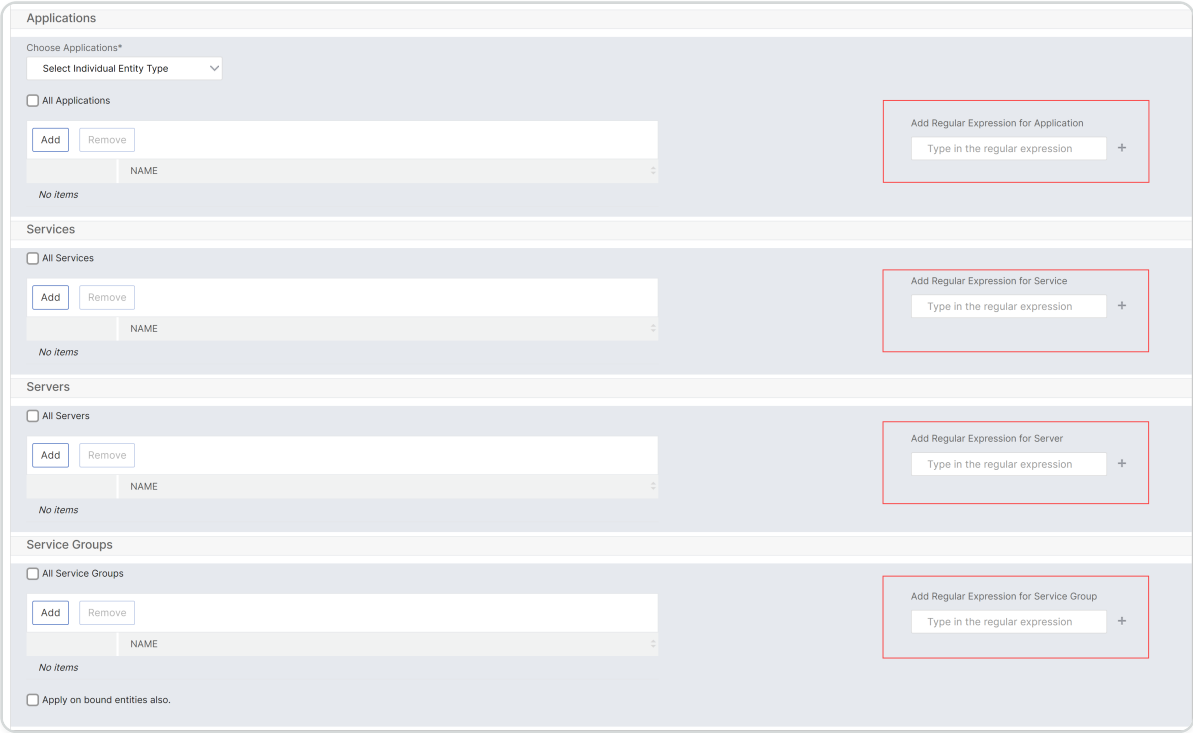
a. 单击“**添加正则表达式**”。
b. 在文本框中指定正则表达式。

下图说明了当您选择“**特定应用程序**”选项时，如何使用正则表达式添加应用程序：



下图说明了当您选择“**选择单个实体类型**”选项时，如何使用正则表达式添加网络功能实体：

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



如果要添加更多正则表达式，请单击“**+**”图标。

注意：

正则表达式仅匹配“**服务器**”实体类型的服务器名称，而不匹配服务器 IP 地址。

如果您为发现的实体选择“**也应用于绑定实体**”选项，则用户可以自动访问绑定到该发现实体的实体。

正则表达式存储在系统中以更新授权范围。当新实体与其实体类型的正则表达式匹配时，NetScaler Console 会将授权范围更新为这些新实体。

配置模板：

如果要选择用户可以查看或管理的特定配置模板，请执行以下步骤：

a. 清除**所有配置模板**复选框，然后单击**添加配置模板**。

b. 从列表中选择所需的模板，然后单击**确定**。

StyleBook：

如果要选择用户可以查看或管理的特定 StyleBook，请执行以下步骤：

a. 清除**所有 StyleBook** 复选框，然后单击**将 StyleBook 添加到组**。您可以选择单个 StyleBook，也可以指定筛选查询来授权 StyleBook。

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

如果要选择单个 StyleBook，请从**单个 StyleBook** 窗格中选择 StyleBook，然后单击**保存选择**。

如果要使用查询搜索 StyleBook，请选择**自定义筛选器**窗格。查询是键值对的字符串，其中键为 `name`、`namespace` 和 `version`。

您还可以使用正则表达式作为值来搜索和添加符合组的正则表达式条件的 StyleBook。用于搜索 StyleBook 的自定义筛选器查询支持 `And` 和 `Or` 操作。

示例：

```
name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
version=1.0
```

此查询列出了符合以下条件的 StyleBook：

- StyleBook 名称为 `lb-mon` 或 `lb`。
- StyleBook 命名空间为 `com.citrix.adc.stylebooks`。
- StyleBook 版本是 `1.0`。

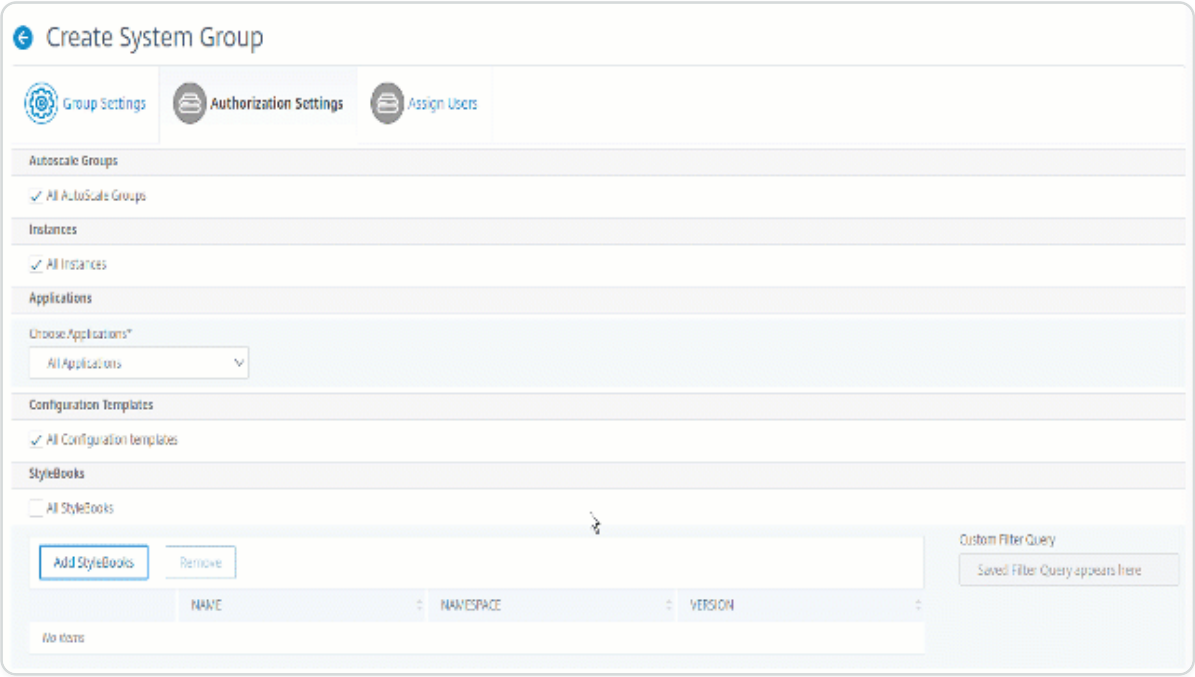
在定义到键表达式的值表达式之间使用 `Or` 操作。

示例：

- 此 `name=lb-mon|lb` 查询有效。它返回名称为 `lb-mon` 或 `lb` 的 StyleBook。
- 此 `name=lb-mon | version=1.0` 查询无效。

按 `Enter` 查看搜索结果，然后单击 **保存查询**。

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



保存的查询显示在 **自定义筛选器查询** 中。根据保存的查询，NetScaler Console 为用户提供对这些 StyleBook 的访问权限。

b. 从列表中选择所需的 StyleBook，然后单击 **确定**。

在创建组并将用户添加到该组时，您可以选择所需的 StyleBook。当您的用户选择允许的 StyleBook 时，所有依赖的 StyleBook 也会被选中。

配置包：

在 **配置包** 中，选择以下选项之一：

- **所有配置**：此选项默认处于选中状态。它允许用户管理 NetScaler Console 中的所有配置。
- **所选 StyleBook 的所有配置**：此选项添加所选 StyleBook 的所有配置包。
- **特定配置**：此选项允许您添加任何 StyleBook 的特定配置。
- **用户组创建的所有配置**：此选项允许用户仅访问由同一组用户创建的配置。

您可以在创建组并将用户分配到该组时选择适用的配置包。

域名：

如果要选择用户可以查看或管理的特定域名，请执行以下步骤：

a. 清除**所有域名**复选框，然后单击**添加域名**。

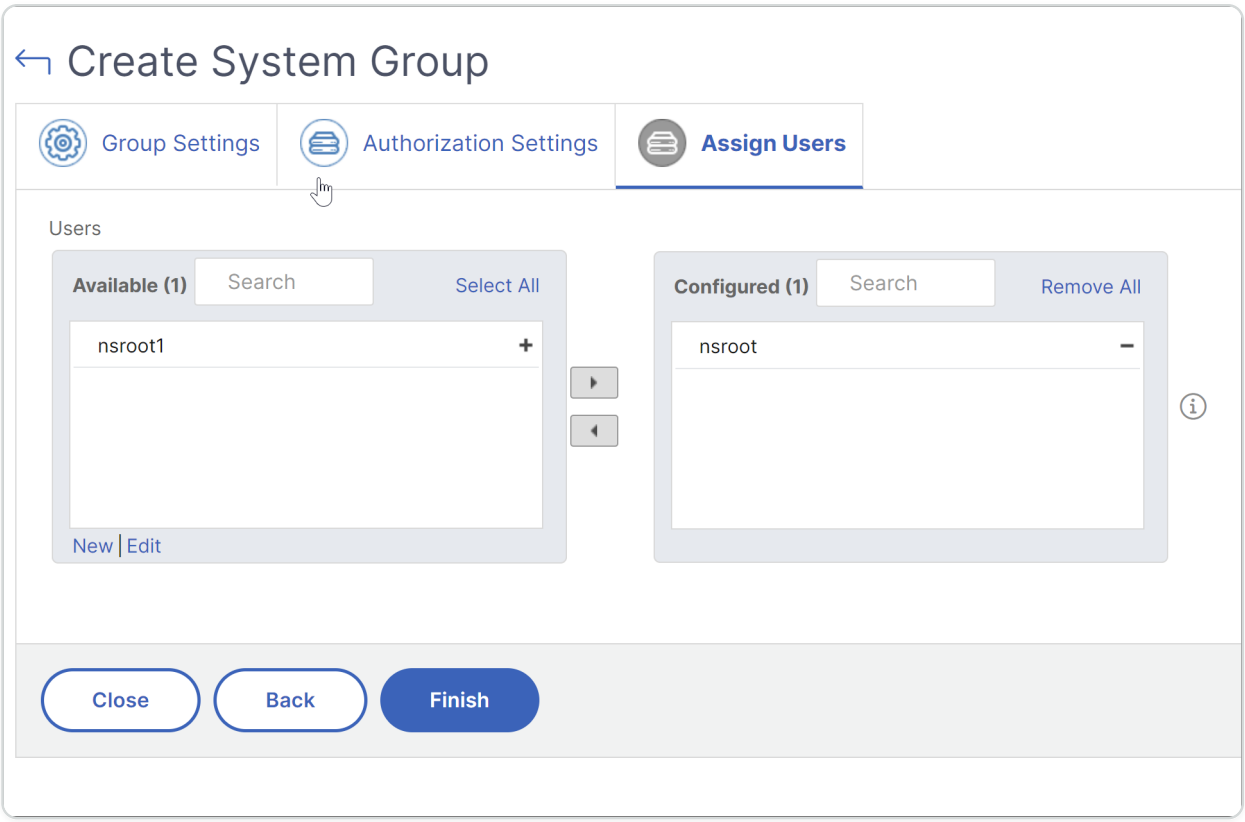
b. 从列表中选择所需的域名，然后单击**确定**。

2. 单击**创建组**。
3. 在**分配用户**部分中，在**可用**列表中选择用户，然后将用户添加到**已配置**列表。

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

注意：

您也可以通过单击**新建**来添加用户。



4. 单击**完成**。

管理跨多个网络功能实体的用户访问

作为管理员，您可以在 NetScaler Console 中管理网络功能实体的单个用户访问。此外，您还可以使用正则表达式筛选器在实体级别动态地为用户或组分配特定权限。

本文档介绍了如何在实体级别定义用户授权。

在开始之前，请创建一个组。有关详细信息，请参阅在 NetScaler Console 上配置组。

使用场景：

考虑这样一个场景：一个或多个应用程序（虚拟服务器）托管在同一台服务器上。超级管理员 (George) 希望授予 Steve（应用程序管理员）仅访问 App1 的权限，而不是访问托管服务器的权限。

下表说明了此环境，其中 Server-A 托管应用程序 App-1 和 App-2。

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

主机服务器	应用程序（虚拟服务器）	服务	服务组
服务器 A	App1	应用服务-1	应用服务组-1
服务器 A	App2	应用服务-2	应用服务组-2

注意

NetScaler Console 将虚拟服务器、服务、服务组和服务器视为网络功能实体。实体类型虚拟服务器被称为应用程序。

要将用户权限分配给网络功能实体，George 定义的用户授权如下：

1. 导航到 **帐户 > 用户管理 > 组** 并添加一个组。
2. 在**授权设置**选项卡中，选择“选择应用程序”。
3. 选择**选择单个实体类型**。
4. 选择**所有应用程序**实体类型，并从可用列表中添加 App-1 实体。
5. 单击**创建组**。
6. 在**分配用户**中，选择需要权限的用户。对于此场景，George 选择 Steve 的用户配置文件。
7. 单击**完成**。

通过此授权设置，Steve 只能管理 App-1，而不能管理其他网络功能实体。

注意：

确保**也应用于绑定实体**选项已清除。否则，NetScaler Console 将授予对绑定到 App-1 的所有网络功能实体的访问权限。因此，也会授予对托管服务器的访问权限。

超级管理员可以为每个实体类型指定正则表达式 (regex)。正则表达式存储在系统中，用于更新用户授权范围。当新实体与其实体类型的正则表达式匹配时，NetScaler Console 可以动态地授予用户对特定网络功能实体的访问权限。

为了动态授予用户权限，超级管理员可以在“**授权设置**”选项卡中添加正则表达式。

在此场景中，George 将 `App*` 添加为应用程序实体类型的正则表达式，并且与正则表达式条件匹配的应用程序将显示在列表中。通过此授权设置，Steve 可以访问所有与 `App*` 正则表达式匹配的应用程序。但是，他的访问权限仅限于应用程序，而不限于托管服务器。

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

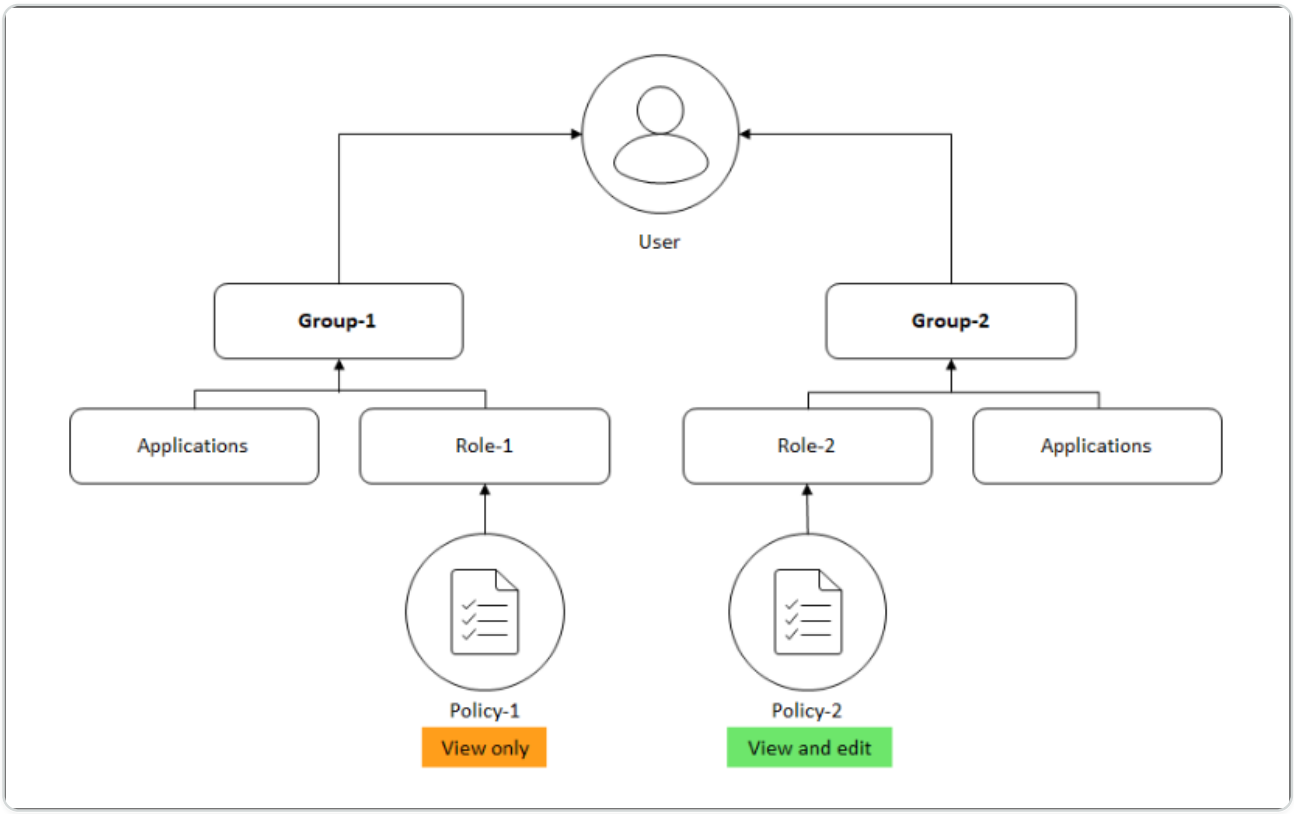
用户访问权限如何根据授权范围而变化

当管理员将用户添加到具有不同访问策略设置的组时，该用户将映射到多个授权范围和访问策略。

在这种情况下，NetScaler Console 根据特定的授权范围授予用户对应用程序的访问权限。

假设一个用户被分配到一个包含两个策略（策略-1 和策略-2）的组。

- **策略-1** – 应用程序的只读权限。
- **策略-2** – 应用程序的查看和编辑权限。



用户可以查看策略-1 中指定的应用程序。此外，该用户可以查看和编辑策略-2 中指定的应用程序。对组-1 应用程序的编辑访问受到限制，因为它不在组-1 授权范围之内。

将 NetScaler Console 从 12.0 升级到更高版本时 RBAC 的映射

将 NetScaler Console 从 12.0 升级到 13.1 时，在创建组时不会看到提供“读写”或“只读”权限的选项。这些权限已被“角色和访问策略”取代，这为您提供了更大的灵活性来为用户提供基于角色的权限。下表显示了 12.0 版本中的权限如何映射到 13.1 版本：

12.0	仅允许应用程序	13.1
管理员读写	否	`admin`
管理员读写	是	`appAdmin`

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

12.0	仅允许应用程序	13.1
管理员只读	否	`readonly`
管理员只读	是	`appReadonly`

配置角色

在 NetScaler Console 中，每个角色都绑定到一个或多个访问策略。您可以在策略和角色之间定义一对一、一对多和多对多的关系。您可以将一个角色绑定到多个策略，也可以将多个角色绑定到一个策略。

例如，一个角色可能绑定到两个策略，其中一个策略定义一个功能的访问权限，另一个策略定义另一个功能的访问权限。一个策略可能授予在 NetScaler Console 中添加 NetScaler 实例的权限，而另一个策略可能授予创建和部署 StyleBook 以及配置 NetScaler 实例的权限。

当多个策略为单个功能定义编辑和只读权限时，编辑权限具有优先权。

NetScaler Console 提供四个预定义角色：

- **admin**。拥有对所有 NetScaler Console 功能的访问权限。（此角色绑定到 adminpolicy。）
- **readonly**。拥有只读访问权限。（此角色绑定到 readonlypolicy。）
- **appAdmin**。仅拥有对 NetScaler Console 中应用程序功能的管理访问权限。（此角色绑定到 appAdminPolicy）。
- **appReadonly**。拥有对应用程序功能的只读访问权限。（此角色绑定到 appReadOnlyPolicy。）

注意：

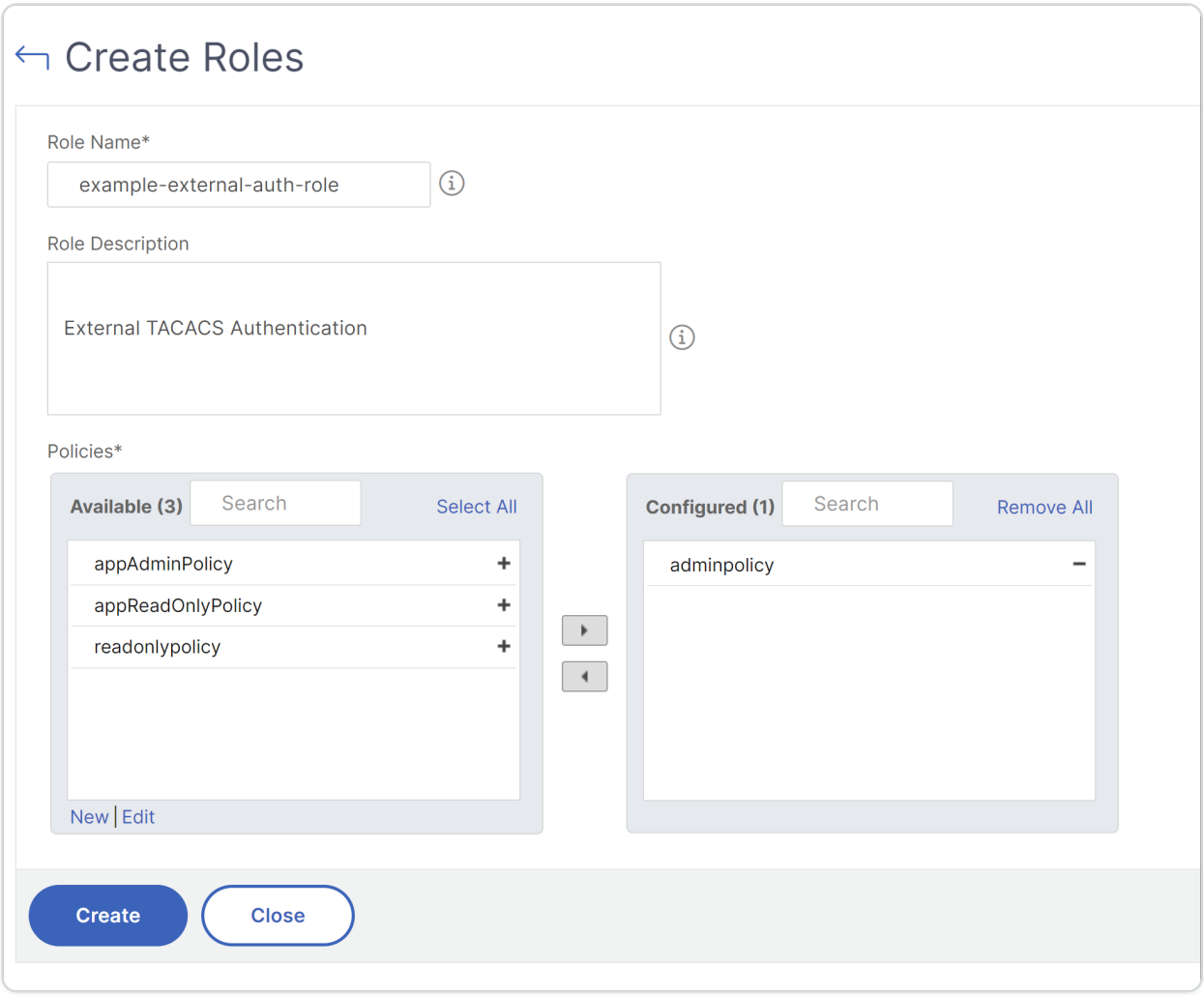
预定义角色无法编辑。

您还可以创建您自己的（用户定义的）角色。

创建角色并为其分配策略：

1. 在 NetScaler Console 中，导航到**设置 > 用户和角色**。
2. 单击**添加**。
3. 在“**角色名称**”字段中，输入角色名称，并在“**角色描述**”字段中提供描述（可选）。
4. 在“**策略**”部分中，添加或移动一个或多个策略到“**已配置**”列表。

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



5. 单击“**创建**”。

配置用户

默认情况下，NetScaler Console 有一个用户：

nsroot - 根用户 (nsroot) 在设备上拥有完全管理权限。nsroot 用户是 NetScaler Console 的超级管理员。

您可以通过为用户配置帐户来创建其他用户。当您向 NetScaler Console 添加新用户时，可以通过分配相应的组、角色和策略来定义他们的权限。

您可以将用户分配给组，并将组绑定到角色。您可以定义用户、组、角色和访问策略之间的一对一、一对多或多对多关系。一个用户可以分配给多个组。一个组可以有多个角色，多个组可以有相同的角色。

在 NetScaler Console 中配置用户：

1. 在 NetScaler Console 中，导航到 **Settings > Users & Roles**。
2. 单击 **Add**。

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

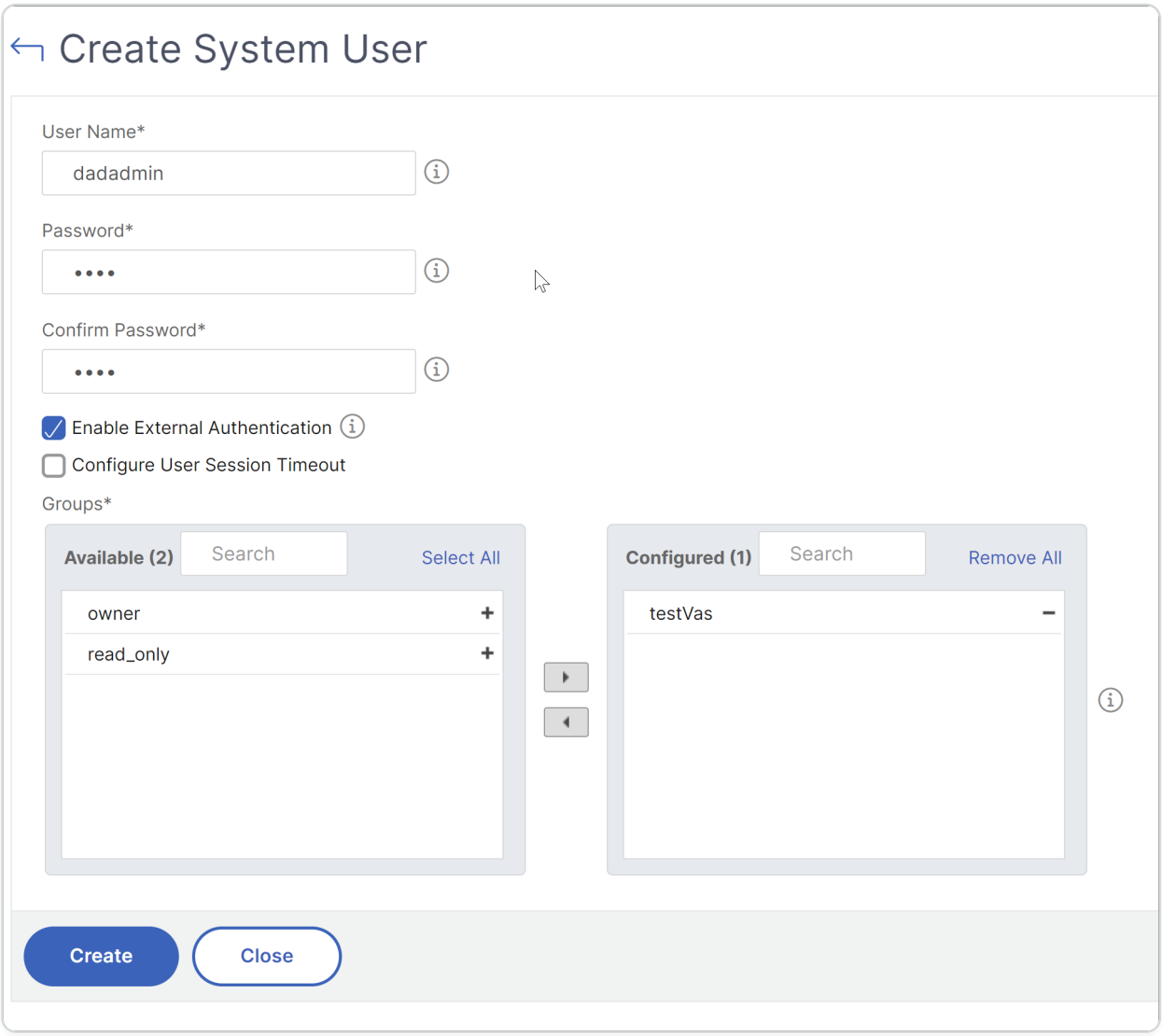
3. 输入以下详细信息：

   a. **User Name**（用户名）。用户的名称

   b. **Password**（密码）。用户登录 NetScaler Console 的密码

4. （可选）选择 **Enable External Authentication**（启用外部身份验证），以便用户可以通过外部身份验证服务器进行身份验证。

5. 如果您已创建组并希望将用户分配给某个组，请在 **Groups**（组）部分中，将一个或多个组从 **Available**（可用）列表移动到 **Configured**（已配置）列表。



6. 单击 **Create**。

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

可操作任务和建议

注意：

- **待办事项**选项卡已重命名为**建议**。在**建议**中，您可以继续查看现有任务，然后单击**引导我**以完成任务。
- **存档**选项卡不再可用。相反，您可以选择从列表中**关闭**建议。

您可能拥有数百个已发现的 NetScaler 实例，并从每个实例配置了多个虚拟服务器（应用程序）。作为管理员，您必须确保所有 NetScaler 实例和您的应用程序都得到高效管理，以获取更好的优先级排序和故障排除见解。

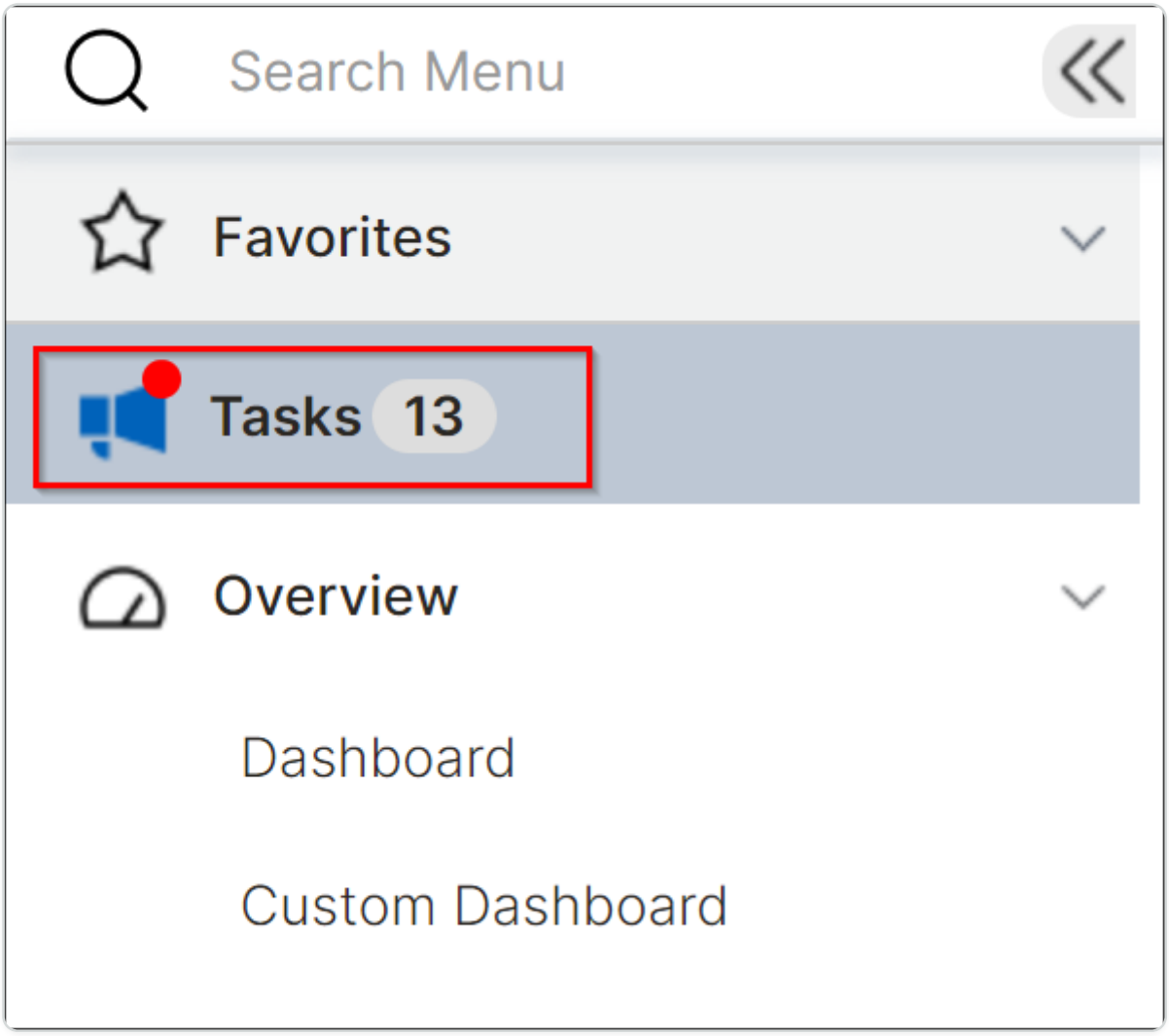
随着您基础设施的进一步扩展，您可能还需要关注影响您的实例和应用程序的需要立即关注的关键问题。您还必须确保您的 NetScaler Console 部署高效、安全且合规。根据您当前的利用率和订阅，NetScaler Console 中的**任务**功能使您能够查看需要立即采取行动的**可操作任务**和确保高效部署的**建议**。

作为管理员，通过利用这些可操作的**任务**和**建议**，您可以：

- 即时了解需要您立即采取行动的任何观察结果或问题。
- 配置通知，以便在 NetScaler Console 检测到任何任务时接收通知并主动采取行动。
- 实现 NetScaler Console 和 NetScaler 实例的高效部署。
- 减少识别关键问题所需的重要时间和精力。
- 确保您正在利用 NetScaler Console 的所有功能，启用产品发现和产品推荐的功能，以实现部署的高效管理。

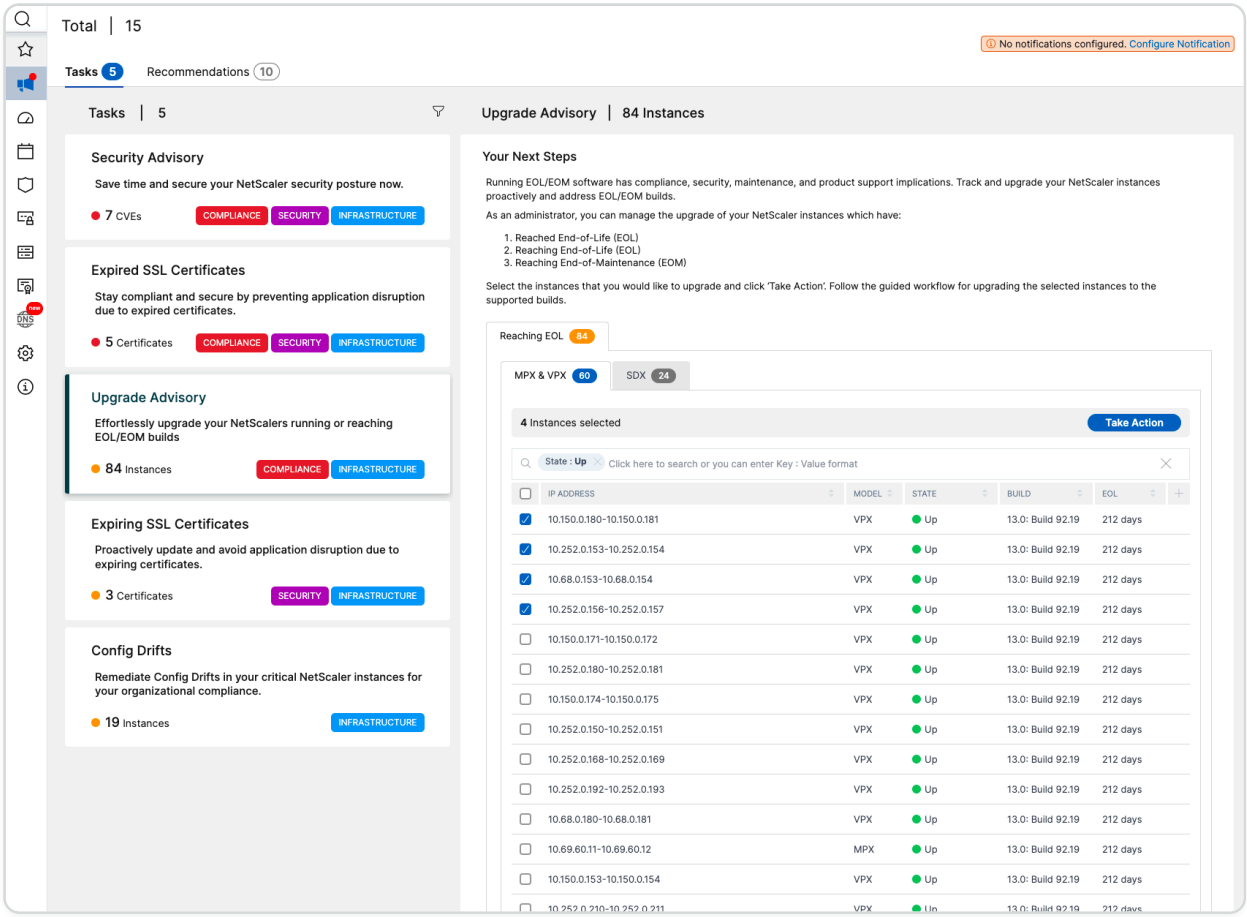
在 NetScaler Console GUI 中，单击**任务**以查看**任务**和**建议**。

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



- **任务** - 使您能够查看需要立即关注和采取行动的任务列表。随着您基础设施的扩展，一些关键问题可能会被忽视，从而导致安全漏洞。例如，具有 CVE 的 NetScaler 实例需要立即关注，您必须立即采取行动，以确保实例在推荐的构建和版本中运行。在**任务**中，您可以立即获得这些见解。根据您当前的利用率，您可以查看总共 4 个任务。任务根据严重性（关键和中等）显示。

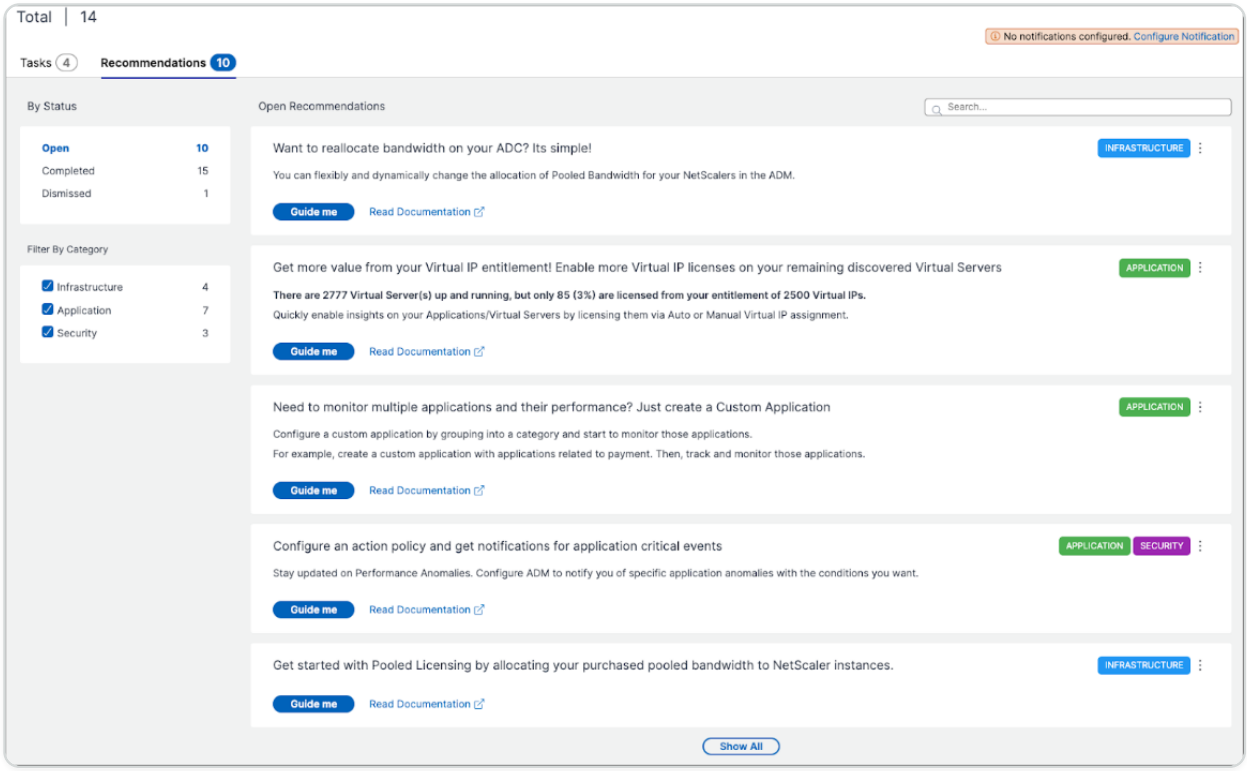
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **建议** - 根据您当前的利用率提供某些建议，以改进您的 NetScaler Console 部署。您可以使用**引导我**选项来完成任何建议。您使用**引导我**选项完成的任何建议都将移至“已完成”。您也可以忽略任何建议，它们将被移至**已忽略**类别下。要查看您已忽略的建议，请使用**按状态**筛选器并选择**已忽略**以查看这些已忽略的建议。

  您还可以使用**按类别筛选**根据类别（基础架构、应用程序和安全性）筛选特定建议。或者，您也可以使用**搜索**栏，键入前几个字符以深入查看任务。

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



任务

在**任务**下，您可以根据当前的 NetScaler Console 部署查看以下 4 个任务。

- **已过期 SSL 证书** – 提供有关安装在 NetScaler Console 中的已过期 SSL 证书的信息。选择此任务以查看以下选项卡：

  - **删除未使用的证书**：显示未在任何 NetScaler 实例中使用的证书。要完成此任务，请查看未使用的证书，选择证书，然后单击**查看和删除**。

    建议操作：您将被重定向到**基础架构 > SSL 控制板 > SSL 证书 - 已过期**。要删除证书，请单击**删除**。如果要更新证书，请选择证书并单击**更新**。有关详细信息，请参阅如何更新已安装的证书。

  - **更新证书**：显示已过期的证书。要完成此任务，请查看证书，选择证书，然后单击**查看和更新**。

    建议操作：您将被重定向到**基础架构 > SSL 控制板 > SSL 证书 - 已过期**。选择证书并单击**更新**或**删除**。有关详细信息，请参阅如何更新已安装的证书。

- **即将过期 SSL 证书** – 提供有关即将过期的 SSL 证书的信息。

  建议操作： 选择此任务以根据到期日前的总天数查看选项卡。要完成此任务，请从选项卡中选择证书，然后单击**查看和更新**。您将被重定向到**基础架构 > SSL 控制板**中的相关页面。选择证书并单击**更新**。有关详细信息，请参阅如何更新已安装的证书。

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

- **配置漂移** – 提供有关 NetScaler 实例中的配置偏差（已保存与正在运行的差异以及模板与正在运行的差异）的信息。选择此任务以查看以下选项卡：
  - **具有未保存配置的实例**：您可以查看具有未保存配置的实例。要完成此任务，请选择实例，然后单击**查看并保存配置**。

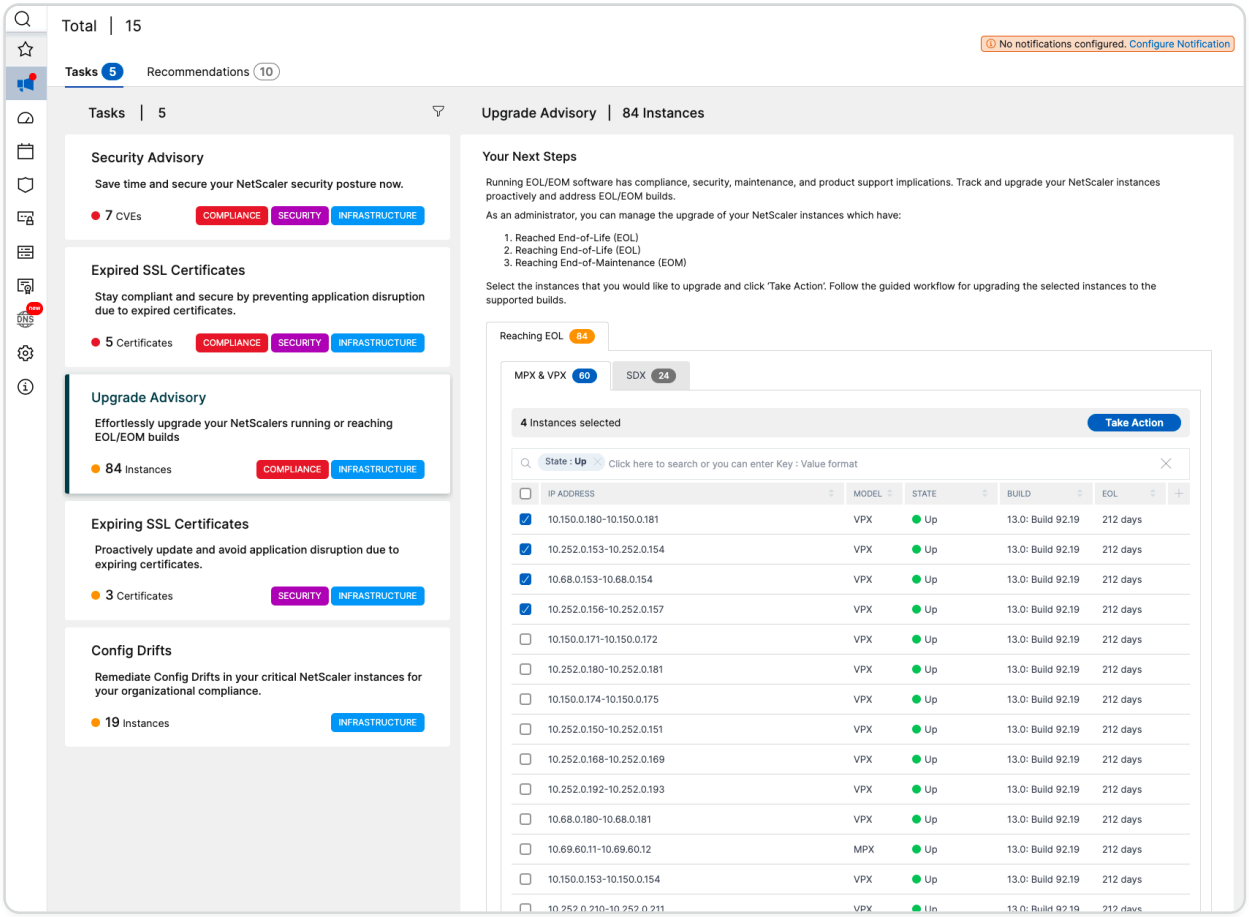
    推荐操作：您将被重定向到**基础设施 > 配置 > 配置审计 > 审计报告**，您可以查看具有未保存配置的实例。单击**保存配置**以完成此任务。有关更多信息，请参阅文档。
  - **模板漂移实例**：您可以查看存在模板偏差的实例。要完成此任务，请选择实例，然后单击**查看并运行正确命令**。

    推荐操作：您将被重定向到**基础设施 > 配置 > 配置审计 > 审计报告**，您可以查看存在模板偏差的实例。按照文档完成此任务。
- **安全通告** – 提供有关影响您的 NetScaler 实例的 CVE 的信息。选择此任务以查看以下选项卡：
  - **检测到的 CVE**：显示检测到的 CVE 以及影响这些 CVE 的 NetScaler 实例。要完成此任务，请选择一个 CVE，然后单击**查看并修复**。

    推荐操作：您将被重定向到**基础设施 > 实例通告 > 安全通告**中的**安全通告**页面。按照文档完成此任务。
  - **受影响的实例**：显示受 CVE 影响的 NetScaler 实例。要完成此任务，请选择实例，然后单击**查看并修复**。

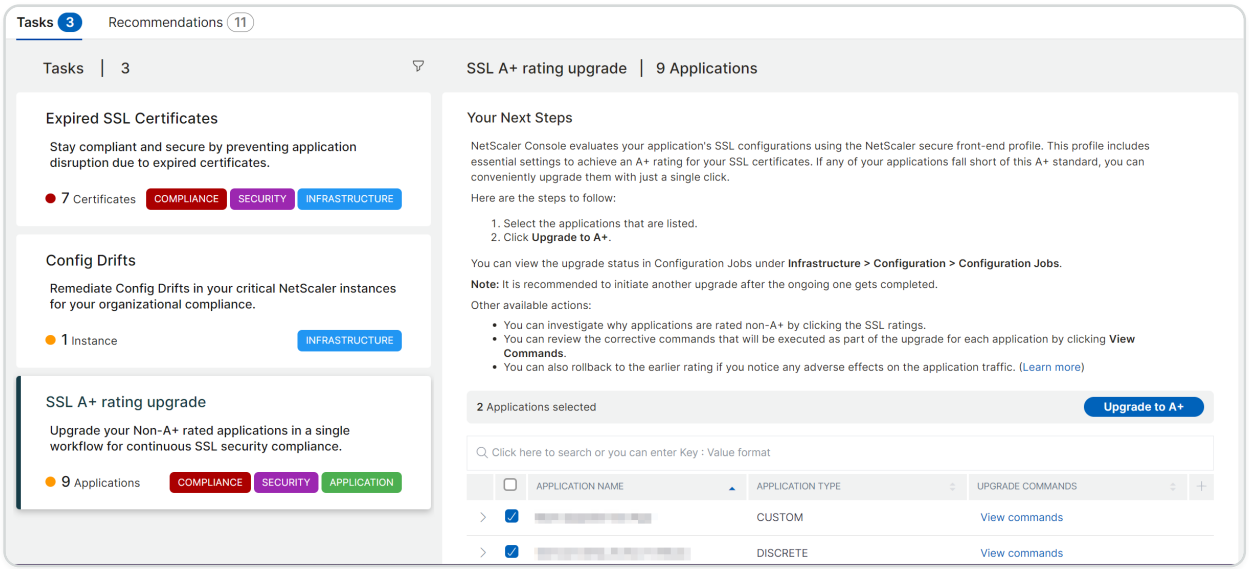
    推荐操作：您将被重定向到**基础设施 > 实例通告 > 安全通告**中的**安全通告**页面。按照文档完成此任务。
- **升级通告**：提供有关您的 NetScaler® 实例的信息，这些实例已达到或即将在 90 天内达到生命周期结束 (EOL) 或维护结束 (EOM)。

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



推荐操作：单击**采取措施**并将实例升级到推荐版本。

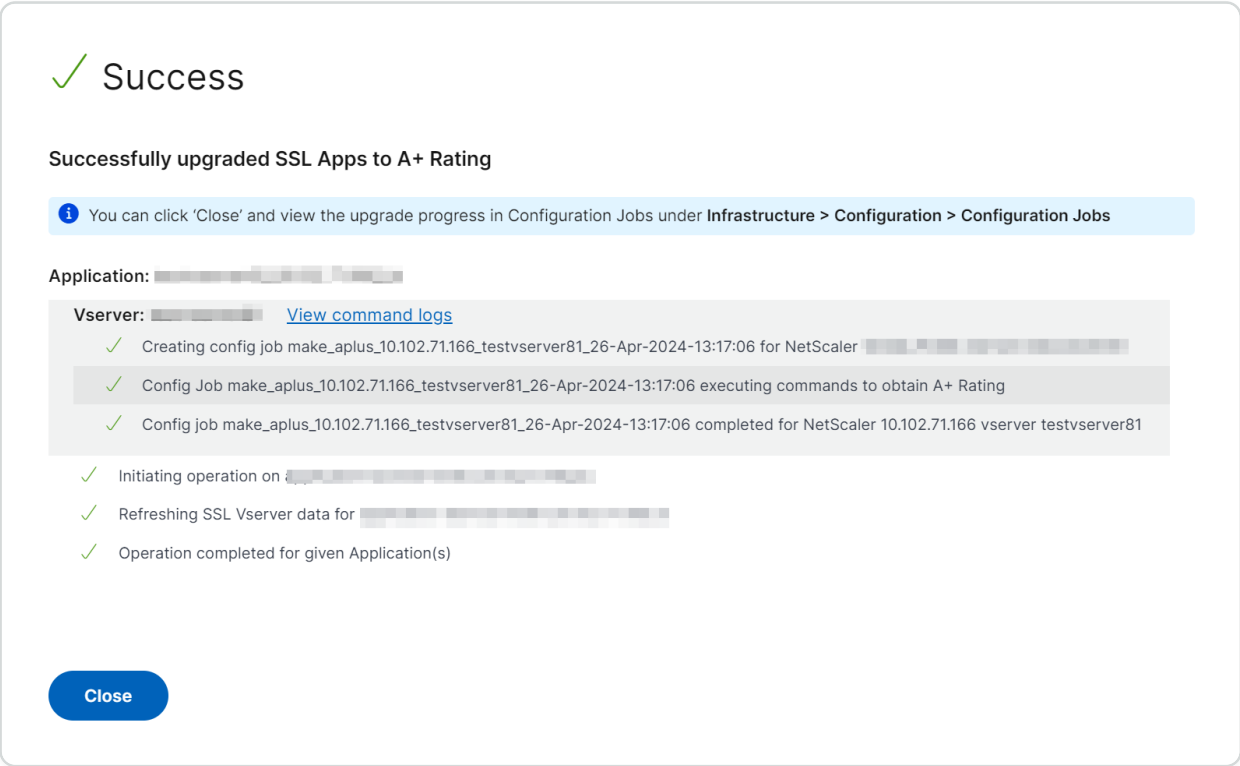
- **SSL A+ 评级升级**：提供有关不符合 A+ 评级的应用程序的信息。



推荐操作：从列表中选择应用程序，然后单击**升级到 A+**。

升级成功后，您将看到以下成功消息：

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



升级完成后，应用程序详细信息将从任务中移除。

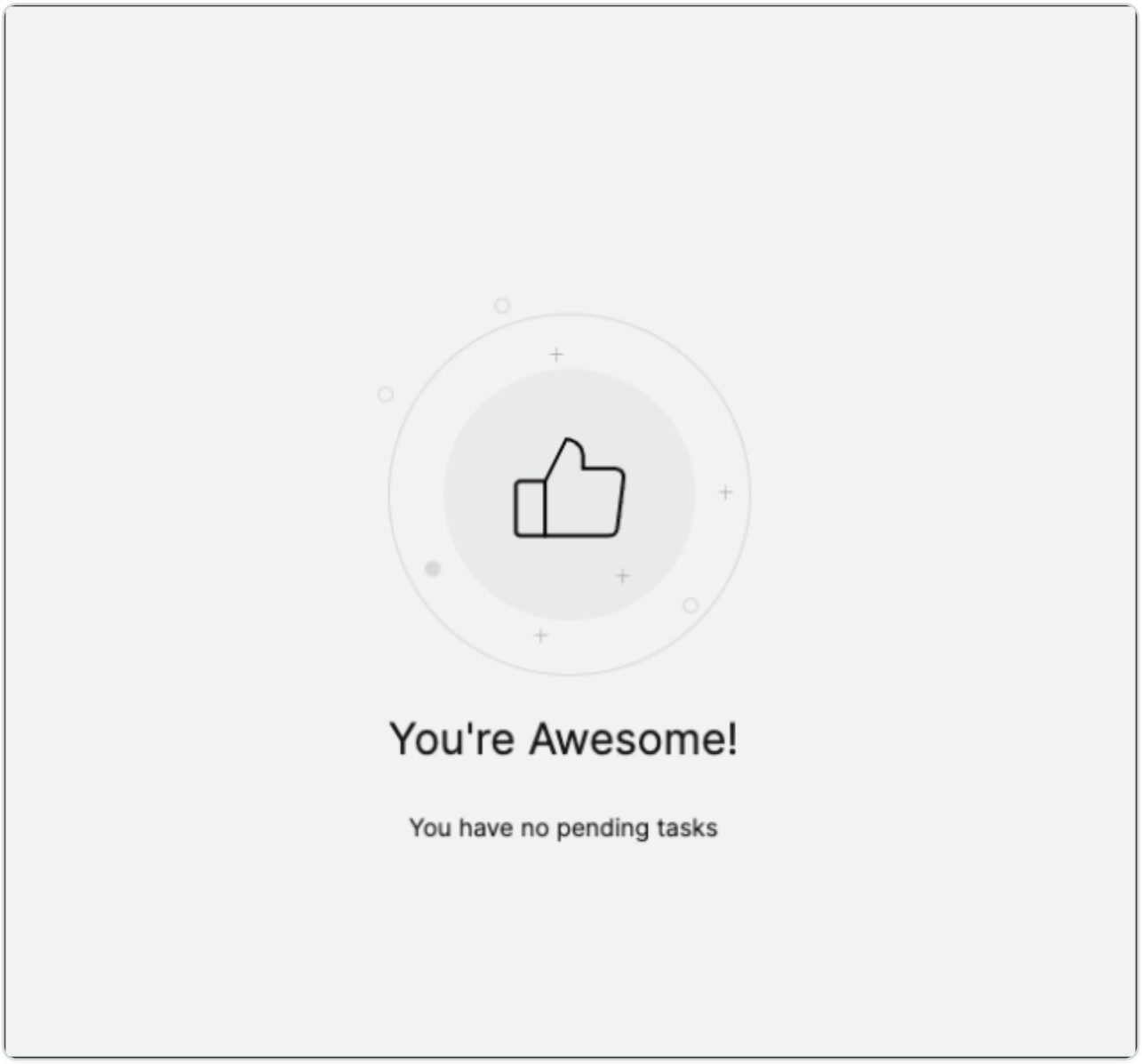
注意事项：

- 根据所选应用程序的数量，升级完成过程的持续时间可能会有所不同。
- 启动升级过程后，建议在当前升级过程完成后再启动另一个升级过程。
- 您还可以在 **Infrastructure > Configuration > Configuration Jobs** 中查看升级过程的状态。
- 如果升级过程不成功，您可以在 **Infrastructure > Configuration > Configuration Jobs** 中查看状态。您可以再次从任务中启动升级过程。
- 如果您执行批量升级，并且一个或多个应用程序未能升级，您只能在任务中查看那些失败的应用程序详细信息。您可以再次启动升级过程以完成。

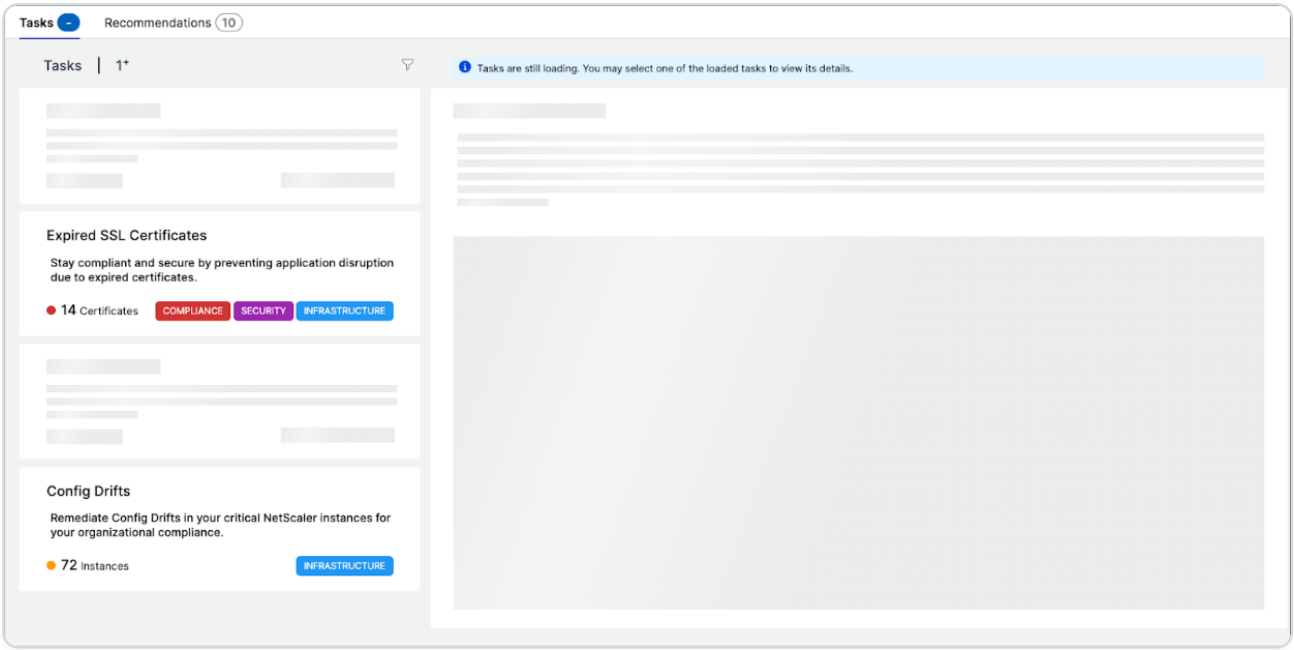
注意：

- 如果您的 NetScaler Console 没有待处理任务，您可以查看以下页面：

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



- 在某些情况下，检查会在所有实例上进行，加载所有任务可能需要额外的时间。



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

建议

下表描述了您可以在 NetScaler Console GUI 中查看的建议：

注意

对于池化许可，您将根据现有的池化许可权益获得建议。

建议名称	任务何时在 GUI 中可见？
添加 NetScaler	在您加入 NetScaler Console 且未发现任何 NetScaler 实例之后。
添加外部代理以利用 NetScaler Console 中的最大功能	如果未配置外部代理。您可以从内置代理开始。但是，需要外部代理才能使用所有功能，例如分析、池化许可等。
将 NetScaler 从内置代理注册到外部代理	在使用 Service Connect 工作流加入 NetScaler Console 后，NetScaler 实例将使用内置代理加入。您可以将这些 NetScaler 实例注册到外部代理，以使用所有功能，例如分析、池化许可等。
想要重新分配 NetScaler 上的带宽？这很简单！	如果池化许可已在 NetScaler GUI 中分配，并且这些 NetScaler 实例已在 NetScaler Console 中发现，则可以使用 NetScaler Console 进行重新分配。
为您的关键企业用户启用精细的基于角色的访问	如果尚未在 NetScaler Console 中配置基于角色的访问控制 (RBAC)。
配置规则，绝不会错过 NetScaler 实例上的任何关键事件	如果尚未配置自定义事件规则。
需要监控多个应用程序及其性能？只需创建自定义应用程序。	如果尚未配置自定义应用程序。
通知并确保不会错过应用程序中的关键事件	如果尚未为应用程序分数偏差、服务器处理时间、客户端网络延迟、服务器网络延迟或响应时间配置操作策略。

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

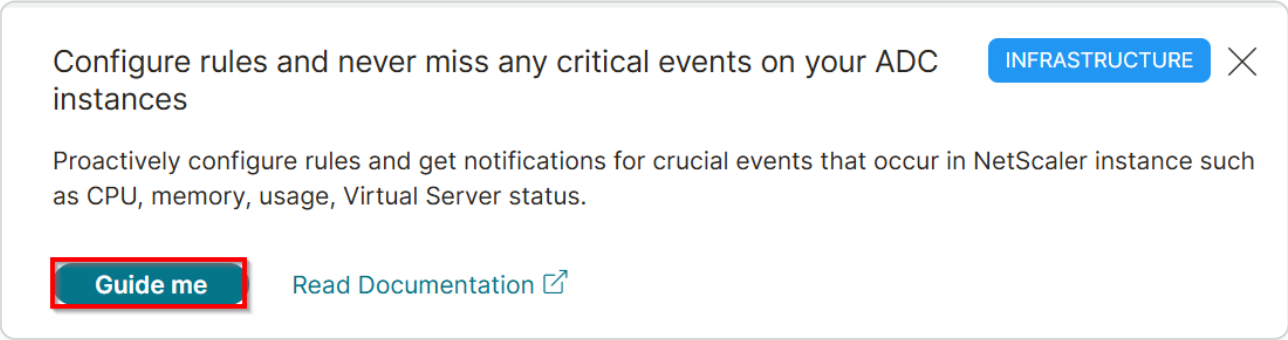
建议名称	任务何时在 GUI 中可见？
避免应用程序中断，确保不会错过应用程序中即将过期的 SSL 证书	如果尚未为即将过期的 SSL 证书配置警报或通知。
安全公告 - 使您的 NetScaler 实例与 CVE 和缓解措施保持同步	如果 NetScaler 实例受到任何 CVE 影响。
配置企业策略并监控任何偏差	如果 SSL 企业设置未更改或仍为默认设置。
手动重复任务？创建配置作业并将其应用于多个 NetScaler 实例	如果尚未配置 **配置作业** 任务。
通过选择您选择的自定义指标来管理和监控您的实例分数。	如果 **实例分数设置** 中的默认设置和阈值未修改。
通过选择您选择的自定义指标来跟踪您的应用程序分数。	如果应用程序仪表板中的应用程序分数组件使用默认设置且未进行任何自定义。
添加私有 IP 块以在地理地图中可视化客户端请求	如果未配置 IP 块。您可以创建 IP 块，以便根据客户端的私有 IP/范围在地理地图上映射和可视化客户端请求。
订阅并将您的 AppSec 违规行为实时导出到 Splunk	如果尚未配置 NetScaler Console 中的 Splunk 集成。
为您的 Kubernetes 服务自定义默认阈值或创建新阈值	如果服务图中仅使用默认阈值，并且未对服务应用单个或双重阈值。
主动配置通知配置文件并在您的通信目的地接收通知	如果尚未配置通知配置文件。
安排定期导出并获取有关基础架构详细信息的通知	如果尚未在 **基础架构 > 实例** 中配置导出计划。
拥有 ServiceNow 并希望与 NetScaler Console 集成？	如果尚未配置 NetScaler Console 中的 ServiceNow 集成。
使用 Venafi 和 NetScaler Console 自动执行 SSL 证书管理	如果 Venafi 服务器尚未在 NetScaler Console 中配置。
在池化许可证到期前续订。	如果现有许可证将在 30 天内到期。

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

建议名称	任务何时在 GUI 中可见？
通过将购买的池化带宽分配给 NetScaler 实例来开始使用池化许可。	如果您尚未开始分配池化许可证权益。
考虑购买更多池化带宽容量。	如果您已使用 90% 或更多的池化带宽权益。
您当前的池化带宽权益未充分利用。请查看并考虑分配更多	如果您的池化许可证分配利用率低于 70%。

如何使用“引导我”工作流并完成建议?

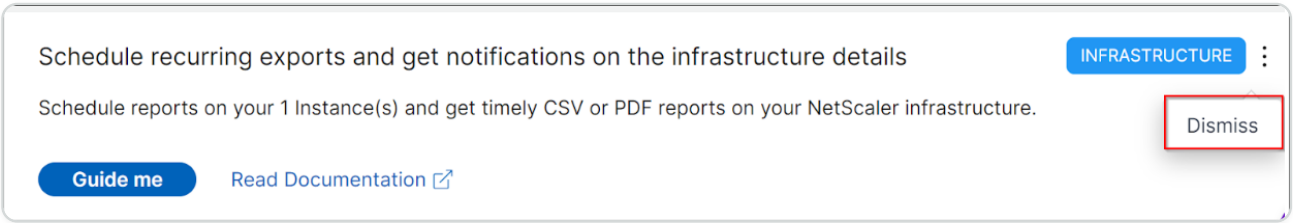
假设您要为任何事件配置规则。单击以下任务的“**引导我**”：



单击“**引导我**”后，您将被重定向到“**基础架构 > 事件 > 规则**”。单击“**添加**”以创建规则。有关详细信息，请参阅创建事件规则。

完成规则创建后，建议即完成，并移至“**已完成**”。

同样，如果您想稍后完成任何建议，可以从列表中选择“**忽略**”，它将被移至“**已忽略**”。



配置通知

每当 NetScaler Console 识别出需要您立即采取行动的任何未完成任务时，您都可以配置并获取通知。如果您尚未配置通知，可以单击右上角的**配置通知**。

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

在**通知**页面中，您可以为**电子邮件**和 **Slack** 配置配置文件，然后单击**保存**以接收通知。对于每种通知类型，NetScaler Console GUI 都会显示已配置的分发列表或配置文件。NetScaler Console 会将通知发送到选定的分发列表或配置文件。

常见问题

1. 管理员会收到哪些类型的建议？

   目前，这些建议专门针对部署，旨在帮助管理员更好地完成配置和设置任务，从而提高部署效率。它还有助于更好地发现产品，管理员无需任何先验知识，也无需知道 NetScaler Console 中是否存在该功能，即可了解任务的作用以及它如何提供帮助。

2. 如果我驳回任何建议，会发生什么？

   您驳回的建议将移至**已驳回**。您可以稍后完成这些建议。

3. 如果我开始引导式操作并中途退出，建议会进入**已完成**状态吗？

   不会，除非操作已保存或完成，否则建议不会完成。

4. 我可以执行搜索或筛选吗？

   可以！您可以使用搜索栏，或通过从列表中选择类别来缩小到特定任务。

5. 我是否会收到针对动态事件采取行动的任务？

   是的！目前您可以查看总共 4 个可操作任务。有关更多信息，请参阅 任务。

6. 即使我没有在 NetScaler Console 中添加 NetScaler 实例，所有可操作任务和 20 多个建议也会显示吗？

   不。您必须在 NetScaler Console 中同时拥有 NetScaler 实例和虚拟服务器，才能显示所有任务和建议。

7. 任务多久刷新一次？

   当您从左侧导航窗格中单击 **任务** 时，它们会刷新并以最新状态显示。详细信息会被获取并更新。

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

统一仪表板，用于查看实例关键指标详细信息

在 NetScaler Console 中，您可以查看有关应用程序使用情况和性能、NetScaler 基础架构、安全（Bot 和 WAF）违规等方面的各种洞察。作为管理员，您可能需要导航到 NetScaler Console GUI 中的各种选项才能查看多个洞察。例如，要检查虚拟服务器（应用程序）和 NetScaler 实例洞察：

- 您必须首先导航到 **应用程序 > 仪表板** 以查看应用程序的洞察。
- 然后，您必须导航到 **基础架构 > 基础架构分析** 以查看 NetScaler 实例的洞察。

为了获得更好的监控体验，您需要拥有一个包含所有所需洞察概览的权限。导航到 **概览 > 仪表板** 以可视化一个单窗格仪表板，其中包含基于以下类别的关键指标详细信息概览：

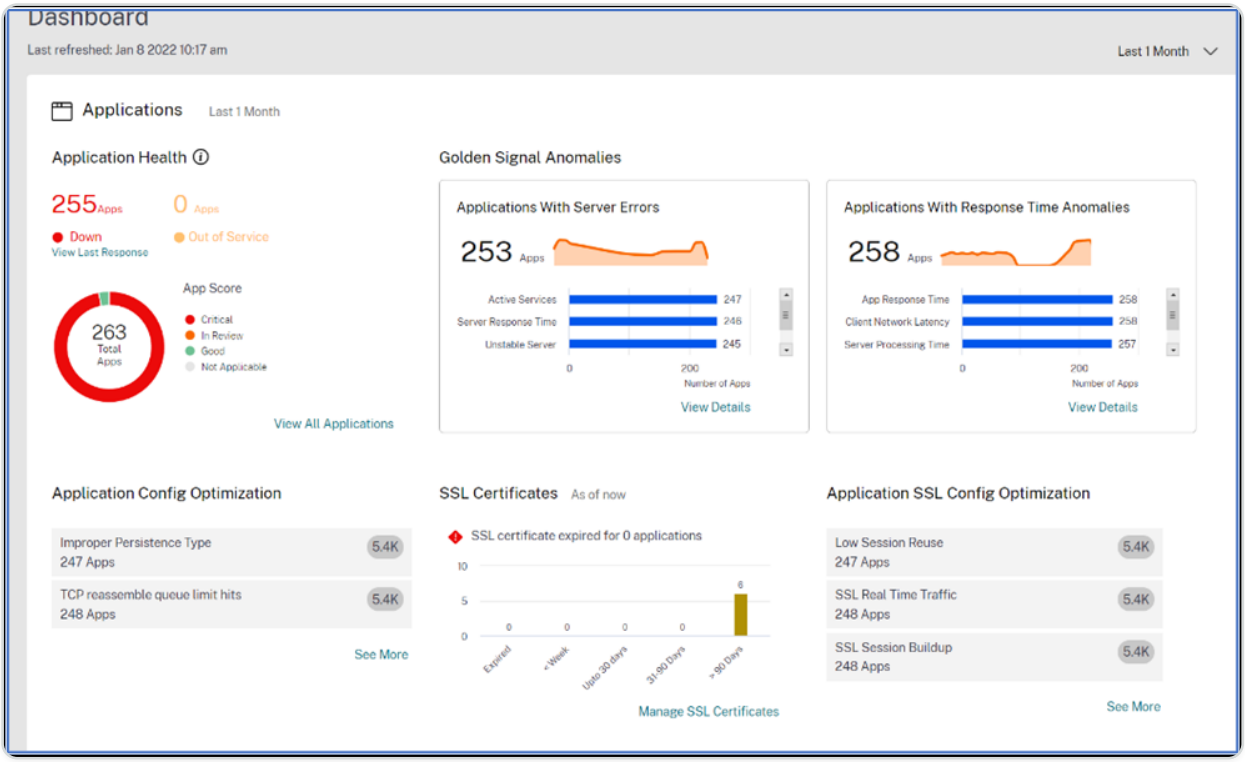
- 应用程序
- NetScaler 基础架构
- 应用程序安全
- 网关

应用程序

在 **应用程序** 下，您可以查看：

- **应用程序运行状况** – 提供处于**关闭**和**停止服务**状态的应用程序概览，并根据其状态（例如**严重**、**审核中**、**良好**和**不适用**）进行分类。单击**查看所有应用程序**可在应用程序仪表板中查看详细信息。
- **黄金信号异常** – 提供具有服务器错误和响应时间异常的应用程序概览。单击**查看详细信息**以获取更多信息。
- **应用程序配置优化** – 提供具有性能问题的应用程序总数概览。单击**查看更多**可在应用程序仪表板中查看问题详细信息。
- **SSL 证书** – 提供 SSL 证书及其有效期的概览。单击**管理 SSL 证书**可在 SSL 仪表板中查看更多信息。
- **应用程序 SSL 配置优化** – 概述了存在 SSL 相关问题的应用程序总数。单击**查看更多**以查看问题详细信息。

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



NetScaler 基础架构

在**NetScaler 基础架构**下，您可以查看以下 NetScaler 实例相关的关键指标：

- **NetScaler 实例运行状况** – 根据实例分数概述了 NetScaler 实例总数。
- **受 CVE 影响的 NetScaler 实例** – 概述了受常见漏洞和披露 (CVE) 影响的 NetScaler 实例总数。
- **NetScaler 实例问题** – 根据问题类别概述了 NetScaler 实例问题。有关详细信息，请参阅基础架构分析。
- **NetScaler 实例升级摘要** – 概述了未运行最新版本的 NetScaler 实例总数。单击“查看 NetScaler 实例控制面板”以获取更多信息。

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

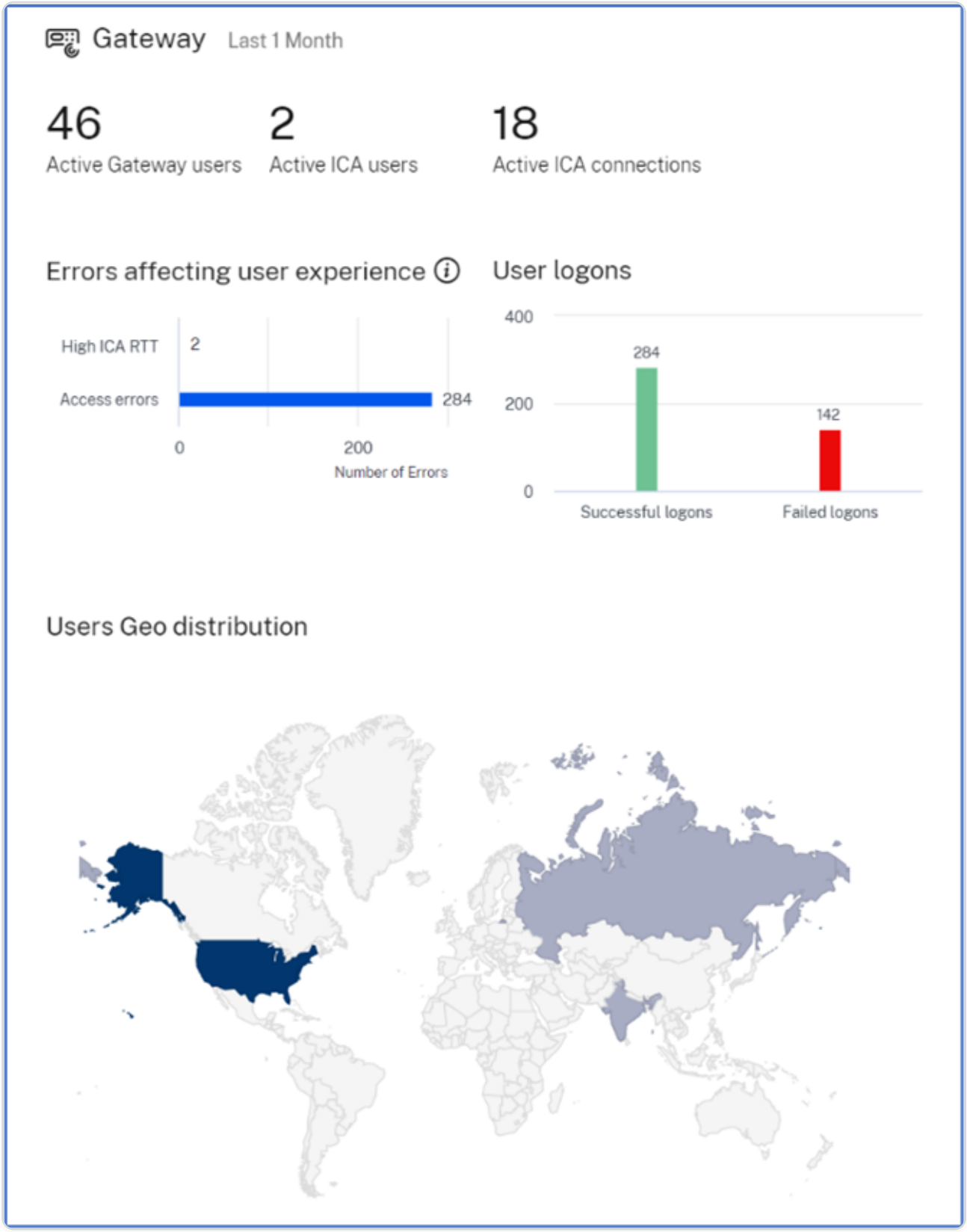
应用程序安全性

概述了所选持续时间内报告的受影响应用程序总数和违规总数（Bot 和 WAF）。单击**查看安全控制面板**以查看安全和 Bot 违规详细信息。

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

网关

概述了活动网关用户总数、活动 ICA® 用户总数和活动 ICA 连接总数。您还可以查看错误、用户登录详细信息以及提供用户位置详细信息的地理地图。



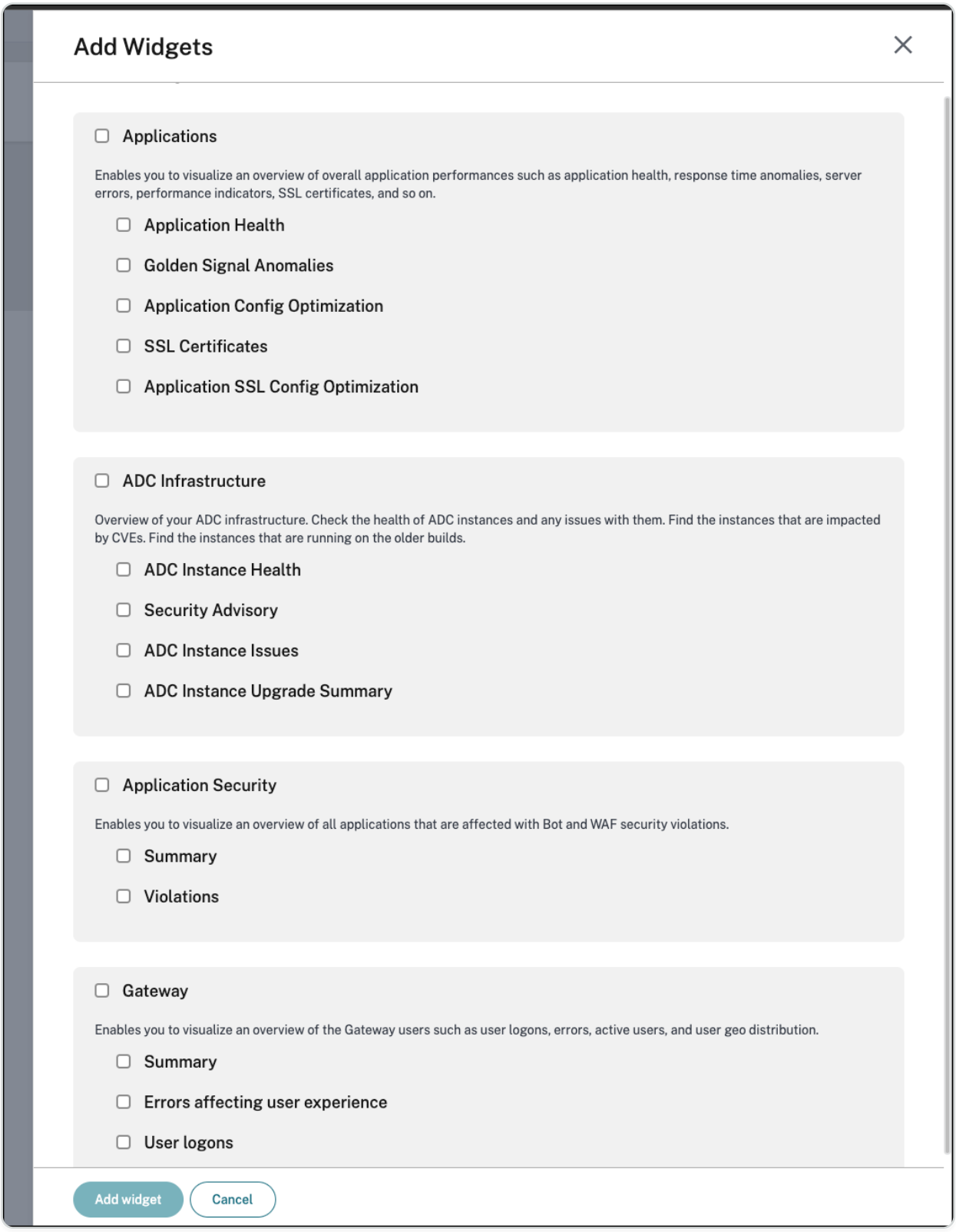
© 1997–2026 Citrix Systems, Inc. All rights reserved.

自定义仪表板

您可以使用**编辑仪表板**选项，根据您的选择自定义仪表板视图。使用**编辑仪表板**选项，您可以：

- 拖动小组件
- 删除整个小组件（应用程序、NetScaler 基础架构、网关或应用程序安全）。
- 删除每个小组件下的小型小组件。
- 单击**添加小组件**并选择您希望在每个小组件下查看的所需关键指标。

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



- 重置为默认值
- 重置为上次保存

进行更改后，单击**保存**。

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

注意

- 默认情况下，所有小组件都会显示。如果您自定义仪表板，保存更改，然后再次使用**重置为默认值**选项，所有小组件都将添加到仪表板中。
- **重置为上次保存**选项将加载之前保存的配置。

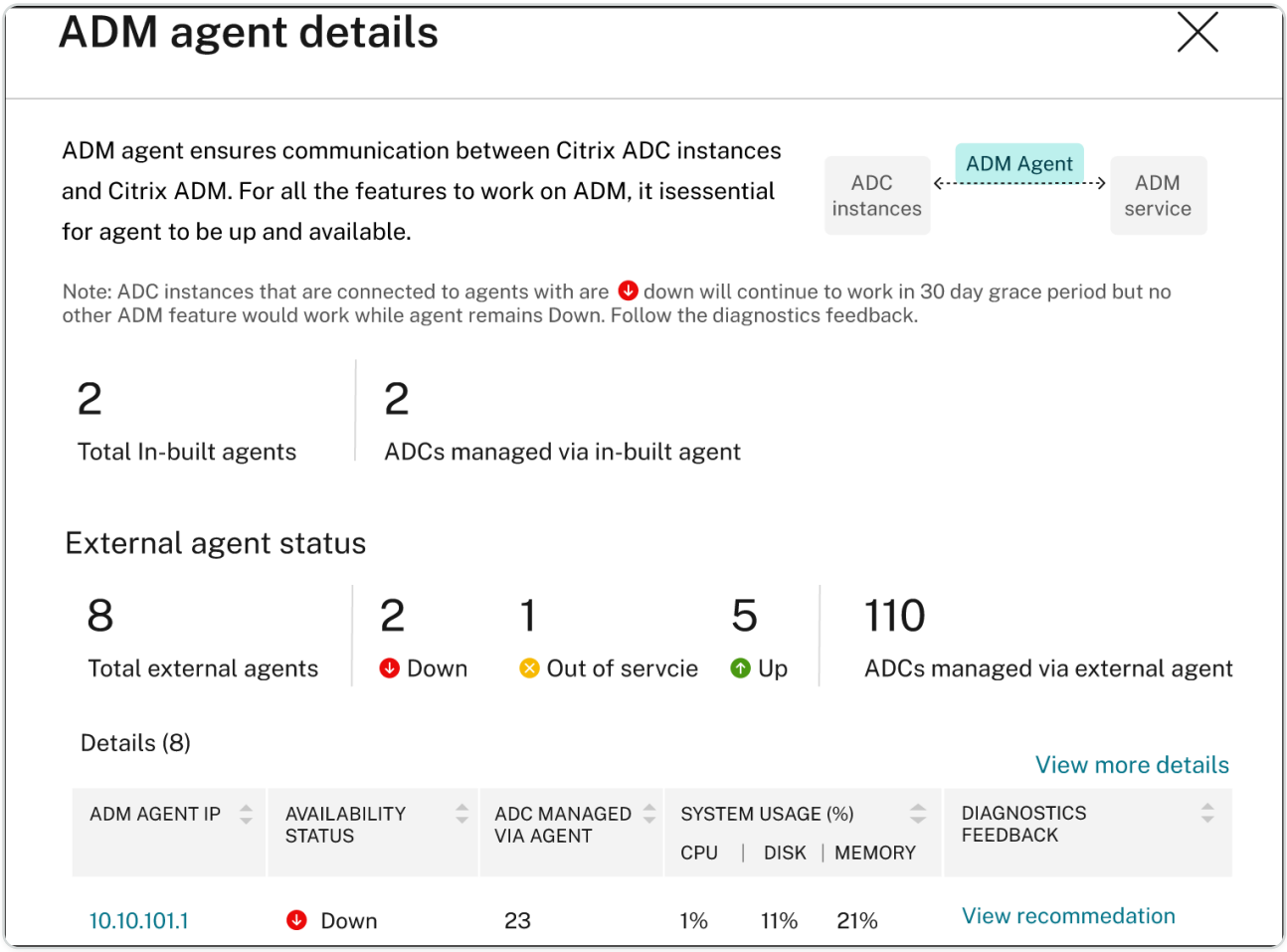
查看代理详细信息

在统一仪表板中，您可以可视化代理详细信息的概览。在**概览 > 仪表板**中，在**NetScaler® 代理状态**旁边，您可以查看以下状态，这使您能够分析代理的整体可用性：

- **全部可用**。表示所有代理都已启动并正在运行。
- **全部不可用**。表示所有代理都已关闭且无法访问。
- **不可用**。表示少数代理已关闭且无法访问。
- **全部停止服务**。表示所有代理都已停止服务。
- **停止服务**。表示少数代理已停止服务。
- **未找到外部代理**。表示未配置任何代理（通过任何虚拟机管理程序）。

单击**查看详细信息**以可视化代理详细信息概览，例如内置代理总数、外部代理总数、代理 IP、状态、系统使用情况、诊断检查等。

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



创建并应用筛选器

您可以应用筛选器并仅查看以下内容中选定实例或应用程序的洞察信息：

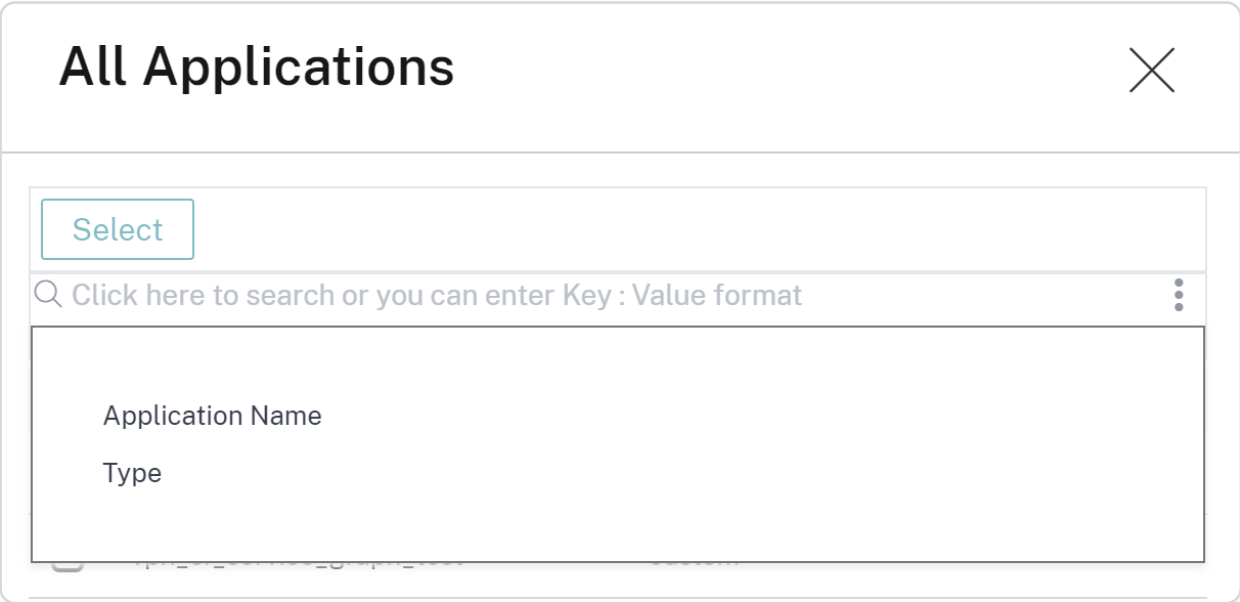
- 应用程序
- NetScaler 基础架构
- 应用程序安全

默认情况下，所有应用程序均已选中。您可以通过单击磁贴中可用的筛选器图标，从控制板创建自定义筛选器。

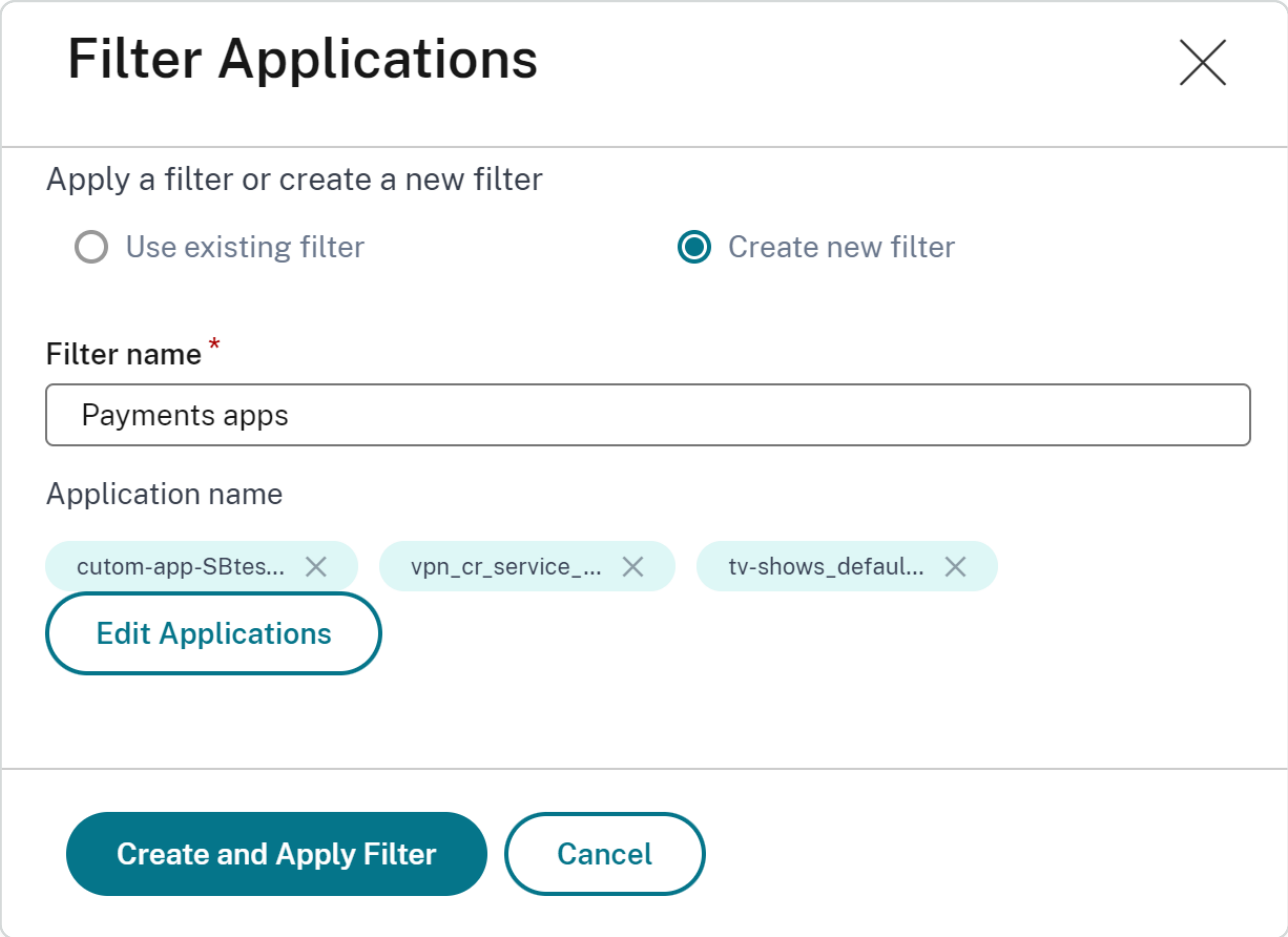
在**筛选应用程序**窗口中：

1. 选择 **创建新筛选器**。
2. 根据您的选择提供筛选器名称。
3. 单击 **选择应用程序**，并添加筛选器所需的所有应用程序。选择应用程序时，您还可以使用筛选器（**应用程序名称** 和 **类型**），然后选择应用程序。

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

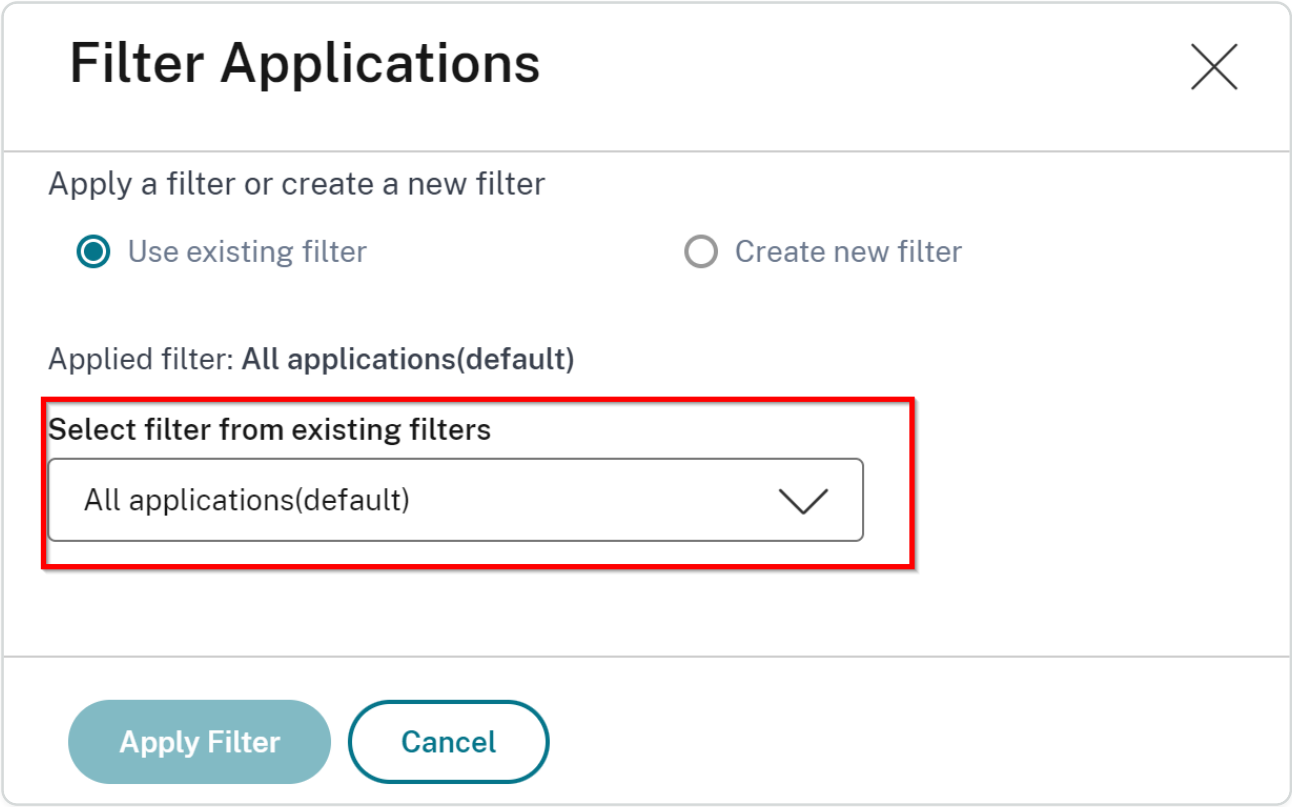


4. 单击 **创建并应用筛选器**。



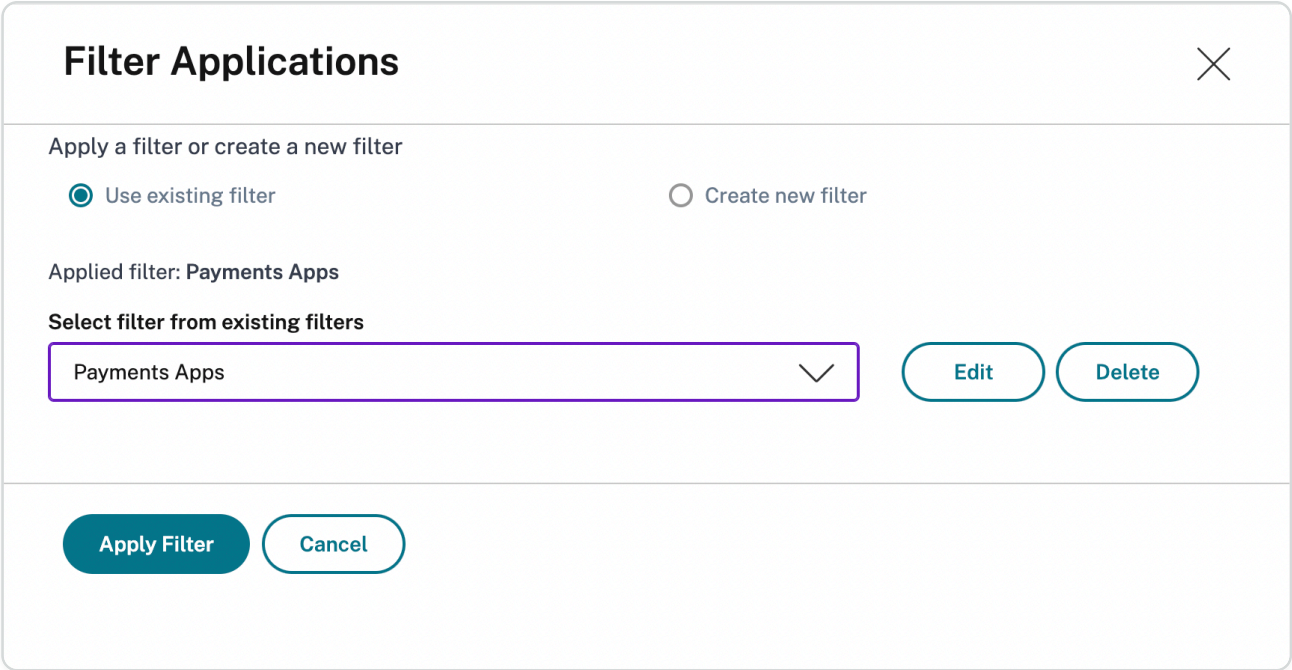
筛选器现已创建并应用。您可以按照相同的步骤创建更多筛选器。创建筛选器后，您可以通过 **从现有筛选器中选择筛选器** 列表选择并应用筛选器。

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



编辑筛选器

您可以通过从列表中选择筛选器并单击 **编辑** 来编辑筛选器。使用编辑选项，您可以添加或删除应用程序，然后更新筛选器。



要删除筛选器，请从列表中选择筛选器并单击 **删除**。

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

注意

当您创建包含应用程序的筛选器时，如果其中一个应用程序在应用程序仪表板中被删除，则该应用程序的详细信息将立即从统一仪表板中删除。

创建自定义仪表板以查看实例关键指标详细信息

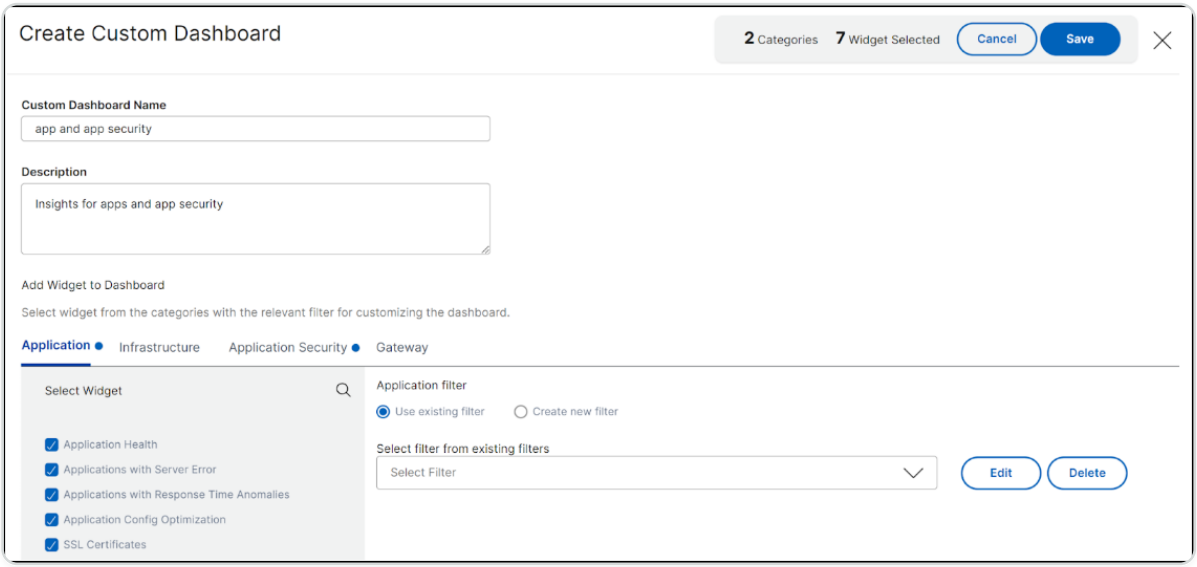
与统一仪表板（**概览 > 仪表板**）类似，您可以通过创建自定义仪表板来根据自己的选择查看实例指标详细信息。您最多可以创建 30 个仪表板，每个仪表板使用一个唯一的名称。作为管理员，此增强功能使您能够创建多个仪表板并仅监控所需的实例洞察。

首先，假设您要监控 **应用程序** 和 **应用程序安全** 的关键指标：

1. 导航到 **概览 > 自定义仪表板**。
2. 单击 **+** 创建新仪表板。

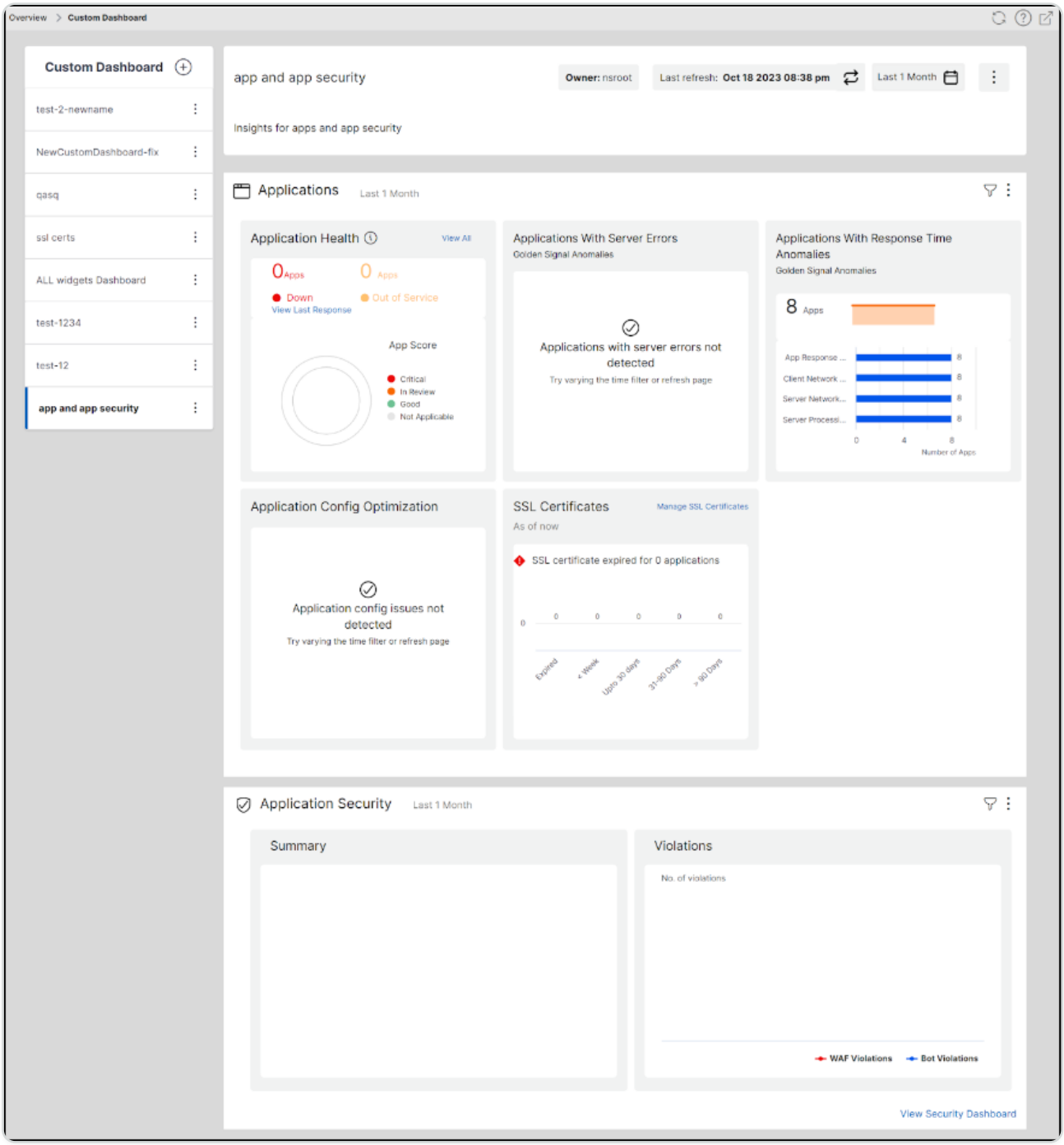
   在 **创建自定义仪表板** 页面中：

   a. **自定义仪表板名称** - 为仪表板指定一个唯一的名称。
   b. **描述** - 提供简要描述以获取更多详细信息。
   c. **将小组件添加到仪表板** - 在此示例中，要求是为应用程序和应用程序安全添加小组件。从 **应用程序** 和 **应用程序安全** 类别中选择您要监控的小组件。
   d. **应用程序筛选器** - 默认情况下，筛选器应用于所有应用程序。您还可以创建筛选器并仅选择特定的应用程序。有关更多信息，请参阅 创建和应用筛选器。
   e. 单击 **保存**。



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

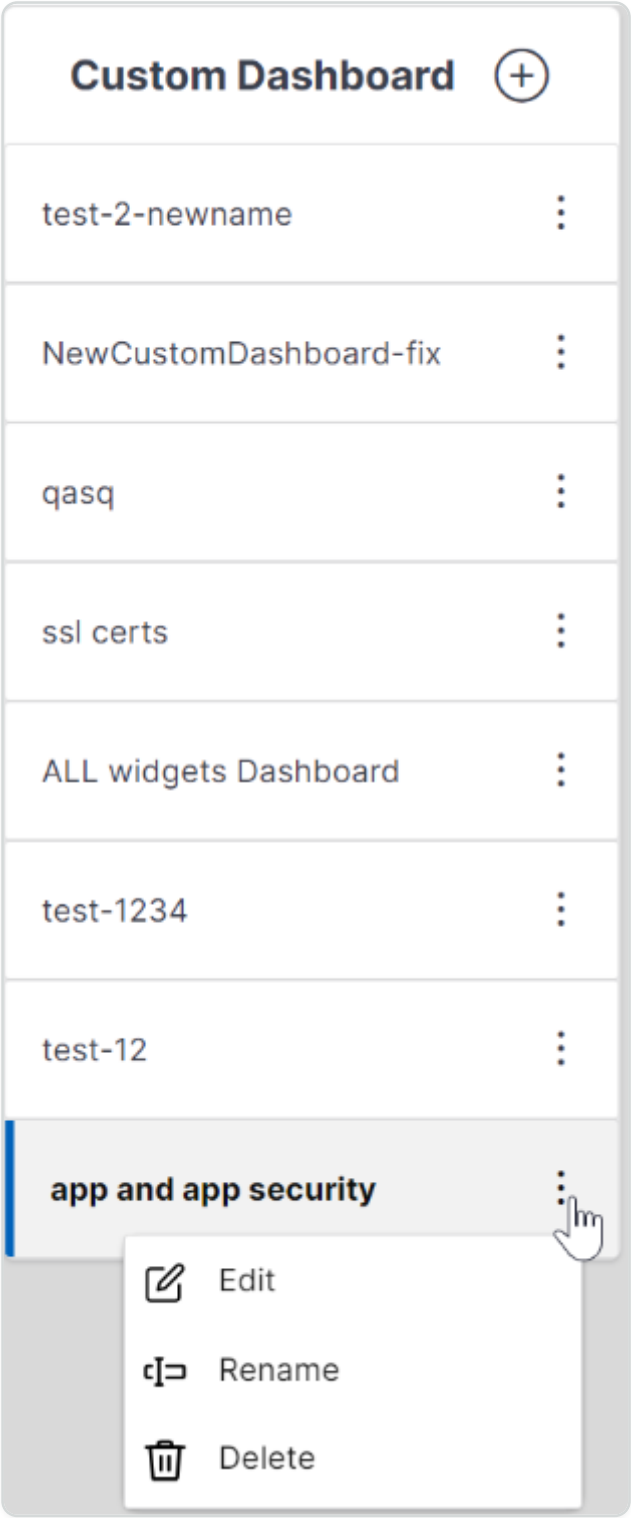
仪表板已成功创建。同样，您最多可以创建 20 个仪表板，并通过为每个仪表板指定唯一的名称来根据自己的选择选择类别。



创建自定义仪表板后，您可以使用以下选项：

- **编辑**：您可以通过添加或删除小组件、应用筛选器等方式编辑仪表板。
- **重命名**：您可以更改仪表板名称。
- **删除**：您可以删除仪表板。

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

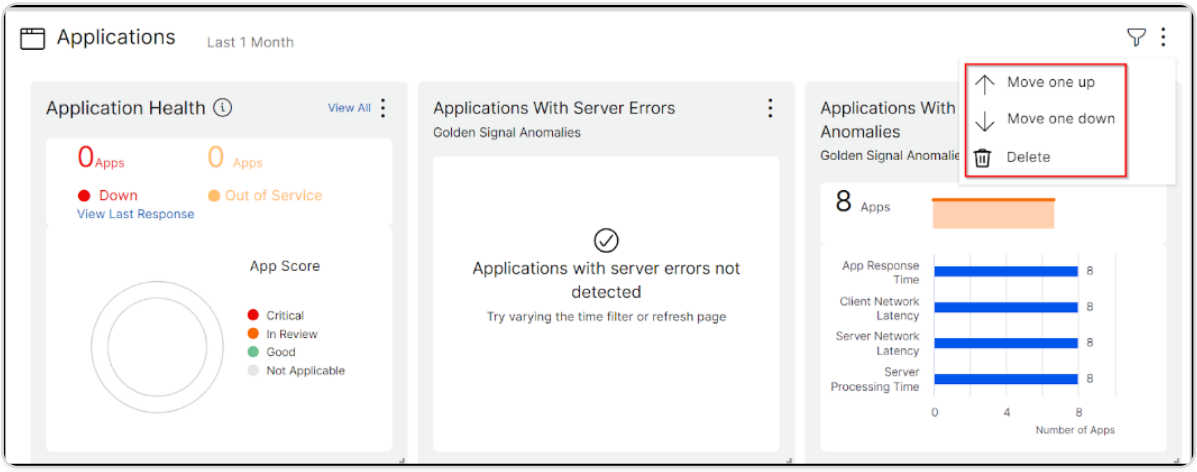


仪表板中的更多选项

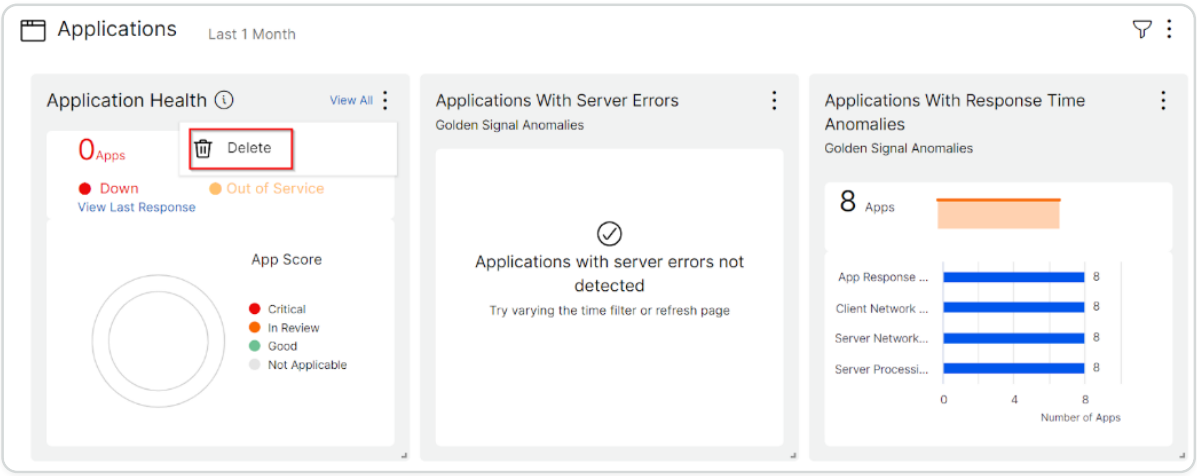
在您创建的自定义仪表板中，可以使用以下选项：

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

- **编辑配置**：您也可以使用此选项通过添加或删除小组件、应用筛选器等方式编辑仪表板。
- **编辑布局**：您可以使用此选项对仪表板进行额外自定义。
  - 您可以选择向上、向下移动或删除。



  - 在小组件中，您可以通过选择“删除”选项来删除任何小组件。



  - 拖放小组件到您想要的任何位置。
  - 增大或减小小组件大小，以便更好地查看某些洞察。

    仪表板更改(/en-us/netscaler-application-delivery-management-software/media/custom-dashboard-customize.png)

进行更改后，单击 **保存** 以查看更新后的仪表板。

将仪表板共享给其他用户

您可以将仪表板共享给其他用户。选择一个现有仪表板，然后单击 **共享**。键入用户名，然后单击 **邀请** 以共享仪表板。被分配的用户可以以只读模式查看仪表板。

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

应用程序

NetScaler Console 的应用程序分析和管理功能使您能够通过以应用程序为中心的方法监控应用程序。此方法可帮助您：

- 检查分数并分析应用程序的整体性能
- 检查服务器或客户端是否存在任何持续性问题
- 检测应用程序流量中的异常并采取纠正措施

> **注意**
>
> 应用程序是指在实例 (NetScaler) 上配置的一个或多个虚拟服务器。

您可以监控应用程序的时长，例如 1 小时、1 天、1 周和 1 个月。

先决条件

- 确保您已在 NetScaler Console 中添加 NetScaler 实例
- 确保您的 NetScaler 实例具有有效的许可证。有关详细信息，请参阅 许可
- 确保您已为虚拟服务器应用许可证。有关详细信息，请参阅 管理虚拟服务器上的许可

应用程序概述

应用程序可以是：

- 离散应用程序
- 自定义应用程序
- 微服务应用程序 (k8s_discrete)

离散应用程序

所有已获得许可的虚拟服务器均称为离散应用程序。

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

自定义应用程序

一个类别下的虚拟服务器称为自定义应用程序。作为管理员，您必须根据类别添加自定义应用程序。然后，您可以通过控制板管理和监视应用程序。您可以轻松监视分组在一个类别下的特定应用程序。

例如，您可以为数据中心1创建一个类别并添加其NetScaler实例。定义类别并为数据中心1添加实例后，应用程序控制板将显示一个单独的类别，其中包含与数据中心1相关的所有应用程序。

注意事项

- 添加到自定义应用程序的离散应用程序将从离散应用程序中移除。
- 所有未添加到任何类别的应用程序都将显示为 **“其他”**。
- 默认情况下，NetScaler Console 允许您为最多 2 个应用程序添加许可证。根据您的许可证，您可以选择并应用您想要监视的应用程序的许可证。

微服务应用程序

在 Kubernetes 集群中，NetScaler 为 NetScaler MPX（硬件）、NetScaler VPX（虚拟化）和 NetScaler CPX（容器化）提供 Ingress Controller。有关更多信息，请参阅 NetScaler Ingress Controller。

使用 NetScaler CPX 实例配置的离散应用程序称为微服务应用程序。

应用程序管理和应用程序仪表板

NetScaler Console 允许您从“**应用程序**”页面管理应用程序，并从“**仪表板**”页面查看应用程序详细信息。

管理应用程序

在应用程序仪表板中，单击“**管理应用程序**”以查看所有自定义和离散应用程序。

作为管理员，您可以从“**管理应用程序**”页面执行以下操作：

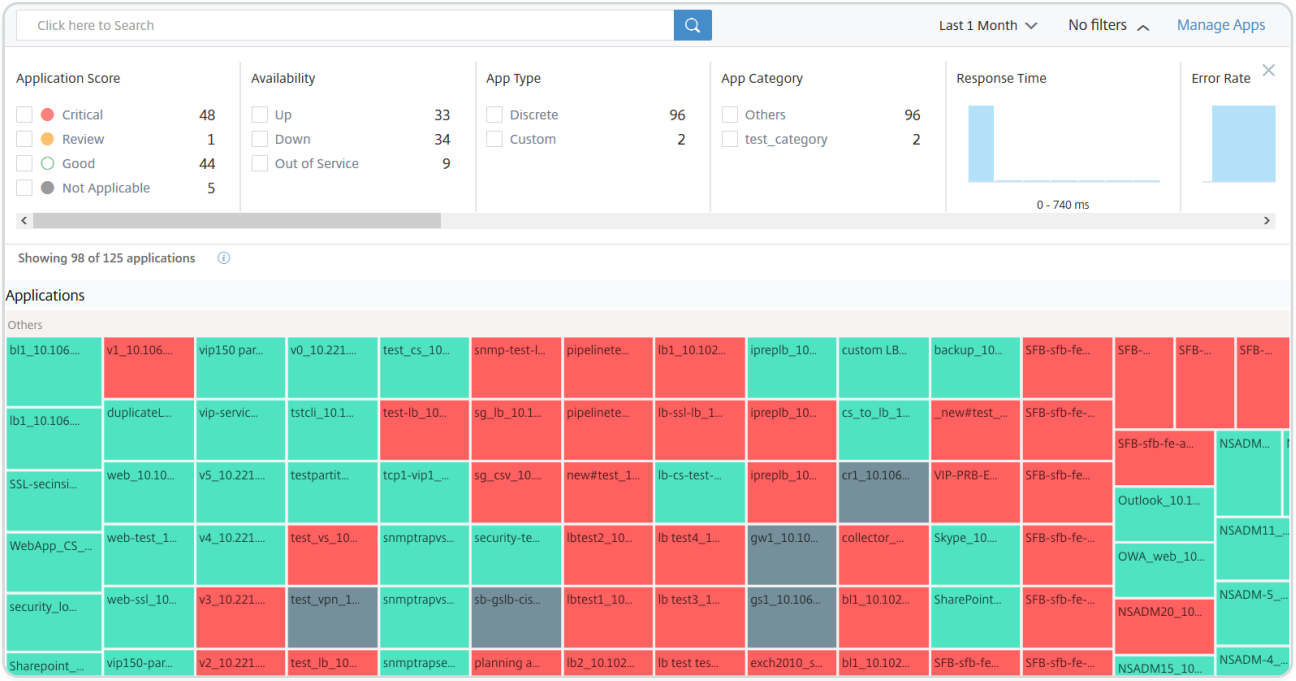
- 添加应用程序
- 查看应用程序详细信息，例如应用程序名称、应用程序类型、应用程序类别、关联的虚拟服务器、关联的服务等。
- 编辑或删除自定义应用程序

有关详细信息，请参阅管理应用程序。

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

应用程序仪表板

导航到“**应用程序**”>“**仪表板**”以表格视图或图形视图查看应用程序列表。



所有应用程序仅在开始填充数据后才会在仪表板中显示。在仪表板中，单击一个应用程序以查看应用程序性能的详细信息。有关详细信息，请参阅应用程序详细信息。

如果应用程序分析在大约 10-15 分钟后仍未显示，请在排查应用程序仪表板问题中执行故障排除步骤。

新仪表板行为与旧仪表板相比的更新

- 添加或编辑自定义应用程序后，可能需要几分钟才能在仪表板中反映该应用程序。
- 如果您删除自定义应用程序，仪表板仍会显示已删除的应用程序，直到 NetScaler Console 拥有其分析数据（最长 1 个月）。

  假设您在 Jan 2, 2020 创建了一个应用程序，并在 Jan 4, 2020 删除了该应用程序。在这种情况下：

  - 当您选择过去 1 天、1 周和 1 个月的时间段时，仪表板仍可在 Jan 4, 2020 显示已删除的应用程序。
  - 当您选择过去 1 周和 1 个月的时间段时，仪表板仍可在 Jan 5, 2020 显示已删除的应用程序。
  - 当持续时间超过应用程序删除日期时，应用程序将不会显示在仪表板中。也就是说，在 Jan 6, 2020（过去 1 天）、Jan 12, 2020（过去 1 周）和 February 5, 2020 之后（过去 1 个月），仪表板将不显示已删除的应用程序。

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

注意

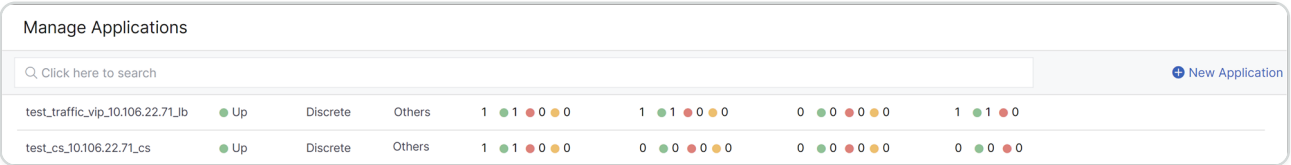
添加应用程序后，如果关联的 NetScaler 实例处于关闭、停止服务或由于临时网络故障而无法访问状态：

-与 NetScaler 实例关联的应用程序仅在“**应用程序**”页面中可见，而不在仪表板中可见。
-NetScaler 实例启动并运行后，应用程序将显示在仪表板中。

管理应用程序

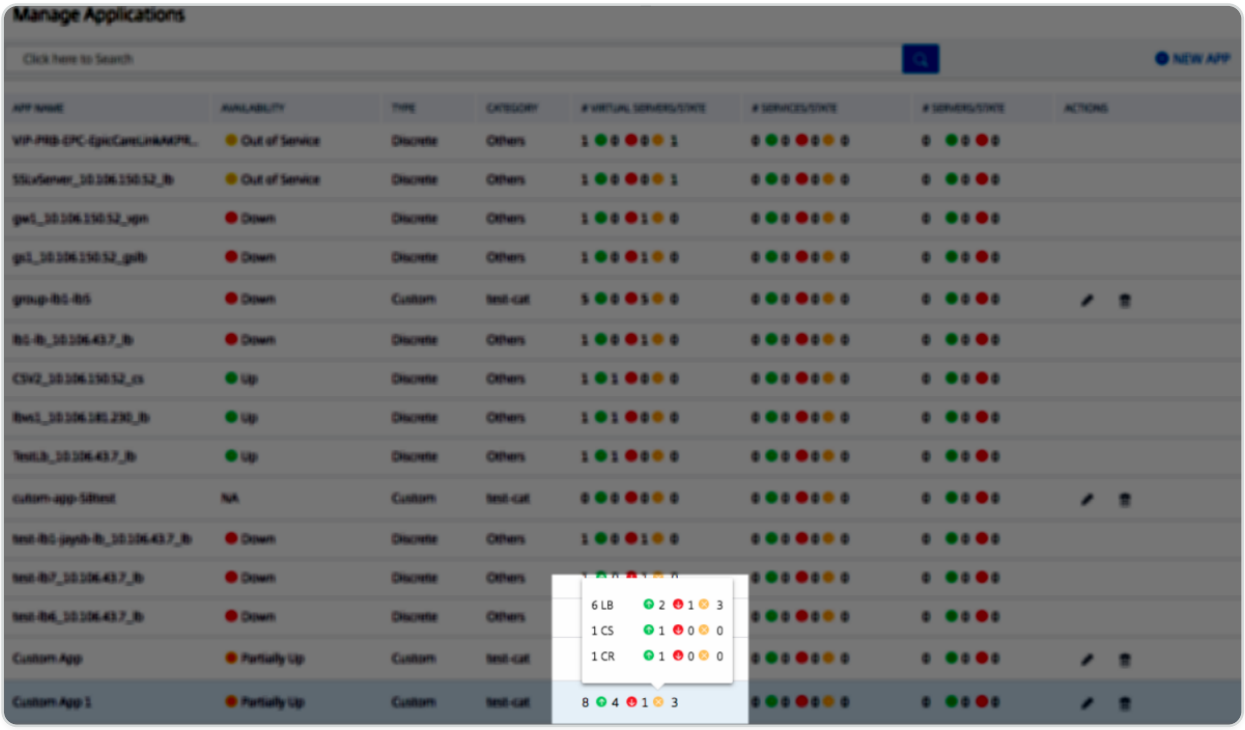
在仪表板中，单击**管理应用程序**以查看应用程序详细信息，并添加、编辑或删除自定义应用程序。

查看应用程序详细信息



- **应用程序名称** – 表示应用程序名称
- **可用性** – 表示应用程序的当前可用性，例如**正常**、**关闭**、**部分正常**、**停止服务**和**不适用**
  - **正常** – 与应用程序关联的所有虚拟服务器都处于正常状态。
  - **关闭** – 与应用程序关联的所有虚拟服务器都处于关闭状态
  - **部分正常** – 与应用程序关联的虚拟服务器中，有一个处于关闭或停止服务状态
  - **停止服务** – 与应用程序关联的所有虚拟服务器都停止服务
  - **不适用** – 未为应用程序配置虚拟服务器
- **类型** – 表示应用程序属于自定义还是离散类型
- **类别** – 表示已分组的应用程序类别
- **虚拟服务器/状态** – 表示已配置的虚拟服务器总数以及所有虚拟服务器的当前状态。将鼠标指针悬停以查看详细信息，例如虚拟服务器总数、虚拟服务器类型和虚拟服务器状态

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

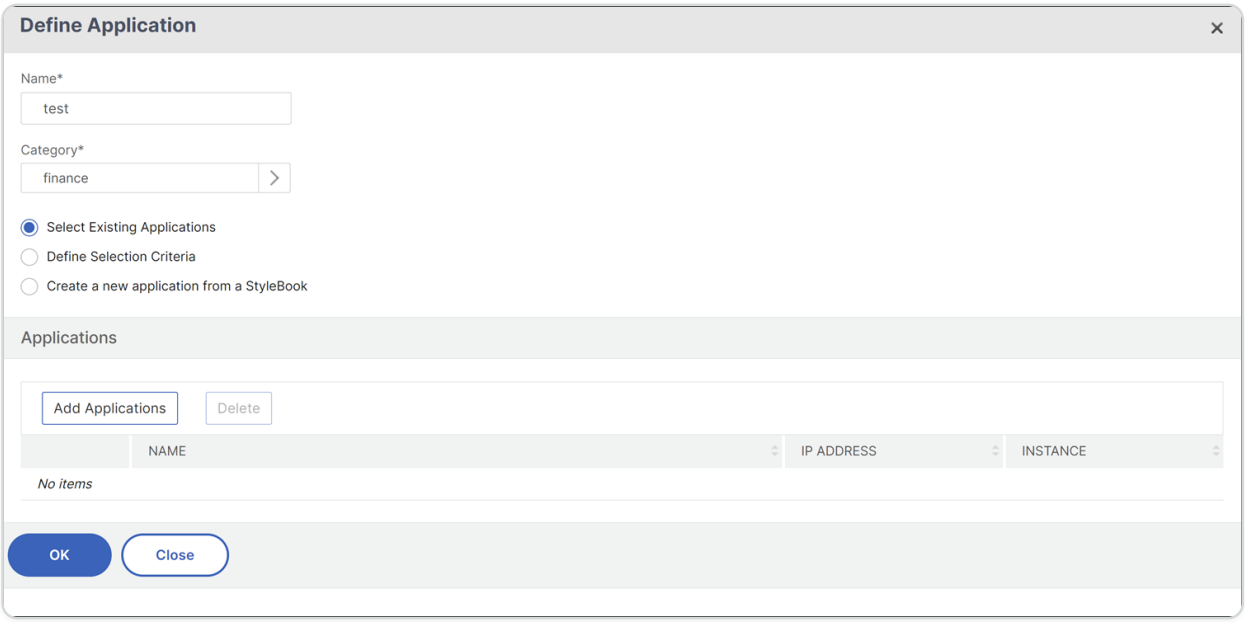


- **服务/状态** – 表示已配置的服务总数以及所有服务的当前状态
- **服务组/状态** – 表示已配置的服务组总数以及所有服务组的状态
- **服务器/状态** – 表示为应用程序配置的服务器总数以及所有服务器的当前状态
- **操作** – 使您能够编辑或删除自定义应用程序

添加应用程序

1. 单击 **新建应用程序** 以创建新应用程序

   显示 **定义应用程序** 页面



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

注意

您也可以单击 **应用程序**，然后选择 **新建应用程序** 以添加新应用程序

2. 设置以下参数：

字段	描述
名称	自定义应用程序的名称。例如，LB_TEST。
类别	可用于对应用程序进行分组的类别。单击以获取“应用程序类别”页面。选择类别，然后单击“**选择**”。要添加类别：
	1. 单击“**添加**”
	2. 输入您选择的名称。
	3. 单击“**创建**”
选择现有应用程序	使您能够选择已添加到 NetScaler 实例的现有应用程序。
添加应用程序	显示在实例上配置的所有虚拟服务器。从列表中选择应用程序，然后单击“**确定**”。
定义选择条件	通过虚拟服务器范围或源服务器/服务 IP 地址范围定义应用程序的选项。
	- **服务器。** 指定应用程序运行的后端服务器的服务器或服务 IP 地址、服务器名称或端口。您可以输入一个 IP 地址、一个 IP 地址范围，或两者以逗号分隔的组合。例如，您可以输入 10.102.29.20、10.102.43.10-60、10.216.43.45。
	- **虚拟服务器。** 您可以指定以下任一选项：虚拟服务器 IP 地址、虚拟服务器名称，或应用程序运行的后端服务器的端口。您可以输入一个 IP 地址、一个 IP 地址范围，或两者以逗号分隔的组合。例如，您可以输入

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

字段	描述
	10.102.29.20、10.102.43.10-60、10.216.43.45。
从 StyleBook 创建新应用程序	使您能够使用 StyleBook 创建应用程序。有关详细信息，请参阅使用 StyleBook 创建应用程序。

a. 点击**确定**。

> **注意**
>
> 目前，应用程序仪表板仅支持负载平衡和内容切换虚拟服务器。

应用程序仪表板现在显示了类别，所有应用程序都归类在其下方。

如果您为自定义应用程序选择**从 StyleBook 创建新应用程序**选项，则必须允许 NetScaler Console 自动选择虚拟服务器进行许可。要启用虚拟服务器的自动选择功能，请执行以下操作：

a. 导航到**设置** > **许可和分析配置**。
b. 在**虚拟服务器许可证分配**下，点击**自动选择虚拟服务器**和**自动选择不可寻址的虚拟服务器**以启用。

使用 StyleBook 创建应用程序

要使用 StyleBook 创建应用程序：

1. 在 NetScaler Console 中，导航到**应用程序** > **仪表板**，然后点击**定义自定义应用程序**以创建自定义应用程序。
2. 在**定义应用程序**页面中，在**名称**字段中输入应用程序的名称。
3. 从“类别”部分选择应用程序类别。NetScaler Console 允许您定义类别以对用户定义的应用程序进行分组。如有必要，您还可以添加更多类别。
4. 点击以选择**从 StyleBook 创建新应用程序**，然后点击**确定**。

   将显示“选择 StyleBook”页面。此页面包含 NetScaler Console 中所有可用的默认 StyleBook。
5. 选择 StyleBook。 将显示**配置详细信息**页面。
6. 在 StyleBook 中输入所有参数的值。您还可以单击“查看定义”以在使用 StyleBook 之前查看其结构。

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

有关详细信息，请参阅使用默认 StyleBook。

7. 单击“**创建**”。

   您还可以单击“**试运行**”以检查 NetScaler Console 尝试在所选 NetScaler 实例上创建的配置。此选项仅用于测试目的，以查看配置的最终检查。即使“试运行”选项成功，所选 NetScaler 上的实际配置仍可能因各种原因（IP 冲突、实例不可达等）而失败。

编辑或删除应用程序

在“**应用程序**”页面上，您可以编辑或删除自定义应用程序。单击编辑按钮编辑应用程序，单击删除按钮删除应用程序。

导出应用程序仪表板和安全仪表板报告

NetScaler Console 允许您获取当前应用程序仪表板的快照并将其导出为报告。应用程序管理员可能需要定期使用这些报告来更新应用程序使用情况和性能损失。

借助此功能，管理员可以将这些数据提取为 .png、.jpeg 或 .pdf 报告。

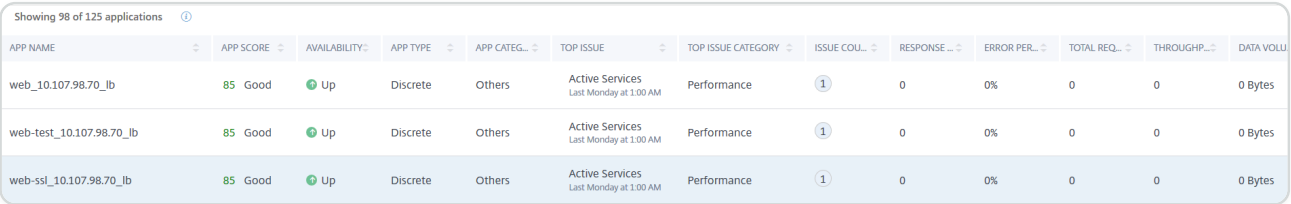
注意

与 NetScaler Console 中的其他报告导出选项不同，您只能将应用程序仪表板和安全仪表板报告导出为 .pdf 或 .png 文件。目前不支持 .csv 格式。

报告将下载到您的系统。在应用程序仪表板和应用程序安全仪表板页面中，您还可以导航到二级页面并将其导出为报告。目前，您一次只能下载一个应用程序的报告。

查看应用程序

默认情况下，应用程序仪表板会显示所有应用程序。您可以根据需要使用筛选选项来查看应用程序。



仪表板显示以下应用程序详细信息：

- **应用程序名称** – 表示应用程序名称
- **应用程序分数** – 表示应用程序分数和状态，例如**严重**、**良好**、**一般**和**不适用**

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

- **可用性** – 表示应用程序的当前可用性，例如**正常**、**关闭**、**部分正常**、**停止服务**和**不适用**
  - **正常** – 与应用程序关联的所有虚拟服务器都处于正常状态。
  - **关闭** – 与应用程序关联的所有虚拟服务器都处于关闭状态。
  - **部分正常** – 与应用程序关联的某个虚拟服务器处于关闭或停止服务状态。
  - **停止服务** – 与应用程序关联的所有虚拟服务器都停止服务。
  - **不适用** – 未为应用程序配置虚拟服务器。
- **主要问题** – 表示应用程序上错误计数最多的问题
- **主要问题类别** – 表示问题的类别
- **问题计数** – 表示应用程序的总问题计数
- **响应时间** – 表示应用程序的平均响应时间
- **错误百分比** – 表示应用程序的 5xx 错误总百分比

> **注意**
>
> 5xx 错误百分比指标仅显示在 **NetScaler 13.0 或更高版本**。对于早期版本，该值显示为 **0**。

- **总请求数** – 表示应用程序收到的总请求数
- **吞吐量** – 表示应用程序的总网络吞吐量。吞吐量通过虚拟服务器的请求字节/秒 + 响应字节/秒计算得出
- **数据量** – 表示应用程序处理的总数据量
- **客户端连接数** – 表示应用程序建立的平均客户端连接数
- **服务器连接数** – 表示应用程序建立的平均服务器连接数

配置并将一个应用程序关联到多个自定义应用程序

在 **应用程序仪表板** 中，您可以配置一个应用程序并将其关联到多个自定义应用程序。使用此功能，您可以将同一个应用程序重用于多个自定义应用程序，而无需为每个自定义应用程序创建单独的应用程序。

假设您分别管理两个名为 **ComABC** 和 **ComCDE** 的电子商务门户，并且您希望为这两个门户使用名为 **PaymentApp** 的支付网关服务器。在这种情况下，您必须：

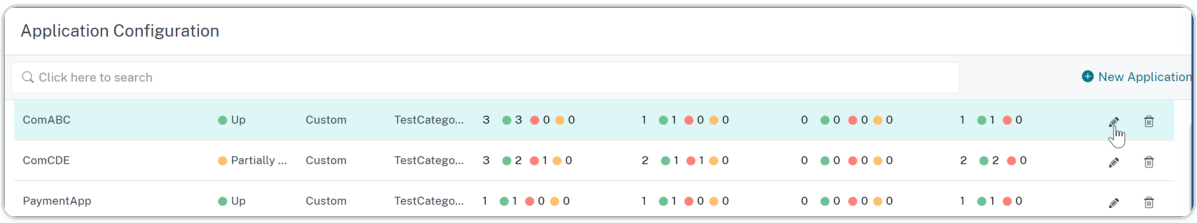
- 创建两个名为 **ComABC** 和 **ComCDE** 的自定义应用程序。

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

- 创建一个名为 **PaymentApp** 的应用程序，并将其关联到 **ComABC** 和 **ComCDE**。

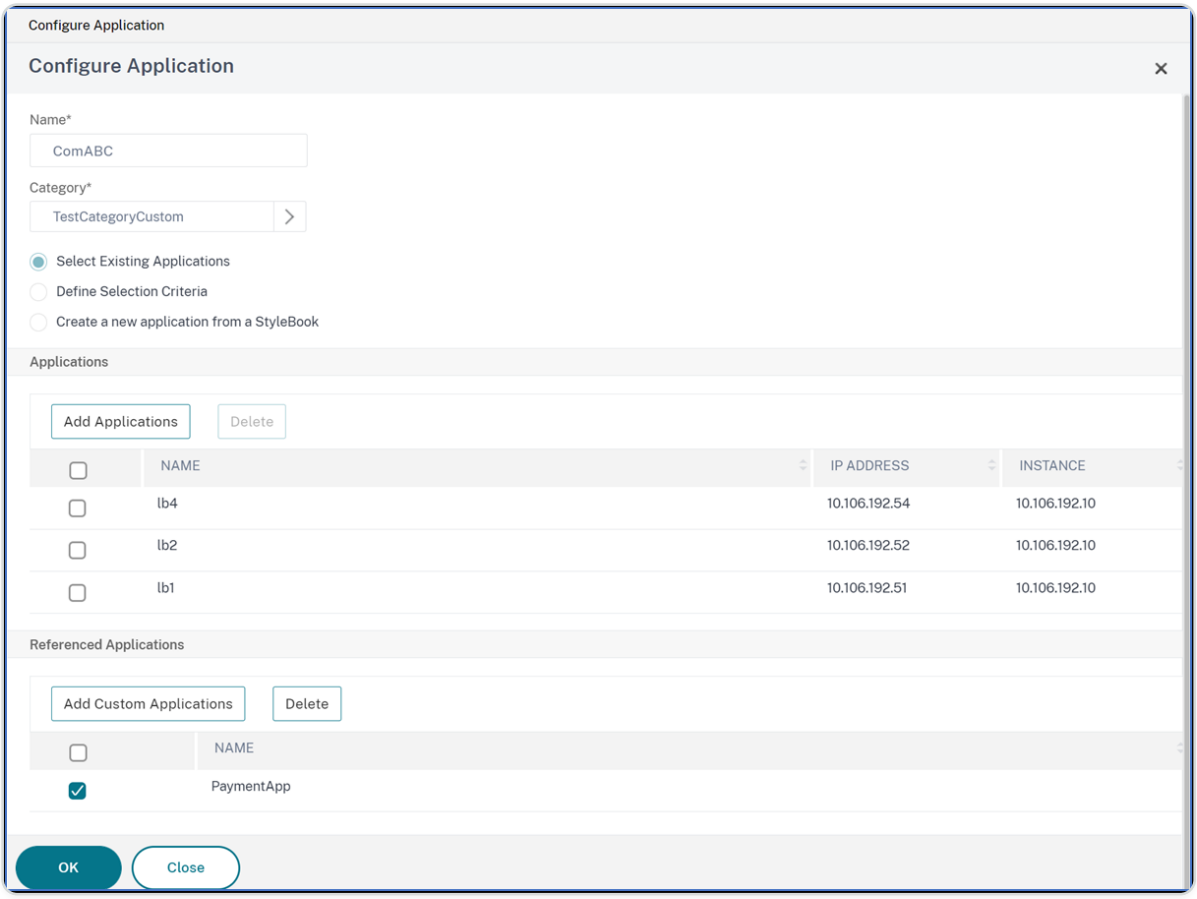
要实现此场景，您必须：

- 创建 **自定义应用程序 (ComABC 和 ComCDE)**：
  a. 导航到 **应用程序 > 仪表板**，然后单击 **管理应用程序**。
  b. 单击 **新建应用程序**。
  c. 指定名称和类别。
  d. 选择用于选择应用程序的类型。在此示例中，选择了 **选择现有应用程序** 选项。有关更多信息，请参阅 添加应用程序。
  e. 在 **应用程序** 下，单击 **添加应用程序**。
  f. 从列表中选择应用程序，然后单击 **确定** 以创建自定义应用程序。
- 创建 **PaymentApp**。为此，您必须将离散应用程序转换为自定义应用程序：
  a. 导航到 **应用程序 > 仪表板**，然后单击 **管理应用程序**。
  b. 单击 **新建应用程序**。
  c. 指定名称和类别。
  d. 选择用于选择应用程序的类型。在此示例中，选择了“选择现有应用程序”选项。有关详细信息，请参阅 添加应用程序。
  e. 在 **应用程序** 下，单击 **添加应用程序**。
  f. 从列表中选择应用程序，然后单击 **确定** 以创建自定义应用程序。
- 接下来，您可以使用 **PaymentApp** 并关联到 **ComABC** 和 **ComCDE**。
  a. 导航到 **应用程序 > 仪表板**，然后 **单击管理应用程序**。
  b. 找到 **ComABC** 应用程序，然后单击 **编辑**。



  c. 在 **引用应用程序** 下，单击 **添加自定义应用程序**，然后选择 **PaymentApp**。
  d. **PaymentApp** 现在可在 **引用应用程序** 下使用。单击 **确定** 以将 **PaymentApp** 关联到 **ComABC** 自定义应用程序。

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



e. 对 **ComCDE** 自定义应用程序重复相同的过程。

注意：

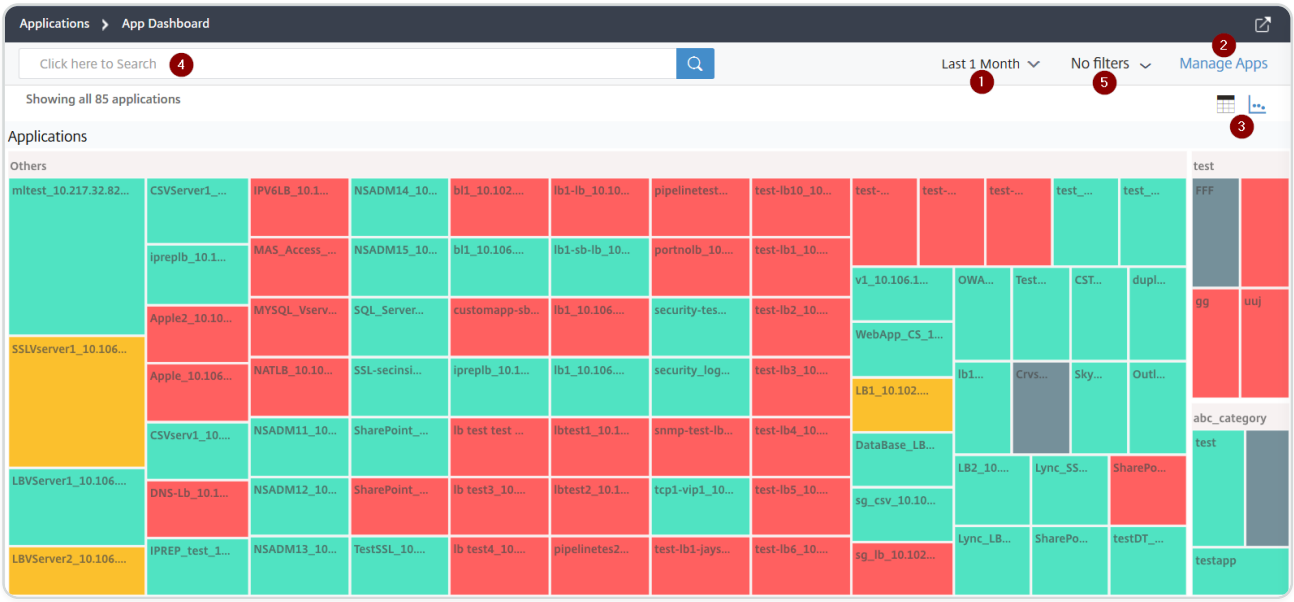
应用程序与自定义应用程序关联后，自定义应用程序的最终应用程序分数是根据自定义应用程序和引用应用程序之间的最低分数计算的。在此示例中，如果 **ComABC** 应用程序分数为 85，**PaymentApp** 分数为 69，则 **ComABC** 应用程序的最终分数将变为 69。

应用程序仪表板概述

应用程序仪表板显示**其他**下的离散应用程序以及按其各自类别分组的自定义应用程序。

导航到**应用程序** > **仪表板**以查看应用程序仪表板。

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



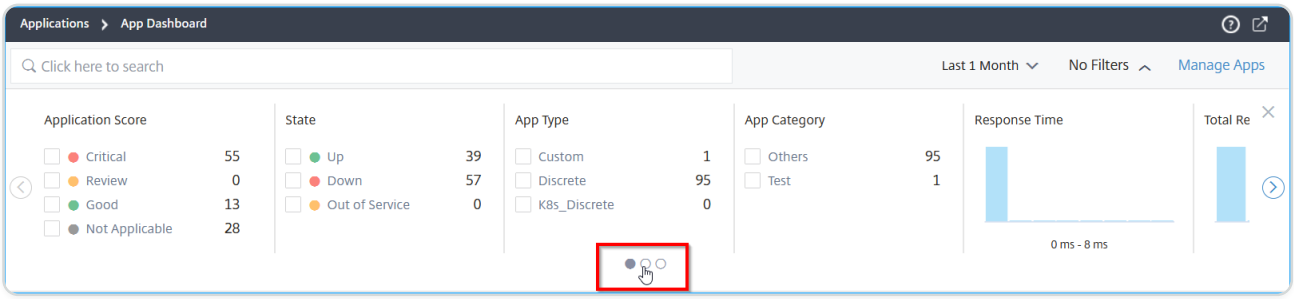
1 – 显示所选时间段（例如 1 小时、1 天、1 周和 1 个月）的应用程序详细信息。

2 – 使您能够管理应用程序和添加新应用程序

3 – 使您能够以表格视图或图形视图查看应用程序

4 – 使您能够使用搜索栏搜索应用程序

5 – 使您能够应用筛选器来查看应用程序。单击以查看详细信息。



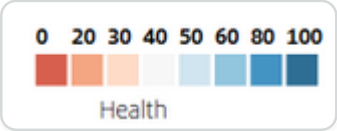
您可以选择轮播滑块，它使您可以轻松访问所有选项。

您可以：

- 选择根据分数查看应用程序。
  - **严重** – 应用程序分数介于 0 和 < 40 之间
  - **一般** – 应用程序分数介于 40 和 < 75 之间
  - **良好** – 应用程序分数大于 75
  - **不适用** – 要么没有为应用程序配置许可的虚拟服务器，要么虚拟服务器类型不是负载均衡或内容切换。

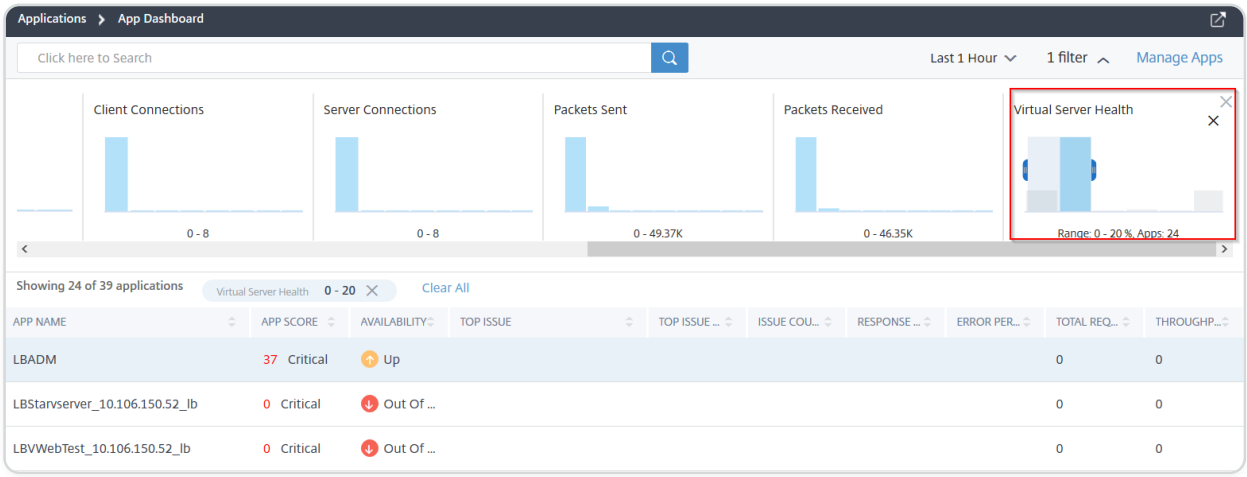
    下表描述了早期应用程序分数与当前应用程序分数之间的差异。

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

应用程序分数（严重、审查、良好、不适用）	应用程序分数（带颜色图例的早期视图）
分数计算方式为 **100 减去所有应用程序当前问题的惩罚分数**	分数计算方式为 **100 – (应用程序服务器资源 + NetScaler 系统资源)**
应用程序以以下颜色显示：**红色（严重）**、**橙色（审查）**、**绿色（良好）**和**灰色（不适用）**	应用程序以颜色图例显示。 

- 选择根据应用程序状态（例如正常、关闭和停止服务）查看应用程序
- 选择根据应用程序类型（例如离散或自定义）查看应用程序
- 选择根据下方分组的类别查看应用程序
- 拖动直方图以应用筛选器并查看应用程序。

例如，如果您想查看虚拟服务器运行状况介于 0 到 20 之间的应用程序，请拖动虚拟服务器运行状况直方图以筛选结果。

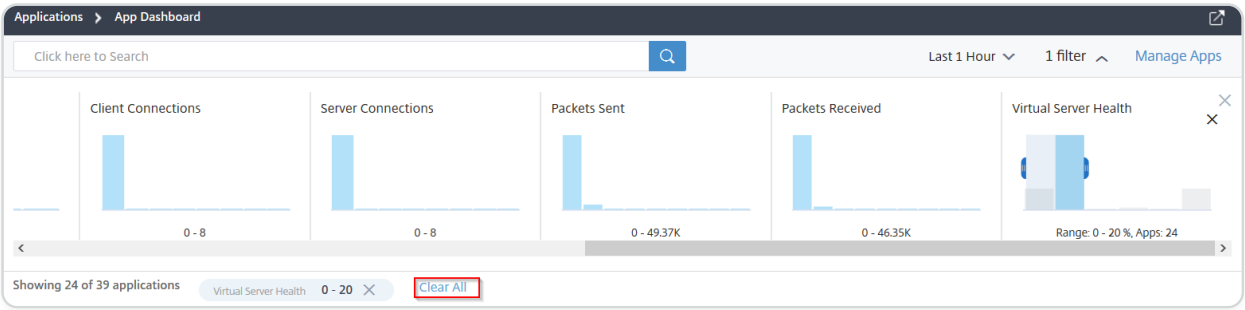


注意

您还可以单击直方图以显示相关应用程序。

单击 **清除所有** 以清除应用的筛选器。

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



以下是您可以应用筛选器的应用程序摘要：

- **响应时间** – 一个直方图，显示应用程序接收到的平均响应时间
- **错误率** – 一个直方图，显示应用程序的 5xx 错误的平均错误百分比
- **总请求数** – 一个直方图，显示应用程序接收到的请求总数
- **吞吐量** – 一个直方图，显示应用程序处理的总网络吞吐量
- **数据量** – 一个直方图，显示应用程序处理的总数据量。数据量通过应用程序的总请求字节和响应字节计算得出。
- **客户端连接** – 一个直方图，显示应用程序建立的平均客户端连接数
- **服务器连接** – 一个直方图，显示应用程序建立的平均服务器连接数
- **已发送数据包** – 一个直方图，显示应用程序发送的数据包总数
- **已接收数据包** – 一个直方图，显示应用程序接收的数据包总数
- **虚拟服务器运行状况** – 一个直方图，显示分数范围在 0% 到 100% 之间的应用程序总数。虚拟服务器运行状况是与应用程序关联的活动服务的百分比。例如，如果虚拟服务器配置了 2 个服务，其中一个服务处于关闭状态，则分数为 50%。

使用搜索栏搜索和筛选结果

您可以将鼠标指针放在搜索栏上，然后选择类别以优化搜索。

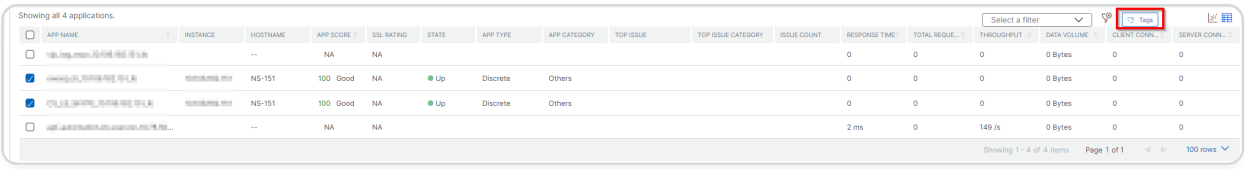
创建标签并将其应用于应用程序

如果您有大量应用程序，可以创建标签并将其应用于应用程序。这些标签可提高搜索功能。

示例：

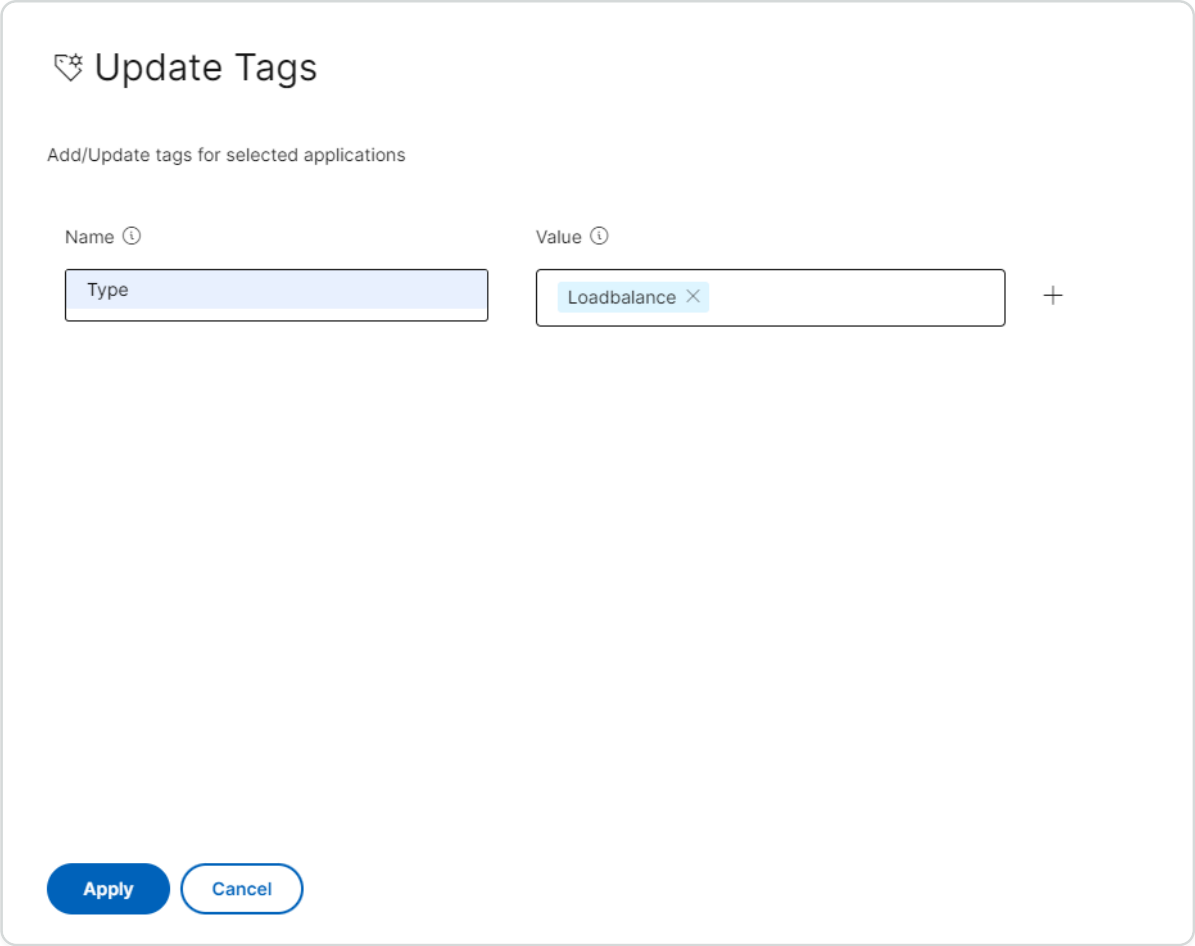
以下过程列出了为负载平衡应用程序创建标签的步骤：

1. 在 **App Dashboard** 中，选择要创建标签的负载平衡应用程序，然后单击 **Tags**。



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

2. 在 **Update Tags** 中：
   - 指定一个您选择的名称。例如：**Type**。
   - 指定使您能够分配标签的值。您还可以输入多个值。例如：**Loadbalance**。
   - 单击 **Apply**。



   标签已创建。

要应用标签并检索负载平衡应用程序：

1. 在应用程序仪表板搜索栏中，点击文本框内部以查看已创建的标签并选择标签名称。

   搜索栏(/en-us/netscaler-application-delivery-management-software/media/app-tags2.png)

2. 选择运算符 (**IN**) 和已创建的值，然后点击 **Search**。

   标签(/en-us/netscaler-application-delivery-management-software/media/app-tags3.png)

   列出了所有在 **Loadbalance** 下标记的负载均衡应用程序。同样，您可以为其他应用程序创建标签。

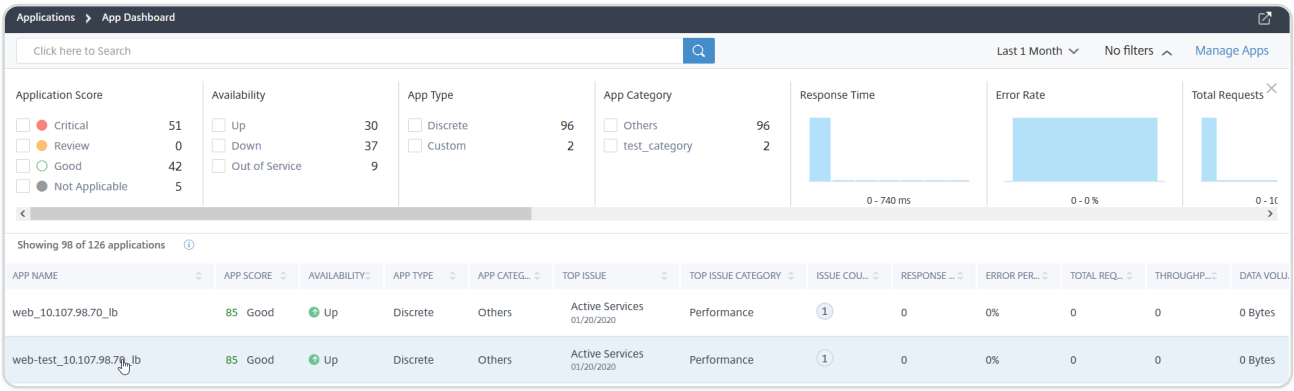
© 1997–2026 Citrix Systems, Inc. All rights reserved.

应用程序详细信息

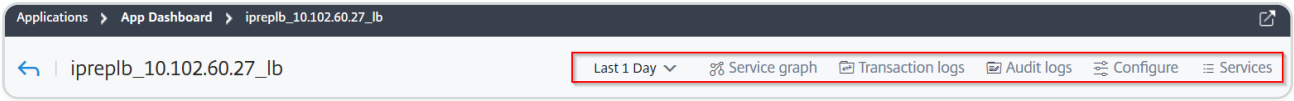
注意：

从 **14.1-21.x** 版本开始，您可以查看从 NetScaler 管理分区创建的应用程序的指标详细信息。

从仪表板中单击一个应用程序，以深入查看更多详细信息。



显示选定的应用程序页面。



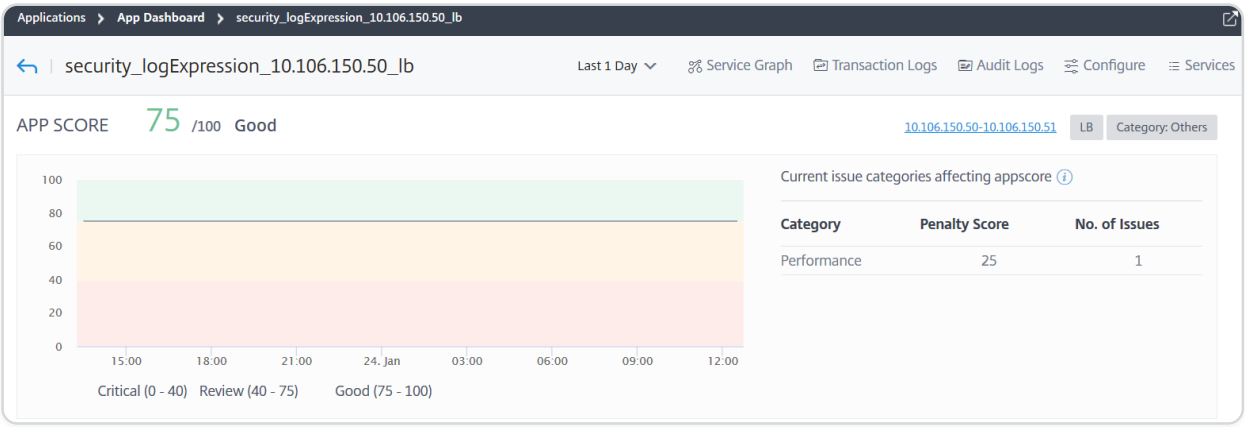
在应用程序详细信息页面中：

- 从列表中选择时间段，以查看特定时间段的详细信息
- 单击 **服务图** 以查看所选应用程序的服务图。有关详细信息，请参阅 应用程序服务图
- 单击 **事务日志** 以查看 5xx 错误的详细事务
- 单击 **审核日志** 以查看详细的审核日志信息
- 单击 **配置** 以查看或编辑应用程序的服务和服务组配置
- 单击 **服务** 以查看绑定到应用程序的服务

选择时间段后，将显示以下应用程序详细信息：

- **应用程序评分** – 所选时间段的应用程序评分。最终评分计算为 **100 减去总罚分**。

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

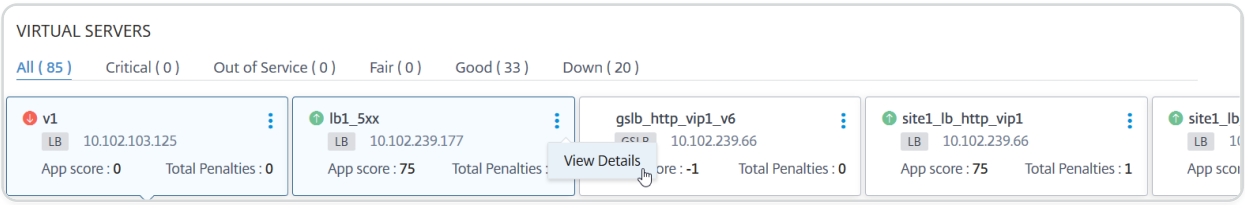


此仪表板还允许您查看影响应用程序评分的当前问题。您可以在“问题”下查看问题详细信息。

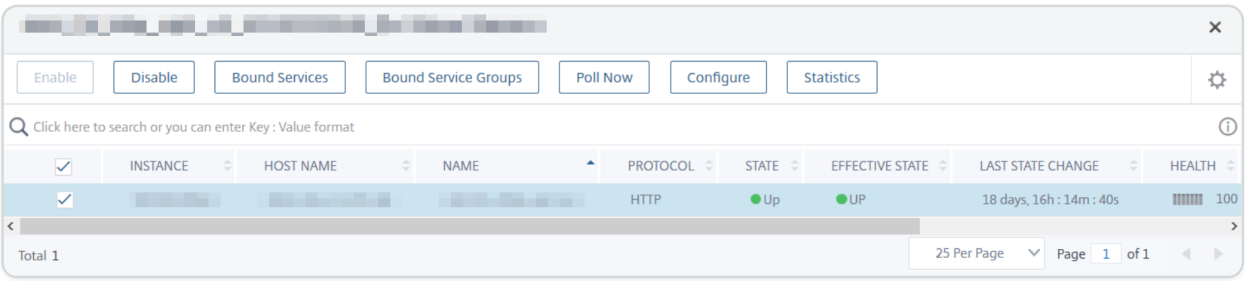
- **虚拟服务器** –

> **注意**
>
> **虚拟服务器**部分仅针对自定义应用程序显示。对于离散应用程序，单击 **IP 地址**以查看虚拟服务器详细信息。

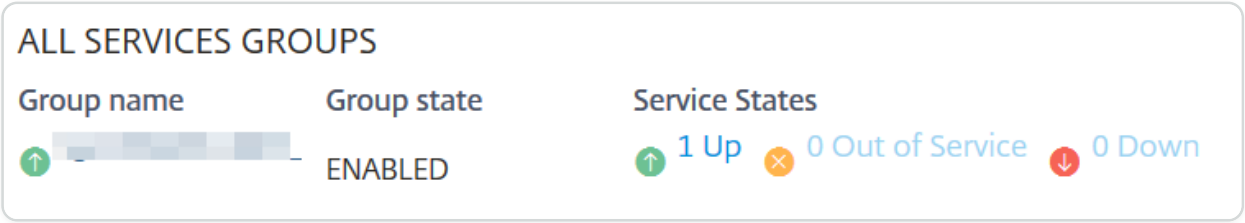
显示与自定义应用程序关联的所有虚拟服务器



单击**查看详细信息**以查看和管理虚拟服务器设置。

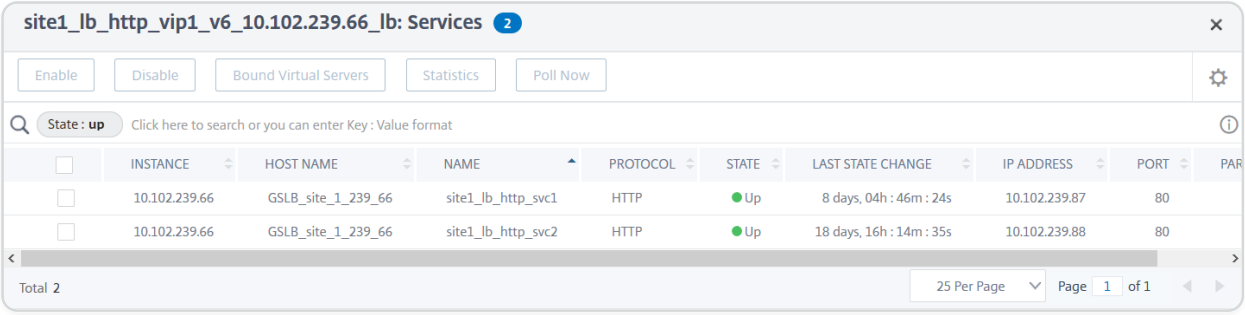


- **所有服务** – 绑定到应用程序的服务

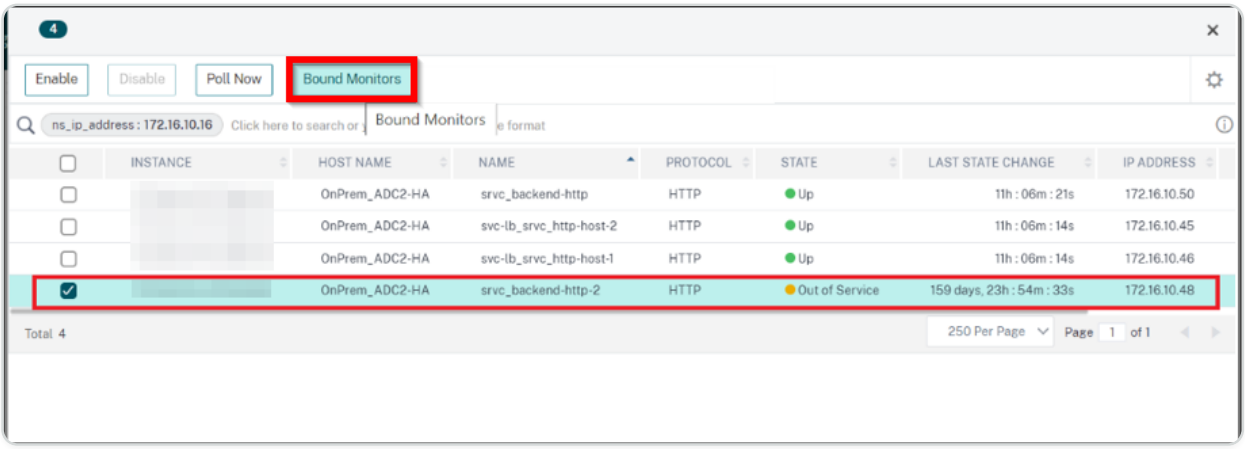


单击以查看服务详细信息并管理服务设置

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



您还可以选择一个服务并使用**绑定监视器**选项查看状态。



- **问题** – 适用于所选应用程序的问题。您可以查看以下问题及其类别：

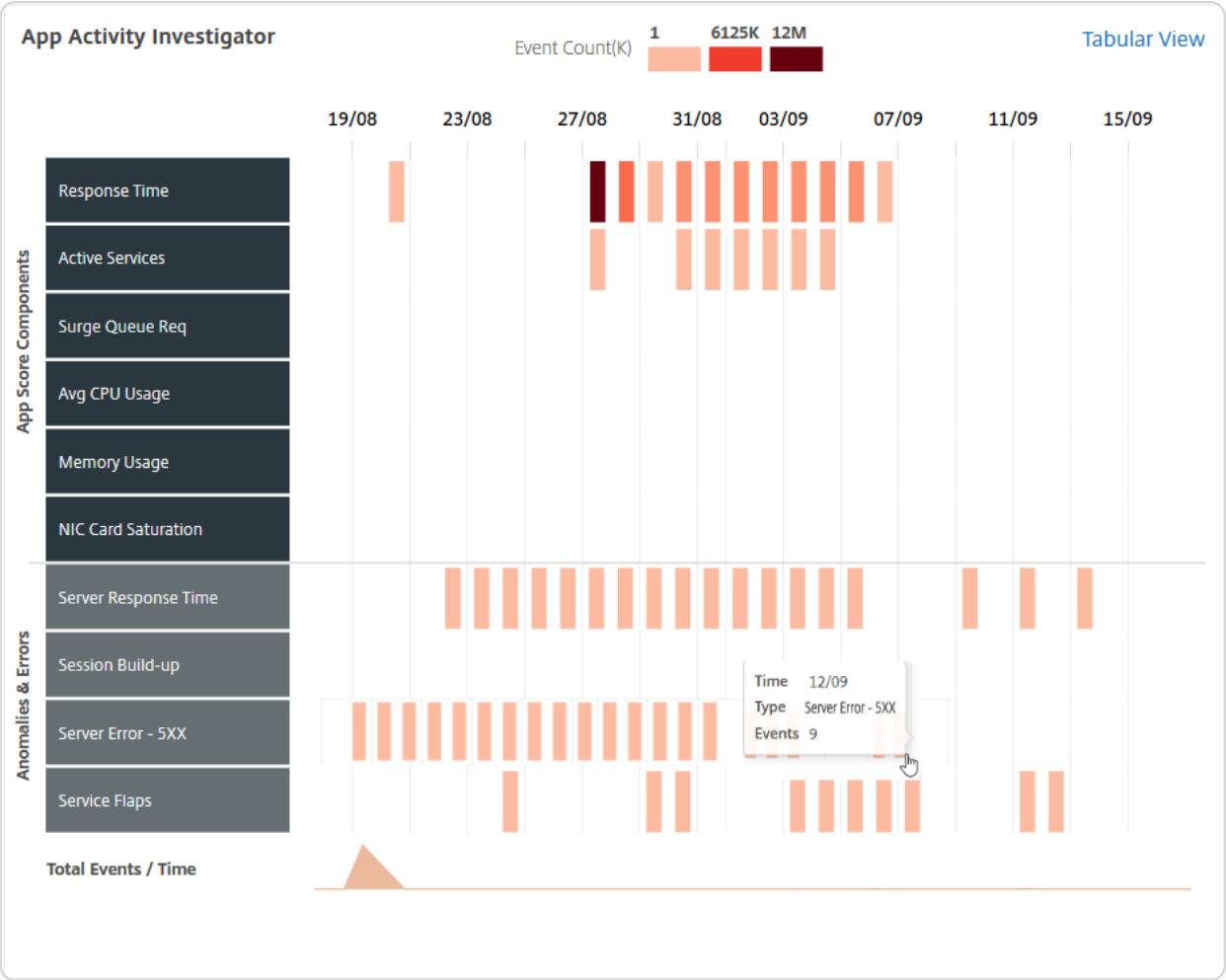
性能	实例运行状况	配置	系统资源
响应时间	平均 CPU 使用率	不稳定服务器	不正确的持久性类型
活动服务	内存使用率	异常大的 HTTP 数据包	网卡饱和
低会话重用		TCP 重组队列达到限制	
SurgeQueue 堆积			
SSL 实时流量			
会话堆积			
服务抖动			

单击每个问题以查看详细信息，例如检测消息、问题发生时间、建议操作和详细信息。

有关更多信息，请参阅应用程序分析的性能指标。

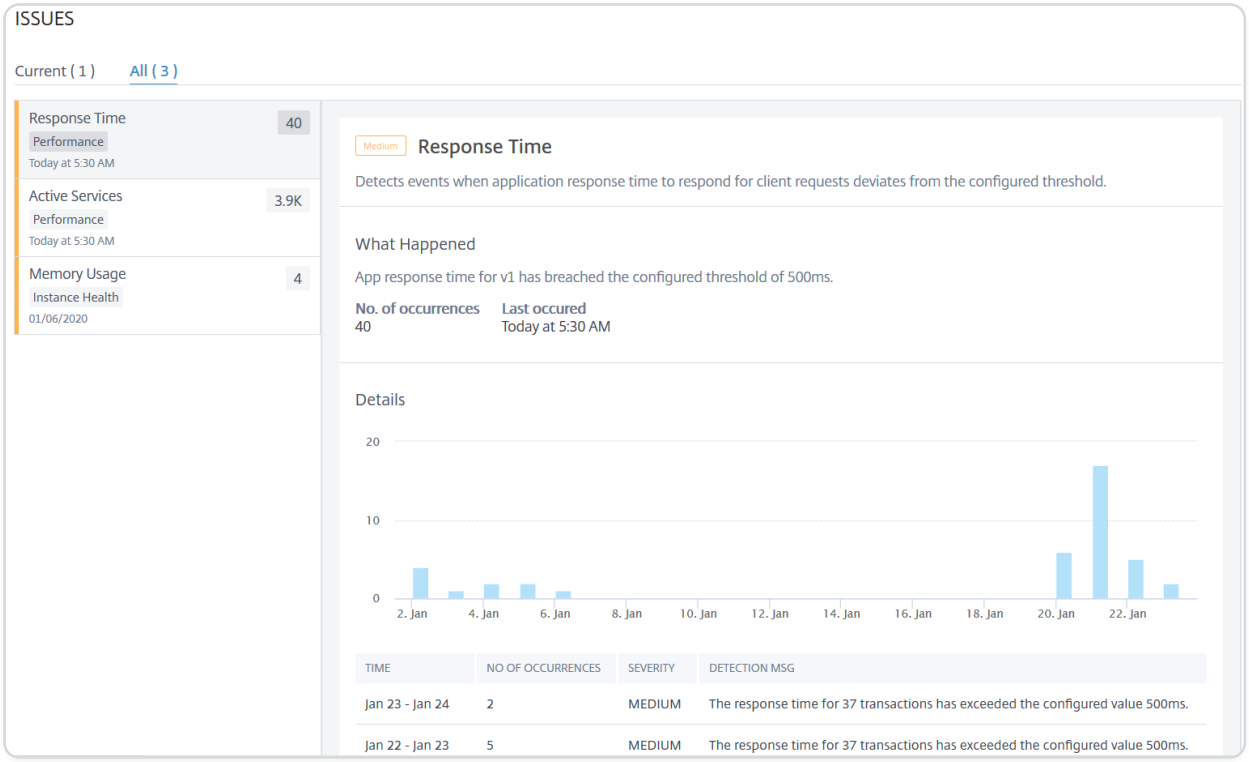
© 1997–2026 Citrix Systems, Inc. All rights reserved.

下图是“应用程序活动调查器”页面的早期视图：



您现在可以在“**问题**”部分查看所有问题，以及您可以在“**应用程序活动调查器**”页面中查看的类别。

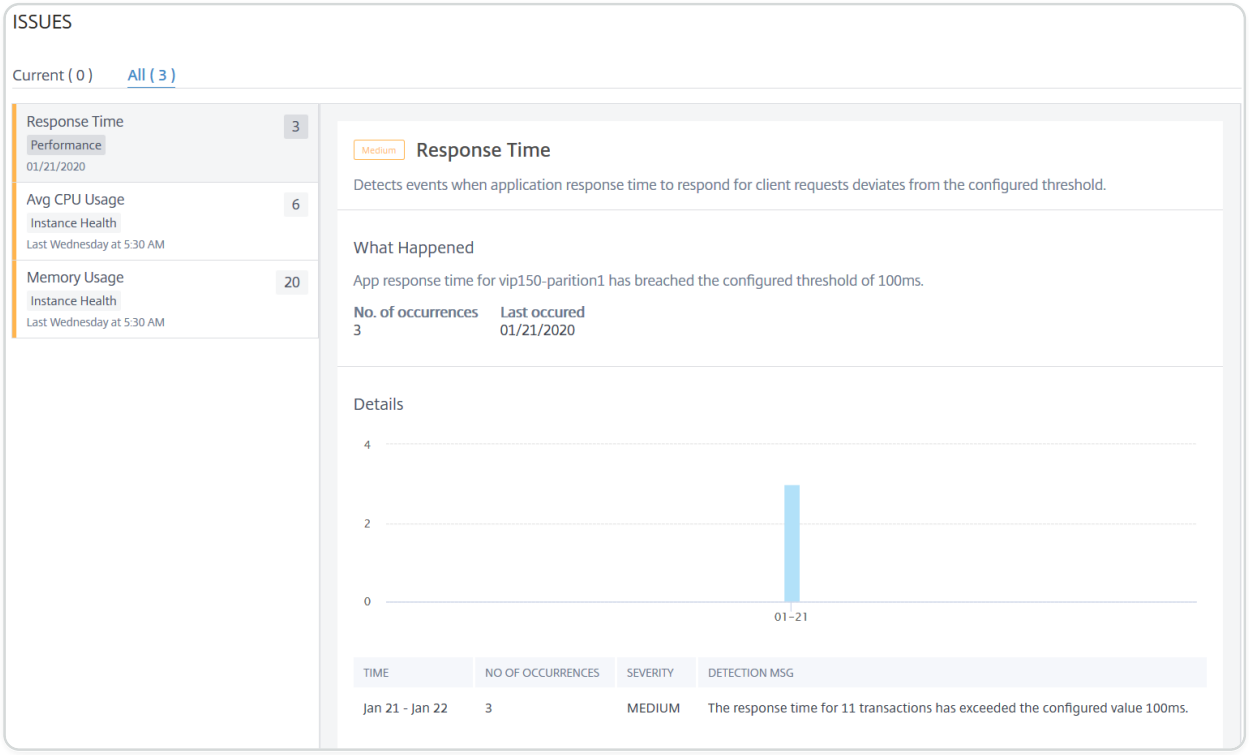
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- “**当前**”选项卡中显示的问题是指所选时间段内的应用程序问题。
- “**所有**”选项卡中显示的问题是指所有应用程序问题。

以下示例是为期 1 天的应用程序问题。“**当前**”选项卡表示没有影响应用程序分数的当前问题。

所有选项卡显示在一天内检测到的问题总数。



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

选择应用评分组件并设置阈值

在**应用仪表板**中，作为管理员，您可以选择组件并配置用于应用评分计算的阈值。应用评分是定义以下内容的评分系统：

- 应用程序的性能如何
- 应用程序在响应能力方面是否表现良好

导航到**应用程序 > 仪表板**，然后选择设置图标。

在**配置应用评分**页面中，您可以选择组件并配置阈值以确定最终的应用评分。

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

Configure App Score

Configure the contributing factors and their thresholds to calculate the App Score values

- [x] ADC Memory Usage
  - Low Memory Threshold (%): 70
  - High Memory Threshold (%): 85
- [x] Surge Queue Build-up
  - Lower Surge Queue Threshold: 0.05
  - Higher Surge Queue Threshold: 0.10
- [x] ADC CPU Usage
  - Low CPU Threshold (%): 80
  - High CPU Threshold (%): 90
- [x] Response Time
  - Response Time (ms): 500
- [x] App CPU Usage
  - Low App CPU Threshold (%): 70
  - High App CPU Threshold (%): 90
- [x] Active Services
  - Active Services Threshold (%): 100
- [x] Improper Persistence Type
- [x] Server Error 5xx
- [x] Unusually Large HTTP Packets
- [x] SSL Real Time Traffic
- [x] SSL Session Build-up
- [x] Low Session Reuse
- [x] NIC Card Saturation
- [x] TCP Reassemble Queue Limit Hits

OK | Close

应用评分计算基于以下组件：

应用评分组件	用户配置的阈值	描述
NetScaler 内存使用情况	是	NetScaler 实例中总内存使用量的低阈值和高阈值
突发队列堆积	是	队列中需要响应的总突发请求的低阈值和高阈值。
NetScaler CPU 使用率	是	NetScaler 实例中总 CPU 使用率的低阈值和高阈值。
响应时间	是	从虚拟服务器上配置的服务发送请求数据包到接收第一个响应数据包之间的时间间隔。
应用程序 CPU 使用率	是	应用程序总 CPU 使用率的低阈值和高阈值。
活动服务	是	绑定到虚拟服务器的必须处于活动状态的服务百分比的阈值。
不正确的持久性类型	否	指示虚拟服务器上的持久性使用率是否较低。
服务器错误 (5xx)	否	指示 Web 服务器是否响应 5xx 错误。
异常大的 HTTP 数据包	否	指示当 HTTP 消息的 HTTP 标头大小超过 NetScaler 实例中的配置值时发生的次数。
SSL 实时流量	否	分析 SSL 流量以识别实时流量，并建议优化配置设置以改善延迟。
SSL 会话建立	否	指示一段时间内会话的建立情况，这可能导致 NetScaler 实例中大量内存被这些会话占用。

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

应用评分组件	用户配置的阈值	描述
会话重用率低	否	指示 NetScaler 实例重用的实际会话数是否较少。
网卡饱和度	否	指示接口丢弃的数据包总数。
TCP 重组队列限制命中	否	指示 TCP 连接上的乱序数据包是否超过配置的乱序数据包队列大小。

默认情况下，所有组件都已启用。如果禁用任何组件，NetScaler Console 将仅根据选定的组件执行最终的应用程序分数计算。

注意

> 您还可以通过导航到 **设置 > 分析设置** 并单击 **配置应用程序分数** 来继续配置阈值。

微服务应用程序的应用程序详细信息

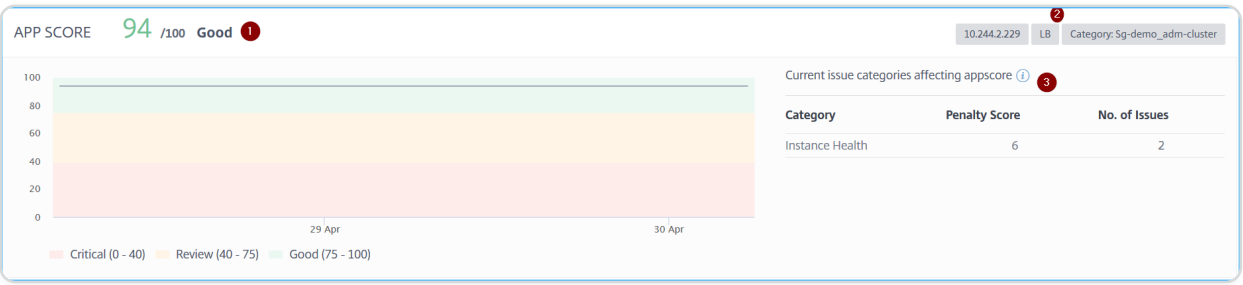
从仪表板中单击微服务应用程序，以深入查看更多详细信息。

显示所选应用程序页面。在应用程序详细信息页面中：

- 从列表中选择时间段以查看特定时间段的详细信息
- 单击 **Service Graph** 查看所选应用程序的服务图。有关更多信息，请参阅 应用程序的服务图
- 单击 **事务日志** 查看所选应用程序的详细事务
- 单击 **审计日志** 查看详细的审计日志信息

选择时间段后，将显示以下应用程序详细信息：

- **应用程序分数** – 所选时间段的应用程序分数。您还可以查看当前应用程序问题，这被称为根据问题类别适用的惩罚分数。最终分数计算为 **100 减去总惩罚**。



1 – 表示当前应用程序分数

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

2 – 表示 CPX IP 地址、应用程序类型（例如负载平衡或内容切换），以及托管服务的服务命名空间和集群名称

3 – 表示影响当前应用程序分数的问题

此仪表板还允许您查看影响应用程序分数的当前问题。您可以在“问题”下查看问题详细信息。

- **K8s 服务详细信息**

  您可以查看以下详细信息：

  K8s SERVICE DETAILS

Service Name	Cluster Name	Namespace	Service Labels
tea-beverage	cluster	sg-demo	app: dev-test, service.kubernetes.io/headless: , environment: production

  - **服务名称** – 服务名称
  - **群集名称** – 托管服务的群集名称
  - **命名空间** – 分配给服务的命名空间
  - **服务标签** – 分配给服务的服务标签

- **Pod 详细信息**

  Pod 是 Kubernetes 群集中托管的一组容器。在一个 Pod 中，您可以部署多个容器化应用程序。每个 Pod 都与一个 IP 地址关联。

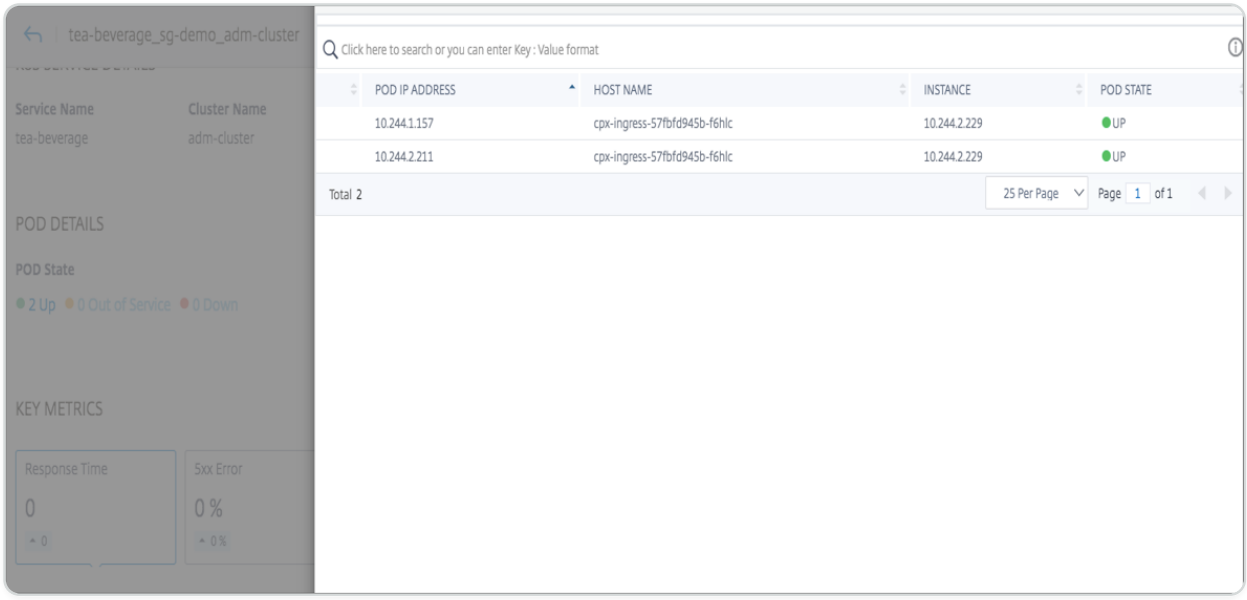
  POD DETAILS

  POD State

  2 Up 0 Out of Service 0 Down

  单击 Pod 状态以查看详细信息

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

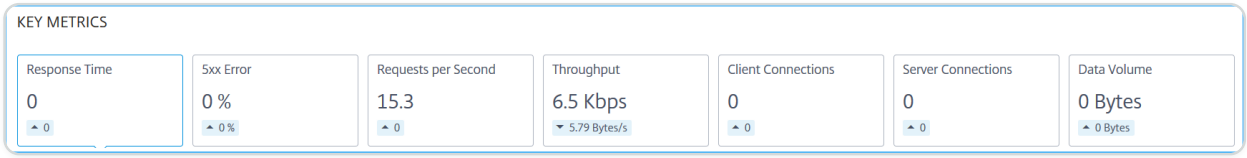


- **Pod IP 地址** – 表示 Pod IP 地址
- **主机名** – 表示分配给 Pod 的主机名
- **实例** – 表示 NetScaler CPX IP 地址
- **Pod 状态** – 表示 Pod 当前状态

- **关键指标** – 将显示关键指标详细信息，例如**响应时间**、**5xx 错误**、**每秒请求数**、**吞吐量**、**客户端连接数**、**服务器连接数**和**数据量**。

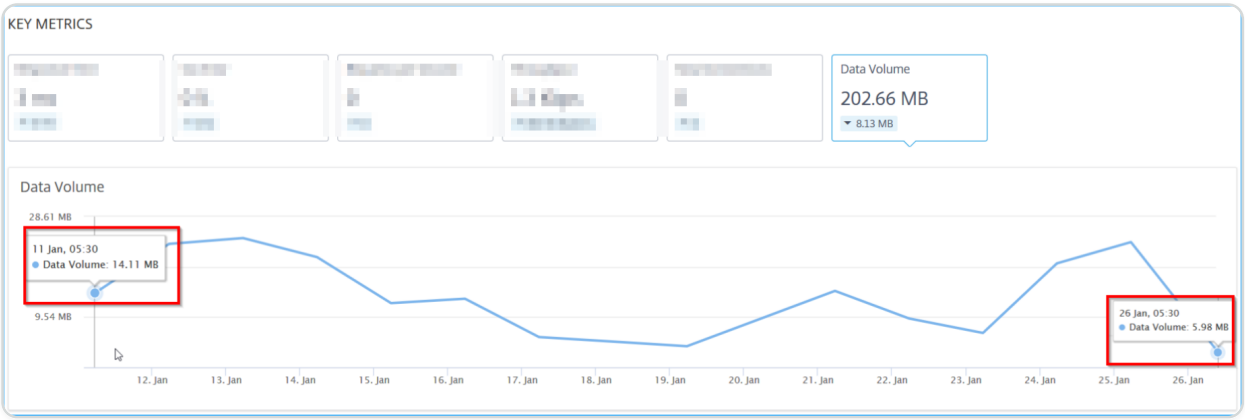
  在每个指标中，您可以查看选定时间段内的平均值和差值。差值计算方式为选定时间段内的**第一个值减去最后一个值**。

  您可以以图表形式查看选定时间段内的以下实例指标：



  下图是关于**数据量**的示例，选定的时间段为 1 个月。值 202.66 MB 是 1 个月期间的总数据量，值 8.13 MB 是差值。在图表中，第一个值是 14.11，最后一个值是 5.98。差值为 14.11 – 5.98 = 8.13 MB。

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



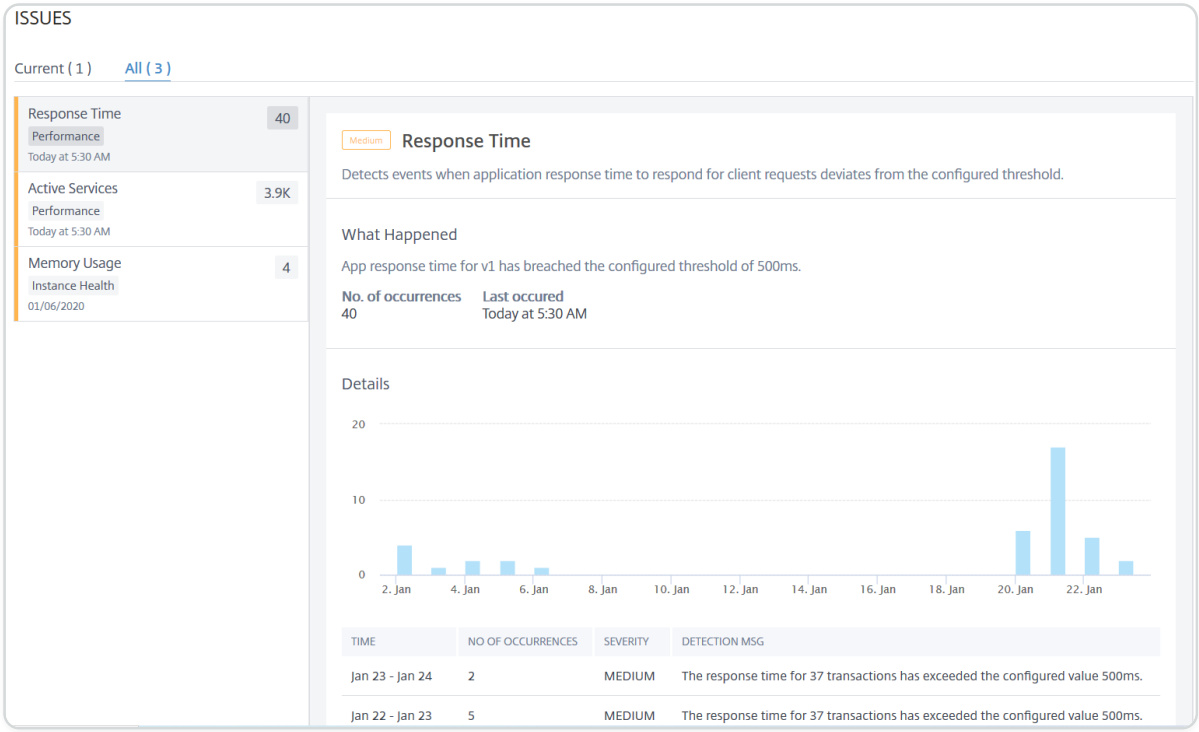
- **问题** – 适用于所选应用程序的问题。您可以查看以下问题及其类别：

性能	实例运行状况	配置	系统资源
响应时间	平均 CPU 使用率	高 5xx 响应	不正确的持久性类型
低会话重用	内存使用情况	异常大的 HTTP 数据包	网卡饱和
SurgeQueue 堆积		TCP 重组队列达到限制	
SSL 实时流量			

单击每个问题以查看以下信息：

- 总发生次数
- 解决问题的建议操作
- 问题详细信息，例如时间、服务名称、总发生次数、严重性和检测消息

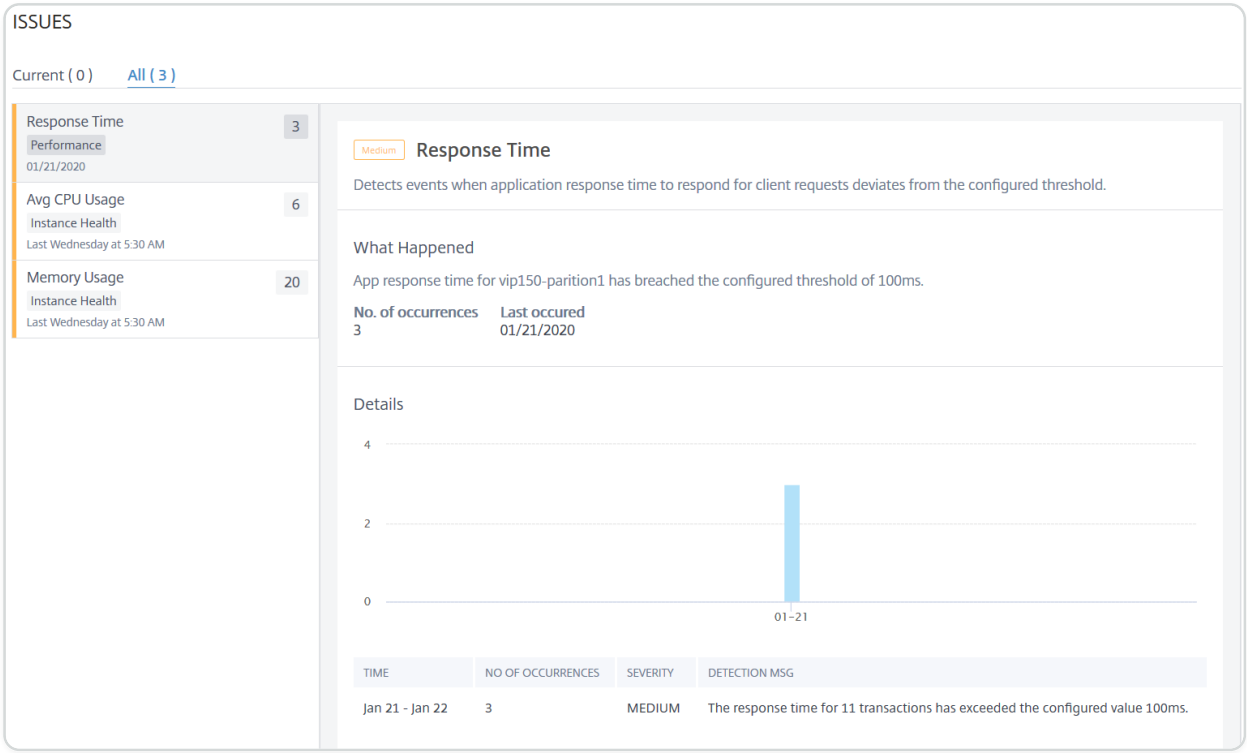
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 在 **Current** 选项卡中显示的问题是指选定时间段内的应用程序问题。
- 在 **All** 选项卡中显示的问题是指所有应用程序问题。

以下示例是 1 天持续时间的应用程序问题。**Current** 选项卡表示没有影响应用程序分数的当前问题。

全部选项卡显示 1 天内检测到的总问题。



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

智能应用分析

智能应用分析使您能够使用机器学习和基于规则的算法识别应用程序性能问题。NetScaler Console 的智能应用分析功能：

- 提供了一个简单且可扩展的解决方案，用于监控和故障排除通过 NetScaler 实例交付的应用程序。
- 监控应用程序的所有级别，以减少故障排除问题的周转时间并提高应用程序的整体正常运行时间。

在典型的部署中，数千台服务器满足用户的数据需求。发送到这些服务器的流量由 NetScaler 设备上配置的虚拟服务器进行负载均衡和监控。每个虚拟服务器都绑定到代表后端服务器的多个服务。在此类部署中，智能应用分析功能可帮助您：

- 在中断和其他事件期间进行监控、管理和决策
- 监控为应用程序配置的虚拟服务器和服务
- 显示有关虚拟服务器和服务的关键信息，以便您可以根据需要更改配置，从而实现应用程序的最佳性能。

当您扩展组织服务器场时，很难跟踪与服务器接收到的巨大流量相关的问题，并缩小范围以进行所需的故障排除。

当应用程序正在运行并接收大量流量时，您可能会遇到各种问题。您可以通过导航到 **应用程序** > **仪表板**，选择一个应用程序，然后向下滚动以在 **问题** 部分中查看问题来查看应用程序分析的性能指标。

配置智能应用分析

注意：

从 **14.1-21.x 版本**开始，在添加到 NetScaler Console 的新 NetScaler 实例中，指标收集器默认处于禁用状态。现有托管实例的指标收集器配置保持不变。

智能应用分析功能仅在 **NetScaler 12.1.50.x 或更高版本**中受支持。**指标收集器**将 NetScaler 计数器数据推送到 NetScaler Console，用于检测应用程序问题。要使用智能应用分析功能，必须在每个 NetScaler 实例上配置**指标收集器**。

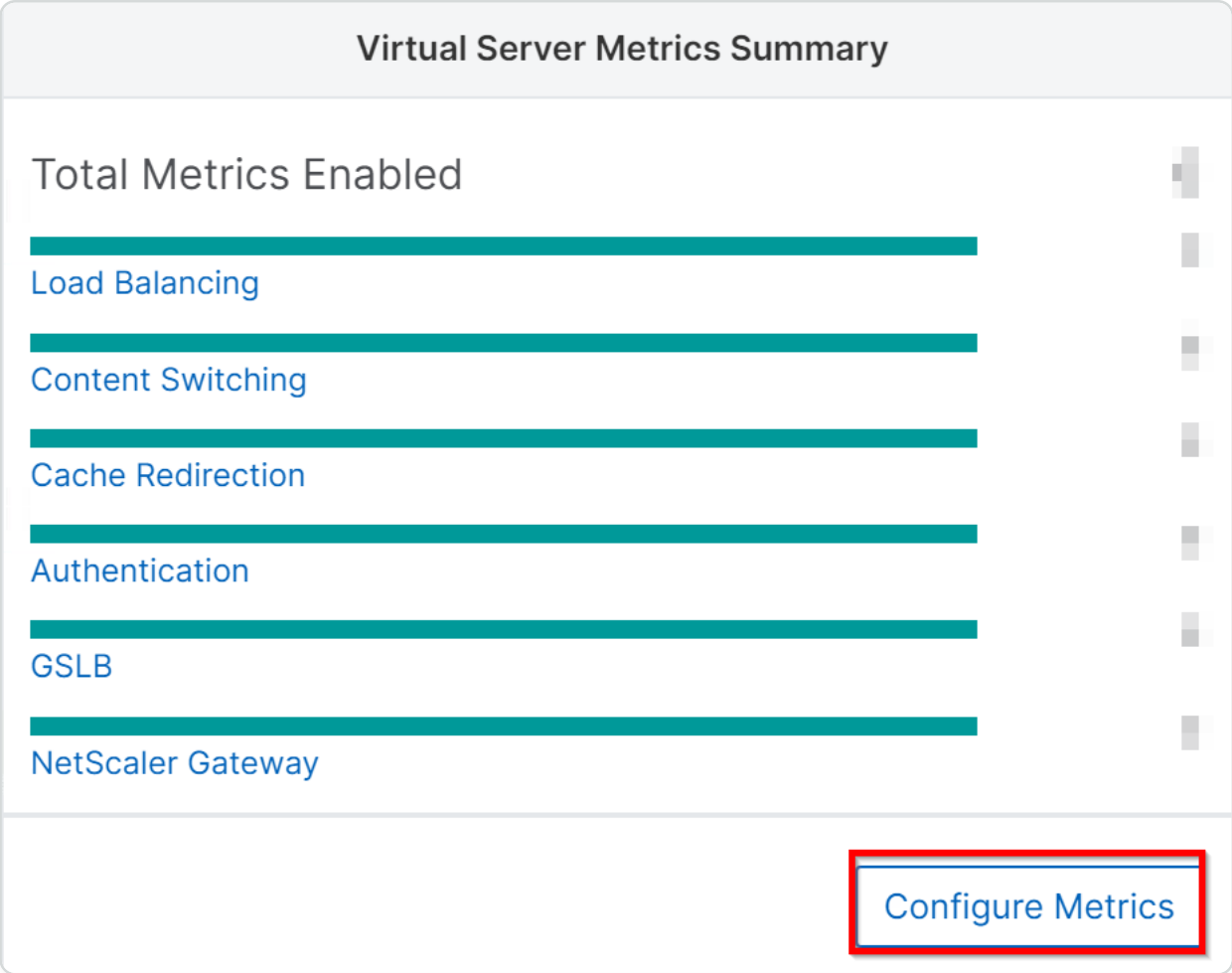
从 14.1-29.x 版本开始，指标收集器和精简使用情况分析在虚拟服务器级别而不是实例级别启用。借助此增强功能，指标收集器和精简使用情况分析仅在具有高流量的活动虚拟服务器上保持启用状态。

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

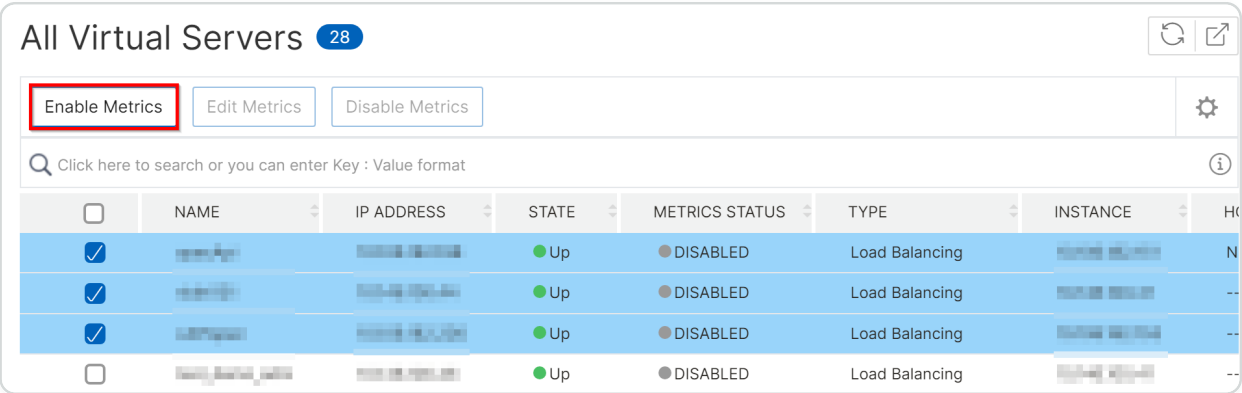
您可以查看您的虚拟服务器，并在其他虚拟服务器上启用指标收集器和精简使用情况

要查看和启用**指标收集器**：

1. 导航到 **设置 > 分析配置**。
2. 在**虚拟服务器指标摘要**下，单击**配置指标**。

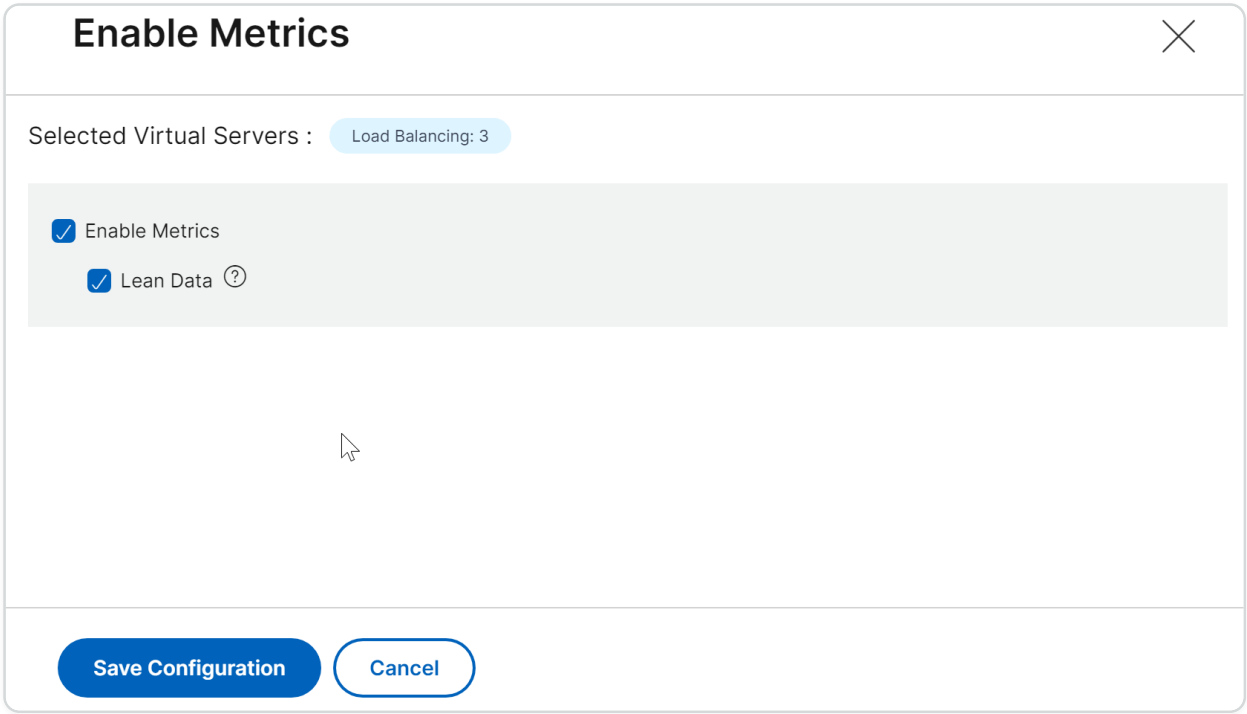


3. 在**所有虚拟服务器**页面上，您可以查看每个虚拟服务器上的指标收集器状态。选择要启用的虚拟服务器，然后单击**启用指标**。



4. 选择**启用指标**以启用指标收集器。如果要启用和查看精简期使用情况分析，还可以选择**精简数据**。选择后，单击**保存配置**。有关详细信息，请参阅高峰期和精简期使用情况分析。

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



或者，您也可以从 NetScaler 实例页面为虚拟服务器启用指标收集器和精简使用情况：

1. 导航到**基础架构 > 实例**，选择实例类型，然后从**选择操作**列表中选择**指标收集器**。
2. 选择要为其启用指标收集器的虚拟服务器，然后单击**启用指标**。
3. 选择**启用指标**以启用指标收集器。如果要启用和查看精简周期使用情况分析，还可以选择**精简数据**。选择后，单击**保存配置**。

在虚拟服务器上启用**指标收集器**选项后，导航到**应用程序** > **仪表板**。选择一个实例以在**问题**部分下查看异常。

注意

要查看**服务器错误**及其**详细 Web 事务**的异常，您必须在虚拟服务器上启用分析。

应用程序分析的性能指标

您可以查看 NetScaler Web 应用程序中出现的性能指标及其类别。要查看这些指标，您必须确保在 NetScaler 实例上启用分析和 (/zh-cn/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/dashboard/intelligent-app-analytics/configure-intelligent-app-analytics.html)：

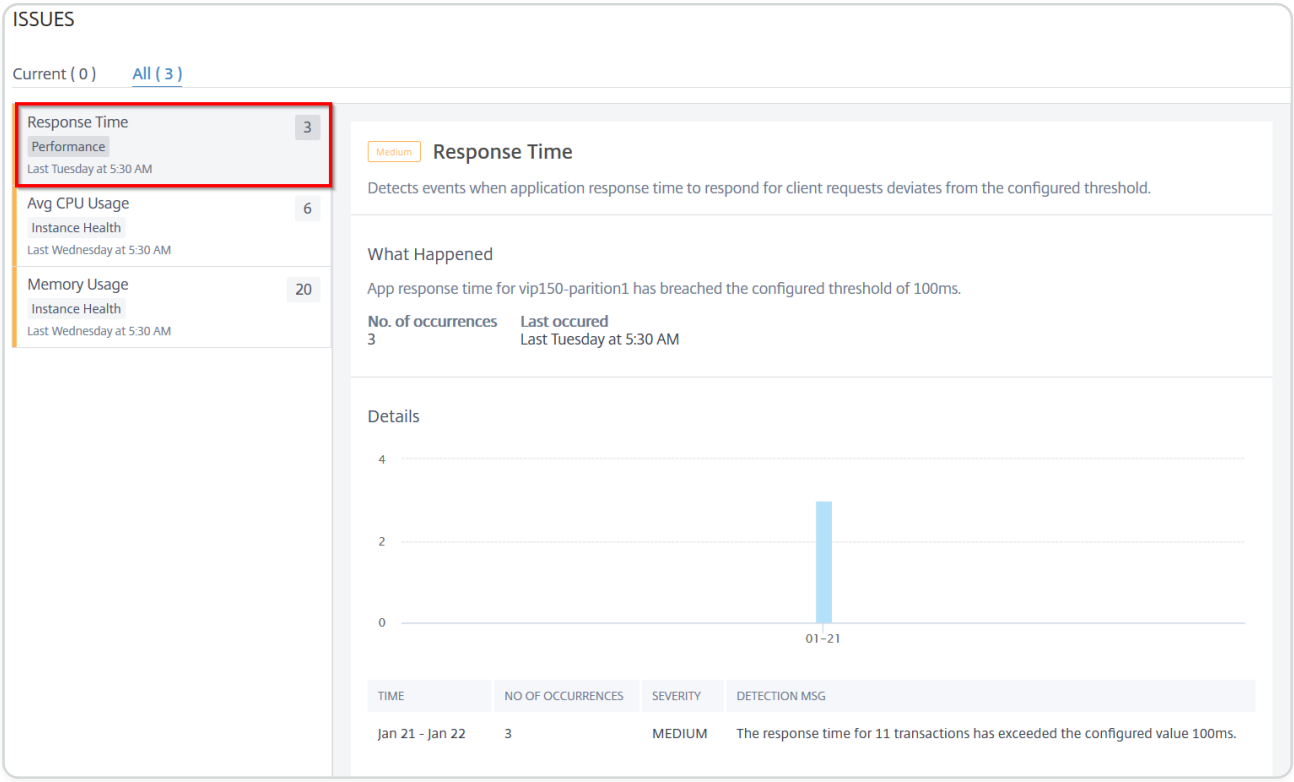
启用分析和指标收集器后，您可以通过导航到 **应用程序** > **仪表板**，选择一个应用程序，然后向下滚动到 **问题** 部分来查看以下指标：

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

- 响应时间
- 活动服务
- 平均 CPU 使用率
- 内存使用率
- 网卡饱和度
- 服务抖动
- 会话重用率低
- 不正确的持久性类型
- 不稳定服务器 (5xx)
- SSL 实时流量
- 异常大的 HTTP 数据包
- TCP 重组队列限制命中
- 激增队列积压

响应时间

当应用程序响应客户端请求的响应时间偏离配置的阈值时，此问题会被检测到。单击“**响应时间**”选项卡可查看问题详细信息。



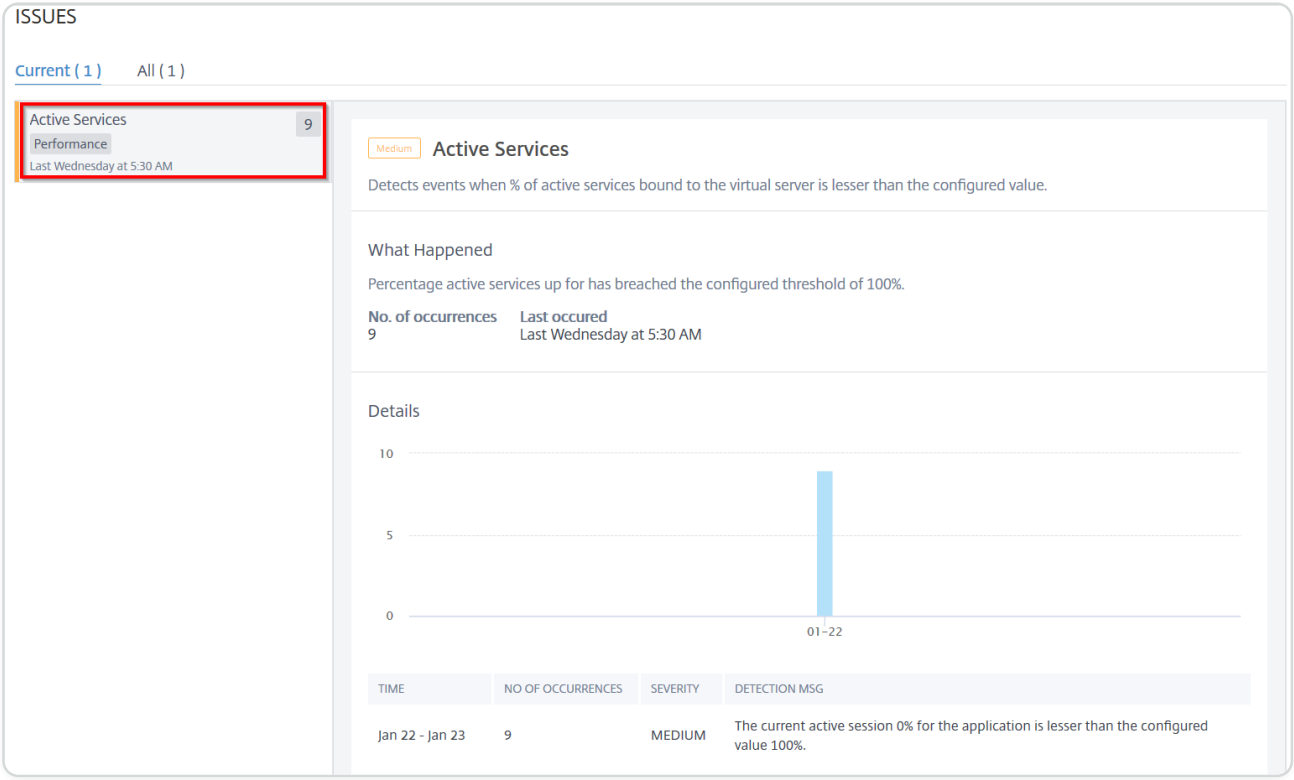
在“**详细信息**”下，您可以查看：

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

- 显示所选时间段内总事件数的图表。单击以应用筛选器并查看详细信息
- 问题发生的时间
- 所选时间段内的总发生次数
- 问题严重性，例如低、中和高
- 检测消息，指示总事务响应时间超过配置的阈值

活动服务

此问题检测到绑定到虚拟服务器的活动服务百分比低于配置的阈值。单击“**活动服务**”选项卡以查看问题详细信息。



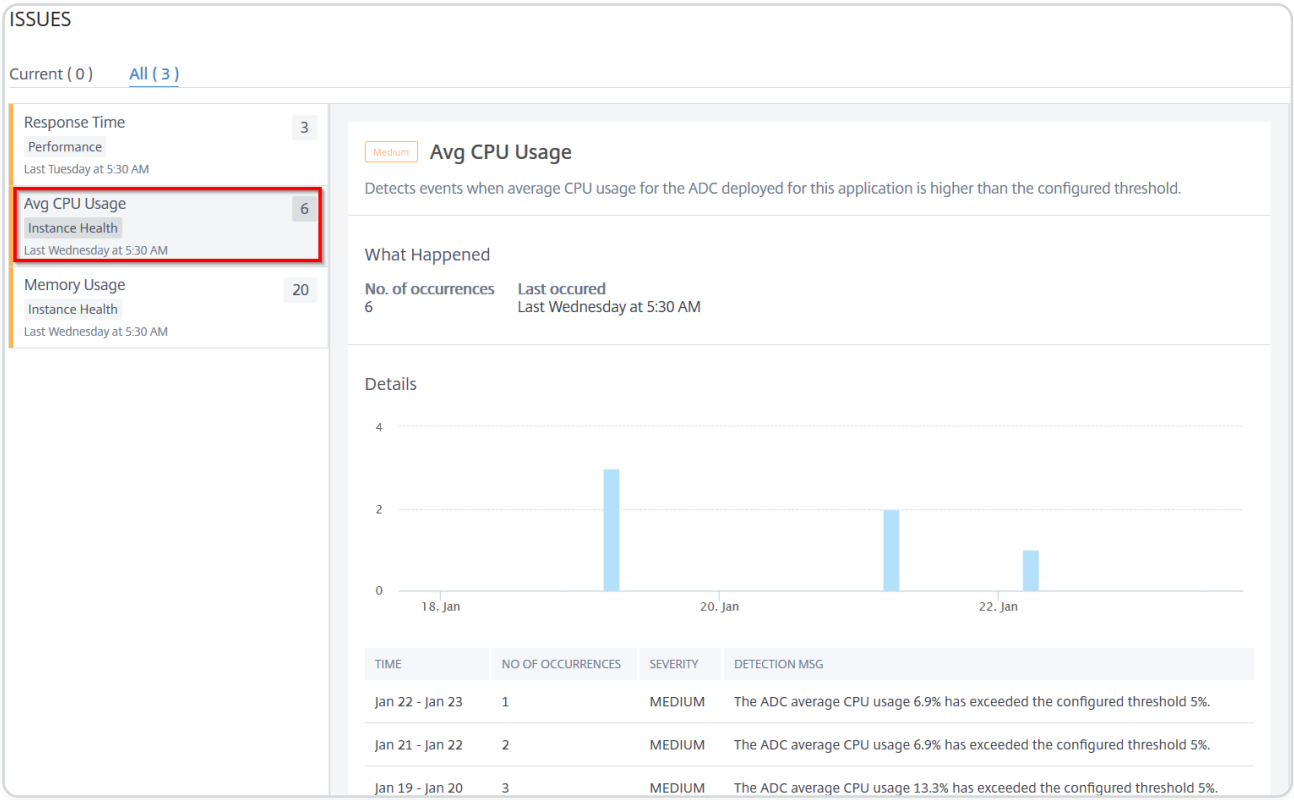
在“**详细信息**”下，您可以查看：

- 显示所选时间段内总事件数的图表。单击以应用筛选器并查看详细信息
- 问题发生的时间
- 所选时间段内的总发生次数
- 问题严重性，例如低、中和高
- 指示活动服务会话百分比和配置的阈值的检测消息

平均 CPU 使用率

此问题检测到此应用程序的 NetScaler CPU 使用率超出配置的阈值。单击“**平均 CPU 使用率**”选项卡以查看问题详细信息。

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



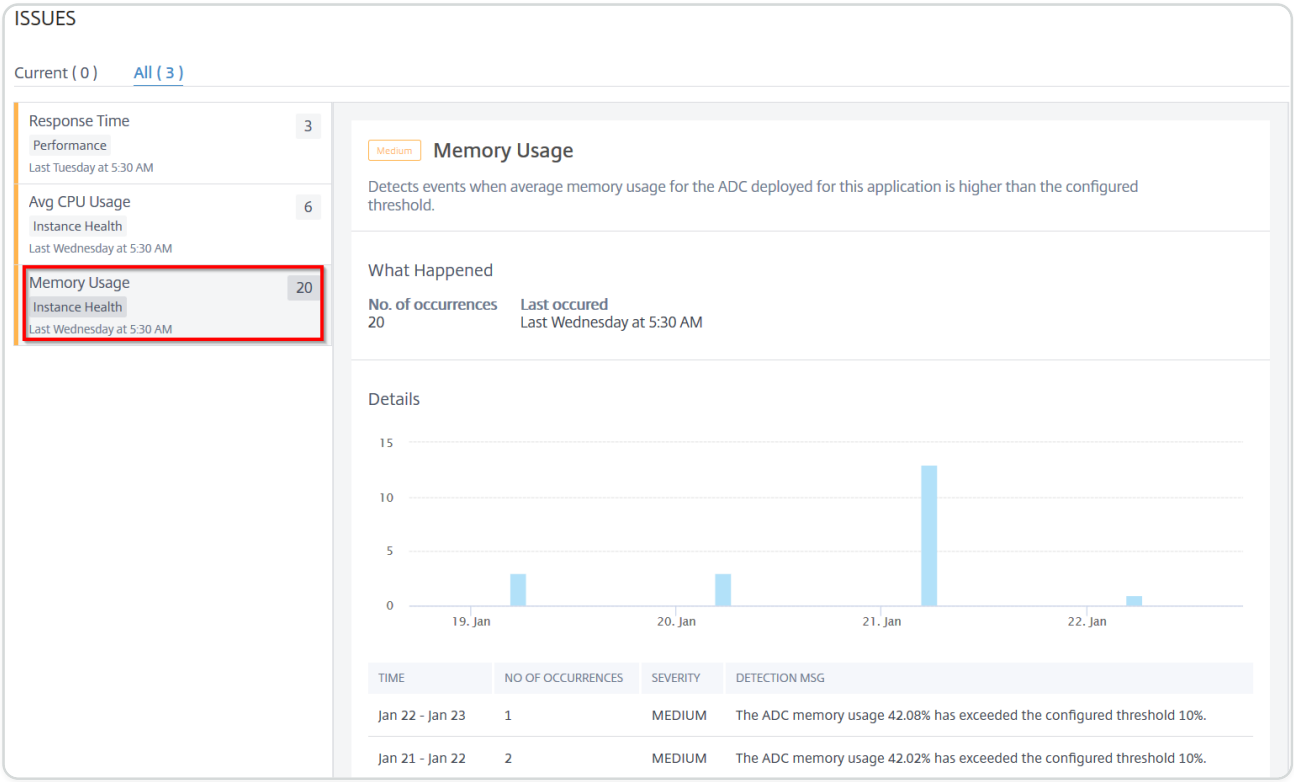
在“**详细信息**”下，您可以查看：

- 显示所选时间段内总事件数的图表。单击以应用筛选器并查看详细信息
- 问题发生的时间
- 所选时间段内的总发生次数
- 问题的严重性，例如低、中和高
- 指示 NetScaler 平均 CPU 使用率百分比和配置阈值的检测消息

内存使用情况

此问题检测到此应用程序的 NetScaler 内存使用情况超出配置的阈值。单击“**内存使用情况**”选项卡可查看问题详细信息。

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



在“**详细信息**”下，您可以查看：

- 指示所选时间段内总事件数的图表。单击以应用筛选器并查看详细信息
- 问题发生的时间
- 所选时间段内的总发生次数
- 问题严重性，例如低、中和高
- 指示 NetScaler 平均内存使用百分比和配置的阈值的检测消息

服务抖动

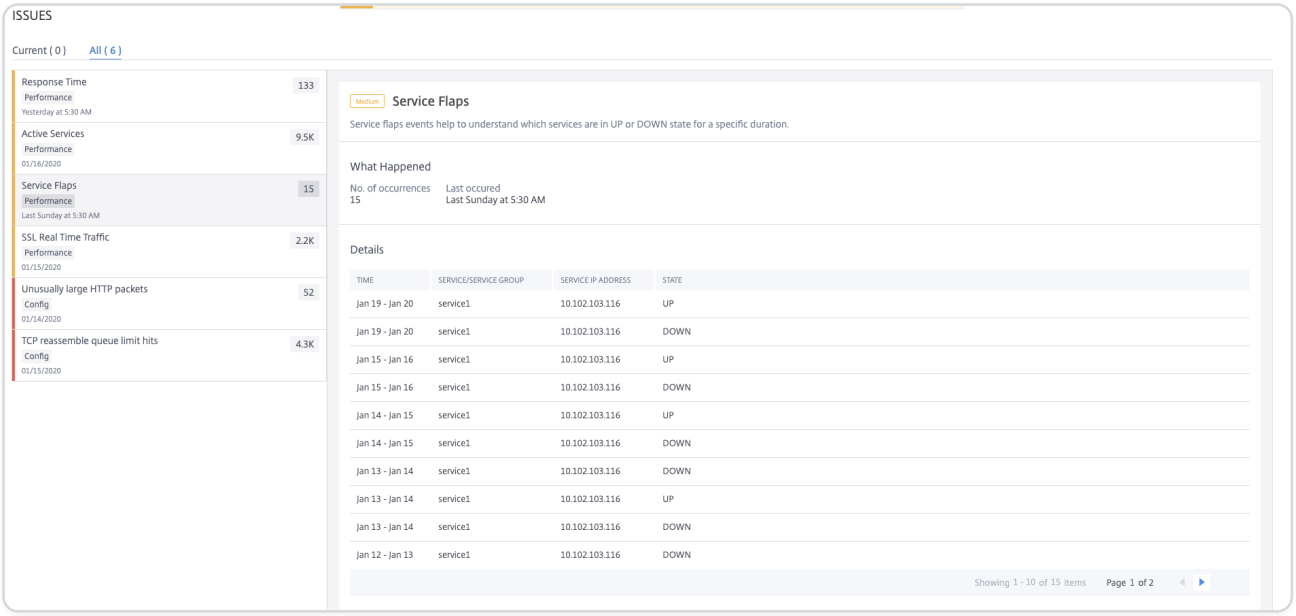
作为网络管理员，您必须确保应用程序的最佳可用性。当存在任何网络问题或配置问题时，应用程序服务器的状态和可用性可能会影响整体性能。

通过服务抖动事件，您可以识别存在问题的应用程序。服务抖动事件还可以帮助您：

- 了解在特定持续时间内处于 DOWN 状态的服务
- 了解在特定持续时间内有多少服务处于 UP 或 DOWN 状态

单击“**服务抖动**”选项卡以查看服务抖动详细信息。

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



您可以查看详细信息，例如发生次数和上次发生时间。

在“**详细信息**”下，您可以查看：

- 发生服务抖动异常的时间
- 服务/服务组名称
- 服务 IP 地址
- 当前服务状态

不稳定服务器

在某些情况下，Web 服务器在无法处理请求时会返回状态码，原因可能是无效请求、临时过载或服务器维护。这些错误会以错误代码的形式显示，这些代码定义了各种错误场景。例如，

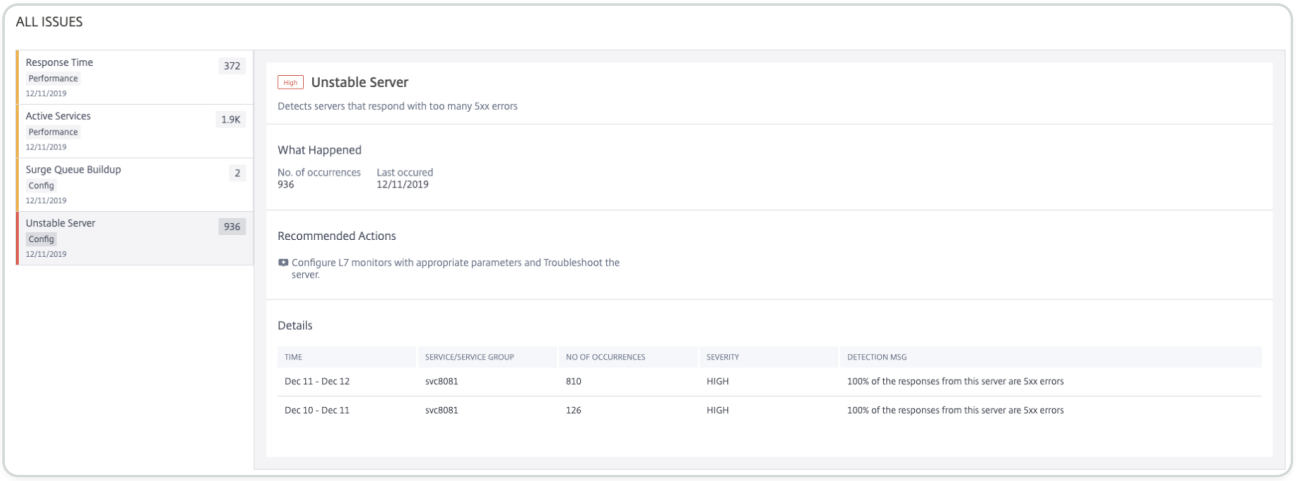
- **502 错误网关** 服务器作为网关或代理，从上游服务器接收到无效响应。
- **503 服务不可用** 服务器当前不可用。服务器可能过载或正在维护中。
- **504 网关超时** 服务器作为网关或代理，未及时从上游服务器接收到响应。

这些可能是临时情况，但有时您必须在 Web 服务器上实施纠正措施，以使网页正常运行并可用。

使用**不稳定服务器**指示器，您可以查看这些故障并决定采取纠正措施来解决问题，确保客户端请求得到服务，并且网页始终可用。

选择**不稳定服务器**选项卡以查看问题详细信息。

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



解决此问题的**建议操作**包括：

- 为响应 5xx 错误的服务器配置具有适当参数的 L7 监视器。监视器是跟踪服务运行状况的实体。设备使用绑定到每个服务的监视器定期探测服务器。如果服务器未在指定的响应超时内响应，并且指定的探测失败，则服务将被标记为 DOWN。然后，设备会在剩余服务之间执行负载平衡。有关配置监视器的更多信息，请参阅自定义监视器
- 对服务器进行故障排除

在**详细信息**下，您可以查看：

- 发生不稳定服务器异常的时间
- 服务/服务组名称
- 总发生次数
- 异常严重性，例如高、低和中
- 检测消息，指示此服务报告 5xx 错误的响应百分比

有关服务器错误 Web 事务的详细信息，请参阅服务器错误的 Web 事务分析

会话堆积

对于所有安全事务，NetScaler 会对第一个事务执行 SSL 卸载过程，然后根据“**会话重用**”配置存储 SSL 会话。

根据流量速率，会话堆积可能会在一段时间内发生，这可能导致 NetScaler 中大量内存被这些会话占用。

会话堆积事件会提醒管理员并提供解决此事件的建议操作。单击“**会话堆积**”选项卡以查看问题详细信息

在“**详细信息**”下，您可以查看：

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

- 发生会话堆积异常的时间
- 虚拟服务器名称
- 异常严重性，例如高、低和中
- 消息指示虚拟服务器中有 **X** 个 SSL 会话可用，并且当前在配置的超时会话中每秒有 **Y** 次 SSL 握手。

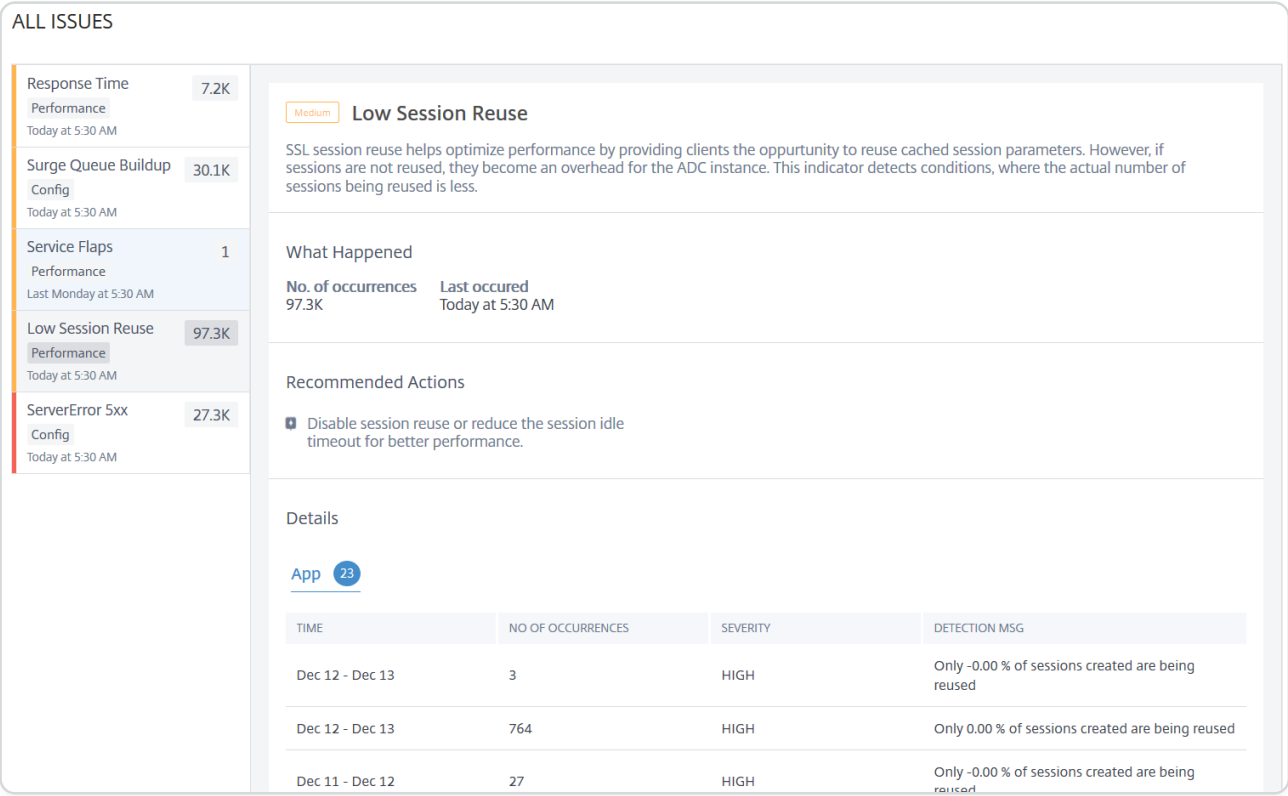
修复此异常的**建议操作**是减少会话超时或禁用会话重用。有关详细信息，请参阅会话超时。

低会话重用

NetScaler 实例通过从服务器卸载 SSL 握手过程来处理 SSL 事务。收到服务器响应后，NetScaler 实例完成与客户端的安全事务。使用缓存的会话参数，NetScaler 实例完成后续请求的 SSL 握手过程。

如果这些会话未被重用，它们将成为 NetScaler 实例的开销。使用**低会话重用**指示器，您可以识别实际重用的会话数量是否较少。

单击**低会话重用**选项卡以查看问题详细信息。



解决此问题的**建议操作**是禁用会话重用或缩短会话超时。有关更多信息，请参阅会话重用。

在**详细信息**下，您可以查看：

- 具有低会话重用率的总应用程序数

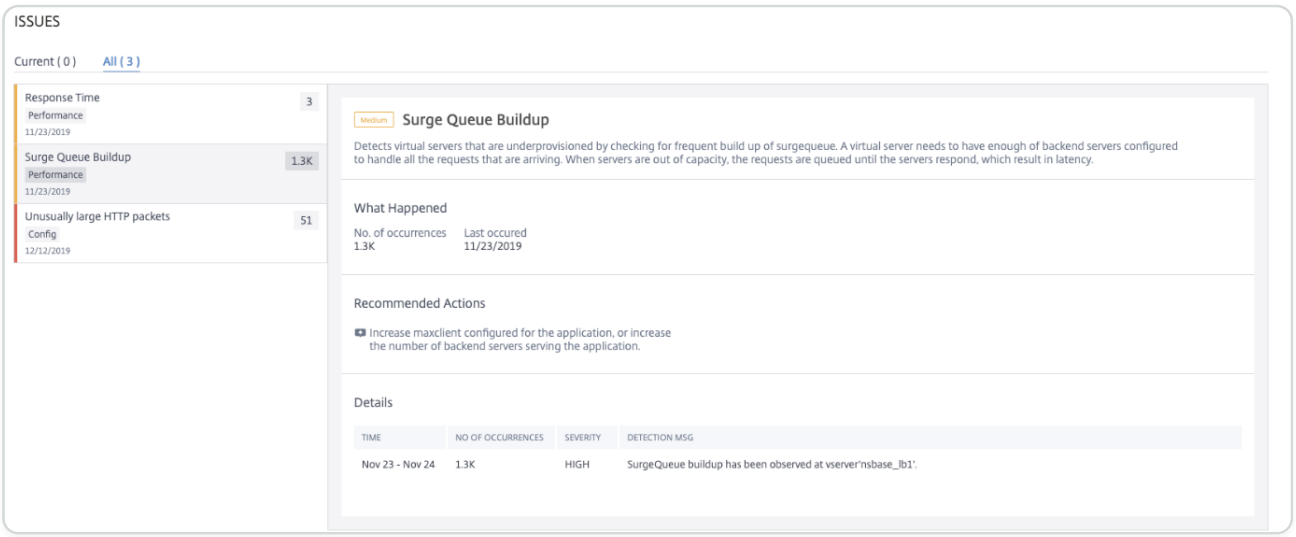
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 发生低会话重用异常的时间
- 总发生次数
- 异常严重性，例如高、低和中
- 检测消息，指示只有 % 的配置会话正在被重用

突发队列积压

当服务器收到大量突发请求时，服务器响应客户端的速度会变慢。通常，过载还会导致客户端收到错误页面。虚拟服务器需要配置足够的后端服务器来处理传入请求。

使用**突发队列积压**指示器，您可以查看存在突发队列积压的虚拟服务器。单击**突发队列积压**选项卡以查看问题详细信息。



解决此问题的**建议操作**包括：

- 增加客户端连接数限制。有关详细信息，请参阅设置客户端连接数限制
- 增加后端服务器以处理应用程序请求

在**详细信息**下，您可以查看：

- 发生突发队列积压异常的时间
- 总发生次数
- 异常严重性，例如高、低和中
- 指示虚拟服务器上突发队列积压的检测消息

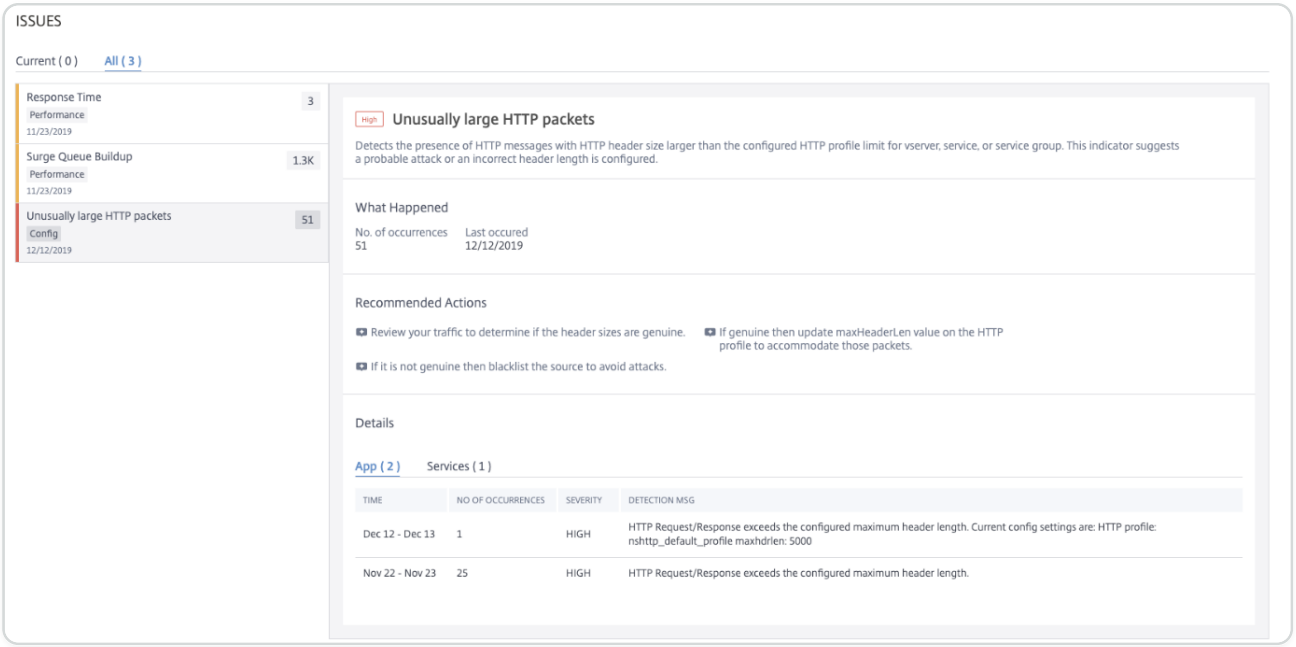
异常大的 HTTP 数据包

HTTP 事务使用客户端和服务器之间的请求-响应消息。在请求和响应消息中，HTTP 标头是 HTTP 协议中显示的值。您可以在虚拟服务器、服务或服务组中配置 HTTP 标头长度，以避免 4xx 错误。

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

当 HTTP 请求/响应超过最大标头长度时，这可能是一种攻击。使用 **异常大的 HTTP 数据包** 指标，您可以查看 HTTP 消息的 HTTP 标头大小超过配置值的情况。

单击 **异常大的 HTTP 数据包** 选项卡以查看问题详细信息。



解决此问题的 **建议操作** 如下：

- 检查流量以确定标头大小是否真实。如果标头大小真实，则更新 HTTP 配置文件上的标头值。有关更多信息，请参阅 缓冲区溢出检查。
- 如果标头大小不真实，则将源列入黑名单以避免攻击。

在 **详细信息** 下，您可以查看：

- 异常发生的时间
- 总发生次数
- 异常严重性，例如高、低和中
- 指示在虚拟服务器、服务器或服务组上配置的当前 HTTP 标头长度的检测消息

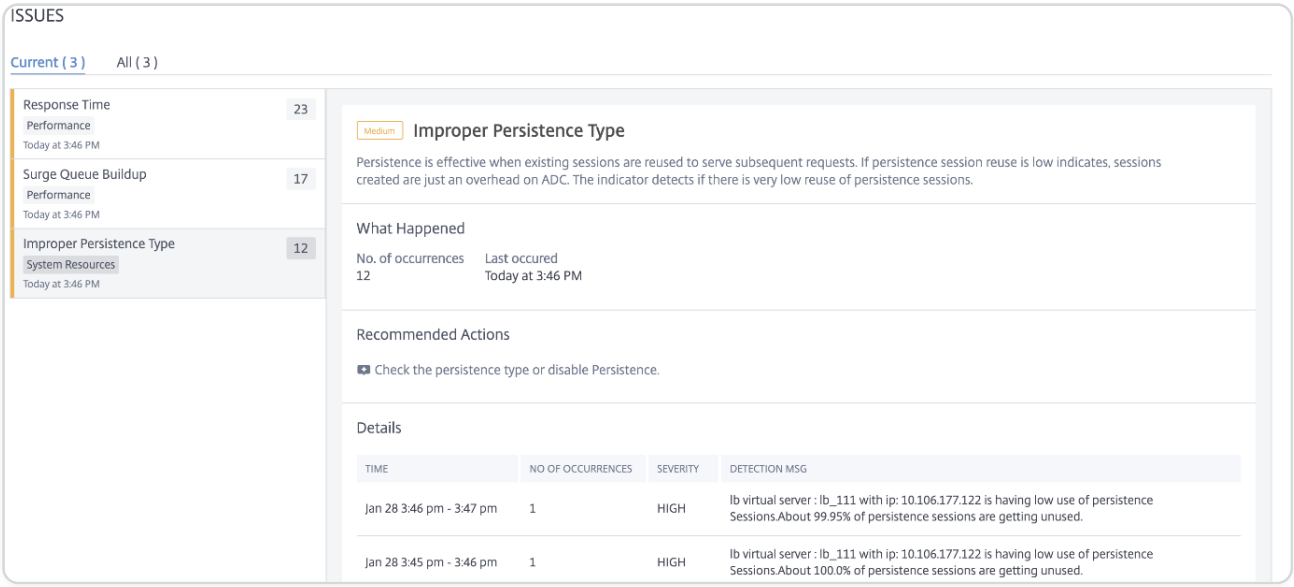
不当的持久性类型

如果您希望在由虚拟服务器表示的服务器上维护连接状态（例如，电子商务中使用的连接），则必须在该虚拟服务器上配置持久性。设备随后会使用配置的负载平衡方法进行初始服务器选择，但会将来自同一客户端的所有后续请求转发到同一服务器。

当现有会话被重用来处理后续请求时，持久性是有效的。如果持久性会话重用率较低，则在 NetScaler 上创建的会话只会增加开销。

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

使用“**不当持久性类型**”指示器，您可以确定虚拟服务器上的持久性使用率是否较低。单击“**不当持久性类型**”选项卡以查看问题详细信息。



解决此问题的“**建议操作**”是检查持久性类型或禁用持久性。有关详细信息，请参阅持久性设置。

在“**详细信息**”下，您可以查看：

- 发生异常的时间
- 总发生次数
- 异常严重性，例如高、低和中
- 指示未使用的会话百分比的检测消息

TCP 重组队列达到限制

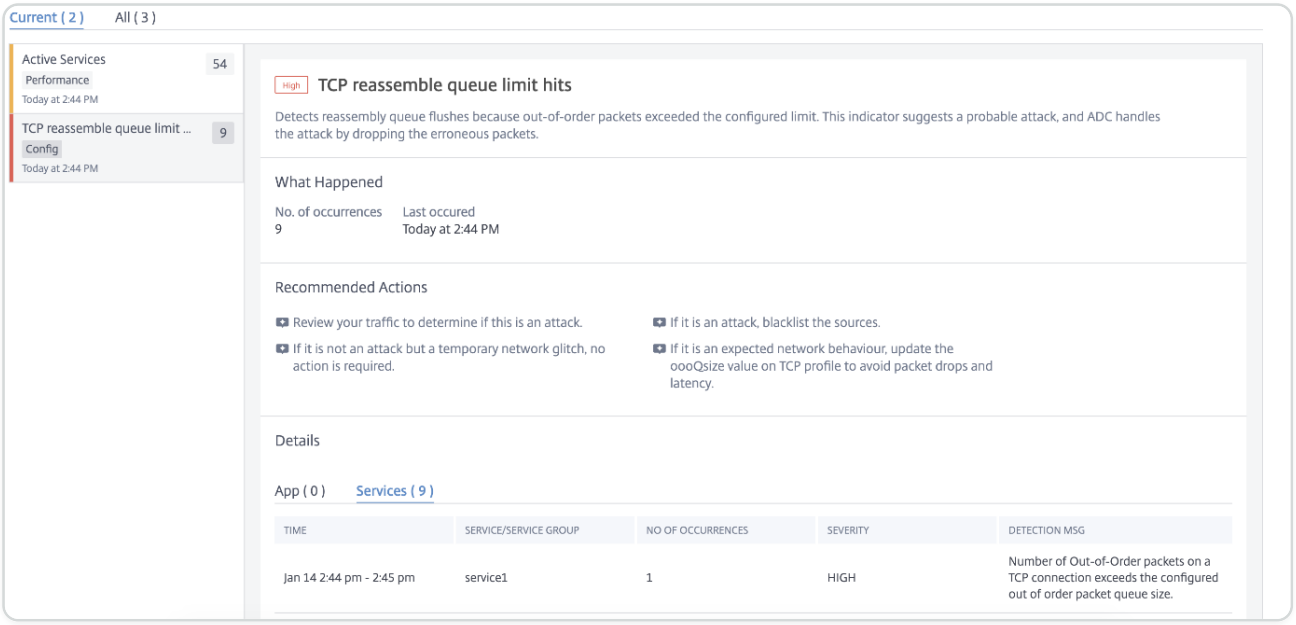
TCP 维护一个乱序队列，用于在 TCP 通信中保存乱序数据包。如果队列大小过长，此设置会影响 NetScaler 内存，因为数据包需要保存在运行时内存中。

此队列大小需要根据网络和应用程序特性调整到优化级别。

使用 **TCP 重组队列达到限制** 指标，您可以查看 TCP 连接上的乱序数据包是否超过了配置的乱序数据包队列大小。

单击 **TCP 重组队列达到限制** 选项卡以查看问题详细信息。

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



解决此问题的 **建议操作** 如下：

- 审查流量，如果是攻击则将源列入黑名单
- 如果此行为是预期的网络行为，请更新 TCP 配置文件中的乱序数据包大小值。有关详细信息，请参阅 TCP 优化
- 如果只是临时网络故障，则无需进一步操作

在 **详细信息** 下，您可以查看：

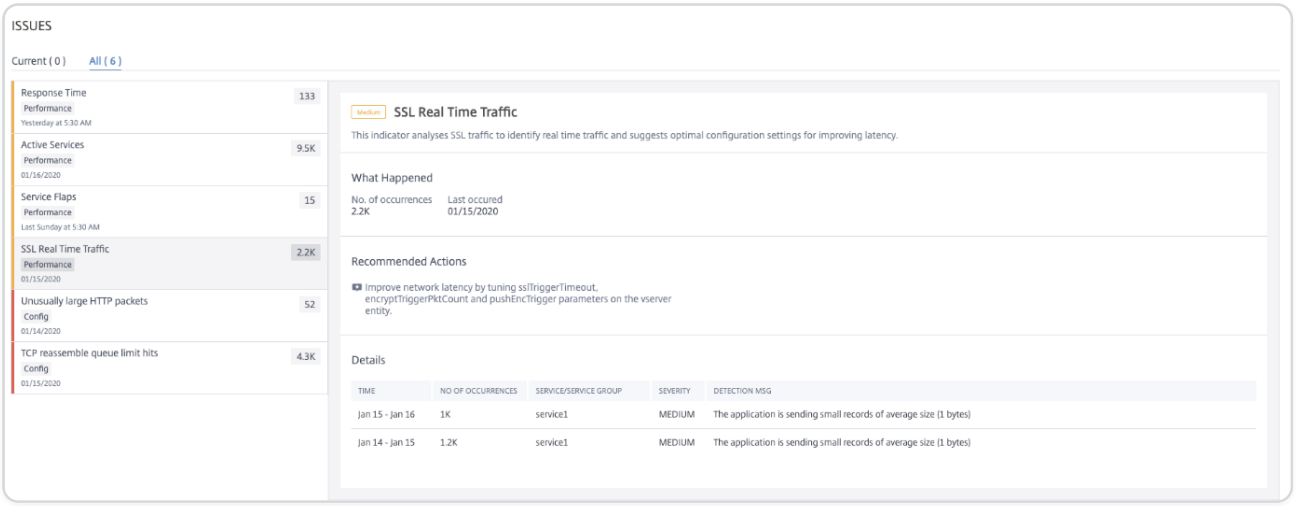
- 异常发生的时间
- 总发生次数
- 异常严重性，例如低、中和高
- 指示当前 TCP 配置文件和 oooQsize 设置的检测消息

SSL 实时流量

在 NetScaler 实例中，您可以使用 SSL 配置文件来处理 SSL 流量。SSL 配置文件包含用于虚拟服务器、服务和服务组的某些 SSL 参数。**SSL 实时流量** 指标分析 SSL 流量以识别实时流量，并建议最佳配置设置以改善延迟。

单击 **SSL 实时流量** 选项卡以查看问题详细信息。

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



解决此问题的**建议操作**是通过更新 SSL 参数来改善网络延迟。有关更多信息，请参阅全局 SSL 参数。

在**详细信息**下，您可以查看：

- 异常发生的时间
- 服务/服务组名称
- 异常严重性，例如低、中和高
- 检测消息以及应用程序上的当前设置

应用程序仪表板故障排除

在应用程序仪表板中添加应用程序后，仪表板会立即显示应用程序的基本配置详细信息。应用程序分析详细信息（例如应用程序分数、关键指标和问题）会在几分钟内（大约 10 到 15 分钟）开始填充。有关详细信息，请参阅 应用程序。

您必须确保来自 NetScaler 实例的指标数据流（AppFlow 收集器或分析配置文件）没有问题。您可以在本文档中获取有关 AppFlow 收集器和分析配置文件的更多信息。

本文档介绍了在以下情况下需要执行的故障排除步骤：

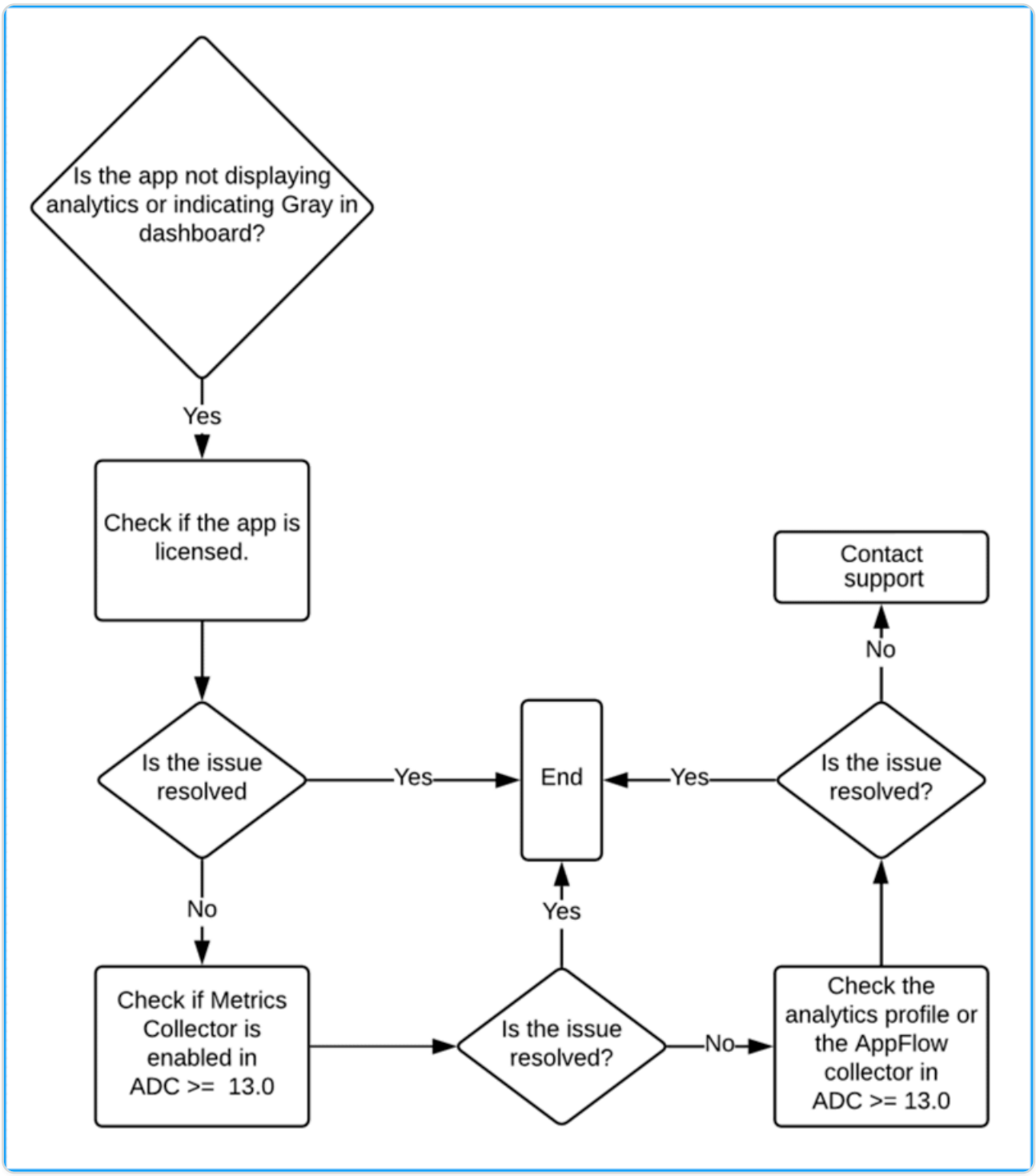
- 您单击应用程序后，即使在指定持续时间（10-15 分钟）之后，所选应用程序的分析数据也未显示所需数据。
- CS 或 LB 应用程序在应用程序仪表板中始终显示灰色（**不适用**状态）。

注意

本文档中提及的故障排除过程仅适用于**内容交换**和**负载平衡**虚拟服务器。

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

故障排除场景



应用程序已获得许可

您必须确保应用程序已获得许可。从 **14.1-21.x** 版本开始，所有虚拟服务器都会自动获得许可。如果您使用的是早期版本，请导航到 **Settings > Licensing & Analytics Configuration** 并验证应用程序是否在 **Virtual Server License Summary** 下获得许可。如果应用程序未获得许可，请参阅 管理许可并在虚拟服务器上启用分析。

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

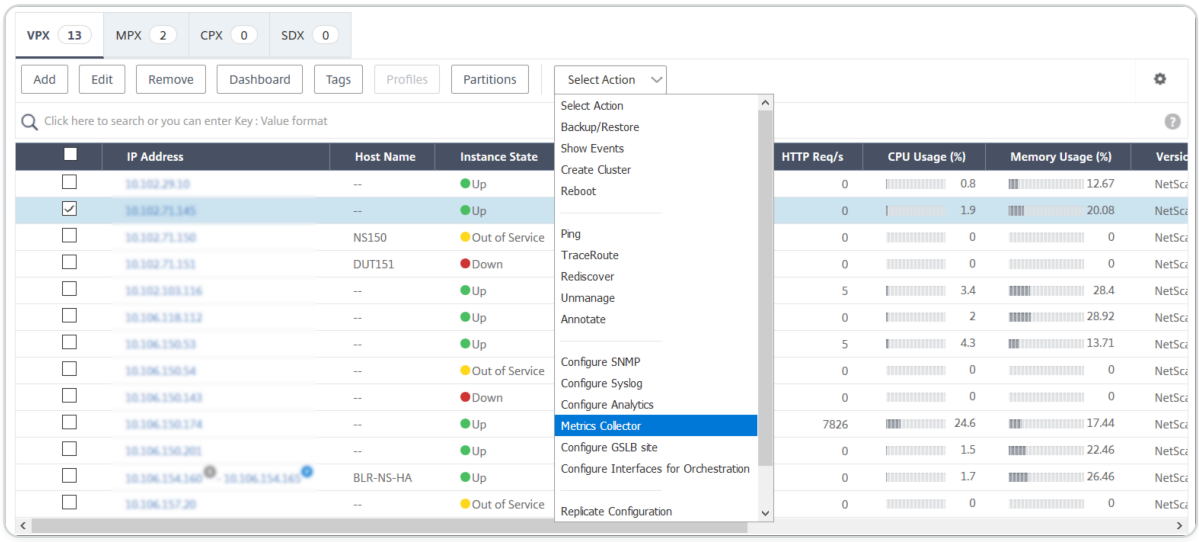
指标收集器已启用

注意：

从 **14.1-21.x 或更高版本**开始，在 NetScaler Console 中添加的新 NetScaler 实例中，指标收集器默认处于禁用状态。现有托管实例的指标收集器配置保持不变。

您必须确保 NetScaler 实例中已启用 **Metrics Collector**。要确保指标收集器已启用：

1. 导航到 **Infrastructure > Instances**。在“实例”下，选择实例类型（例如，NetScaler VPX）。
2. 选择 NetScaler 实例。
   a. 从 **Select Action** 列表中，选择 **Metrics Collector**。



3. 在 **Configure Metrics Collector settings** 页面上，确保已选择 **Enable** 选项。如果未选择，请选择 **Enable** 选项，然后单击 **OK**。

启用指标收集器后，如果仍然无法查看数据，请验证：

- NetScaler 实例版本 13.0 **早于 47.x 版本** 中的 AppFlow 收集器。
- NetScaler 实例版本 **47.x 或更高版本** 中的 分析配置文件。

NetScaler® 实例早期版本

在 NetScaler 中：

1. 运行以下命令以确保收集器处于 **UP** 状态并在端口 5563 上运行：

```
sh appflow collector af_collector_rest_<adm_receiver_ip>
```

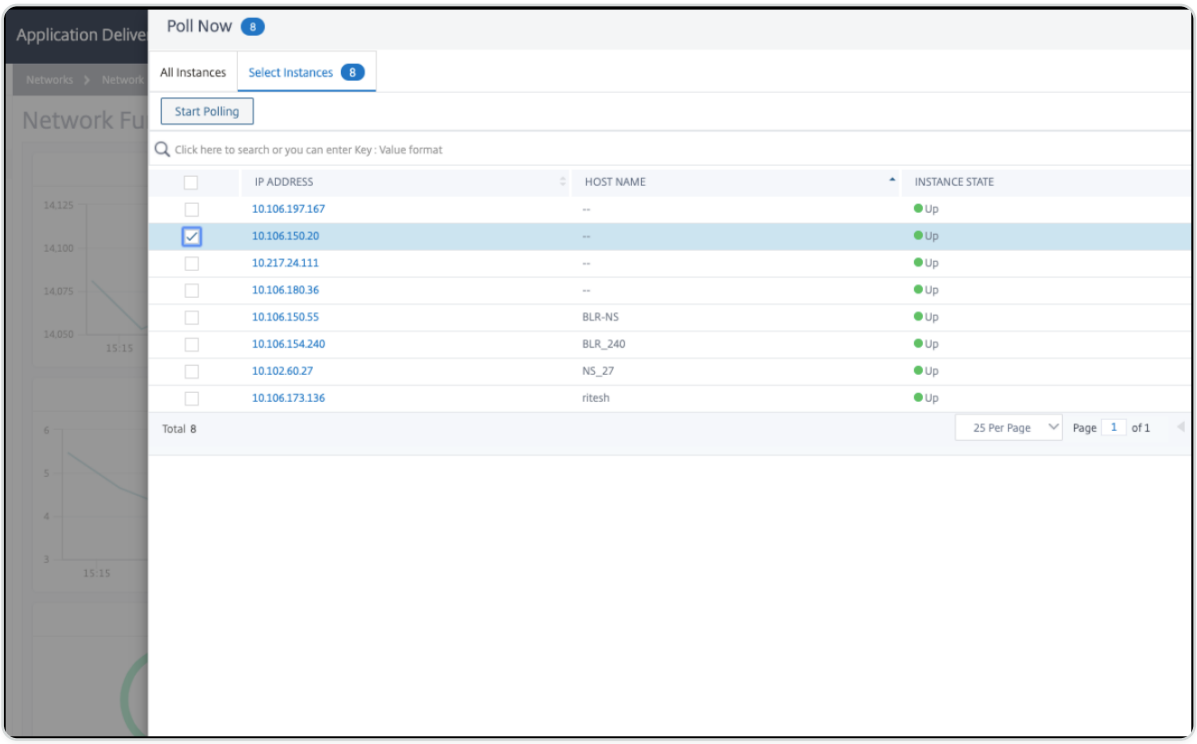
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> sh appflow collector af_collector_rest_10.102.103.114
1) Name: af_collector_rest_10.102.103.114
IPv4 address: 10.102.103.114
Port: 5563
Netprofile:
Transport: rest
State: UP
Done
```

2. 如果没有可用的收集器，请在 NetScaler Console 中执行实例手动轮询。

   a. 导航到 **基础架构 > 网络功能 > 立即轮询**

   b. 选择实例，然后单击 **开始轮询**。



   如果轮询失败，请从 NetScaler Console 中移除 NetScaler 实例，然后再次添加 NetScaler 实例。添加 NetScaler 实例时，收集器将添加到 NetScaler 上。

如果收集器指示 **关闭** 状态：

1. 确保是否已配置 SNIP。

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP            Active    Enabled  Enabled  NA       Enabled
```

   如果未配置 SNIP，则必须配置 SNIP。有关更多信息，请参阅 配置 SNIP。

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

2. 确保 NetScaler 实例可访问 NetScaler Console。

   您可以通过执行 ping 测试进行验证。运行 `ping -S <SNIP> <adm_receiver_ip>`

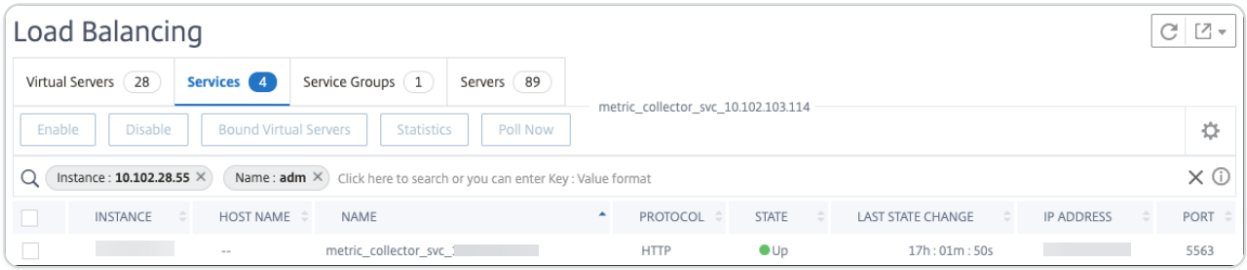
```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

NetScaler 实例后续版本

在 NetScaler Console 中，确保指标收集器服务可用：

1. 导航到 **基础架构 > 网络功能 > 负载平衡 > 服务**。
2. 在搜索栏中，按 **实例: (IP 地址)** 和 **名称: NetScaler Console** 进行筛选。
3. 确保 `adm_metric_collector_svc_<adm_receiver ip>` 可用。IP 地址可以是 NetScaler Console 管理 IP 或代理 IP。

   确保此服务处于 **UP** 状态并在端口 5563 上运行。



如果仍然无法查看数据，请确保收集器服务已绑定到 NetScaler 中的时间序列分析配置文件。

1. 登录到 NetScaler
2. 运行以下命令：

   `sh analytics profile ns_analytics_time_series_profile`

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

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

如果收集器指示 **Down** 状态：

1. 确保是否已配置 SNIP。

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP            Active   Enabled  Enabled  NA       Enabled
```

   如果未配置 SNIP，则必须配置 SNIP。有关详细信息，请参阅配置 SNIP。

2. 确保 NetScaler 实例可访问 NetScaler Console。

   您可以通过执行 ping 测试进行验证。运行 `ping -S <SNIP> <adm_receiver_ip>`

```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

3. 确保通过 telnet 的流量连接能够连接到服务。

```
root@ns# telnet 10.102.103.114 5563
Trying 10.102.103.114...
Connected to 10.102.103.114.
Escape character is '^]'.
^]
telnet> q
Connection closed.
```

   如果 telnet 能够连接到服务，则存在防火墙并正在阻止指标数据流。您必须解决防火墙阻止问题。

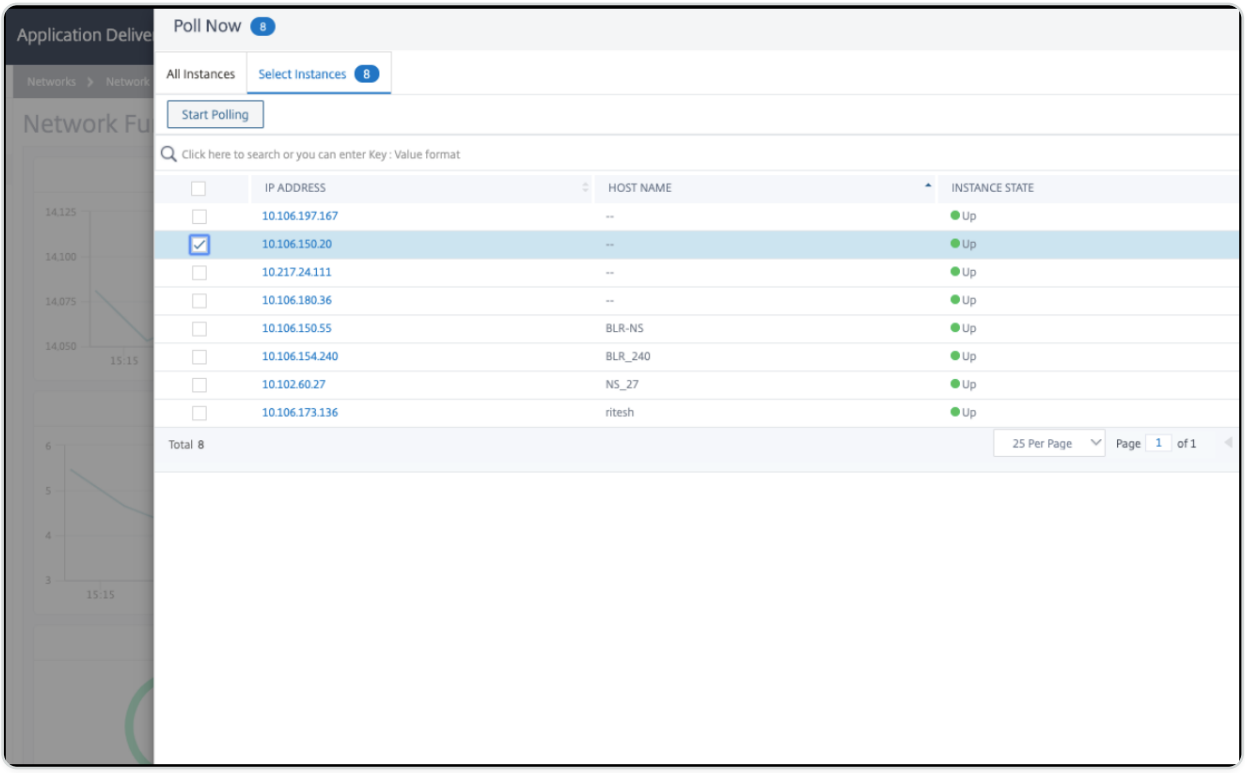
© 1997–2026 Citrix Systems, Inc. All rights reserved.

如果 NetScaler 中没有收集器服务绑定到时间序列分析配置文件，则收集器将显示为空白。

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector:
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

您必须在 NetScaler Console 中执行实例手动轮询。

1. 导航到 **Infrastructure > Network Function > 立即轮询**
2. 选择实例并点击 **开始轮询**。



如果轮询失败，请使用以下命令直接在 NetScaler 实例上添加收集器服务：

```
add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip> HTTP 5563
```

```
unset analyticsprofile ns_analytics_time_series_profile -collectors
```

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

`set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -events enabled`

分析时间序列配置文件已更新。

```
> add service adm_metric_collector_svc_10.102.103.114 10.102.103.114 HTTP 5563
 Done
> unset analyticsprofile ns_analytics_time_series_profile  -collectors
 Done
> set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_10.102.103.114 -metrics enab
 Done
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

如果在执行了所有提到的故障排除步骤之后问题仍然存在，请联系 **NetScaler 支持**。

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

应用程序使用情况和异常

作为管理员，您必须确保应用程序的利用方式。应用程序关键指标可以帮助您识别应用程序使用情况。由于应用程序的流量范围不可预测，因此在特定持续时间内可能会出现一些异常的应用程序性能偏差。在这种情况下，作为管理员，您可能希望查看和分析此类突发异常，并确保是否需要立即进行故障排除。

NetScaler Console 会检测此类异常并提供必要的详细信息。导航到 **应用程序 > 控制板**，单击一个应用程序，然后选择 **关键指标** 选项卡。NetScaler Console 会监控流量模式并分析关键指标是否在预期范围内。如果存在超出预期范围的任何偏差，NetScaler Console 会将这些偏差报告为异常。

您可以查看以下关键指标的异常：

- 响应时间
- 吞吐量
- 数据量
- 每秒请求数

  异常指标(/en-us/netscaler-application-delivery-management-software/media/anomaly-metrics.png)

单击 **异常指标** 选项卡以查看详细信息。

异常指标(/en-us/netscaler-application-delivery-management-software/media/anomaly-metrics1.png)

在每个指标中，您还可以单击 **查看更多** 选项以查看详细信息。以下示例是针对应用程序数据量的：

查看更多(/en-us/netscaler-application-delivery-management-software/media/see-more-data-volume.png)

您可以查看：

- 指示最大值、总值、预期范围和异常的图表
- 用于排查问题的**建议的操作**
- 在**详细信息**下的时间和异常详细信息

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

峰值和低谷使用情况分析

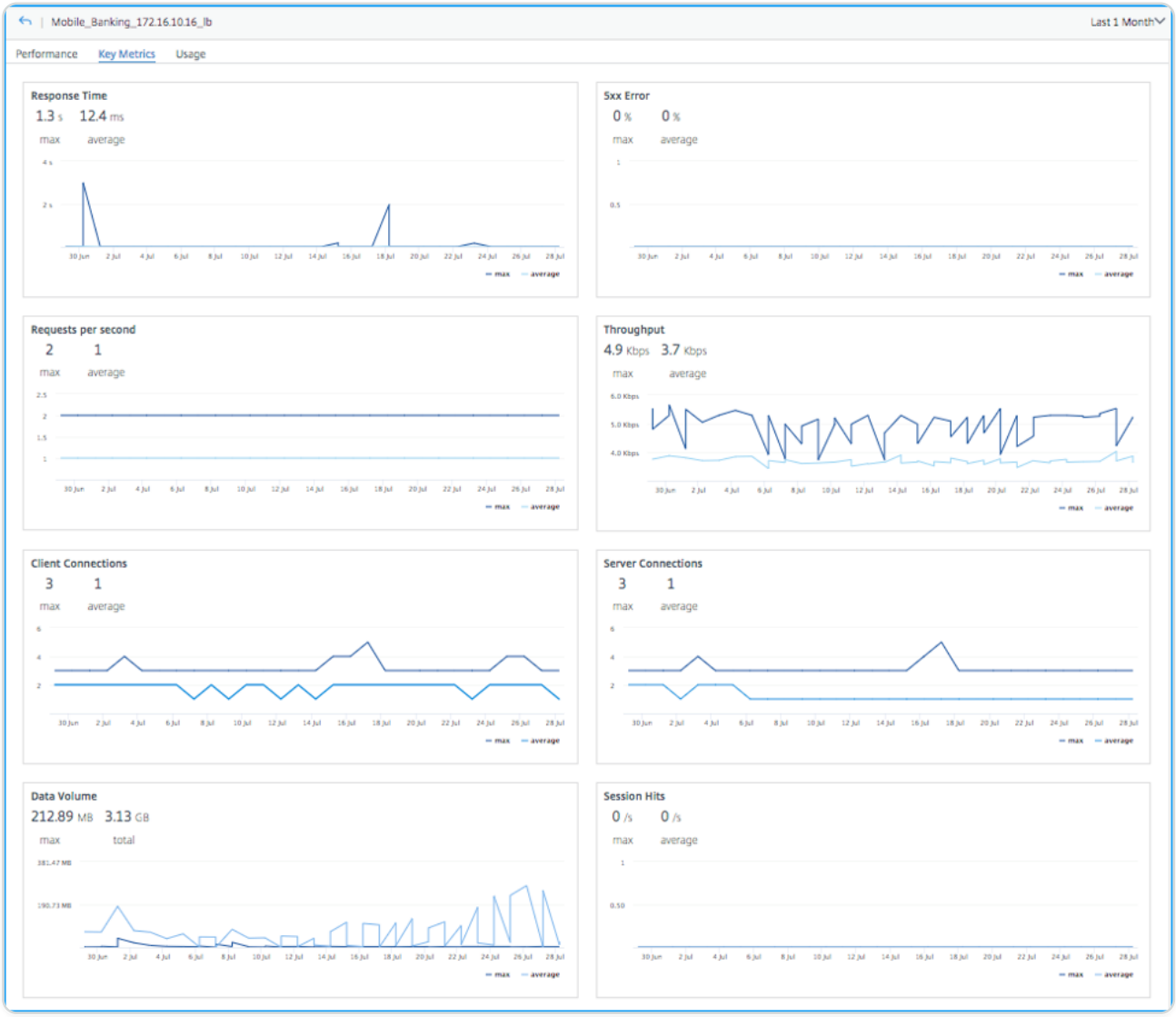
Web 应用程序可能会接收高流量或低流量，并且每天或每小时的流量范围肯定无法预测。同样，Web 应用程序在计划维护或升级期间也需要特定持续时间的停机。作为管理员，您必须分析流量并找到合适的时间来：

- 扩展 Web 应用程序
- 规划 Web 应用程序停机时间

NetScaler Console 中的峰值使用率和低谷期分析功能使您能够分析选定时间段的关键指标。通过这些指标，您可以分析流量并决定何时扩展 Web 应用程序或规划计划停机。

评估应用程序扩展限制

从 **App Dashboard** 中单击一个应用程序，然后选择 **Key Metrics** 选项卡以可视化所有指标的合并视图。从列表中选择时间段以分析指标。



对于每个指标，您可以查看：

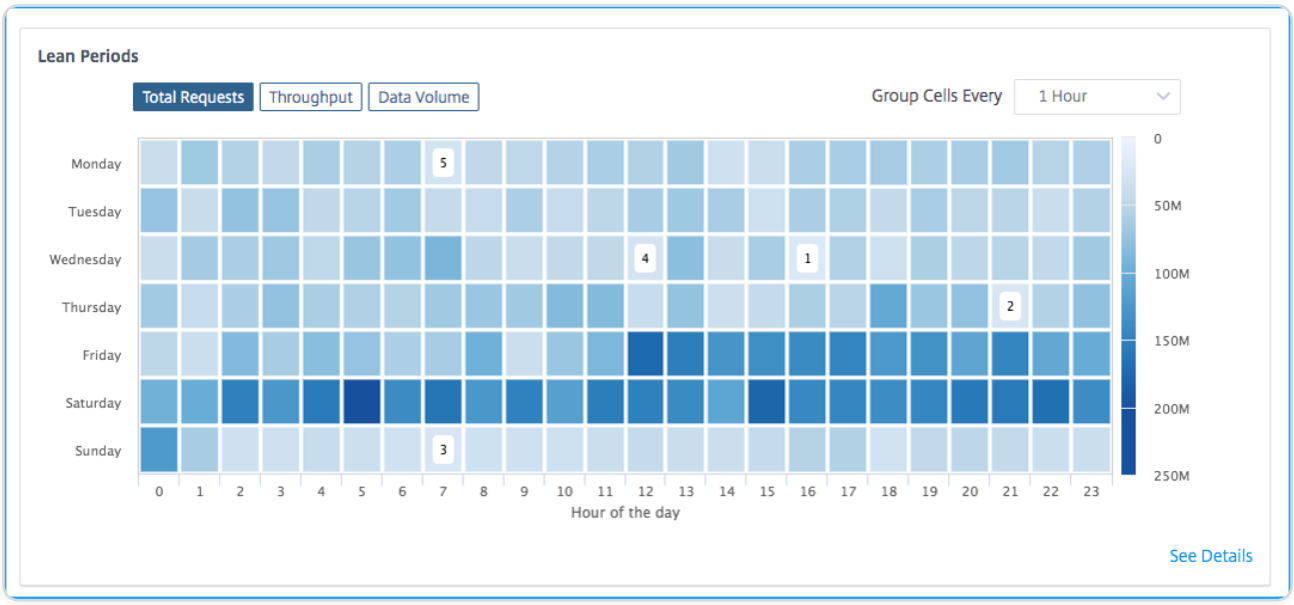
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **最大值** – 表示选定持续时间的最大值
- **平均值** – 表示选定持续时间的平均值

根据图像中的示例，响应时间的最大值表示 1.3 秒。从图表中，您可以分析在选定时间段内高响应时间发生了多少次。同样，您还可以查看其他指标的详细信息，分析应用程序是否已达到峰值使用率，并决定扩展生产环境。

识别前 5 个应用程序维护窗口

从 **App Dashboard** 中单击一个应用程序，然后选择 **Key Metrics** 选项卡以查看应用程序的低谷期。应用程序的典型停机时间可以是 1 小时、2 小时或 4 小时，具体取决于要求。您可以从列表中选择要规划停机的时间（1 小时、2 小时或 4 小时）。从列表中选择时间后，您可以分析总请求数、吞吐量和数据量等指标的流量。当应用程序使用率较低时，您可以选择合适的时间安排停机。 以下示例是分析 1 小时持续时间的停机时间。



热力图视图显示了所选时间段内的应用程序使用情况。颜色越深（蓝色），表示应用程序使用率越高。

热力图视图还建议了规划应用程序停机时间的 5 个最低使用时段（1、2、3、4 和 5）。

1 – 表示周三下午 4 点至 5 点的第一个建议

2 – 表示周四晚上 9 点至 10 点的第二个建议

3 – 表示周日上午 7 点至晚上 8 点的第三个建议

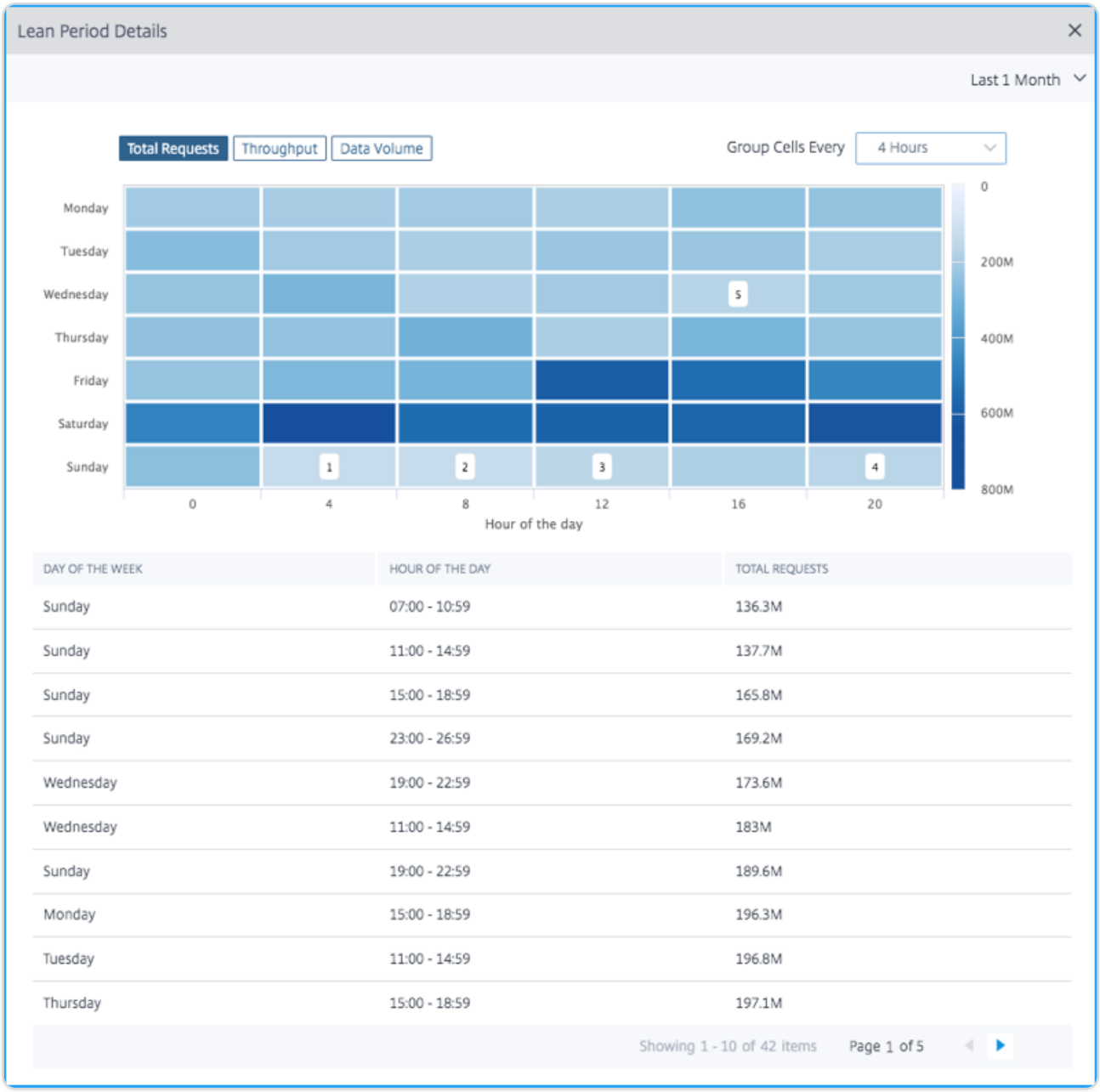
4 – 表示周三中午 12 点至下午 1 点的第四个建议

5 – 表示周一上午 7 点至晚上 8 点的第五个建议

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

在分析了所有其他日期的流量后，您还可以选择任何其他日期和时间来安排停机。

单击 **See Details** 查看更多详细信息。单击 **Total Requests**、**Throughput** 或 **Data Volume** 选项卡可查看前 5 个最低使用时段以及其他日期的详细信息。



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

应用程序使用情况分析

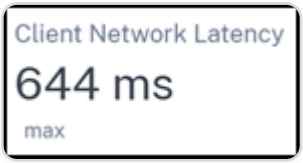
应用程序所有者必须能够从性能和使用情况的角度评估和可视化整个应用程序。

改进后的 **App Dashboard** 使您能够一起查看所有应用程序性能和使用情况指标。当您单击某个应用程序时，除了现有的应用程序性能指标外，**Web Insight** 选项卡还会显示有助于您了解以下内容的指标详细信息：

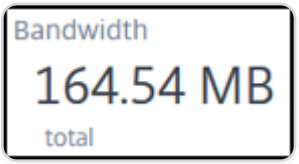
- 了解您的应用程序使用情况。
- 将任何性能偏差与使用情况指标关联起来。

注意

- 从版本 14.1 build 51.x 开始，Web Insight 分析对配置了 IPv6 地址的虚拟服务器可见。
- 从 **14.1-4.x** 版本开始，当您深入查看某个指标时，时间序列图中的分析视图会显示所选持续时间的零值（例如，0 毫秒和 0 请求）。以前，如果所选持续时间没有收到流量或事务，分析视图会通过跳过这些零值来显示图表。
- 对于每个指标，您可以查看指示最大值和总值的选项。例如：

  - - 所选持续时间的最大客户端网络延迟。假设客户端 1 的网络延迟为 644 毫秒，客户端 2 为 15 毫秒，客户端 3 为 3 毫秒。在这种情况下，**客户端网络延迟** 显示 644 毫秒。

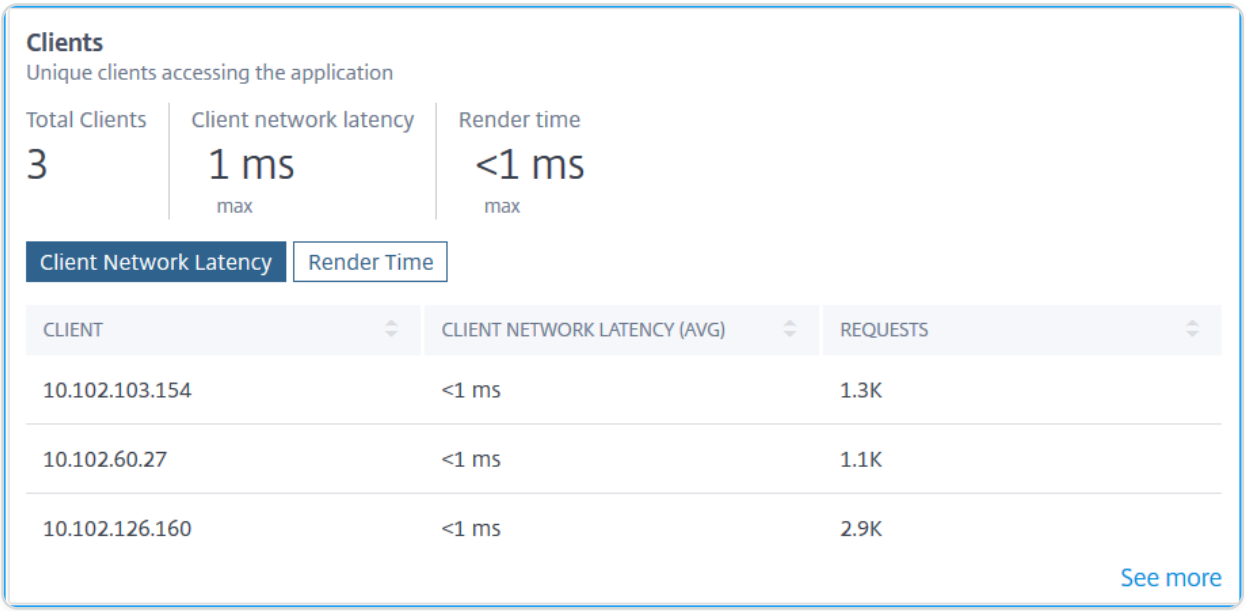
  

  - - 所选持续时间内所有可用客户端/服务器消耗的总带宽。假设客户端 1 的带宽消耗为 79.54 MB，客户端 2 为 45 MB，客户端 3 为 40 MB。在这种情况下，带宽显示 (79.54 MB + 45 MB + 40 MB) = 164.54 MB。

以下是您可以从“**使用情况**”选项卡查看的 Web Insight 指标：

- **客户端** – 显示访问应用程序的客户端的洞察信息：

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

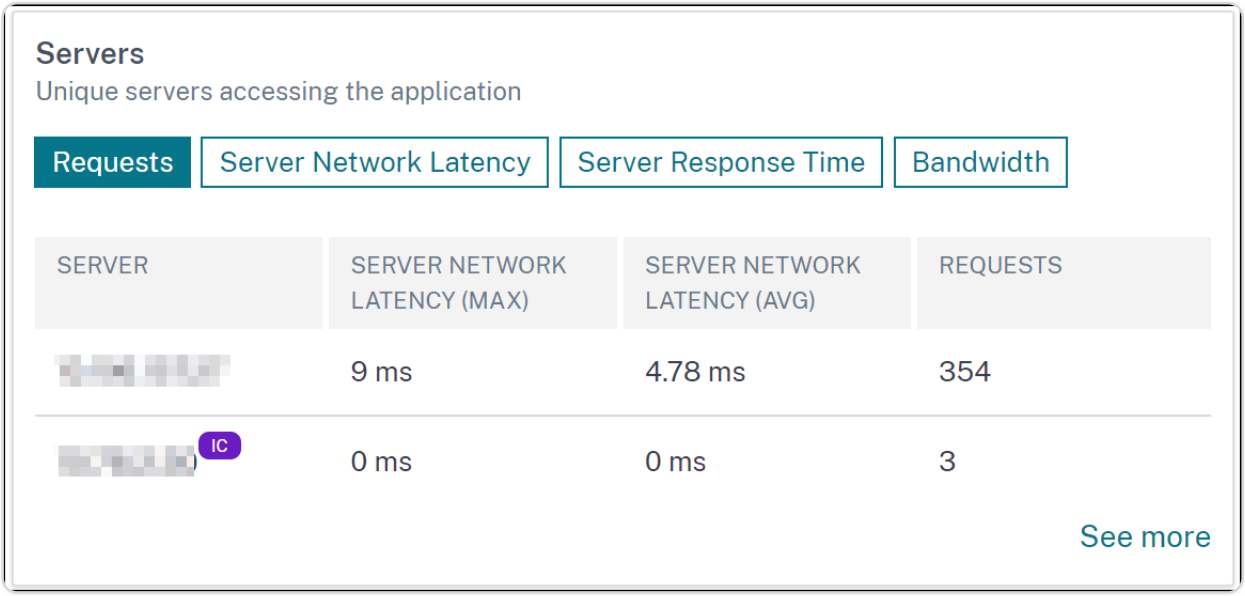


- **总客户端** – 显示访问应用程序的总客户端数。单击“**请求**”选项卡以查看：
  - **客户端** – 客户端 IP 地址。
  - **客户端网络延迟（平均）** – 来自客户端的平均网络延迟。
  - **客户端网络延迟（最大值）** – 来自客户端的最大网络延迟。
  - **请求数** – 来自客户端的总请求数。
  - **按请求数百分比分布** – 基于请求数的百分比分布。例如，如果客户端总数为 4，每个客户端有 100 个请求，则每个客户端的百分比分布为 25%。
- **客户端网络延迟** – 显示从客户端到 NetScaler 的网络延迟。单击**客户端网络延迟**选项卡可查看：
  - **客户端** – 客户端 IP 地址。
  - **客户端网络延迟（平均值）** – 来自客户端的平均网络延迟。
  - **客户端网络延迟（最大值）** – 来自客户端的最大网络延迟。
  - **请求数** – 来自客户端的总请求数。
  - **按请求数百分比分布** – 基于请求数的百分比分布。
- **渲染时间** – 显示渲染服务器响应所需的时间。单击**渲染时间**选项卡可查看：
  - **客户端** – 客户端 IP 地址。
  - **渲染时间（平均值）** – 来自客户端的平均渲染时间。
  - **请求数** – 来自客户端的总请求数。
  - **按请求数百分比分布** – 基于请求数的百分比分布。

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

- **服务器** – 显示访问应用程序的服务器的洞察信息：

> **注意**
>
> 对于集成缓存请求，您可以查看 NetScaler 虚拟服务器 IP 地址以及 IC 通知。有关详细信息，请参阅集成缓存请求。

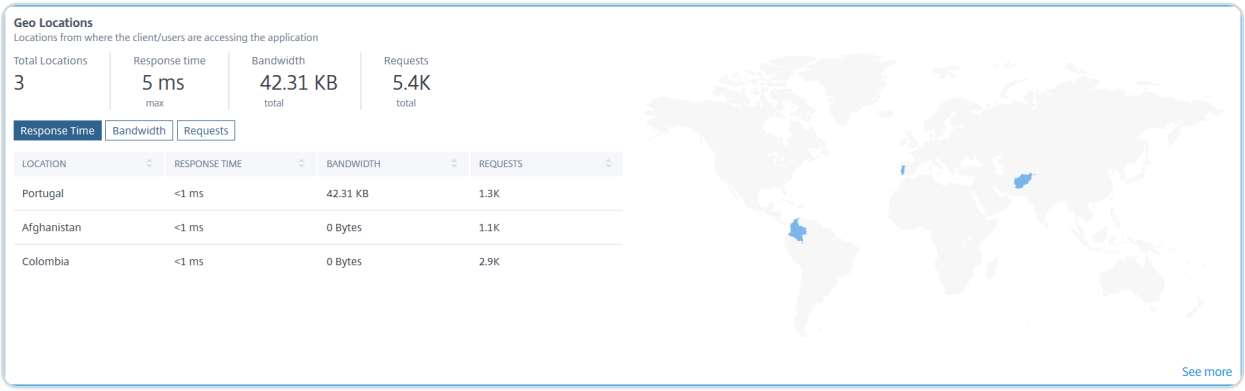


  - **服务器总数** – 显示访问应用程序的服务器总数。单击“**请求**”选项卡可查看：
    - **服务器** – 服务器 IP 地址。
    - **服务器网络延迟（平均）** – 来自服务器的平均网络延迟。
    - **服务器网络延迟（最大）** – 来自服务器的最大网络延迟。
    - **请求** – 来自服务器的总请求数。
    - **按请求百分比分布** – 基于请求的百分比分布。例如，如果服务器总数为 10，并且每个服务器有 1000 个请求，则每个服务器的百分比分布为 10%。
  - **服务器网络延迟（最大）** – 显示从服务器到 NetScaler 的最大网络延迟。单击“**服务器网络延迟**”选项卡可查看：
    - **服务器** – 服务器 IP 地址。
    - **服务器网络延迟（平均）** – 来自服务器的平均网络延迟。
    - **服务器网络延迟（最大）** – 来自服务器的最大网络延迟。
    - **请求** – 来自服务器的总请求数。
    - **按请求百分比分布** – 基于总请求的百分比分布。

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

- **服务器响应时间** – 显示服务器响应请求所花费的时间。单击“**服务器响应时间**”选项卡以查看：
  - **服务器** – 服务器 IP 地址。
  - **服务器响应时间（平均）** – 服务器的平均响应时间。
  - **服务器响应时间（最大）** – 服务器的最大响应时间。
  - **请求** – 服务器的总请求数。
  - **按请求百分比分布** – 基于总请求数的百分比分布。
- **带宽** – 显示服务器消耗的总带宽。单击“**带宽**”选项卡以查看：
  - **服务器** – 服务器 IP 地址。
  - **带宽** – 服务器消耗的总带宽。
  - **请求** – 服务器的总请求数。
  - **按请求百分比分布** – 基于总请求数的百分比分布。

- **地理位置** – 显示从特定位置访问应用程序的客户端的见解：



  - **总位置数** – 显示访问应用程序的客户端总位置数。
  - **响应时间** – 显示来自客户端位置的响应时间。
  - **带宽** – 显示所有位置的客户端消耗的总带宽。
  - **请求** – 显示所有客户端位置的总请求数。

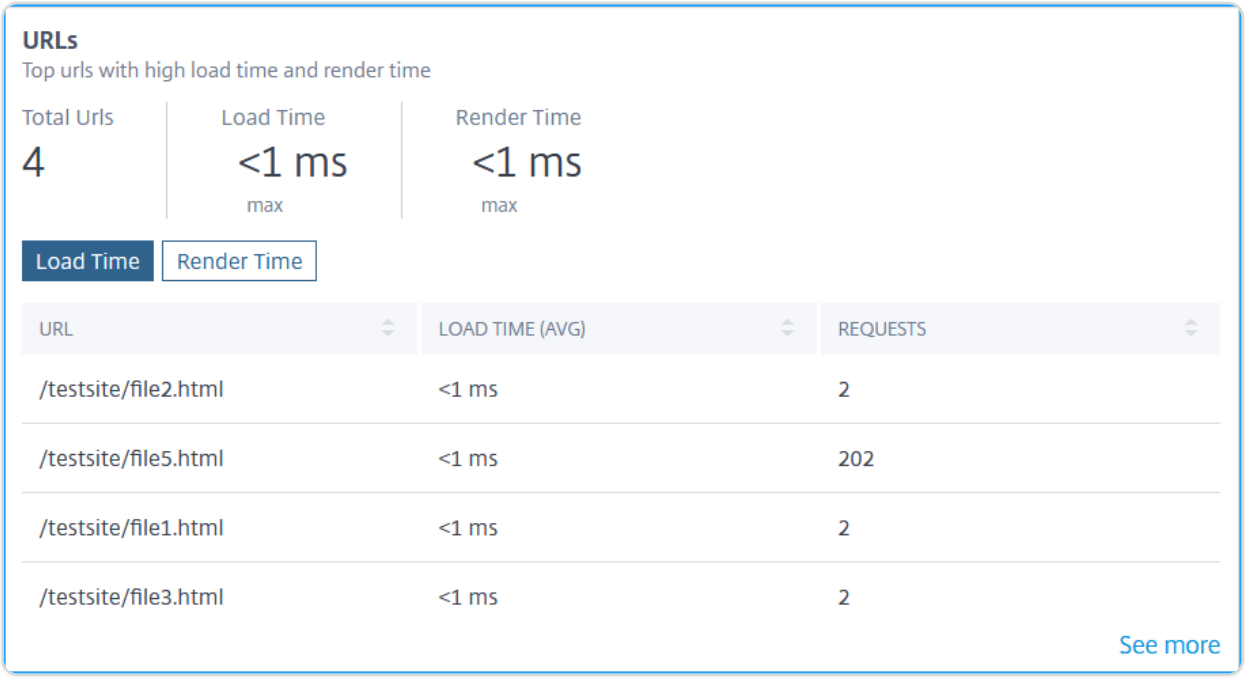
  单击每个选项卡以查看：

  - **位置** – 位置名称。
  - **响应时间** – 客户端位置的平均响应时间。
  - **带宽** – 客户端位置消耗的带宽。
  - **请求** – 客户端位置的总请求数。

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

- **按请求百分比分布** – 基于总请求的百分比分布。例如，如果总位置数为 10，总请求数为 100 万，而国家 A 单独接收 90 万，则国家 A 的百分比分布为 90%。其他国家根据各自国家收到的请求接收剩余的百分比分布。

- **URL** – 显示加载和渲染时间较长的 URL 的洞察信息：

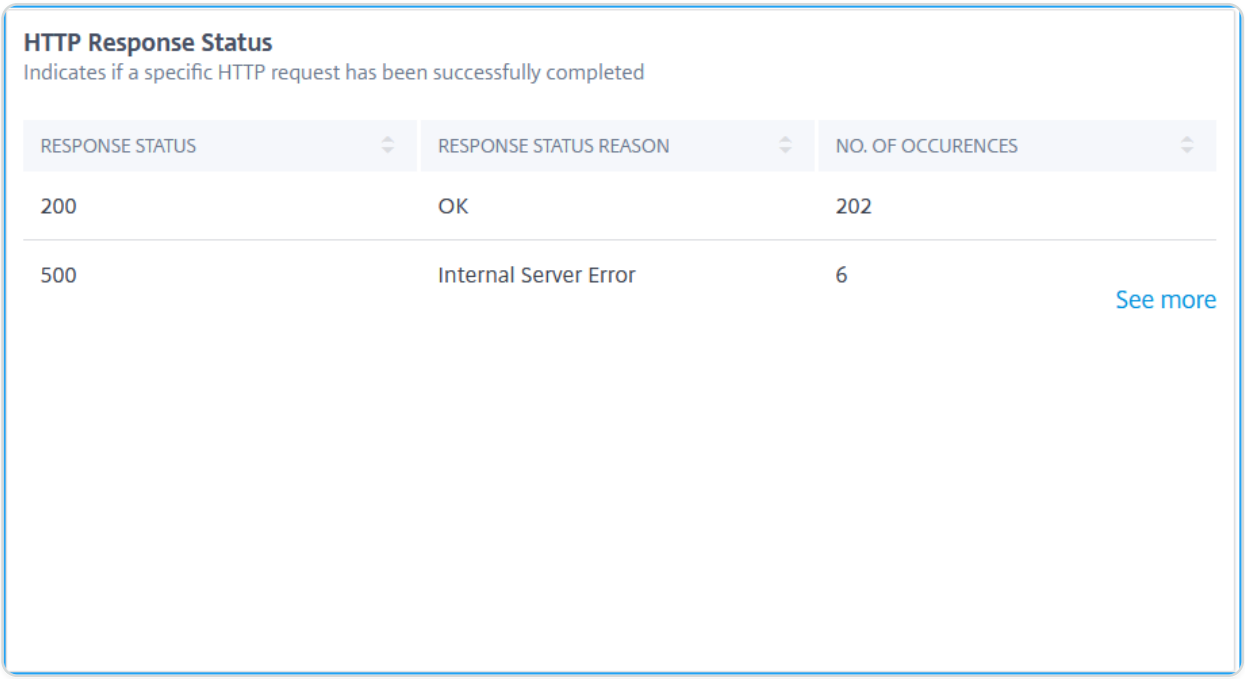


  - **总 URL 数** – 显示总 URL 数。单击“**请求**”选项卡以查看：
    - **URL** – URL 名称。
    - **加载时间（平均）** – URL 加载所需的平均时间。
    - **请求** – 来自该 URL 的总请求数。
    - **按请求百分比分布** – 基于总请求和每个 URL 的百分比分布。
  - **加载时间** – 显示 URL 加载所需的时间。单击“**加载时间**”选项卡以查看：
    - **URL** – URL 名称。
    - **加载时间（平均）** – URL 加载所需的平均时间。
    - **请求数** – 来自该 URL 的总请求数。
    - **按请求数百分比分布** – 基于总请求数的百分比分布。
  - **渲染时间** – 显示 URL 渲染和显示所需的时间。单击“**渲染时间**”选项卡以查看：
    - **URL** – URL 名称。
    - **渲染时间（平均）** – URL 渲染所需的平均时间。
    - **请求数** – 来自该 URL 的总请求数。

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

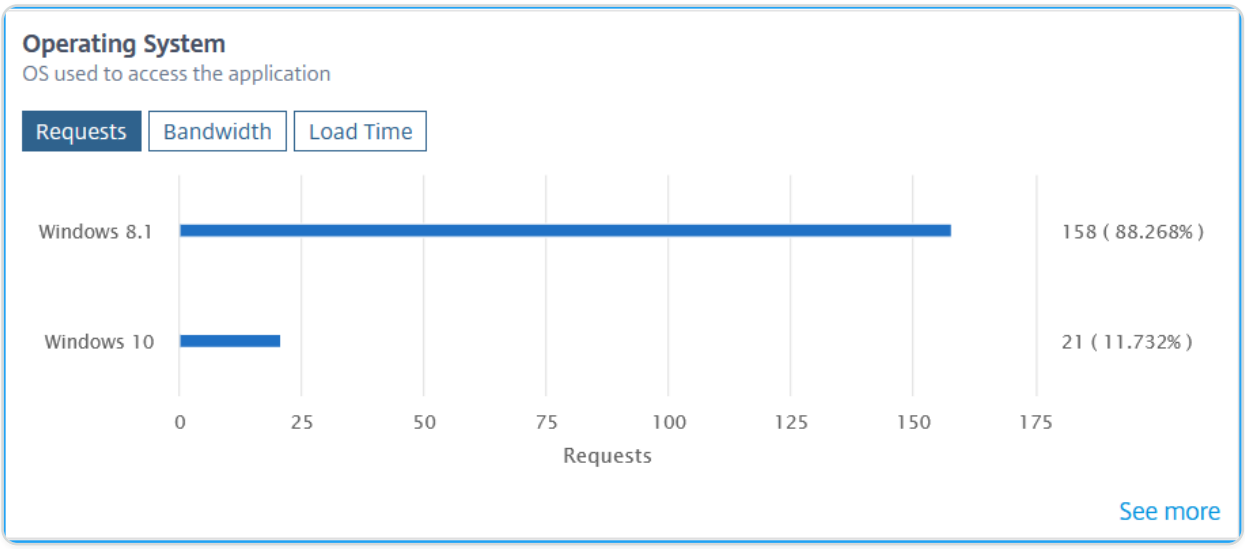
- **按请求数百分比分布** – 基于总请求数的百分比分布。

- **HTTP 响应状态** – 显示特定已完成 HTTP 请求的洞察信息。



  - **响应状态** – 显示响应代码，例如 2xx、4xx、5xx 等。
  - **响应状态原因** – 显示响应原因，例如内部服务器错误、未找到等。
  - **出现次数** – 显示总出现次数。

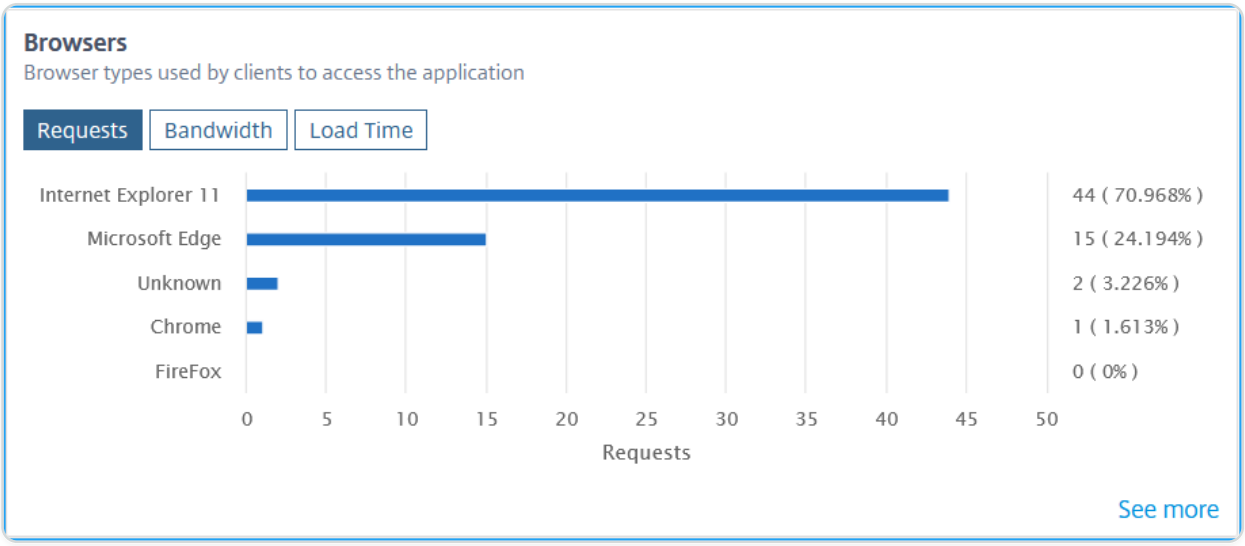
- **操作系统** – 显示访问应用程序的操作系统的洞察信息。



  - **请求** – 显示每个操作系统发出的总请求数。
  - **带宽** – 显示每个操作系统消耗的总带宽。
  - **加载时间** – 显示每个操作系统从服务器加载所花费的总时间。

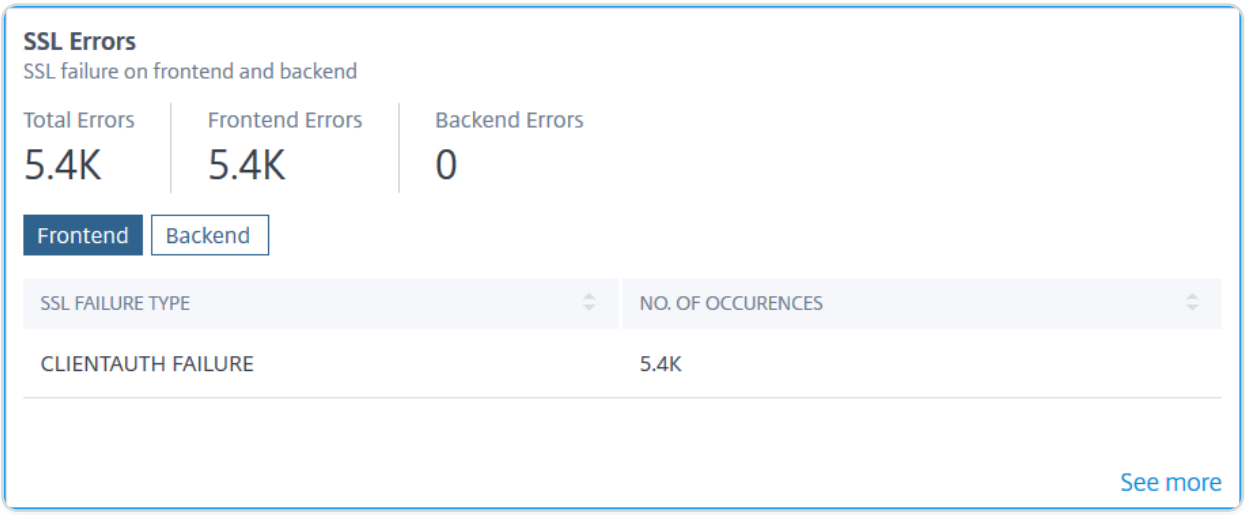
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **浏览器** – 显示客户端用于访问应用程序的浏览器类型的洞察信息。



  - **请求** – 显示每个浏览器发出的总请求数。
  - **带宽** – 显示每个浏览器消耗的总带宽。
  - **加载时间** – 显示浏览器从服务器加载所花费的总时间。

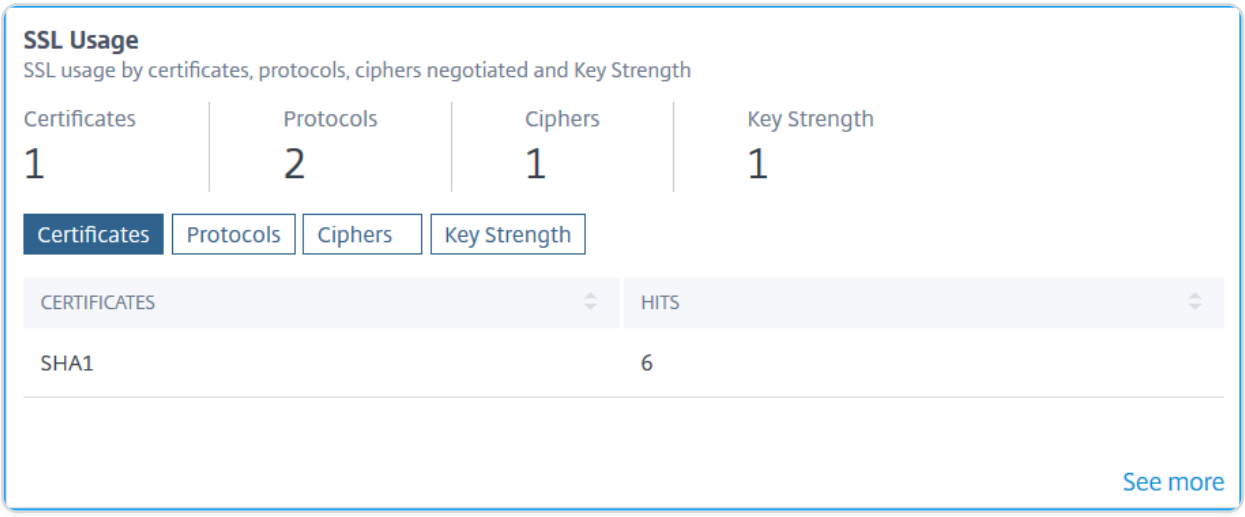
- **SSL 错误** – 显示来自前端服务器和后端服务器的 SSL 错误的洞察信息。



  - **总错误** – 显示 SSL 错误的总发生次数。
  - **前端** – 显示来自前端服务器的 SSL 错误总数。单击“**前端**”选项卡可查看 SSL 错误类型和总发生次数。
  - **后端** – 显示来自后端服务器的 SSL 错误总数。单击“**后端**”选项卡可查看 SSL 错误类型和总发生次数。

- **SSL 使用情况** – 显示 SSL 使用情况的洞察信息，例如 SSL 证书、协议、密码和密钥强度。

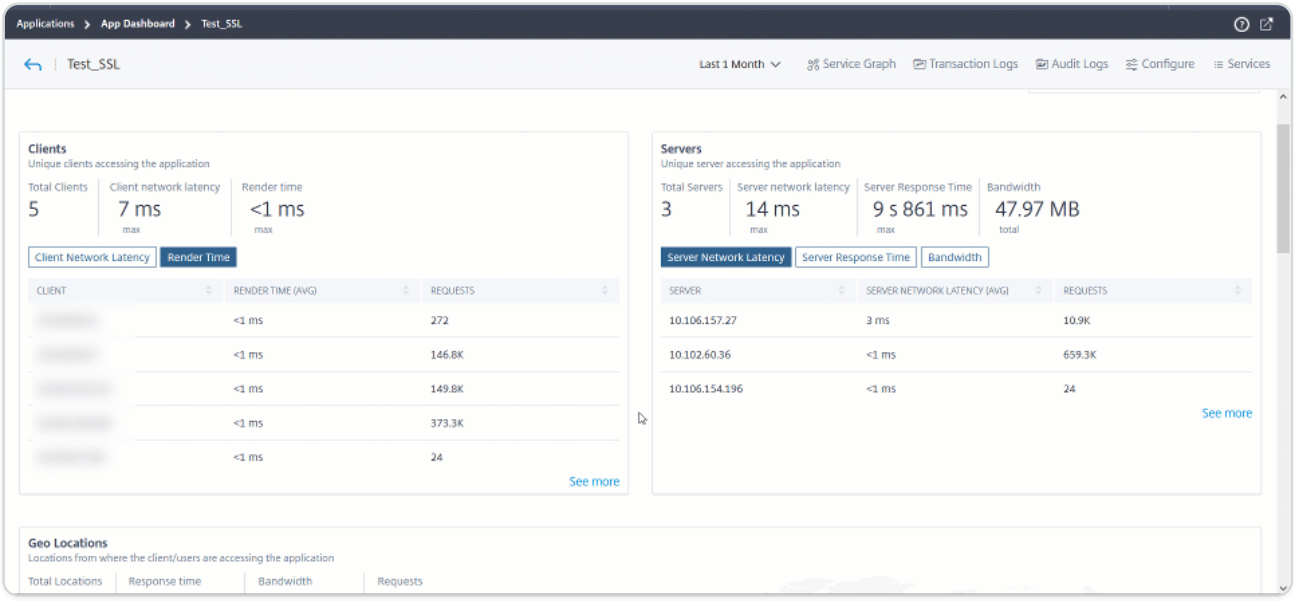
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **证书** – 显示 SSL 证书总数。单击“**证书**”选项卡可查看证书名称和总命中数。
- **协议** – 显示 SSL 协议总数。单击“**协议**”选项卡可查看 SSL/TSL 协议和总命中数的详细信息。
- **密码** – 显示密码总数。单击“**密码**”选项卡可查看每个密码套件名称和总命中数的详细信息。
- **密钥强度** – 显示 SSL 证书中使用的密钥总强度。单击“**密钥强度**”选项卡可查看每个密钥强度和总命中数的详细信息。

以图形格式查看指标详细信息

对于每个指标，您可以通过单击“**查看更多**”选项以图形格式查看更多详细信息。单击“**>**”以图形格式查看详细信息。



单击“**查看更多**”选项后，您可以查看每个指标的以下详细信息：

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

洞察名称	指标	描述
客户端	客户端	表示客户端列表
	渲染时间（平均）	表示客户端渲染服务器响应所需的平均时间
	客户端网络延迟（平均）	表示从客户端到 NetScaler 实例的平均网络延迟
	请求数	表示来自客户端的总请求数
服务器	服务器	表示服务器列表
	服务器处理时间（平均）	表示服务器处理请求所需的平均时间
	服务器网络延迟（平均）	表示从服务器到 NetScaler 实例的平均网络延迟
	命中数	表示服务器收到的总点击数
地理位置	位置	表示客户端位置
	响应时间	表示来自客户端位置的总响应时间
	带宽	表示从该位置消耗的总带宽
	请求	表示来自该位置的总请求数
URL	渲染时间（平均）	表示从服务器加载页面所需的平均时间
	加载时间（平均）	表示 URL 渲染和显示所需的平均时间
	点击量	表示来自 URL 的总点击量
HTTP 响应状态	名称	表示响应状态名称，例如 OK、Not found、Internal Server Error 等

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

洞察名称	指标	描述
	响应状态	表示从服务器接收到的响应状态码，例如 200、400、500 等
	点击量	表示来自响应代码的总点击量
	带宽	表示消耗的总带宽
操作系统	操作系统	表示操作系统名称，例如 Windows、MAC
	加载时间	表示操作系统从服务器加载所需的总时间
	带宽	表示操作系统消耗的总带宽
	请求	表示操作系统发出的总请求数
浏览器	浏览器	表示浏览器名称，例如 Mozilla Firefox、Chrome 等
	加载时间	表示浏览器从服务器加载所需的总时间
	带宽	表示浏览器消耗的总带宽
	请求	表示浏览器发出的总请求数
SSL 错误	SSL 故障类型	表示错误名称，例如 CLIENTAUTH FAILURE
	出现次数	表示 SSL 错误的出现总次数
SSL 使用情况	SSL 使用情况	表示协议名称和版本，例如 TLS、SSL
	命中数	表示来自该协议的总命中数

排查 Web Insight 问题

有关详细信息，请参阅故障排除文档 排查 Web Insight 问题

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

A+ SSL 评级分析

注意：

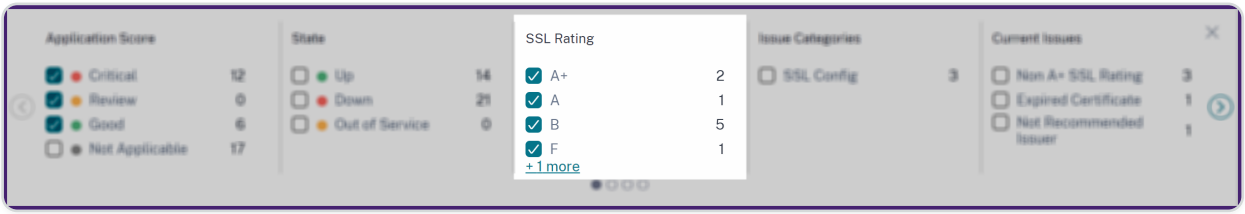
对于不合规 SSL 证书的批量升级，您可以在“**任务**”中使用“**SSL A+ 评级升级**”。

应用程序必须使用安全的密码和协议进行 SSL 事务。否则，它可能会影响访问该应用程序的用户的隐私、数据完整性和安全性。NetScaler Console 会使用 NetScaler 安全前端配置文件审查应用程序的虚拟服务器 SSL 设置。A+ 评级所需的设置已预加载到安全前端配置文件中。

作为应用程序所有者，您可以评估您的应用程序是否具有 **A+** 评级。您还可以查看应用程序的协议和密码套件分数。如果您的应用程序没有 **A+** 评级，您可以升级到 **A+** 评级。

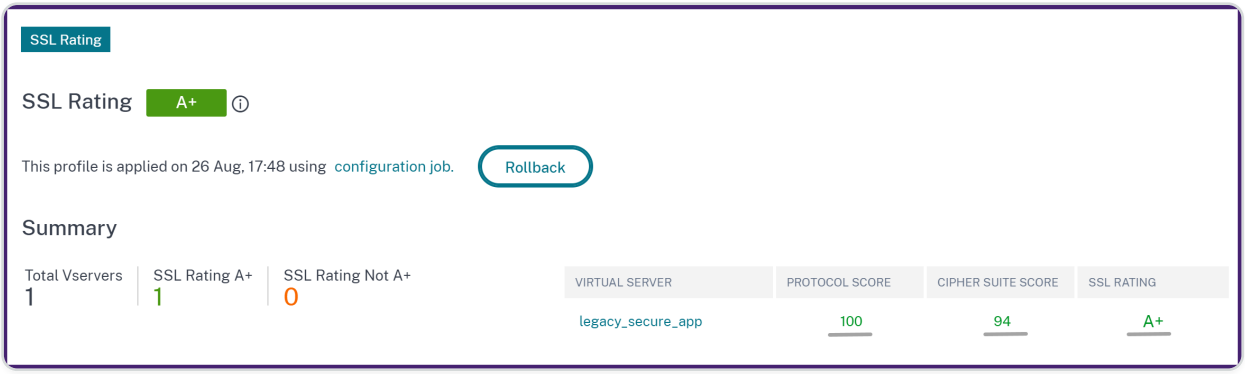
要查看应用程序的 SSL 评级，请执行以下操作：

1. 转到“**应用程序 > 控制板**”。
2. 根据应用程序的 SSL 评级筛选应用程序。



如果应用程序没有评级，则归类为“**不适用**”。

3. 从 GUI 中选择所需的应用程序网格。
4. 选择“**SSL**”选项卡。此选项卡显示应用程序的 SSL 评级。



“**SSL**”选项卡提供以下选项之一来更改或升级应用程序的评级：

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

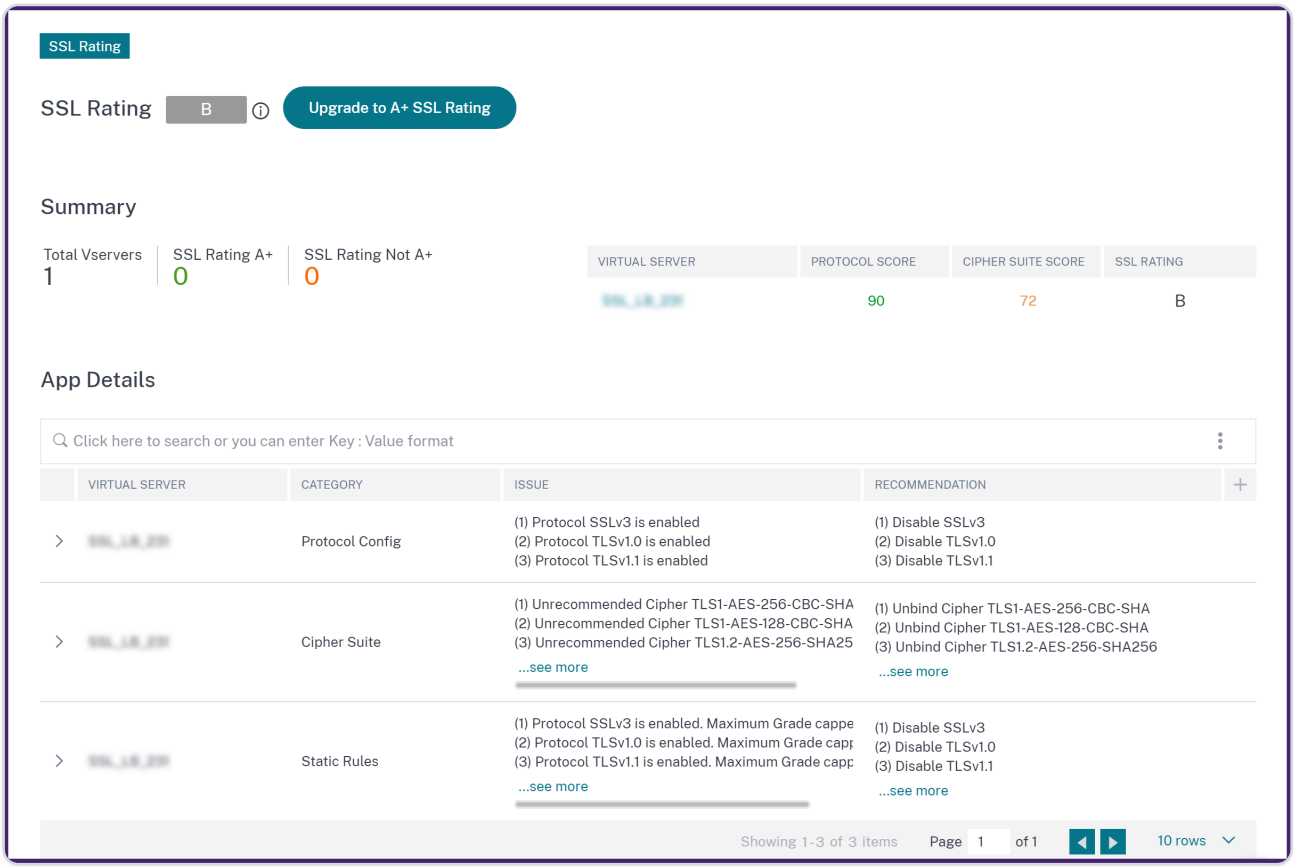
- 升级到 A+ SSL 评级
- 回滚 SSL 评级

升级到 A+ SSL 评级

当您将应用程序升级到 A+ SSL 评级时，会发生以下更改，具体取决于 NetScaler 实例上默认 SSL 配置文件的状态：

- 如果默认 SSL 配置文件已禁用，NetScaler Console 会修改为 SSL 虚拟服务器上推荐的 SSL 设置。
- 如果默认 SSL 配置文件已启用，NetScaler Console 会基于安全配置文件创建一个具有推荐 A+ 设置的新 SSL 配置文件。

没有 **A+** 评级的应用程序在 **SSL** 选项卡中显示受影响的虚拟服务器的详细信息。

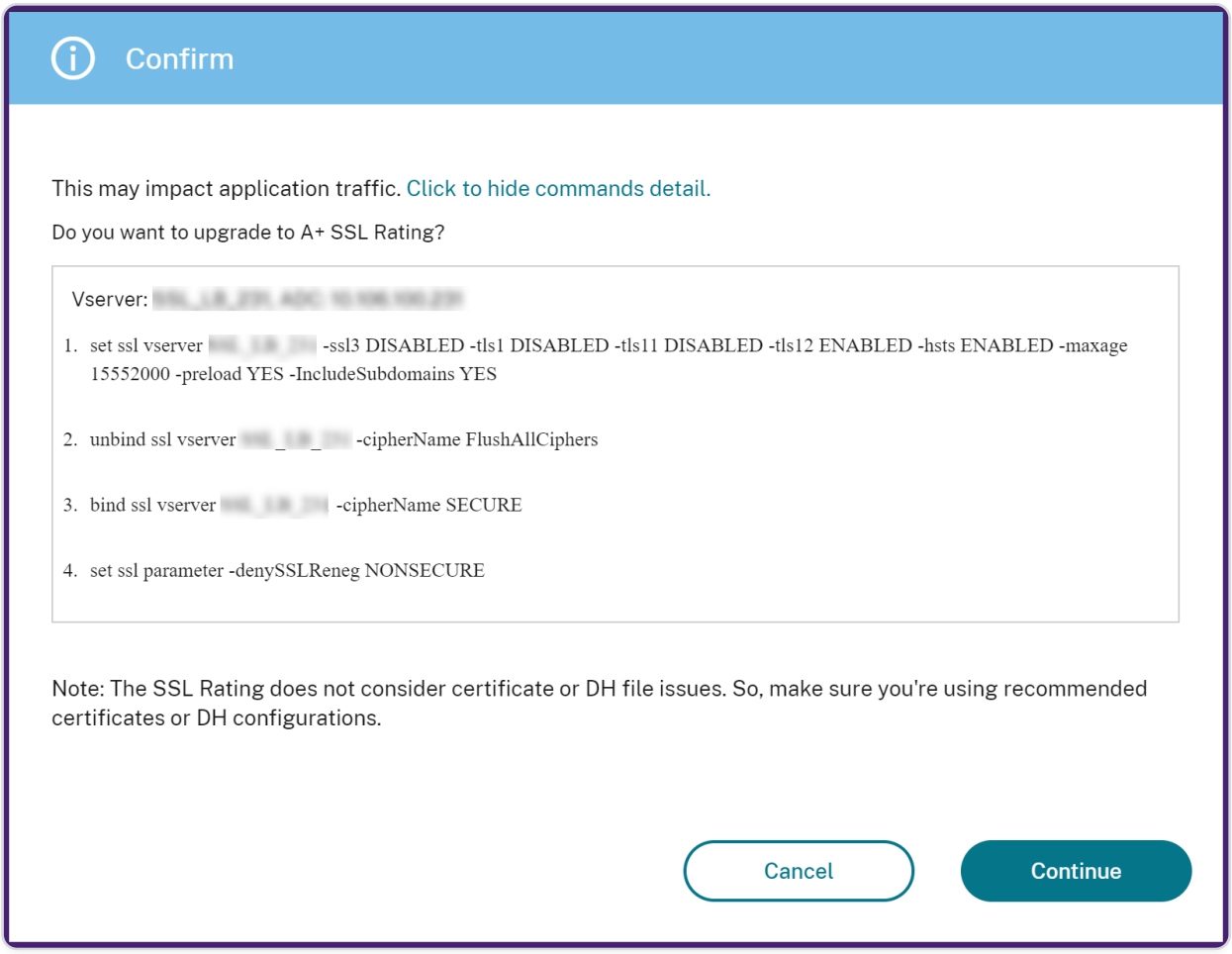


在 **App Details**（应用程序详细信息）中，您可以查看其配置不符合安全前端配置文件的虚拟服务器详细信息。此外，它还在 **Recommendation**（建议）列中显示了补救措施。提供这些措施是为了使您的应用程序符合安全前端配置文件。

在此示例中，虚拟服务器存在一些安全问题。**Protocol TLSv1.0 enabled**（协议 TLSv1.0 已启用）就是其中一个问题。**App Details**（应用程序详细信息）部分建议采取适当的操作来解决此问题。要通过相应的建议解决所有此类问题，请执行以下操作：

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

1. 单击 **升级到 A+ 评级**。



确认消息显示在虚拟服务器上运行的命令。这些命令可能会影响您的应用程序流量。

2. 查看命令，然后单击 **Confirm**（确认）。

回滚 SSL 评级

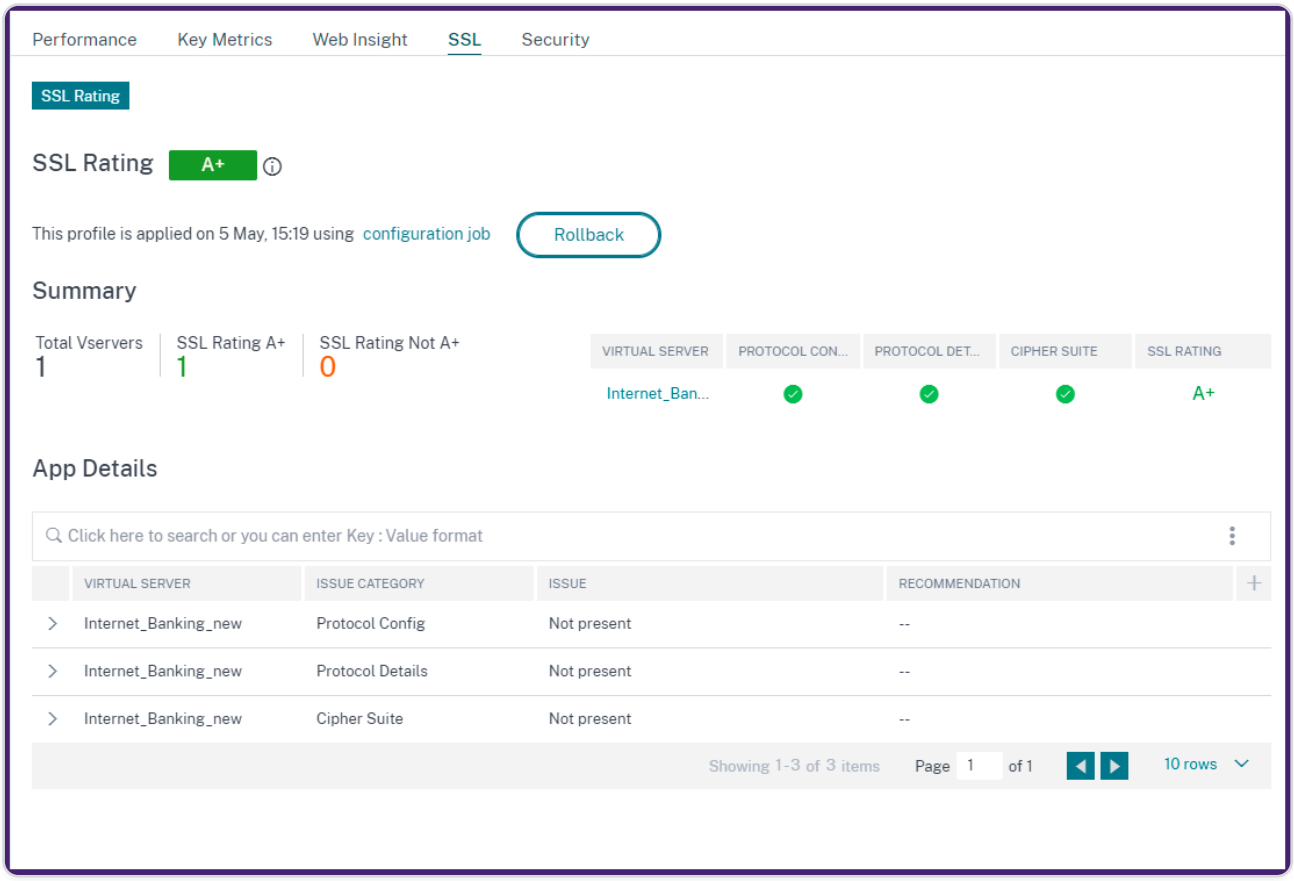
注意：

如果您将应用程序升级到 A+ SSL 评级，则只能在升级后的 7 天内恢复到其原始评级。

将应用程序升级到 A+ 评级后，您可以在 SSL insight 中分析传入流量。此页面显示协商 SSL 事务所用的密码和协议。

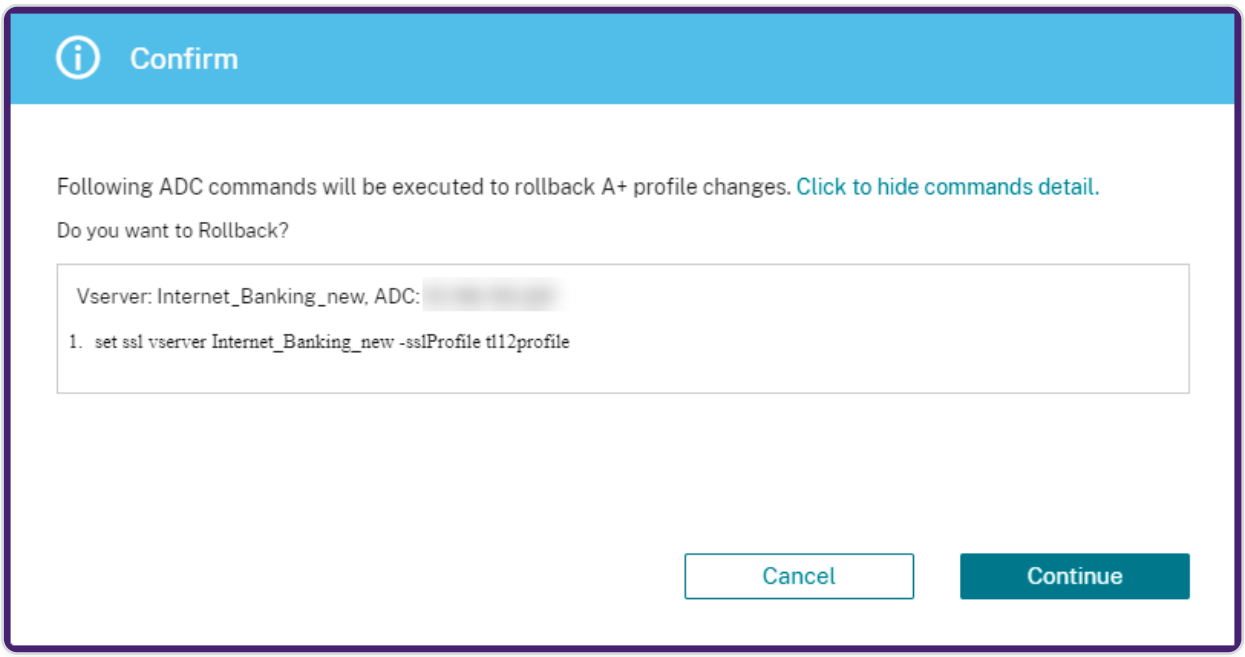
但是，如果您发现某些合法流量被丢弃，您可以回滚在应用程序上配置的安全前端配置文件。此操作会将 SSL 评级更改为先前的评级。

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



要回滚 SSL 评级：

1. 单击 **回滚**。



确认消息显示在虚拟服务器上运行的命令。

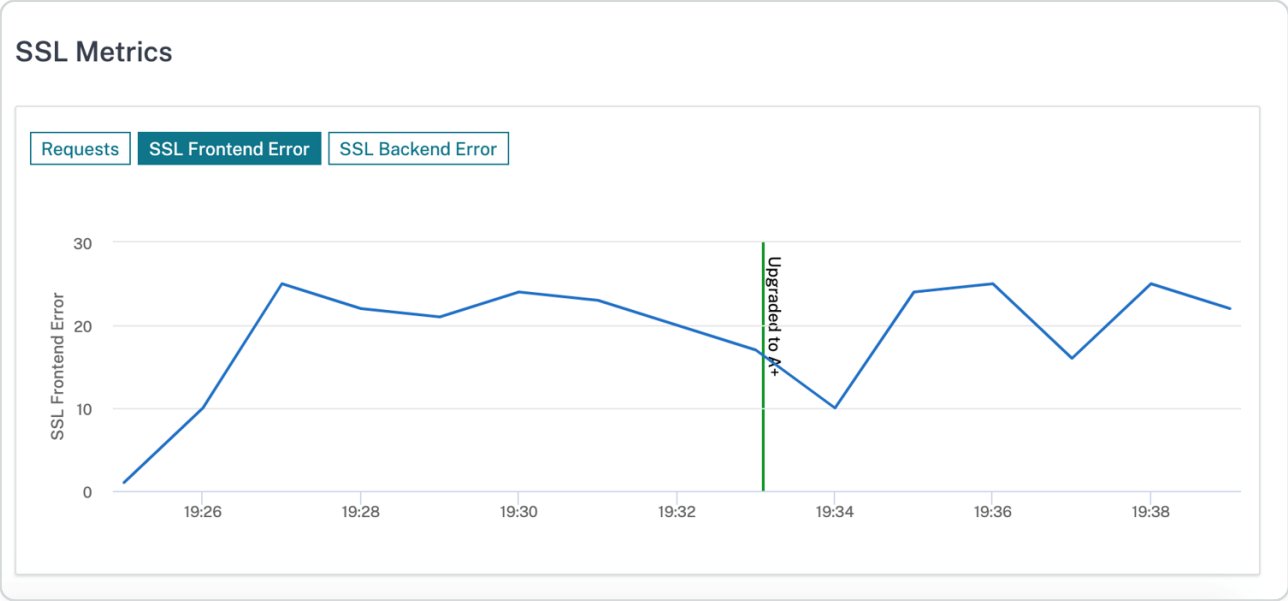
2. 检查命令并单击 **确认**。

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

确定 SSL 评级对应用程序流量的影响

升级 SSL 评级时，应用程序流量可能会受到影响。在 **SSL 指标** 中，您可以观察升级后连接是否断开。根据此信息，您可以决定继续或回滚 SSL 评级。

在以下示例图中，将 SSL 评级升级到 **A+** 后，某些连接被丢弃。



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

Web Insight 仪表板

注意：

从版本 14.1 build 51.x 开始，Web Insight 分析数据对配置了 IPv6 地址的虚拟服务器可见。

改进的 Web Insight 功能得到了增强，并提供了对 Web 应用程序、客户端和 NetScaler 实例的详细指标的可见性。此改进的 Web Insight 使您能够从性能和使用情况的角度一起评估和可视化整个应用程序。作为管理员，您可以查看以下各项的 Web Insight：

- 应用程序。导航到 **应用程序 > 仪表板**，单击一个应用程序，然后选择 **Web Insight** 选项卡以查看详细指标。有关详细信息，请参阅 应用程序使用情况分析。
- 所有应用程序。导航到 **应用程序 > Web Insight**，然后单击每个选项卡（应用程序、客户端、实例）以查看以下指标：

应用程序	客户端	实例
应用程序	客户端	实例指标
服务器	地理位置	应用程序
域	HTTP 请求方法	域
地理位置	HTTP 响应状态	URL
URL	URL	HTTP 请求方法
HTTP 请求方法	操作系统	HTTP 响应状态
HTTP 响应状态	浏览器	客户端
SSL 错误	SSL 错误	服务器
SSL 使用情况	SSL 使用情况	操作系统
		浏览器

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

Applications Clients Instances Last 1 Month

Applications
Top apps with high bandwidth and response time

Requests | Bandwidth | Response Time

APPLICATION	BANDWIDTH (AVG)	RESPONSE TIME (AVG)	REQUESTS
lb_114	9.15 MB	923 ms	14.9K
SSL_VS	0 Bytes	<1 ms	121
test_vs_ssl	0 Bytes	<1 ms	121
k8s-10.244.2.112_80_http	55.07 KB	20 ms	81
vpn_gw	0 Bytes	<1 ms	12

See more

Servers
Unique servers accessing the application

Requests | Server Network Latency | Server Response Time | Bandwidth

SERVER	SERVER NETWORK LATENCY (...	REQUESTS
10.102.103.113	921 ms	14.9K
10.102.71.225	<1 ms	121
10.102.71.226	<1 ms	121
10.244.1.95	<1 ms	23
10.102.71.228	<1 ms	12

See more

Domains
Top domains

Requests | Bandwidth | Response Time

DOMAIN	BANDWIDTH (AVG)	REQUESTS
10.102.103.99	8.51 MB	14.4K
--NA--	513.6 KB	453
10.102.103.99:80	62.67 KB	52
netflix-frontend-service	14.82 KB	23
recommendation-engine-s...	8.75 KB	12

See more

Geo Locations
Locations from where the clients/users are accessing the applications

Total Locations	Response Time	Bandwidth	Requests
1	20.51 s (max)	16.56 MB (total)	15.3K (total)

Requests | Response Time | Bandwidth

LOCATION	RESPONSE TIME	BANDWIDTH	REQUESTS
*	95 ms	16.56 MB	15.3K

See more

URLs
Top urls with high load time and render time

Total Urls	Load Time	Render Time
5.7K	<1 ms (max)	<1 ms (max)

Requests | Load Time | Render Time

URL	LOAD TIME (AVG)	RENDER TIME (AVG)	REQUESTS
/	<1 ms	<1 ms	446
/console/login/LoginForm.jsp	<1 ms	<1 ms	139
/index.php	<1 ms	<1 ms	116
/q79w_38jg__.shtml	<1 ms	<1 ms	96
/admin_ui/mas/ent/login.html	<1 ms	<1 ms	79

See more

HTTP Request Methods
Indicates HTTP request methods used to access the applications

REQUEST METHODS	BANDWIDTH	NO. OF OCCURENCES
GET	8.65 MB	14.5K
POST	459.6 KB	368
Unknown	35.85 KB	324
HEAD	17.1 KB	39
OPTIONS	35.1 KB	18

HTTP Response Status
Indicates if a specific HTTP request has been successfully completed

RESPONSE STATUS	RESPONSE STATUS REASON	NO. OF OCCURENCES
404	Not Found	12.2K
401	Unauthorized	2.2K
302	Found	337
0	Unknown	254
200	OK	152

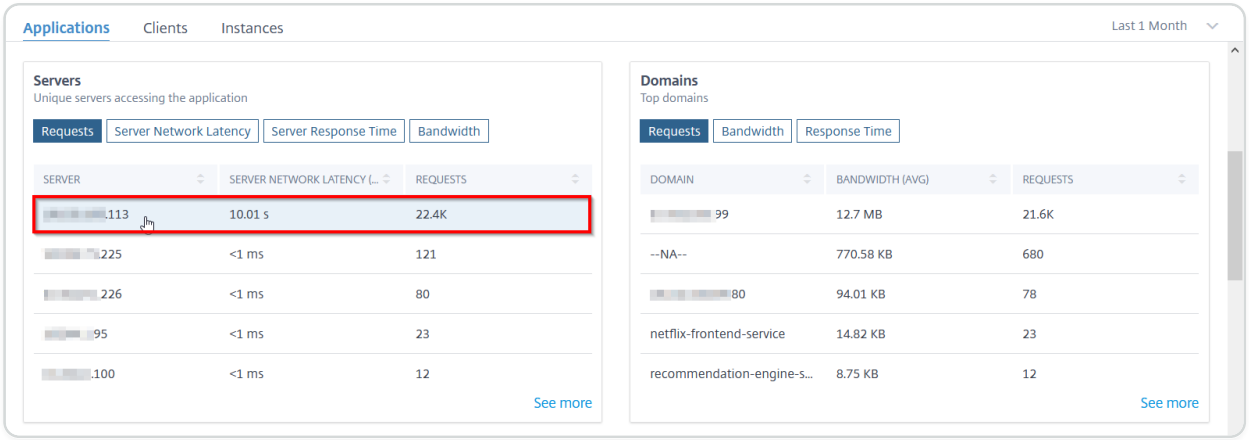
在每个指标中，您可以查看前 5 个结果。您可以单击以进一步深入分析问题并更快地采取故障排除措施。

注意：

- 从 **14.1-4.x** 版本开始，当您深入查看某个指标时，时间序列图中的分析视图会显示所选持续时间的空值（例如，0 毫秒和 0 请求）。此前，如果所选持续时间没有收到流量或事务，分析视图会通过跳过这些空值来显示图表。
- 在某些情况下，NetScaler 可能无法计算某些事务的 RTT 值。对于此类事务，NetScaler Console 将 RTT 值显示为
  - **NA** – 当 NetScaler 实例无法计算 RTT 时显示。
  - **< 1ms** – 当 NetScaler 实例计算出 0 毫秒到 1 毫秒之间的十进制 RTT 值时显示。例如，0.22 毫秒。

例如，假设您想分析服务器网络延迟在一个月时间内的表现，并决定是扩展还是缩减生产环境。要进行此分析，请执行以下操作：

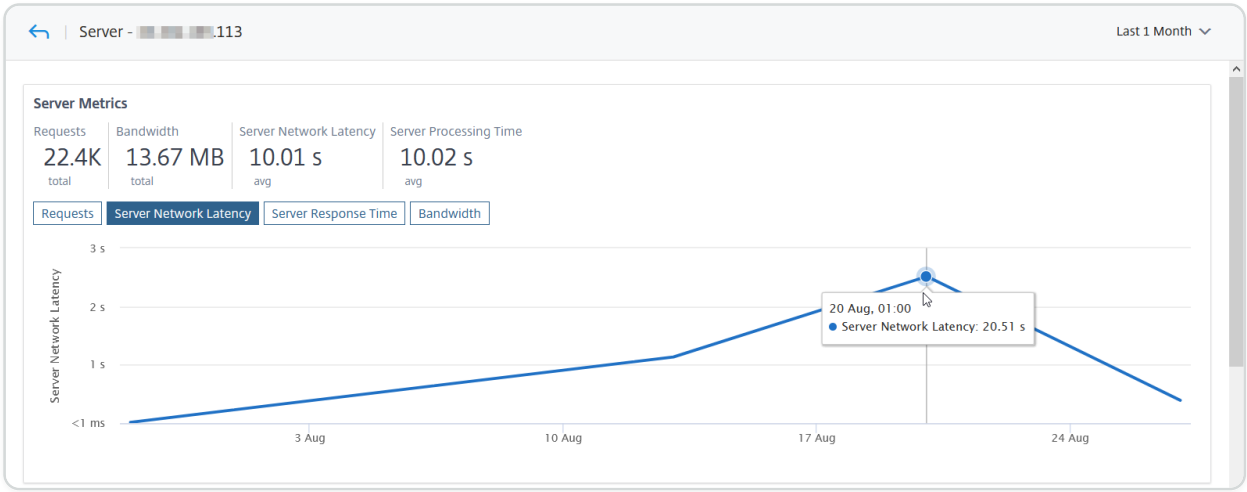
1. 从列表中选择“最近 1 个月”，然后从“**应用程序**”选项卡中向下滚动到“**服务器**”，然后单击一个服务器。



   所选服务器的指标详细信息已显示。

2. 选择**服务器网络延迟**选项卡以分析延迟。

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

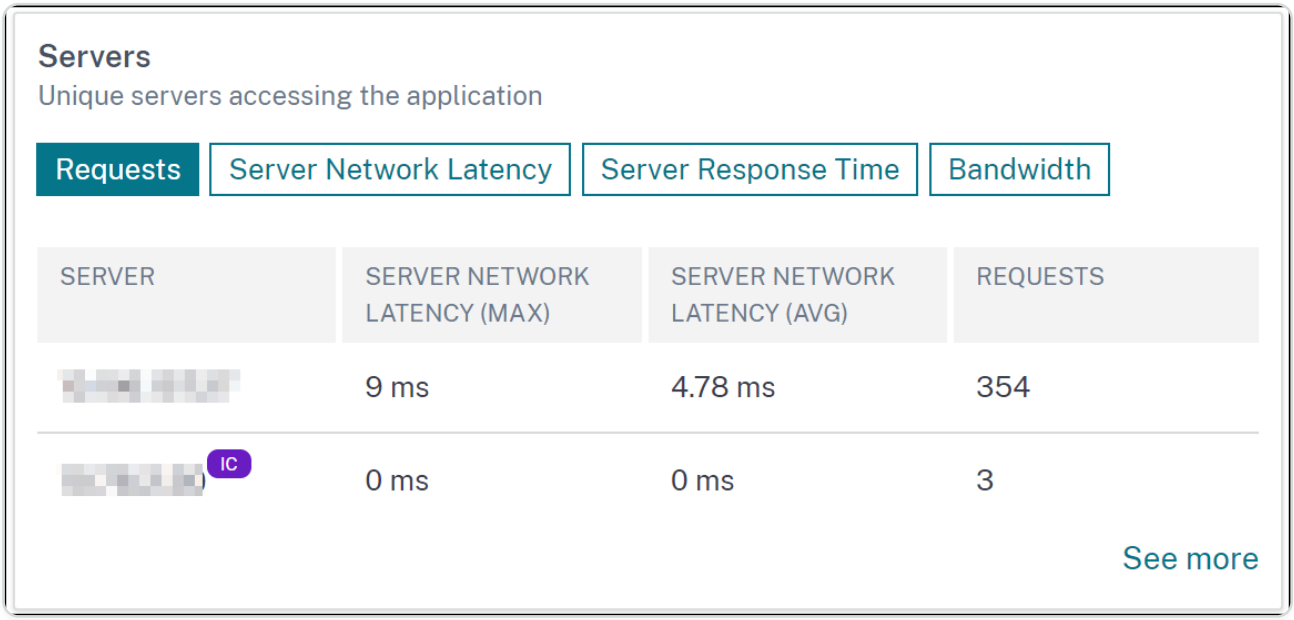


平均延迟显示为 10.01 秒，从图中可以看出，过去 1 个月的服务器网络延迟似乎很高。作为管理员，您可以决定扩展生产环境。

集成缓存请求

集成缓存为 NetScaler 设备提供内存存储，并向用户提供 Web 内容，而无需往返源服务器。

集成缓存请求目前在**服务器**下可见，NetScaler 虚拟服务器 IP 地址旁边带有 IC 通知。所有其他请求都显示源服务器 IP 地址。

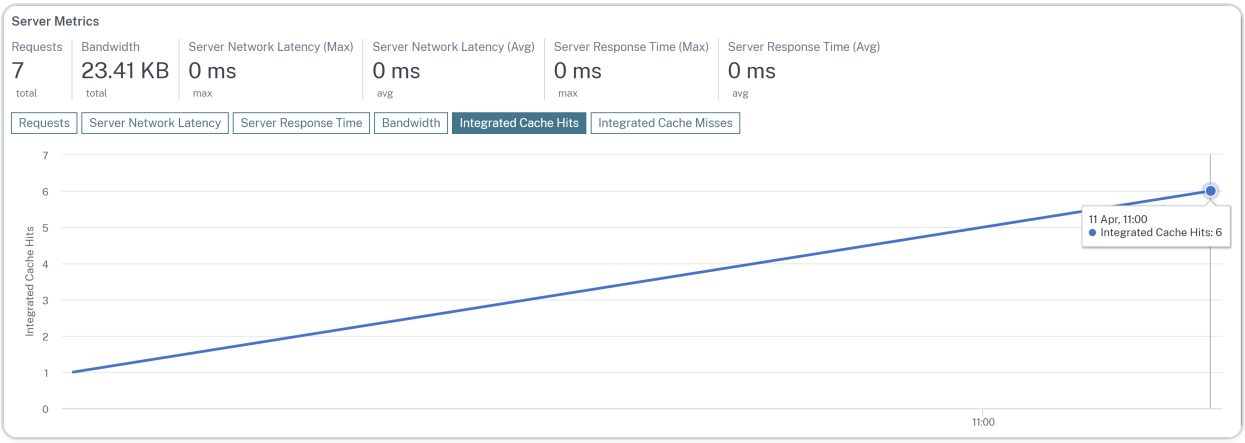


当您深入查看服务器以查看更多详细信息时，**服务器指标**会显示集成缓存命中和未命中选项卡。

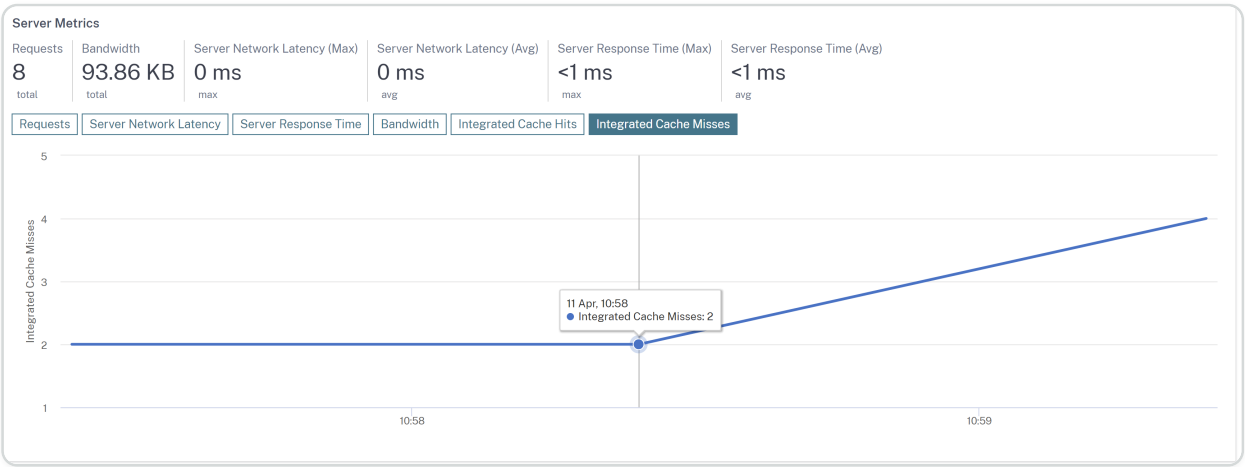
图表视图：

- **集成缓存命中**选项卡使您能够查看 NetScaler 设备从缓存提供的总响应。

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



- **集成缓存未命中**选项卡使您能够查看 NetScaler 设备从源服务器提供的总响应。



排查 Web Insight 问题

有关详细信息，请参阅故障排除文档 排查 Web Insight 问题。

查看应用程序延迟的根本原因

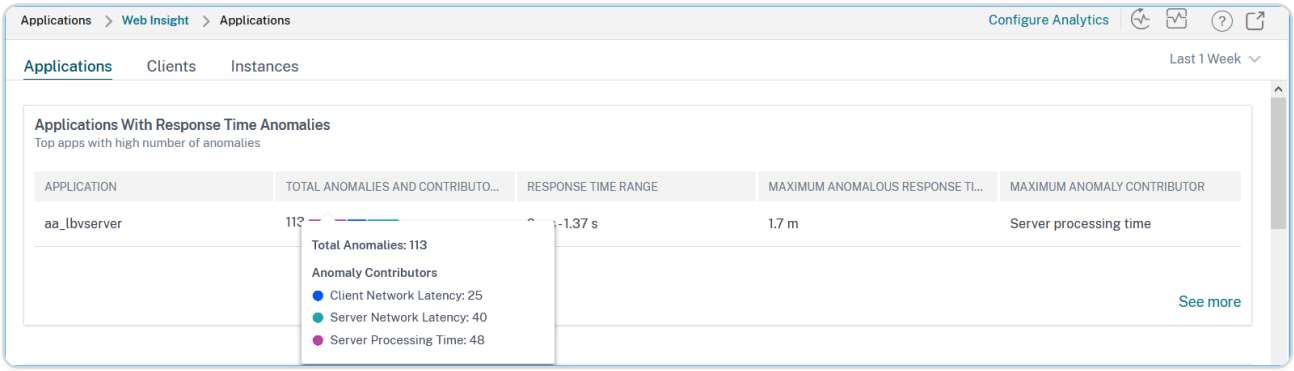
应用程序缓慢是任何组织都非常关注的问题，因为它会导致业务影响或生产力下降。在**应用程序 > Web Insight** 中，您现在可以查看一个名为“**响应时间异常的应用程序**”的新指标。作为管理员，您可以使用此指标分析应用程序延迟是否由以下原因引起：

- 客户端网络延迟
- 服务器网络延迟
- 服务器处理时间

NetScaler Console 每小时执行一次异常检查，并根据某些先决条件报告过去 1 小时流量的异常。例如，为避免误报结果，如果响应时间 < 1 毫秒，则会跳过这些结果的异常检查。

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

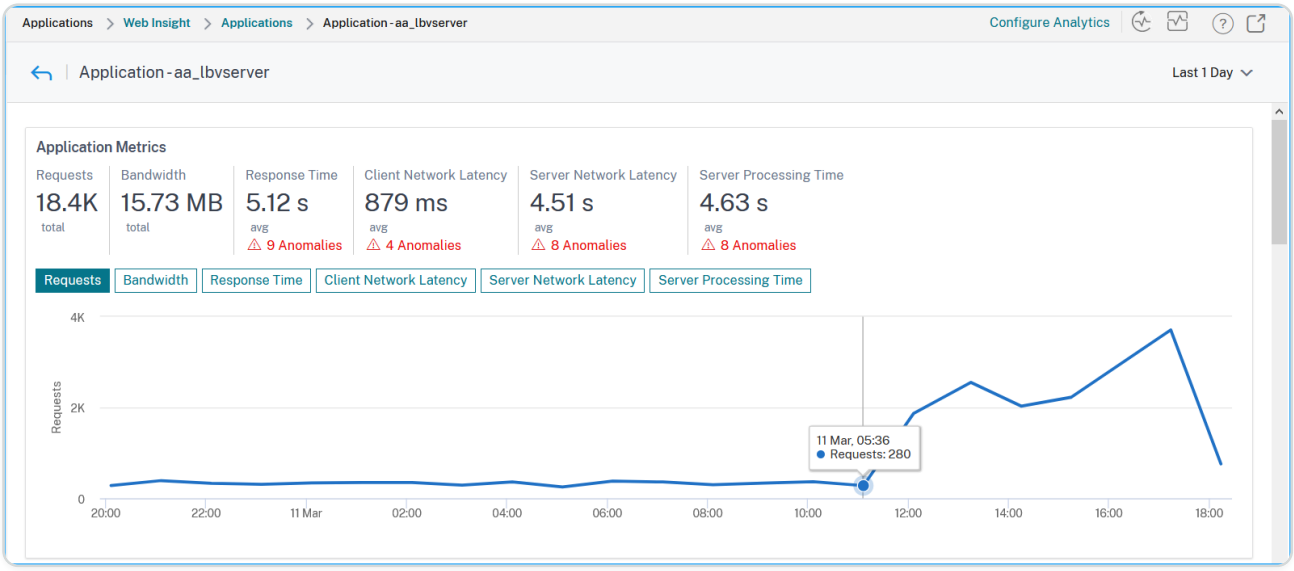
应用程序 > Web Insight 页面使您能够查看所选持续时间内响应时间异常的应用程序。“**响应时间异常的应用程序**”指标根据总异常数显示前五个应用程序。单击“**查看更多**”可查看所有应用程序。



- **应用程序** – 表示应用程序名称。
- **总异常和贡献者** – 表示应用程序的总异常。将鼠标指针悬停时，您可以分别查看来自客户端网络延迟、服务器网络延迟和服务器处理时间的总异常。
- **响应时间范围** – 表示应用程序的预期响应时间范围。
- **最大异常响应时间** – 表示应用程序的最高响应时间。
- **最大异常贡献者** – 表示应用程序的最大异常数是来自客户端网络延迟、服务器网络延迟还是服务器处理时间。

应用程序深入分析

单击应用程序可查看所选持续时间的**应用程序指标**详细信息。



应用程序指标使您能够查看：

- **摘要** – 可视化应用程序性能（例如响应时间、请求和带宽）的概述。
- **请求** – 应用程序收到的总请求数。您还可以根据总请求数查看来自前 5 个客户端的请求。

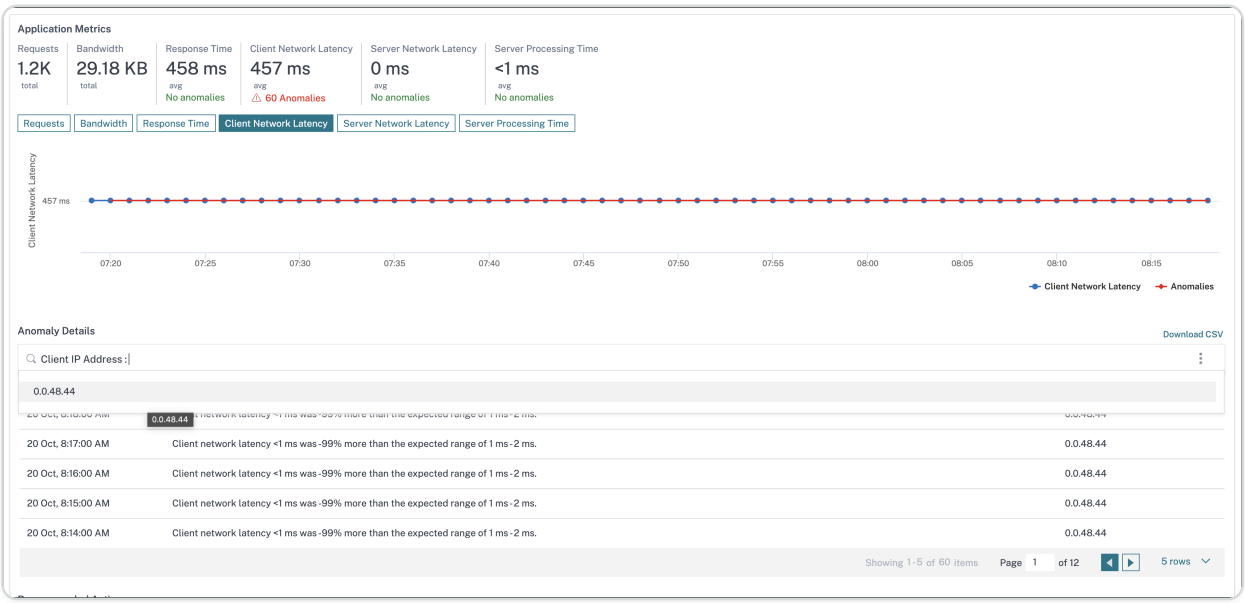
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **带宽** – 应用程序处理的总带宽。您还可以根据总带宽消耗查看来自前 5 个服务器的带宽消耗。
- **响应时间** – 在同一图表上可视化客户端网络延迟、服务器网络延迟和服务器处理时间的概述。
- **客户端网络延迟** – 平均客户端网络延迟（从客户端到 NetScaler）。
- **服务器网络延迟** – 平均服务器网络延迟（从 NetScaler 到服务器）。
- **服务器处理时间** – 平均服务器处理时间（从服务器到 NetScaler）。

如果应用程序存在异常，您可以查看异常是来自客户端网络延迟、服务器网络延迟还是服务器处理时间。单击每个选项卡可查看详细信息。

在**客户端网络延迟**和**服务器网络延迟**选项卡中，您可以查看：

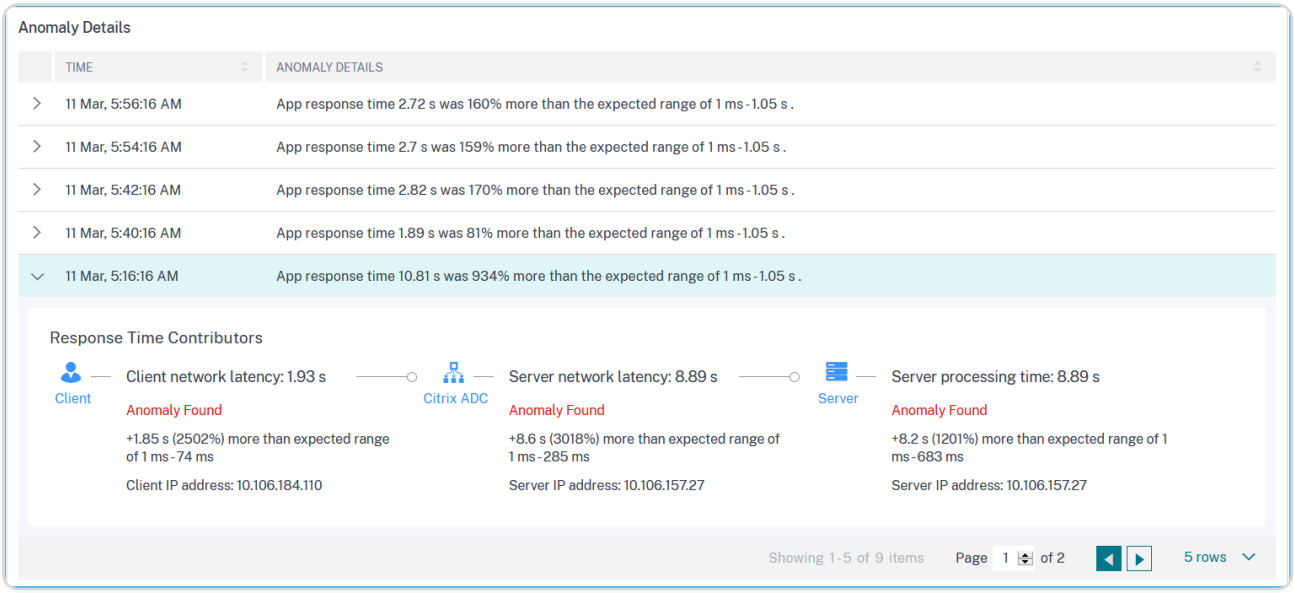
- **搜索栏** - 单击搜索栏可查看所有客户端（在客户端网络延迟中）和服务器（在服务器网络延迟中）的 IP 地址。您可以选择 IP 地址来筛选结果。
- **导出选项** - 单击**下载 CSV** 以 CSV 格式导出详细信息。



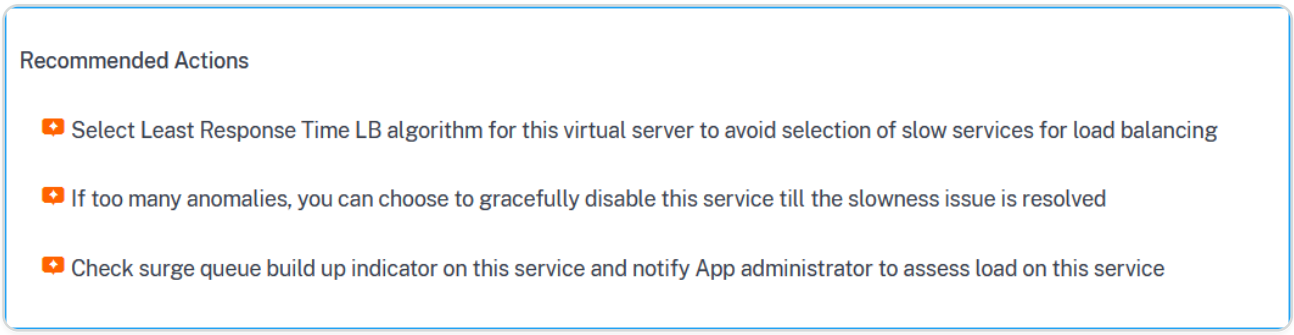
响应时间

在**异常详情**下，点击查看响应时间贡献者（从客户端到服务器）的详细信息。以下示例显示了客户端网络延迟、服务器网络延迟和服务器处理时间的异常。您还可以查看预期范围以及超出预期范围的违规情况。

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



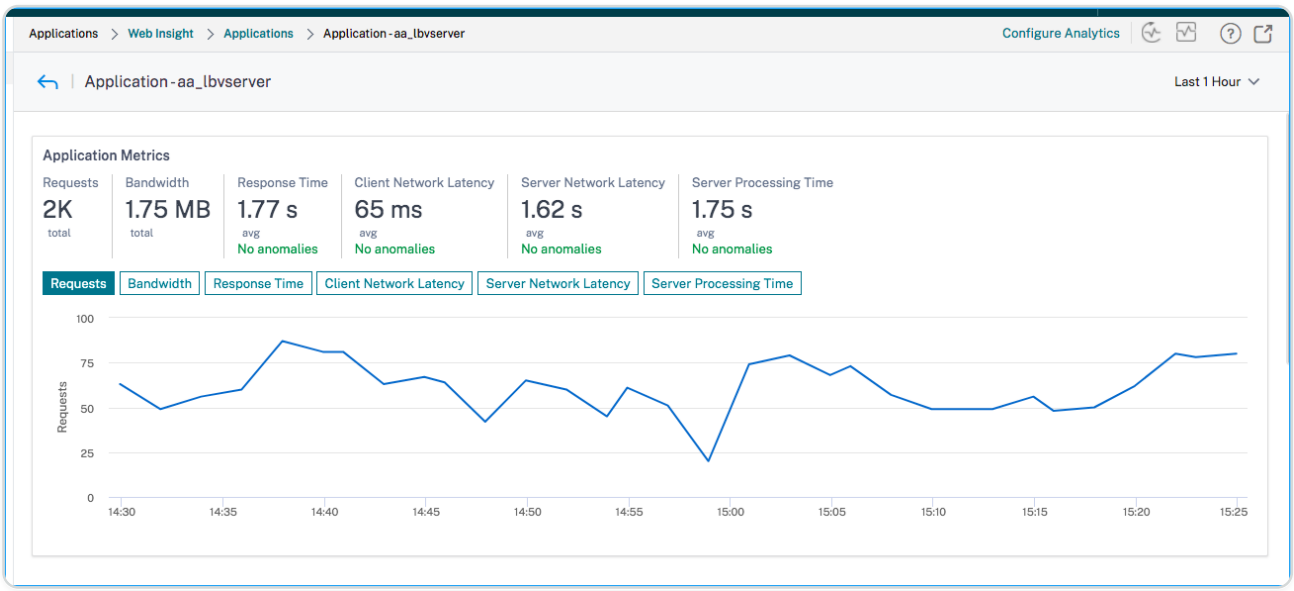
建议操作为您提供异常的可能解决方案。



同样，您可以点击**客户端网络延迟**、**服务器网络延迟**和**服务器处理时间**选项卡来查看：

- 超出预期范围的异常。
- 为您提供可能解决方案的建议操作。

如果应用程序运行良好，您可以将应用程序指标视为无异常。



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

服务图

NetScaler Console 中的服务图功能使您能够以图形方式监控所有服务。此功能还使您能够查看服务的详细分析和可操作指标。您可以查看以下服务的服务图：

- 在所有 NetScaler 实例中配置的应用程序
- Kubernetes 应用程序
- 三层 Web 应用程序

所有 NetScaler 实例中应用程序的服务图

全局服务图功能使您能够全面可视化 `clients to infrastructure to application` 视图。通过此单一窗格服务图视图，作为管理员，您可以：

- 了解用户从哪个区域访问特定应用程序（三层 Web 应用程序和微服务应用程序）
- 可视化处理客户端请求的基础设施 (NetScaler 实例) 视图
- 了解问题是来自客户端、基础设施还是应用程序
- 进一步深入排查问题

导航到 **Applications > Service Graph**，然后单击 **Global** 选项卡以查看：

- 从客户端到后端服务器连接的所有应用程序的端到端详细信息
- 所有连接到其各自数据中心的 NetScaler 实例

  注意

  只有当您拥有 GSLB 应用程序时，才能查看数据中心。

- 客户端指标信息
- NetScaler 指标信息
- 所有具有离散应用程序、自定义应用程序和离散微服务应用程序的 NetScaler 实例
- 属于自定义应用程序、离散应用程序和微服务应用程序的得分最低的 4 个应用程序
- 得分最低的 4 个虚拟服务器的指标信息

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

- 应用程序（离散应用程序、自定义应用程序和微服务应用程序）的状态，例如 **Critical**、**Review**、**Good** 和 **Not Applicable**。

有关更多信息，请参阅 服务图中的应用程序整体视图。

Kubernetes 应用程序的服务图

导航到 **Applications > Service Graph**，然后单击 **Microservices** 选项卡以查看：

- 确保端到端应用程序的整体性能
- 识别由应用程序不同组件之间的相互依赖性造成的瓶颈
- 深入了解应用程序不同组件的依赖关系
- 监控 Kubernetes 集群中的服务
- 监控哪些服务存在问题
- 检查导致性能问题的因素
- 查看服务 HTTP 事务的详细可见性
- 分析 HTTP、TCP 和 SSL 指标

通过在 NetScaler Console 中可视化这些指标，您可以更快地分析问题的根本原因并采取必要的故障排除措施。服务图将您的应用程序显示为各种组件服务。这些在 Kubernetes 集群中运行的服务可以与应用程序内部和外部的各种组件进行通信。要开始使用，请参阅设置服务图。

三层 Web 应用程序的服务图

导航到 **应用程序 > 服务图** 并单击 **Web 应用程序** 选项卡以查看：

- 有关应用程序如何配置的详细信息（包括内容交换虚拟服务器和负载平衡虚拟服务器）

  对于 GSLB 应用程序，您可以查看数据中心、NetScaler 实例、CS 和 LB 虚拟服务器。
- 从客户端到服务的端到端事务
- 客户端访问应用程序的位置
- 处理客户端请求的数据中心名称以及相关的数据中心 NetScaler 指标（仅适用于 GSLB 应用程序）
- 客户端、服务和虚拟服务器的指标详细信息
- 错误是来自客户端还是来自服务
- 服务状态，例如 **严重**、**审查** 和 **良好**。NetScaler Console 根据服务响应时间和错误计数显示服务状态。

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

  - **严重（红色）** - 表示平均服务响应时间 > 200 毫秒 且 错误计数 > 0 时
  - **审查 (橙色)** - 表示当平均服务响应时间 > 200 毫秒 或 错误计数 > 0 时
  - **良好 (绿色)** - 表示无错误且平均服务响应时间 < 200 毫秒
- 客户端状态，例如**严重**、**审查**和**良好**。NetScaler Console 根据客户端网络延迟和错误计数显示客户端状态。
  - **严重 (红色)** - 表示当平均客户端网络延迟 > 200 毫秒 且 错误计数 > 0 时
  - **审查 (橙色)** - 表示当平均客户端网络延迟 > 200 毫秒 或 错误计数 > 0 时
  - **良好 (绿色)** - 表示无错误且平均客户端网络延迟 < 200 毫秒
- 虚拟服务器状态，例如**严重**、**审查**和**良好**。NetScaler Console 根据应用程序分数显示虚拟服务器状态。
  - **严重 (红色)** - 表示当应用程序分数 < 40 时
  - **审查 (橙色)** - 表示当应用程序分数介于 40 和 75 之间时
  - **良好 (绿色)** - 表示当应用程序分数 > 75 时

注意事项：

- 只有负载平衡、内容交换、GSLB 虚拟服务器才会在服务图中显示。
- 如果没有虚拟服务器绑定到自定义应用程序，则该应用程序的详细信息在服务图中不可见。
- 只有当虚拟服务器和 Web 应用程序之间发生活动事务时，您才能在服务图中查看客户端和服务的指标。
- 如果虚拟服务器和 Web 应用程序之间没有可用的活动事务，您只能根据配置数据（例如负载平衡、内容交换、GSLB 虚拟服务器和服务）在服务图中查看详细信息。
- 如果应用程序配置有任何更改，可能需要 10 分钟才能在服务图中反映出来。

有关更多信息，请参阅应用程序的服务图。

适用于 Kubernetes 应用程序的服务图

使用适用于 Kubernetes 应用程序的服务图来可视化、监视和排查 Kubernetes 群集中的微服务。以下主题可帮助您设置、查看和分析服务图：

- 设置服务图
- 查看服务图中的详细信息
- 在服务图中配置阈值

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

- 查看服务详细信息
- 查看入口详细信息以进行故障排除
- 分布式跟踪
- 查看诊断

设置服务图

软件要求

KUBERNETES 发行版	KUBERNETES 版本	容器网络接口 (CNI)	CPX 版本	CIC 版本	NETSCALER CONSOLE 版本	NETSCALER 代理版本
开源	v1.16.3	弗兰内尔、卡利科 或 卡纳尔	13.0–41.28 或更高版本	1.5.25 或更高版本	13.0–47.22 或更高版本	13.0–47.22 或更高版本

您可以配置具有各种部署拓扑的 Kubernetes 集群，下表提供了服务图中支持的拓扑：

拓扑	服务图支持
单层或统一入口	是
双层	是
云	是，但云负载均衡器未在图中显示
轻量级服务网格	是
服务网格	是
类型为 LoadBalancer 的服务	否
NodePort 类型的服务	否

要在 NetScaler Console 中完成服务图设置，请单击您为 Kubernetes 集群配置的拓扑类型，并完成以下步骤：

- 单层或统一入口拓扑

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

- 双层或 Service Mesh Lite 拓扑
- 服务网格拓扑

注意

双层和 Service Mesh Lite 拓扑的服务图设置过程保持不变。

开始之前

您可以使用以下场景查看服务图：

- NetScaler Console 和 Kubernetes 集群位于同一网络（例如，NetScaler Console 和 Kubernetes 集群托管在同一 Citrix Hypervisor 上）。
- NetScaler Console 和 Kubernetes 集群位于不同的网络。在这种情况下，您必须配置一个 本地代理 并在托管 Kubernetes 集群的网络上注册该代理。

单层或统一入口拓扑

请确保您已完成以下操作：

- 配置了具有单层或统一入口拓扑的 Kubernetes 集群。
- 在 NetScaler Console 中添加了 (/zh-cn/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-unified-single-ingress-topology.html#add-vpx-or-sdx-or-mpx-or-blx-instance-in-citrix-adm) 并启用了 **Web Insight**。
- 在 NetScaler Console 中添加了 (/zh-cn/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-unified-single-ingress-topology.html#add-kubernetes-cluster-in-citrix-adm)。

双层或 Service Mesh Lite 拓扑

确保您已完成以下操作：

- 配置了具有任何受支持拓扑之一的 Kubernetes 集群。
- 在 NetScaler Console 上配置了 (/zh-cn/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#configure-static-routes-in-citrix-adm-agent)，以启用 NetScaler Console 与 NetScaler CPX 之间的通信。

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

> **注意**
>
> 如果您已将 NetScaler Console 作为微服务部署在同一集群中，则可以忽略此过程。

- 从 GitHub 存储库下载了 (/zh-cn/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#download-the-sample-deployment-files-from-github)。
- 在 CPX YAML 文件中添加了 (/zh-cn/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#add-parameters-in-cpx-yaml-file)，以确保 CPX 成功注册到 NetScaler Console。
- 在 NetScaler Console 中添加了 (/zh-cn/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#add-vpx-or-sdx-or-mpx-or-blx-instance-in-citrix-adm)。
- 在 NetScaler Console 中添加了 (/zh-cn/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#add-kubernetes-cluster-in-citrix-adm)。
- 部署了 (/zh-cn/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#deploy-a-sample-microservice-application)。
- 部署了 NetScaler CPX 并 (/zh-cn/netscaler-application-delivery-management-software/current-release/application-analytics-and-management/service-graph/sg-service-mesh-dual-tier-topology.html#deploy-cpx-and-register-cpx-in-adm)（仅适用于双层架构）
- 已启用 自动选择虚拟服务器 以许可虚拟服务器。
- 已启用 Web 事务和 TCP 事务设置 为 **所有**，以便 NetScaler 代理获取 HTTP 和 TCP 事务。
- 已发送 流量 到微服务。

服务网格拓扑

请确保您已完成以下操作：

- 配置了 Kubernetes 集群版本 `1.14.0` 并采用以下任一服务网格拓扑：
  - 将 NetScaler CPX 作为 Istio 的 Sidecar 代理
  - 将 NetScaler 作为 Istio 的入口网关
- 已启用 `admissionregistration.k8s.io/v1beta1` API。您可以使用以下方式验证 API：

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

`kubectl api-versions | grep admissionregistration.k8s.io/v1beta1`

以下输出表明 API 已启用：

`admissionregistration.k8s.io/v1beta1`

- 已安装 Istio `istio v.1.3.0`。
- 已安装 Helm 版本 3.x。
- 已在 NetScaler Console 上配置 静态路由，以启用 NetScaler Console 和 NetScaler CPX 之间的通信。

> **注意**
>
> 如果已在同一集群中将 NetScaler 代理部署为微服务，则可以忽略此过程。

- 配置了 所需参数 以填充服务网格拓扑数据。
- 部署了 示例应用程序。
- 在 NetScaler Console 中添加了 Kubernetes 集群。
- 启用了 自动选择虚拟服务器 以许可虚拟服务器。

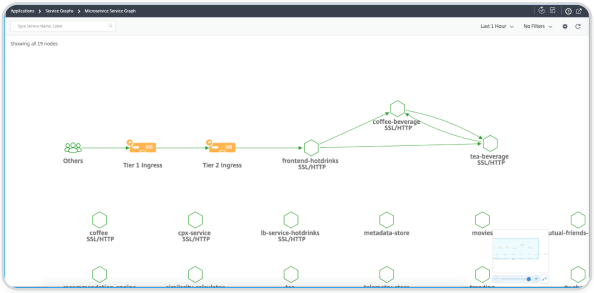
> **注意**
>
> 当 CPX 作为 sidecar 代理部署在服务网格部署中时，只有当 IP 地址与 CPX NS IP 匹配时，虚拟服务器才会被许可。

- 为 NetScaler 代理启用了 Web 事务和 TCP 事务设置 为 **所有**，以获取 HTTP 和 TCP 事务。
- 将 流量 发送到微服务。

在服务图中查看详细信息

在 NetScaler Console 中，导航到 **Applications（应用程序）> Service Graphs（服务图）> Kubernetes service graph（Kubernetes 服务图）**，然后从列表中选择时间段以查看服务图详细信息。

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

两层/SERVICE MESH LITE 拓扑	单层/统一入口拓扑
	

- **第 1 层入口** – Kubernetes 集群内的 NetScaler Ingress Controller 配置 Kubernetes 集群外的 NetScaler 实例 (VPX/MPX/SDX/BLX)。
- **第 2 层入口** – NetScaler Ingress Controller 作为 sidecar 与 Kubernetes 集群内的 NetScaler CPX 实例一起运行。
- **入口** – 显示所有其他部署拓扑。

服务图仪表板

1 - 应用程序的端到端网络映射，显示组件服务如何通信

2 – 显示特定时间段内命中和错误的图表

3 – 用于搜索服务的搜索栏

4 – 用于选择时间段的时间列表

5 - 应用筛选器以显示服务

6 – 设置图标

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

7 – 放大和缩小视图

8 – 图形视图或表格视图

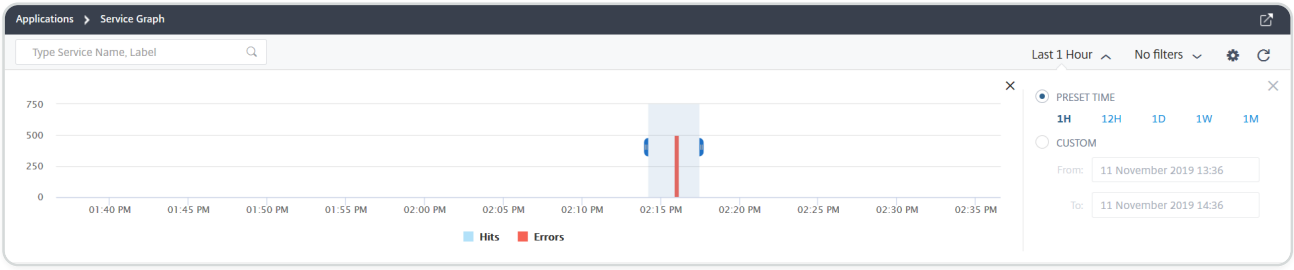
根据所选的时间范围，您可以查看服务图。

服务图标	描述
	边缘宽度表示命中次数。边缘宽度越大，表示命中次数越高。
	带有警告图标的服务表示该服务存在错误。
	带有秒表图标的服务表示该服务存在延迟或响应时间问题。
	同时带有秒表和警告图标的服务表示该服务同时存在错误和延迟/响应时间问题。

注意

如果服务没有警告或秒表图标，则表示该服务存在异常或命中数超出阈值。

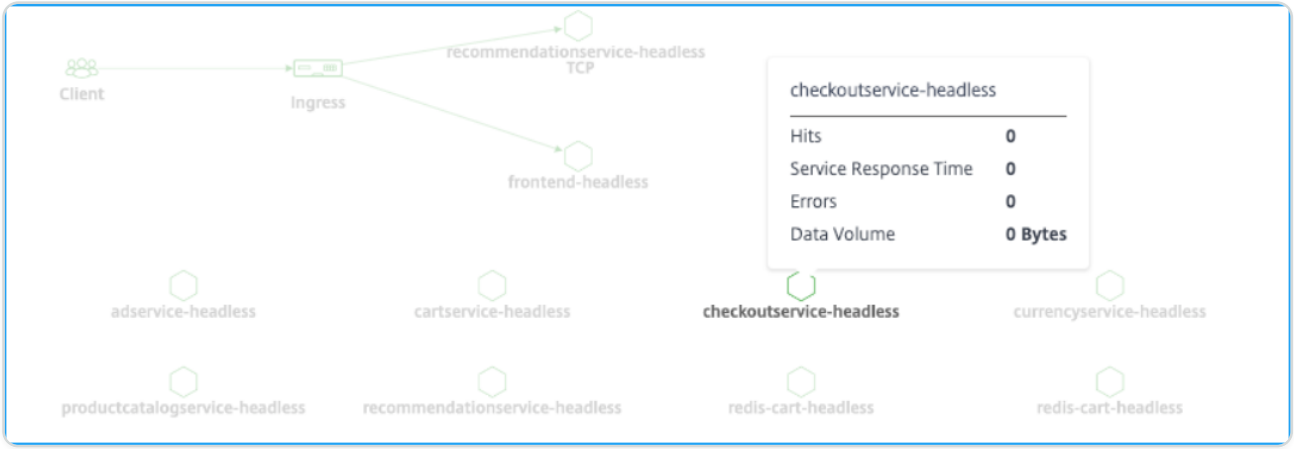
根据所选的时间段，您可以查看服务图。从图中选择指示命中数的时间段，以进一步深入查看更多信息。



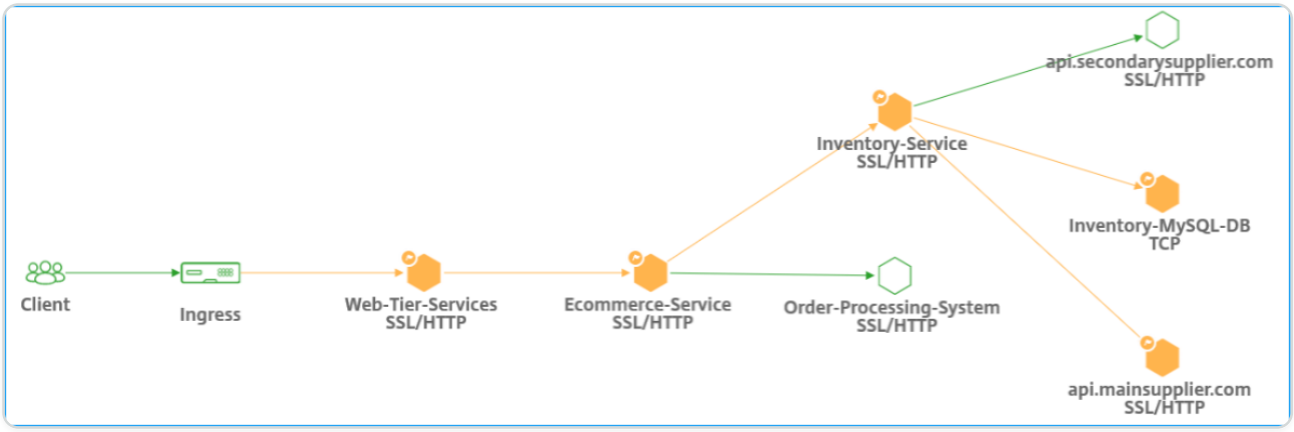
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

如果 NetScaler Console 未收到活动事务，则只能查看由 NetScaler 实例负载平衡的服务。当您将鼠标指针悬停在服务上时，所有指标都显示为 0。



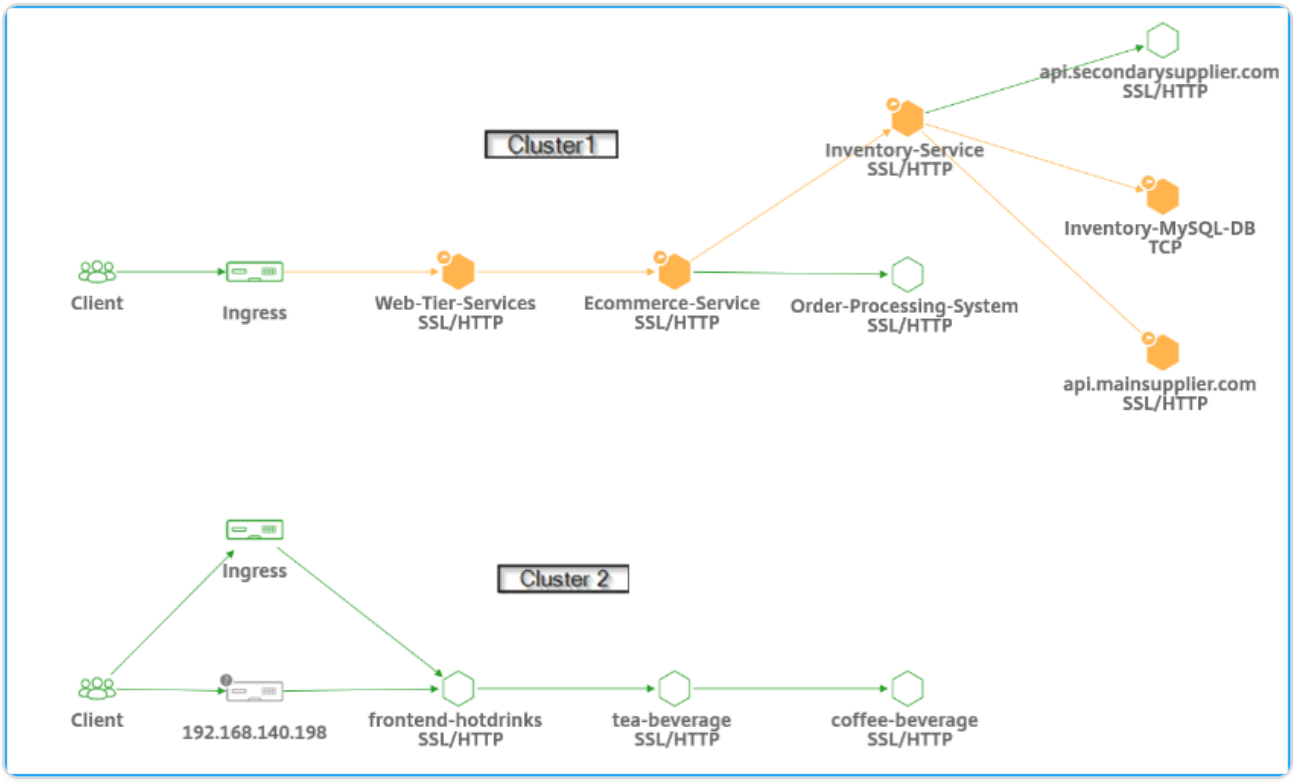
服务图显示了服务使用的协议。假设您的 Kubernetes 集群中运行着以下服务，如图像所示：



注意

如果您在 **编排** > **Kubernetes** > **集群** 中添加了多个集群，则可以查看与每个集群关联的服务。

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



您可以查看服务的以下状态：

- **严重（红色）** - 表示平均服务响应时间 > 200 毫秒且错误计数 > 0 时
- **审查（橙色）** - 表示平均服务响应时间 > 200 毫秒或错误计数 > 0 时
- **良好 (绿色)** - 表示无错误且平均服务响应时间 < 200 毫秒

以下协议可帮助您识别服务使用的协议：

- **TCP** – 表示服务正在使用 TCP 协议。
- **SSL, HTTP** – 表示服务正在使用基于 HTTP 的 SSL 协议。
- **SSL, TCP** – 表示服务正在使用基于 TCP 的 SSL 协议。

> **注意**
>
> 没有协议的服务表示该服务正在使用 HTTP 协议。

使用表格视图查看关键指标趋势

使用表格视图，您可以查看：

- 服务的关键指标
- 源服务与目标服务之间的关键指标

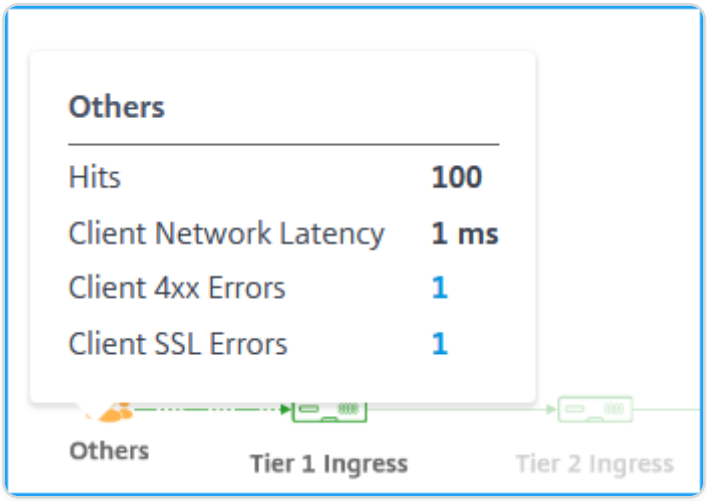
© 1997–2026 Citrix Systems, Inc. All rights reserved.

作为管理员，您可以使用这些关键指标分析所选时间段内黄金信号的趋势。

查看客户端指标

您可以查看客户端从哪个位置访问服务。作为管理员，您可以可视化客户端指标并分析客户端出现的问题。

将鼠标指针悬停在客户端区域上以查看指标。



- **命中数** - 指示客户端收到的总命中数。
- **客户端网络延迟** - 指示平均客户端网络延迟。
- **客户端 4xx 错误** - 指示客户端 4xx 错误总数。
- **客户端 SSL 错误** - 指示客户端 SSL 错误总数。

NetScaler Console 中的 IP 块 - 如果客户端使用公共 IP 地址，NetScaler Console 可以识别客户端位置。NetScaler Console 具有内置的位置 CSV 文件，可根据客户端 IP 地址范围匹配位置。

仅当 IP 地址添加到 NetScaler Console 服务器时，NetScaler Console 才能识别具有私有 IP 地址的客户端位置。例如，如果客户端 IP 地址落在与城市 A 关联的私有 IP 地址范围内，NetScaler Console 会识别出该客户端的流量源自城市 A。

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

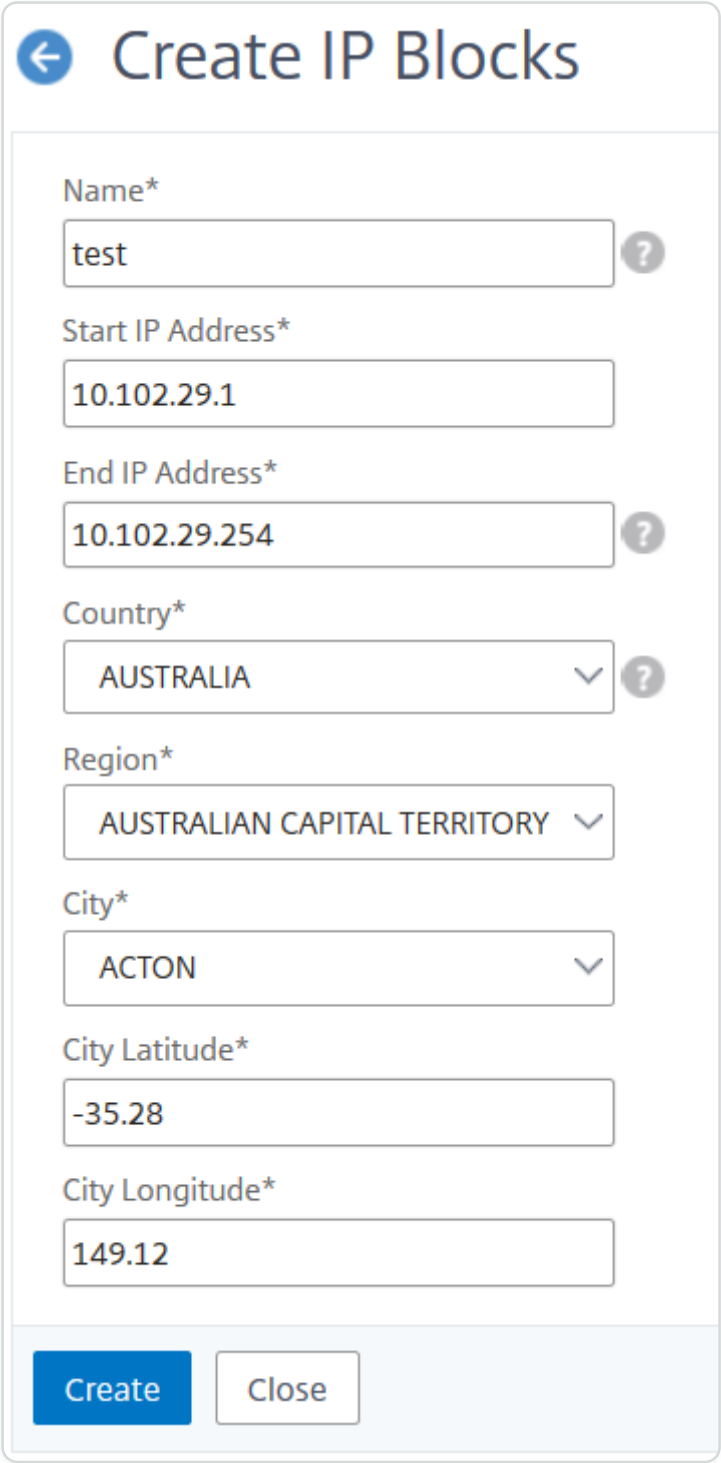
创建私有 IP 块

当客户端私有 IP 地址添加到 NetScaler Console 服务器时，NetScaler Console 可以识别客户端的位置。例如，如果客户端的 IP 地址落在与城市 A 关联的私有 IP 地址块范围内，NetScaler Console 会识别出该客户端的流量源自城市 A。

要创建 IP 块：

1. 在 NetScaler Console 中，导航到 **设置** > **分析设置** > **IP 块**，然后单击 **添加**。
2. 在 **创建 IP 块** 页面中，指定以下参数：
   - **名称**。为私有 IP 块指定一个名称
   - **起始 IP 地址**。为 IP 块指定最低 IP 地址范围。
   - **结束 IP 地址**。指定 IP 块的最高 IP 地址范围。
   - **国家/地区**。从列表中选择国家/地区。
   - **区域**。区域会根据国家/地区自动填充，但您可以选择自己的区域。
   - **城市**。城市会根据区域自动填充，但您可以选择自己的城市。
   - **城市纬度**和**城市经度**。纬度和经度会根据您选择的城市自动填充。
3. 单击**创建**以完成。

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



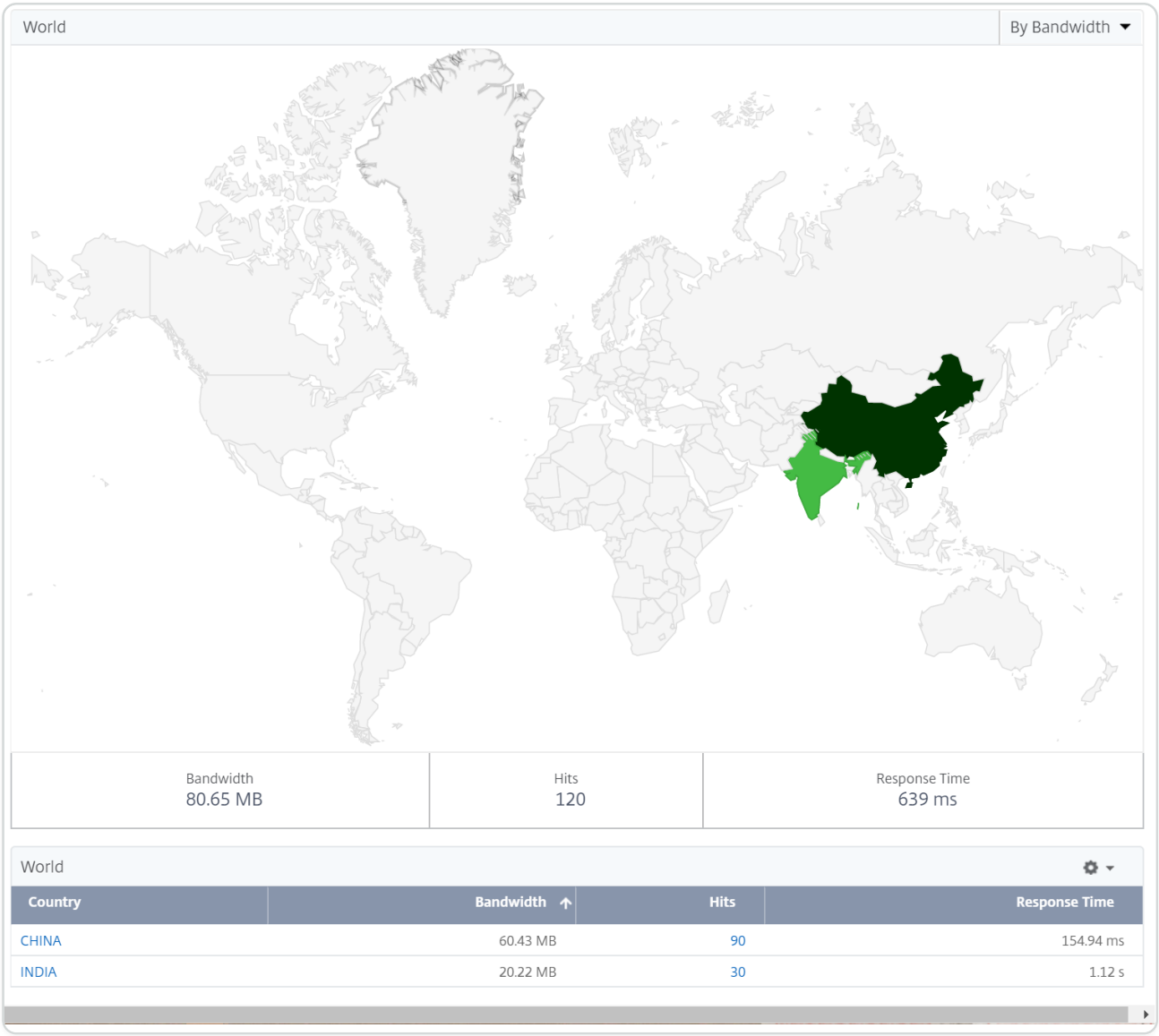
公共 IP 块

如果客户端使用公共 IP 地址，NetScaler Console 还可以识别客户端的位置。NetScaler Console 具有内置的位置 CSV 文件，可根据客户端 IP 地址范围匹配位置。要使用公共 IP 块，唯一的要求是您必须从**配置 Insight** 页面启用**启用地理数据**收集。

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

注意

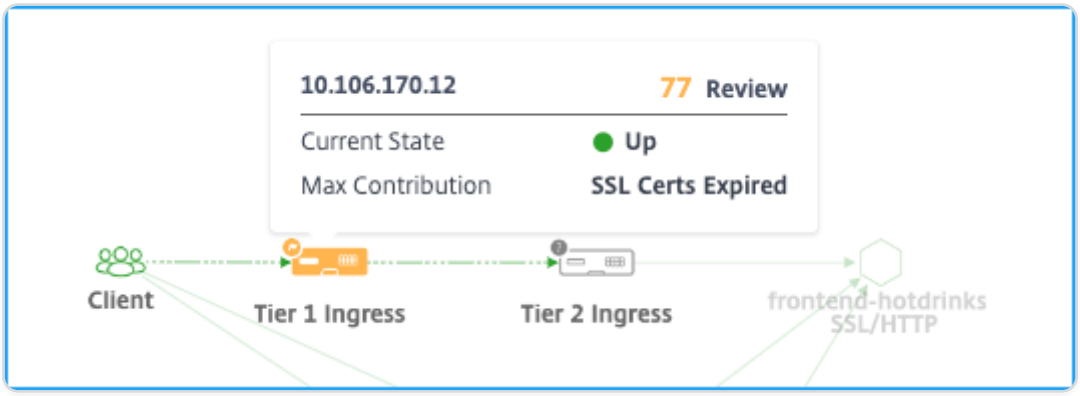
NetScaler Console 需要互联网连接才能显示特定地理位置的地理地图。导出 .pdf、.png 或 .jpg 格式的地理地图也需要互联网连接。



查看入口指标

您可以查看 Kubernetes 集群中使用的入口类型。

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



- NetScaler IP 地址及其分数
- **当前状态** – 指示 NetScaler 实例是处于“正常”、“关闭”还是“状态异常”
- **最大贡献** – 指示影响实例分数的问题

对于单层拓扑，您只能查看一个 **入口**。

单击 **入口** 以深入查看详细信息。有关更多信息，请参阅查看入口详细信息以排查问题。

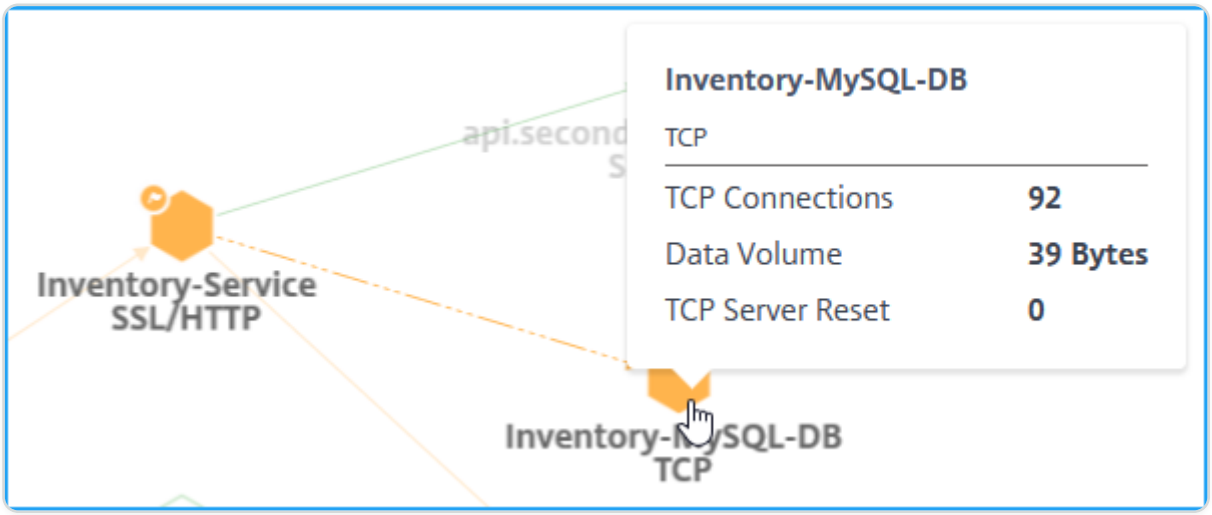
查看 TCP 和 SSL 指标

使用 TCP 和 SSL 指标，您可以：

- 查看服务之间的 TCP 连接详细信息
- 确定 TCP 相关问题是来自源服务还是目标服务
- 查看 SSL 错误是来自源服务还是目标服务
- 查看 SSL 服务使用的 SSL 协议版本

TCP 指标

将鼠标指针悬停在 TCP 服务或其关联的传入服务上，以查看 TCP 指标。



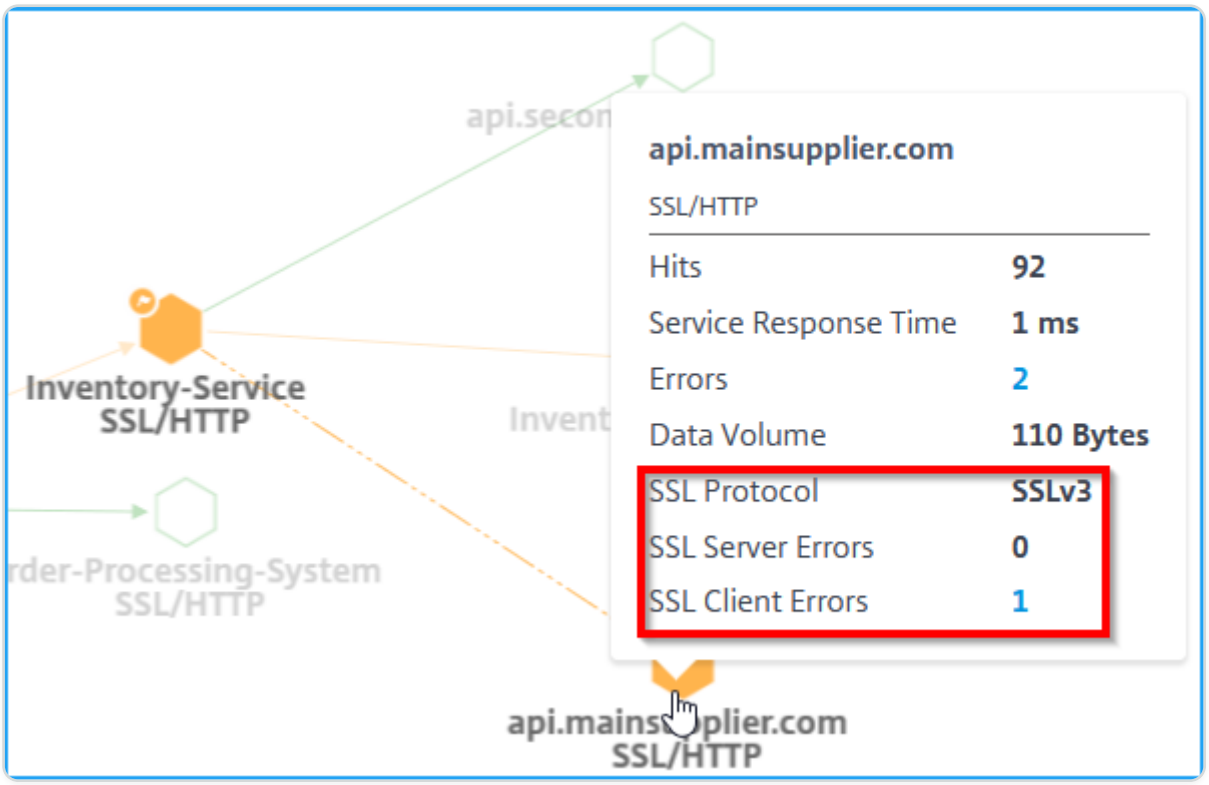
- **TCP 连接** – 服务之间建立的总连接数

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

- **数据量** – 服务处理的总数据量
- **TCP 服务器重置** – 服务器发起的 TCP 重置总数

SSL 指标

将鼠标指针悬停在使用 SSL 协议的服务上，以查看 SSL 指标。



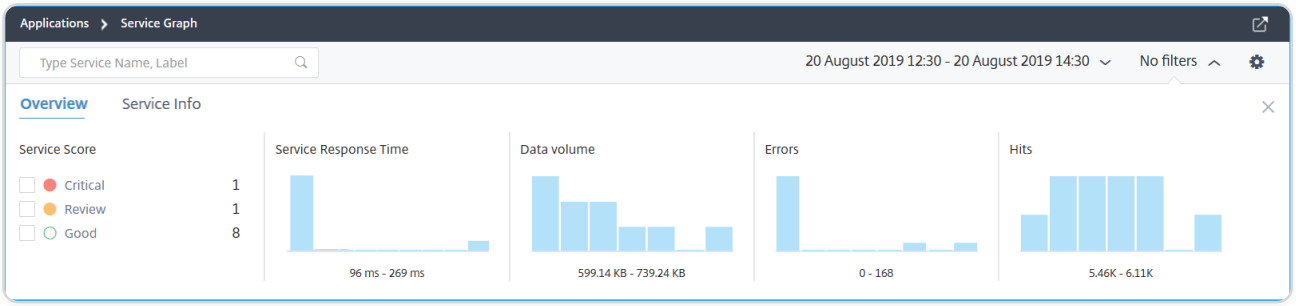
- **SSL 服务器错误** – 指示来自服务器的 SSL 错误总数。（例如，SSL 证书未知）
- **SSL 协议** – 指示服务使用的 SSL 协议版本
- **SSL 客户端错误** - 指示来自客户端的 SSL 错误总数。（例如，SSL 客户端身份验证错误）

查看服务详情

单击服务并选择**查看详情**以查看服务详情。有关更多信息，请参阅查看服务详情。

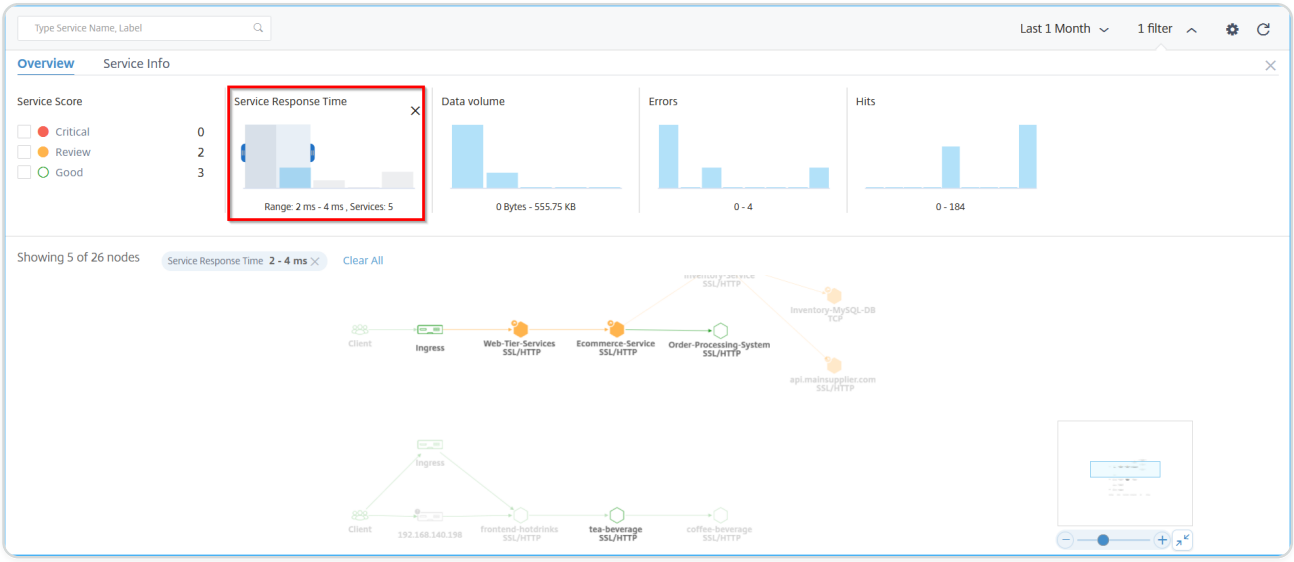
应用筛选器

您可以应用筛选器来查看特定的服务信息。单击**无筛选器**列表以获取筛选选项。



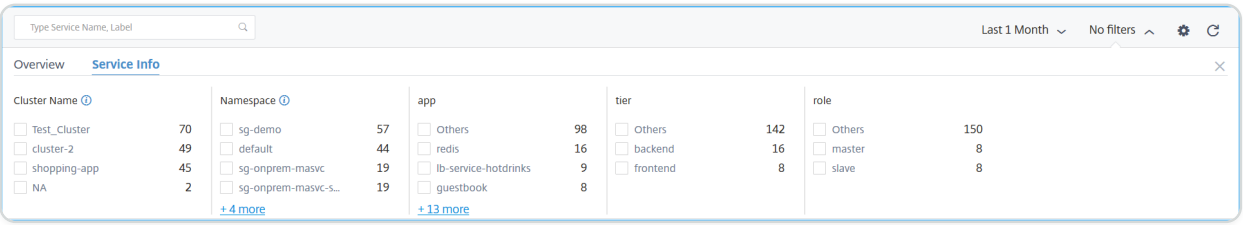
© 1997–2026 Citrix Systems, Inc. All rights reserved.

例如，如果您想查看延迟小于 150 毫秒的服务，请单击**服务响应时间**下的条形图以显示结果。



单击 **服务信息** 以选择并应用以下筛选器：

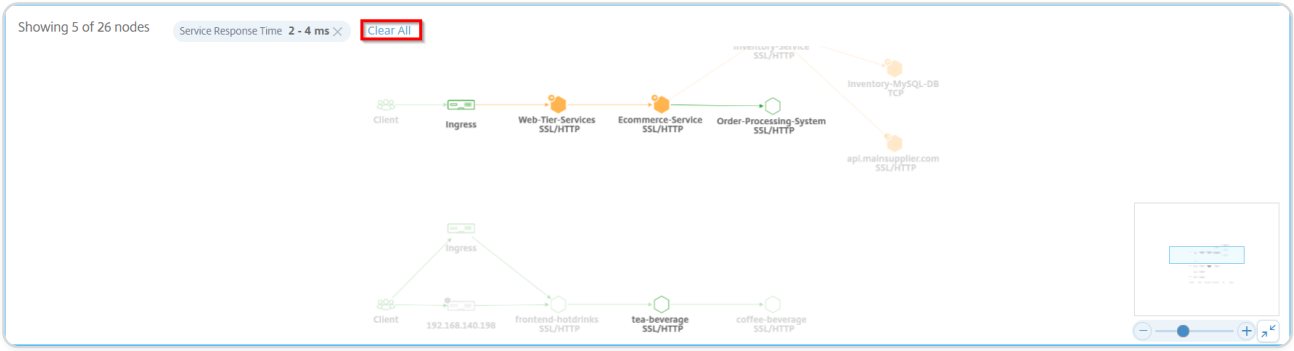
- **群集** – 显示适用于所选群集或多个群集的所有服务。
- **命名空间** – 显示适用于所选命名空间的所有服务。



注意

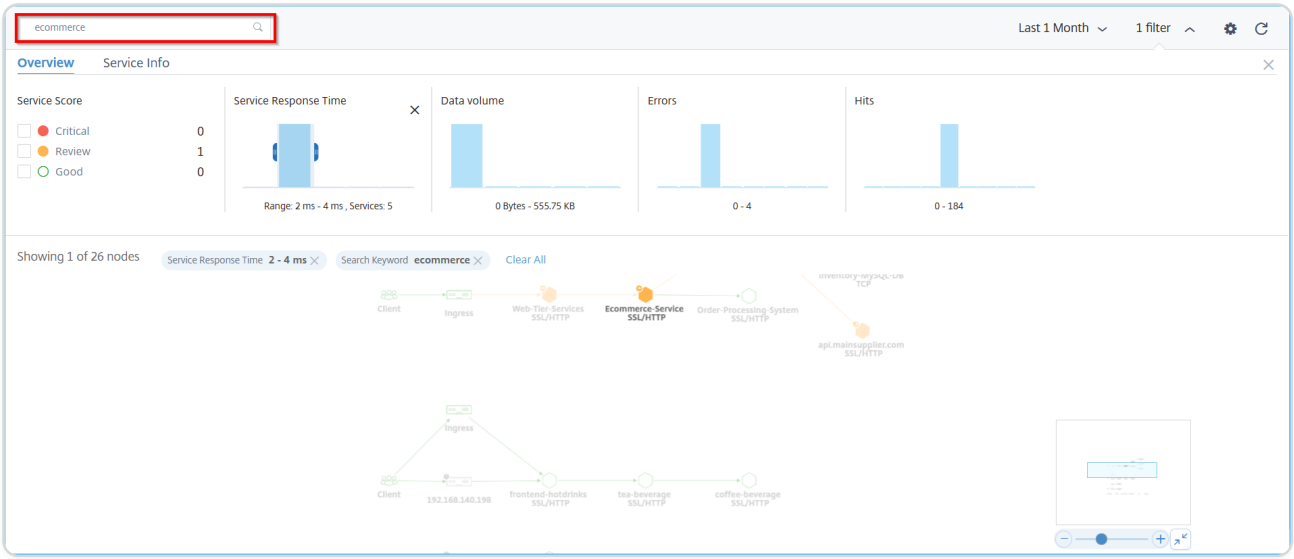
> 根据 Kubernetes 服务定义 YAML 中为服务配置的标签，您可能还会看到更多筛选器选项。

单击 **清除所有** 以清除所有筛选器。

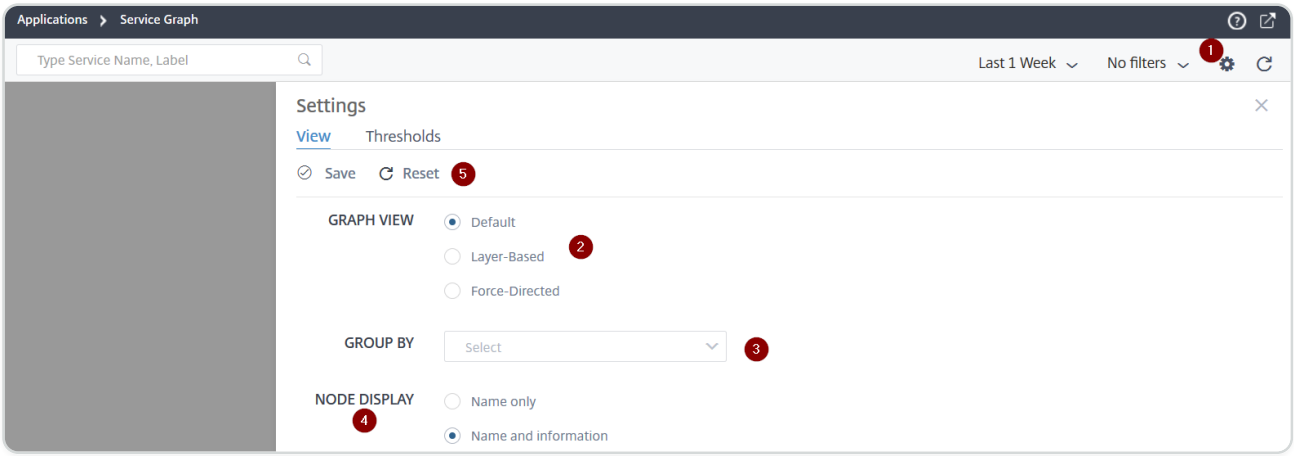


或者，您也可以使用搜索文本框并键入服务名称，以在服务图中显示结果。

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



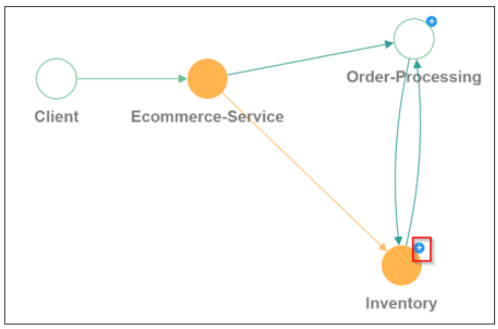
使用设置选项



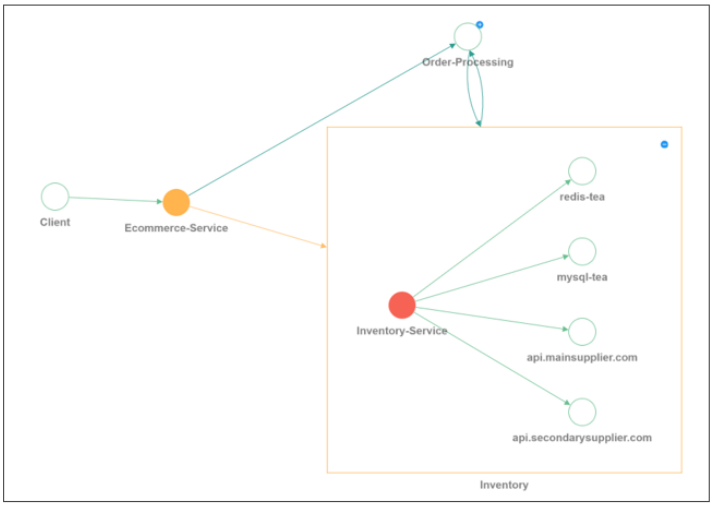
1 – 设置图标

2 – 将服务图显示为默认、基于层或力导向视图的选项

3 – 从列表中选择选项以根据类别查看服务。从列表中选择类别后，单击图表上的 **+** 以查看所有服务



Collapsed view



Expanded view

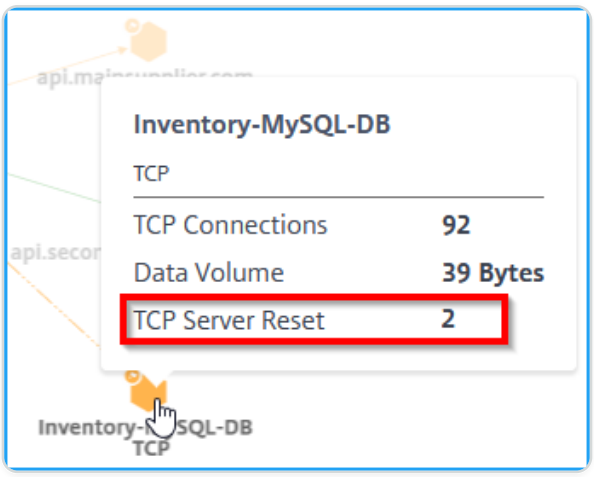
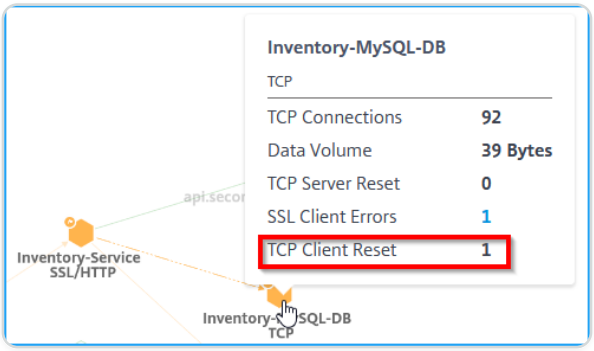
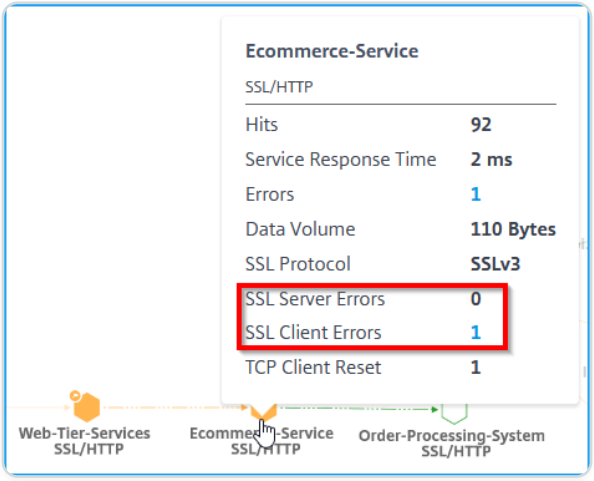
© 1997–2026 Citrix Systems, Inc. All rights reserved.

4 – 使您能够选择如何显示服务的选项。

5 - 用于保存设置或重置为默认值的选项。

分析错误

将鼠标指针悬停在指示错误的某个服务上。

错误	描述
	**TCP 服务器重置**表示从服务器发起的 TCP 重置总数。
	**TCP 客户端重置**表示由客户端发起的 TCP 重置总数。
	SSL 客户端错误表示来自客户端的 SSL 错误总数。（例如，SSL 客户端身份验证错误）。
	SSL 服务器错误表示来自服务器的 SSL 错误总数。（例如，SSL 证书未知）

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

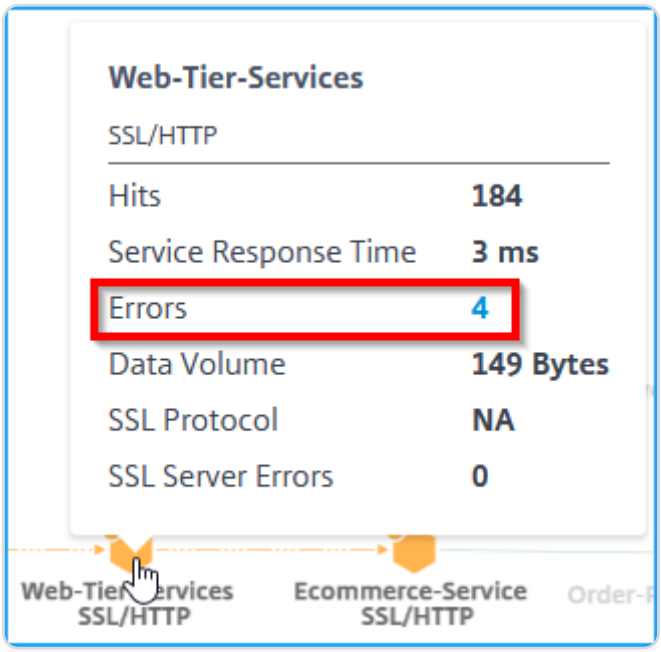
注意

- 客户端错误计数（无论协议类型如何）在任何服务中显示，如果客户端错误计数为 **1 或更高**。
- 任何服务显示的客户端错误计数表示错误来自客户端。

查看 HTTP 事务详情

注意

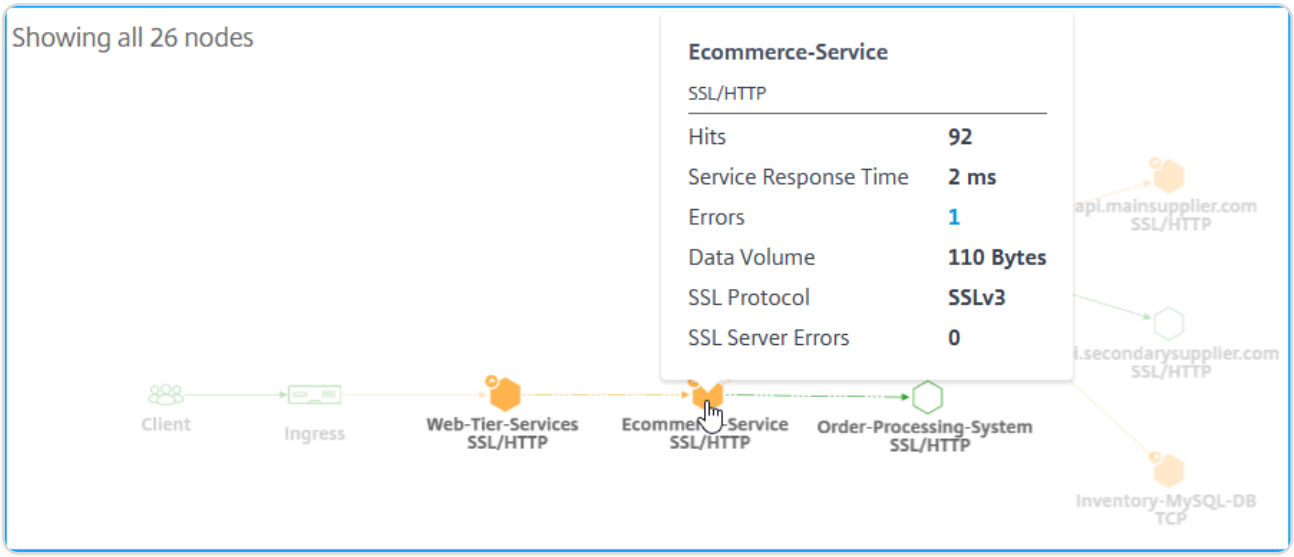
您可以通过将鼠标指针悬停在有错误的服务上并单击问题计数来查看错误。



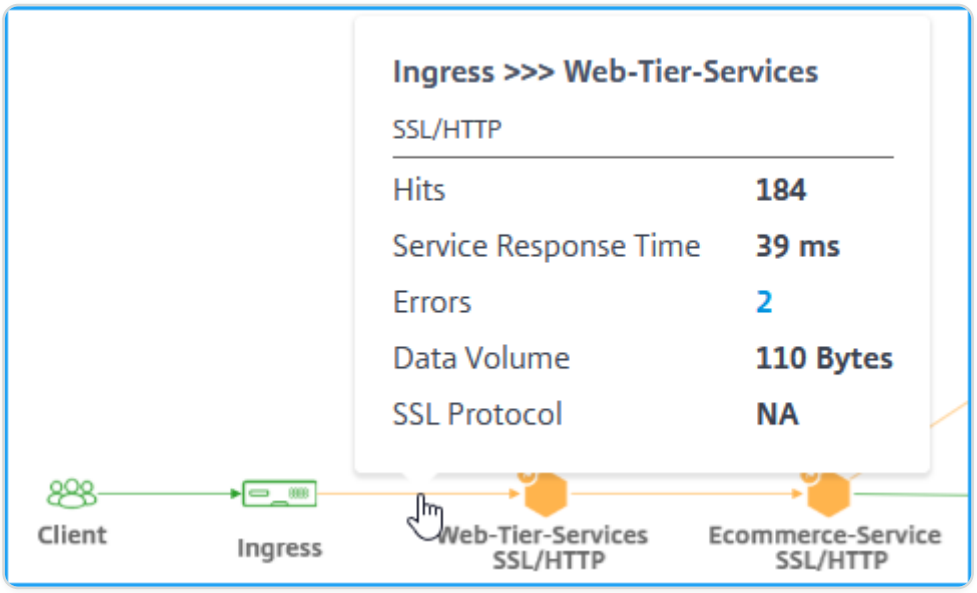
根据图像中显示的示例，您可以查看应用程序的端到端网络映射，其中显示了您的组件服务如何通信。

当您将鼠标指针悬停在 **Ecommerce-Service** 上时，您可以查看 **Ecommerce-Service** 的指标详情。

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



NetScaler Console 还允许您查看 Ingress 和服务之间的事务详情。将鼠标指针悬停以查看 Ingress 和服务之间的总错误、平均服务响应时间等详情。



命中数 – 表示服务接收到的总命中数。

服务响应时间 – 表示服务响应首字节时间 (TTFB) 所花费的平均响应时间。

错误 – 表示总错误，例如 4xx、5xx 等。

数据量 – 表示服务处理的数据总量。

SSL 协议 – 指示 SSL 协议版本。

单击 **入口** 和 **服务** 之间的箭头以查看详细事务。

有关详细信息，请参阅 查看 Web 事务分析。

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

在服务图中配置阈值

作为管理员，您可以为 Kubernetes 服务配置阈值。NetScaler Console 根据服务响应时间和错误计数显示服务状态（严重、审查和良好）。默认情况下，您可以查看应用于所有服务的**默认阈值**（服务响应时间 = 200 毫秒，错误计数 = 0）。

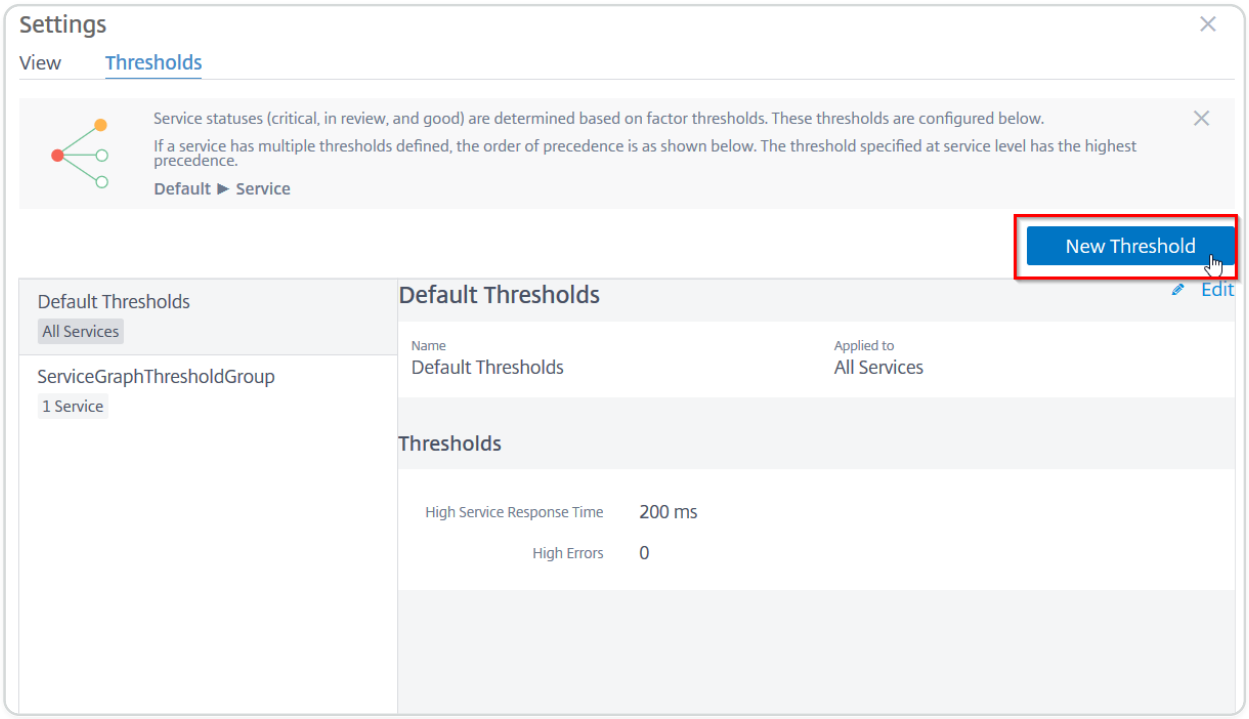
注意

您无法删除默认阈值。

要配置新阈值：

在服务图中：

1. 单击设置图标并选择**阈值**选项卡。
2. 单击**新建阈值**以配置新阈值。



新建阈值页面随即显示。

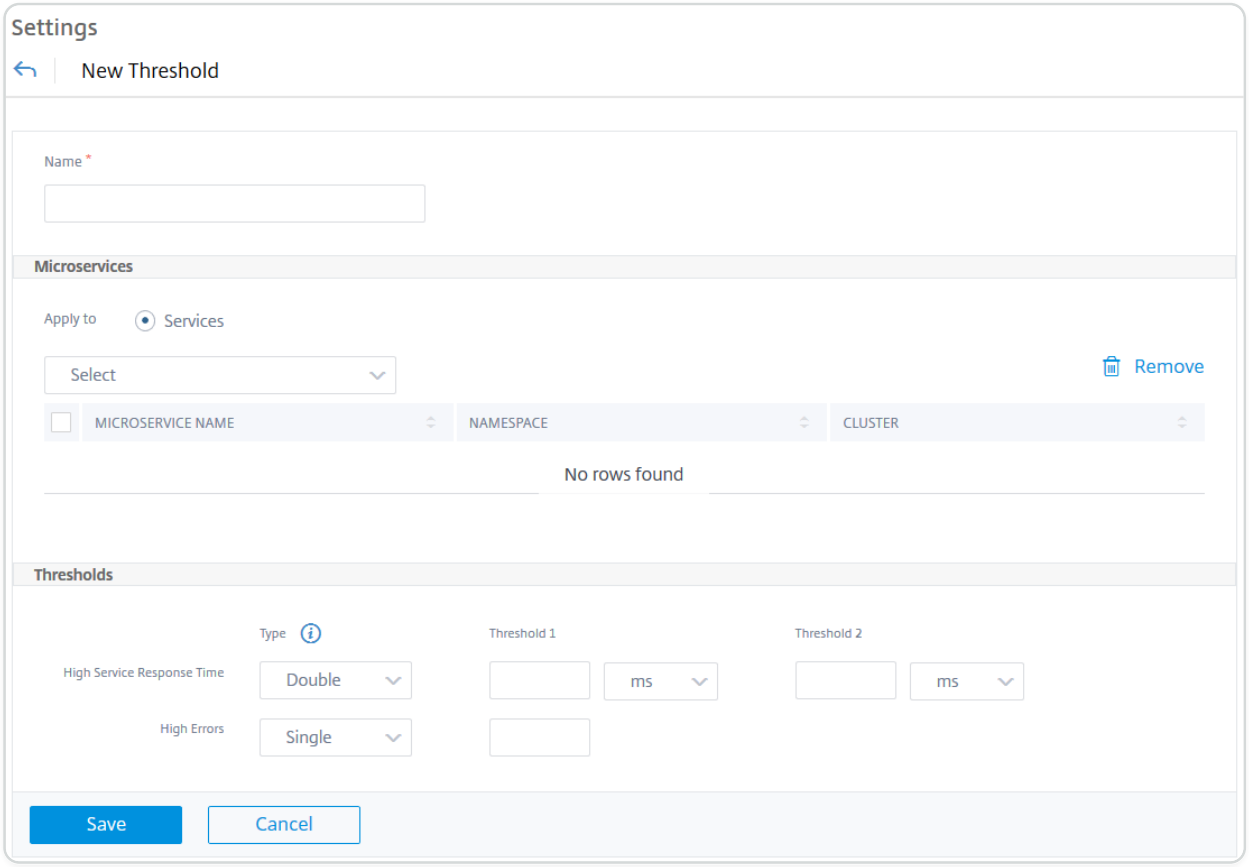
3. 配置以下参数：
   a. **名称** – 为阈值指定一个名称。
   b. 在**微服务**下，选择要应用阈值的服务
   c. 在**阈值**下，为高响应时间和高错误选择**单个**或**双重**
   d. 指定阈值。

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

> **注意**
>
> 如果选择双阈值，请确保：

- 阈值 1 的值小于阈值 2 的值。例如，如果将阈值 1 配置为 250 毫秒，则阈值 2 必须为 251 毫秒或更高。
- 阈值 1 的值不能与阈值 2 的值相同。

4. 单击“**保存**”。



阈值已成功创建。您可以在“**阈值**”页面中查看阈值详细信息。

单阈值

配置单阈值时，NetScaler Console 会执行以下操作：

- 将当前值与配置的阈值进行比较
- 根据超出阈值计算总罚分
- 根据罚分计算显示服务分数和服务状态

双阈值

配置双阈值时，NetScaler Console 会执行以下操作：

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

- 将当前值与配置的阈值进行比较
- 检查当前值是否为：
  - 小于阈值 1
  - 介于阈值 1 和阈值 2 之间
  - 大于阈值 2
- 根据超出阈值计算总惩罚
- 根据惩罚计算显示服务分数和服务状态

查看服务详情

单击服务并选择**查看详情**。

服务详情选项(/en-us/netscaler-application-delivery-management-software/media/sg-details.png)

服务详情页面可让您查看：

- 托管服务的集群名称 (1)
- 服务的命名空间和服务标签 (2) (4)
- 与所选服务连接的所有相关入站和出站服务 (3)
- 以图表形式显示服务关键指标，例如命中数、响应时间、错误、数据量、SSL 前端错误和 TCP 前端错误 (5)。
- 与服务关联的后端 Pod (6)。

  服务详情(/en-us/netscaler-application-delivery-management-software/media/sg-details-more.png)

利用这些关键指标趋势，您可以分析服务在特定时间段内的性能表现。

响应时间指标可让您查看：

- **99 百分位** – 表示所选持续时间内 99% 的请求小于 32 毫秒（根据示例图像）。
- **平均值** – 表示服务的平均响应时间
- **99.9 百分位** – 表示服务的最高响应时间

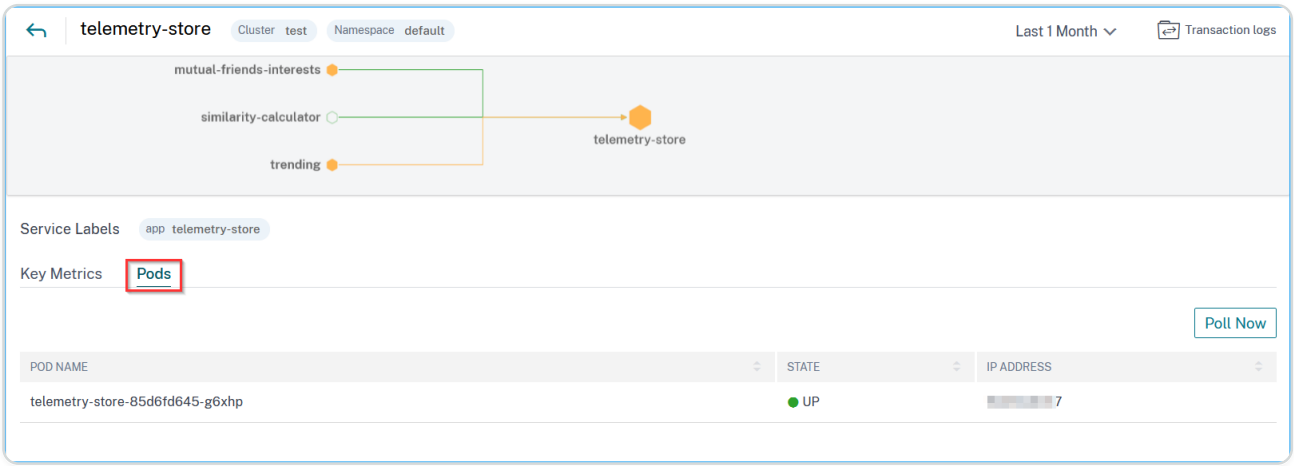
© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标详情

指标	描述
请求数	服务收到的请求总数
错误	服务产生的 HTTP 错误总数
服务响应时间	服务响应首字节 (TTFB) 的平均响应时间。
数据量	服务处理的数据总量
SSL 前端错误	服务产生的 SSL 前端错误总数。例如：SSL CLIENTAUTH FAILURE
SSL 后端错误	服务产生的 SSL 后端错误总数。例如：SSL Client Errors
TCP 后端错误	服务中的 TCP 后端错误总数。例如：TCP 服务器重置
TCP 前端错误	服务中的 TCP 前端错误总数。例如：TCP 客户端重置

查看后端 Pod 详细信息

单击“**Pod**”选项卡可查看与服务关联的后端 Pod。

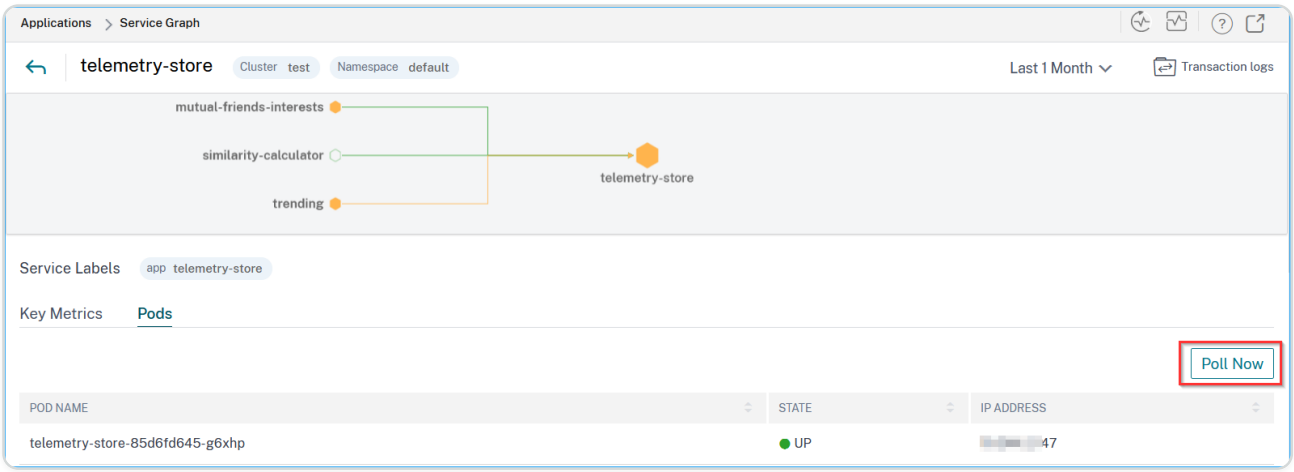


- **Pod 名称** – 表示 Pod 名称
- **状态** – 表示 Pod 是否正在运行 (UP) 或未运行 (DOWN)。
- **IP 地址** – 表示 Pod IP 地址

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

使用“立即轮询”选项获取 Pod 状态

“**立即轮询**”选项从集群中获取最新的 Pod 状态。



查看入口详细信息以排查问题

在服务图中，单击入口并选择**查看详细信息**以可视化为 Kubernetes 集群配置的 NetScaler 实例的详细信息。

入口详细信息(/en-us/netscaler-application-delivery-management-software/media/ingress-details.png)

单击**实例详细信息**以查看详细信息。

实例详细信息(/en-us/netscaler-application-delivery-management-software/media/instanceinfo-ingress.png)

显示以下详细信息：

- **信息** - 实例详细信息，例如实例类型、部署类型、版本、型号等。

  信息(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-instanceinfo.png)

- **功能** – 默认情况下，显示未获得许可的功能。单击**许可功能**以查看已获得许可的功能。

  功能(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-instancefeature.png)

- **模式** – 默认情况下，显示实例上所有已禁用的模式。单击**查看已启用模式**以查看实例上已启用的模式。

  模式(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-instancemodes.png)

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

实例仪表板显示实例概述，您可以在其中查看以下详细信息：

- **实例分数**

  实例分数(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-instancescore.png)

  1 – 指示所选时间段内当前的 NetScaler 实例分数。最终分数计算为 **100 减去总罚分**。图表显示了所选时间段的分数范围。

  2 – 指示 NetScaler 实例的当前状态，例如“**正常**”、“**关闭**”和“**停止服务**”。

  3 – 指示 NetScaler 实例正常运行的持续时间。

  4 – 指示为实例启用和禁用的网络接口总数。单击可查看详细信息，例如网络接口名称和状态（已启用或已禁用）。

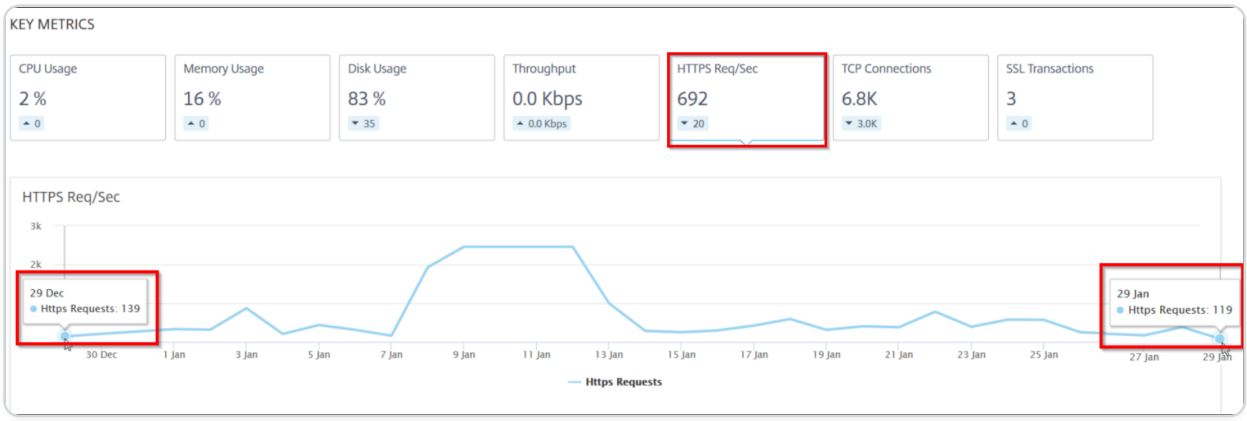
  5 – 从列表中选择时间段以查看实例详细信息。

  6 – 显示 NetScaler 实例的总问题和问题类别。

- **关键指标**

  单击每个选项卡可查看详细信息。在每个指标中，您可以查看所选时间的平均值和差值。

  下图是 HTTPS Req/Sec 的示例，所选时间段为最近 1 个月。值 **692** 是最近 1 个月期间的平均 HTTPS Req/Sec，值 **20** 是差值。在图表中，第一个值是 **139**，最后一个值是 **119**。差值为 **139 – 119 = 20**。



  您可以以图表格式查看所选时间段的以下实例指标：

  - **CPU 使用率** – 实例在所选持续时间内的平均 CPU 百分比（同时显示数据包 CPU 和管理 CPU）。
  - **内存使用率** – 实例在所选持续时间内的平均内存使用百分比。
  - **磁盘使用率** – 实例在所选持续时间内的平均磁盘空间百分比。

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

- **吞吐量** – 实例在所选持续时间内处理的平均网络吞吐量。
- **每秒 HTTPS 请求数** – 实例在选定持续时间内接收的平均 HTTPS 请求数。
- **TCP 连接数** – 客户端和服务器在选定持续时间内建立的平均 TCP 连接数。
- **SSL 事务数** – 实例在选定持续时间内处理的平均 SSL 事务数。

- **问题**

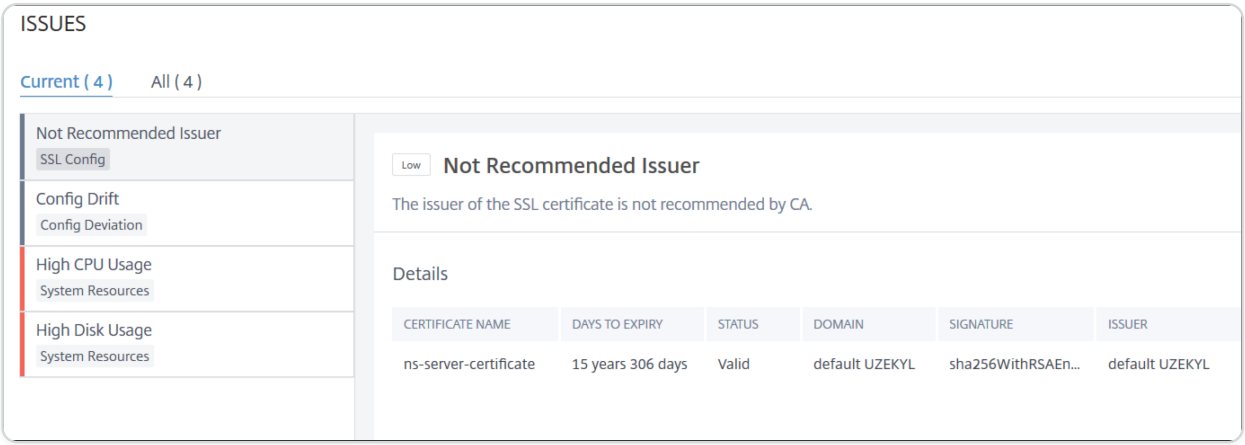
  您可以查看 NetScaler 实例中出现的以下问题：

问题类别	描述	问题
系统资源	显示与 NetScaler 系统资源相关的所有问题，例如 CPU、内存、磁盘使用情况等。	- CPU 使用率过高
		- 内存使用率过高
		- 磁盘使用率过高
		- SSL 卡故障
		- 电源故障
		- 磁盘错误
		- 闪存错误
		- 网卡丢弃
SSL 配置	显示与 NetScaler 实例上的 SSL 配置相关的所有问题。	- SSL 证书过期
		- 不推荐的颁发者
		- 不推荐的算法
		- 不推荐的密钥强度
配置偏差	显示与 NetScaler 实例中应用的配置作业相关的所有问题。	- 配置漂移

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

问题类别	描述	问题
		- 运行中与模板
容量问题	显示 NetScaler 容量问题。NetScaler Console 每五分钟从 NetScaler 实例轮询这些事件，并显示是否存在数据包丢弃或速率限制计数器增量。问题按以下容量参数分类。	- 吞吐量限制已达到
		- PE CPU 限制已达到
		- PPS 限制已达到
		- SSL 吞吐量速率限制
		- SSL TPS 速率限制
网络	显示实例中出现的操作问题。	有关更多信息，请参阅具有新指标的增强型基础架构分析。

单击每个选项卡以分析和排查问题。例如，假设某个实例在选定的时间段内出现以下错误：



- “**当前**”选项卡显示影响实例分数的当前 NetScaler 操作问题。
- “**所有**”选项卡显示在选定持续时间内检测到的所有基础架构问题。

分布式追踪

在服务图中，您可以使用分布式追踪视图来：

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

- 分析整体服务性能。
- 可视化所选服务与其相互依赖服务之间的通信流。
- 识别哪些服务指示错误并对错误服务进行故障排除
- 查看所选服务与其每个相互依赖服务之间的事务详情。

先决条件

要查看服务的追踪信息，您必须：

- 确保应用程序在发送任何东西向流量时维护以下追踪标头：

  - `x-request-id`
  - `x-b3-traceid`
  - `x-b3-spanid`
  - `x-b3-parentspanid`
  - `x-b3-sampled`
  - `x-b3-flags`
  - `x-ot-span-context`

- 对于 **早于 1.7.23 的 CIC 版本**，请使用 `NS_DISTRIBUTED_TRACING` 和值 `yes` 更新 CPX YAML 文件

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

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: cpx-ingress
spec:
  selector:
    matchLabels:
      app: cpx-ingress
  replicas: 1
  template:
    metadata:
      name: cpx-ingress
      labels:
        app: cpx-ingress
      annotations:
    spec:
      serviceAccountName: cpx-ingress-k8s-role
      containers:
        - name: cpx-ingress
          image: "quay.io/citrix/citrix-k8s-cpx-ingress:13.0-47.103"
          securityContext:
             privileged: true
          env:
          - name: "EULA"
            value: "yes"
          - name: "KUBERNETES_TASK_ID"
            value: ""
          - name: "NS_MGMT_SERVER"
            value: "192.168.0.1"
          - name: "NS_MGMT_FINGER_PRINT"
            value: "12:12:AB:CD:EA:72:E3:10:47:CD:AF:AG:C3:B7:82:6D:97:3D:E2:5D"
          - name: "NS_HTTP_PORT"
            value: "9080"
          - name: "NS_HTTPS_PORT"
            value: 9443"
          - name: "LOGSTREAM_COLLECTOR_IP"
            value: "192.168.0.1"
          imagePullPolicy: Always
```

- 对于 **晚于 1.7.23 的 CIC 版本**，您必须使用 ConfigMap。

  ConfigMaps 允许您将配置与 Pod 分离，并使您的工作负载可移植。使用 ConfigMaps，您可以轻松更改和管理工作负载配置，并减少将配置数据硬编码到 Pod 规范的需要。

  借助 ConfigMap 支持，您可以在保持 NetScaler Ingress Controller Pod 运行的同时自动更新配置。更新后无需重新启动 Pod。有关更多信息，请参阅 Ingress Controller 的 ConfigMap 支持。

  使用 ConfigMap，您可以启用或禁用分布式跟踪、事件、审计日志等。要使用 ConfigMap：

  a. 使用所需参数创建 YAML 文件。

     以下示例 YAML 文件已启用分布式跟踪，并禁用了审计日志、事件和事务等其他变量：

```yaml
apiVersion: v1

kind: ConfigMap

metadata:

  name: cic-configmap
```

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

```
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <Console-AgentIP> / <Console-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'false'
      events:
        enable: 'false'
    transactions:
```

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

```
      enable: 'false'

      port: 5557
```

注意

> 您可以为 `Samplingrate` 提供 0 到 100 之间的值。NetScaler Console 将显示指定数量的跟踪事务。

b. 使用以下方式部署 ConfigMap：

`kubectl create -f <configmap-yaml>.yaml`

c. 编辑 CPX YAML 文件，并使用 `envFrom` 或 `args` 来指定以下参数：

```
envFrom:

 - configMapRef:

     name: cic-configmap
```

或

```
 args:
    - --configmap
      default/cic-configmap
```

d. 如果要更改任何变量的值，请编辑 ConfigMap 中的值。在此示例中，所有其他变量都从 `false` 更改为 `true`。

```
apiVersion: v1

kind: ConfigMap

metadata:

  name: cic-configmap

  namespace: default
```

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

```
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <Console-AgentIP> / <Console-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'true'
      events:
        enable: 'true'
    transactions:
      enable: 'true'
```

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

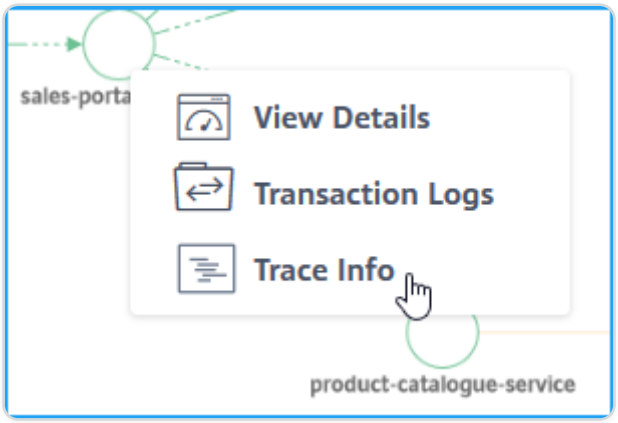
```
        port: 5557
```

e. 使用以下命令重新应用 ConfigMap：

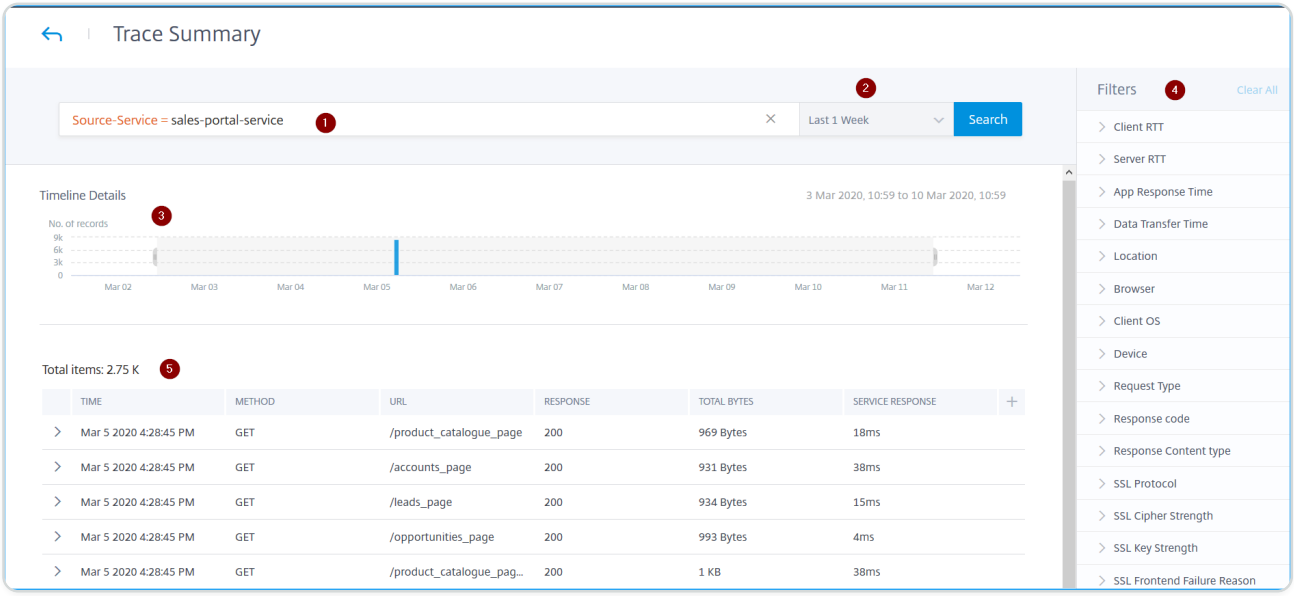
```
kubectl apply -f <yaml-file>.yaml
```

查看服务跟踪详细信息

在服务图中，单击一个服务，然后选择 **Trace Info**。



将显示选定服务的跟踪摘要页面。



跟踪摘要显示：

- 高级搜索，允许您通过建议和运算符搜索事务 (1)。有关更多信息，请参阅高级搜索。
- 时间持续时间列表，允许您选择时间持续时间，例如 1 小时、12 小时、1 天、1 周、1 个月和自定义时间 (2)。
- 时间线详细信息图，允许您拖动并选择以显示特定时间段的结果 (3)。
- 筛选器面板，允许您从每个指标中选择选项 (4)。

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

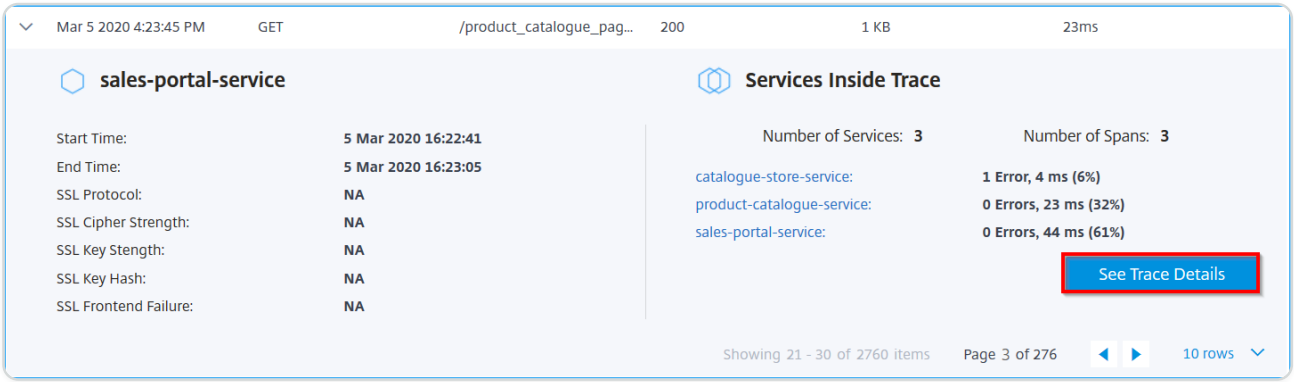
- 选定服务的事务详细信息 (5)。

查看事务详细信息

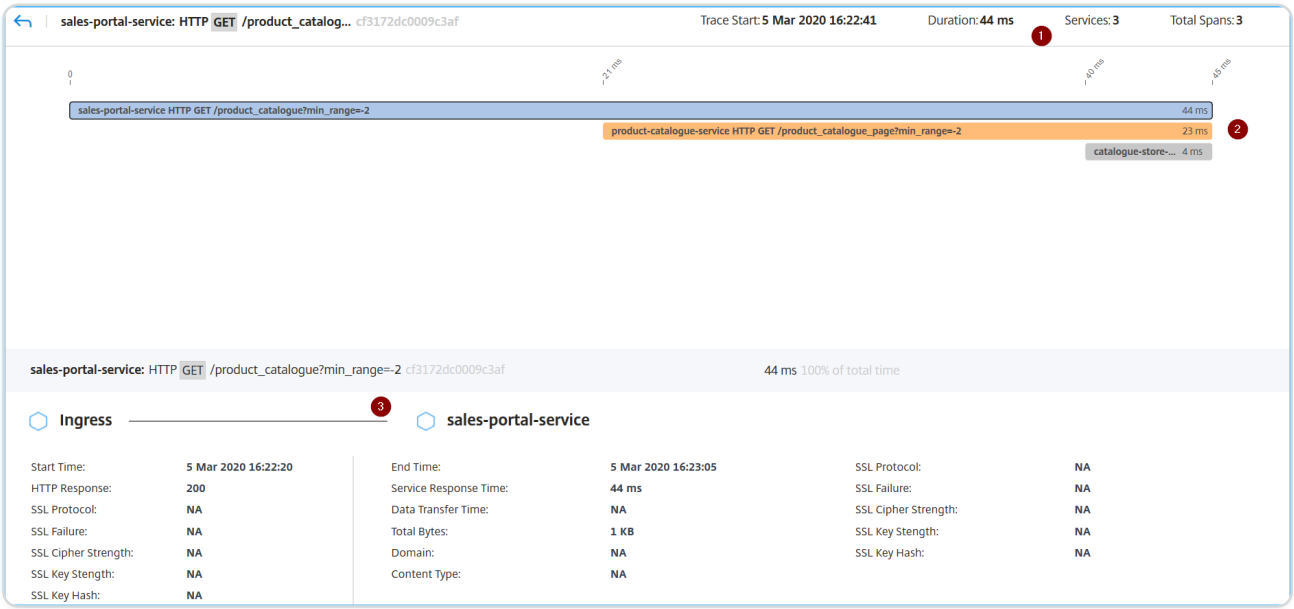
单击事务以深入查看详细信息。您可以查看选定服务的事务详细信息，例如：

- 开始时间
- 结束时间
- SSL 指标
- 与相互依赖服务的通信（以及每个服务的错误和响应时间）。

以下示例表示 `catalogue-store-service` 中的错误。单击“**查看跟踪详细信息**”以获取更多详细信息。



将显示“跟踪详细信息”页面。



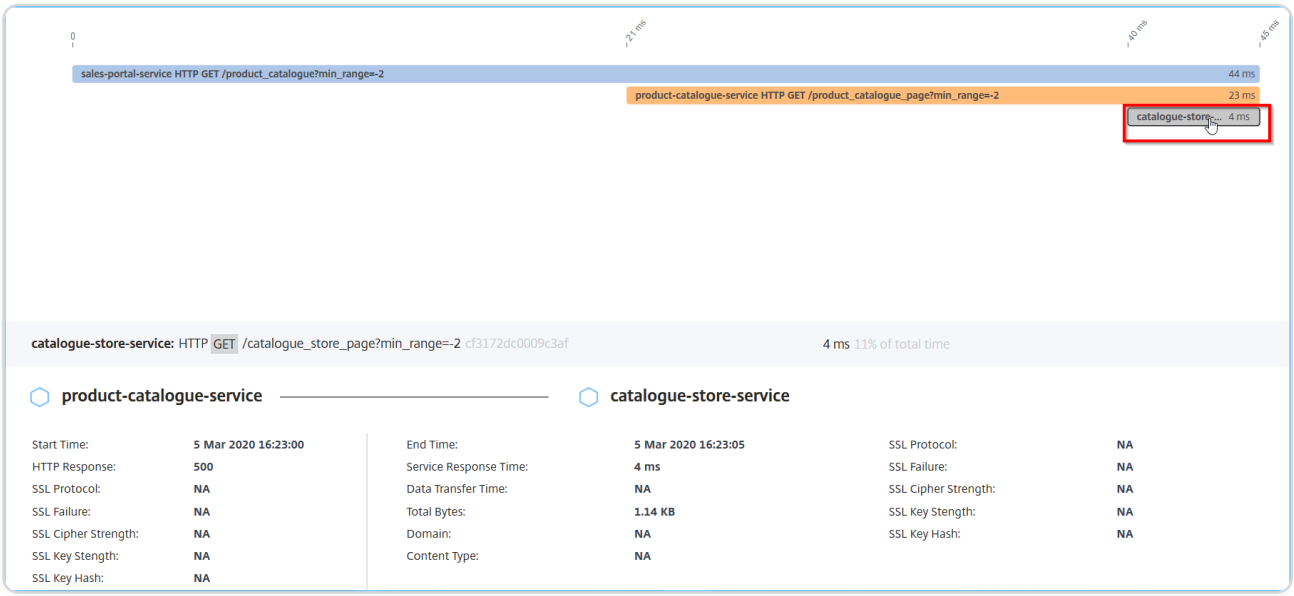
1 – 显示事务的开始时间、响应时间、总服务数和总跨度数。

2 – 显示已与其相互依赖服务通信的所选服务的详细信息。您可以单击每个事务以查看详细信息。

3 – 显示每个服务的事务详细信息。

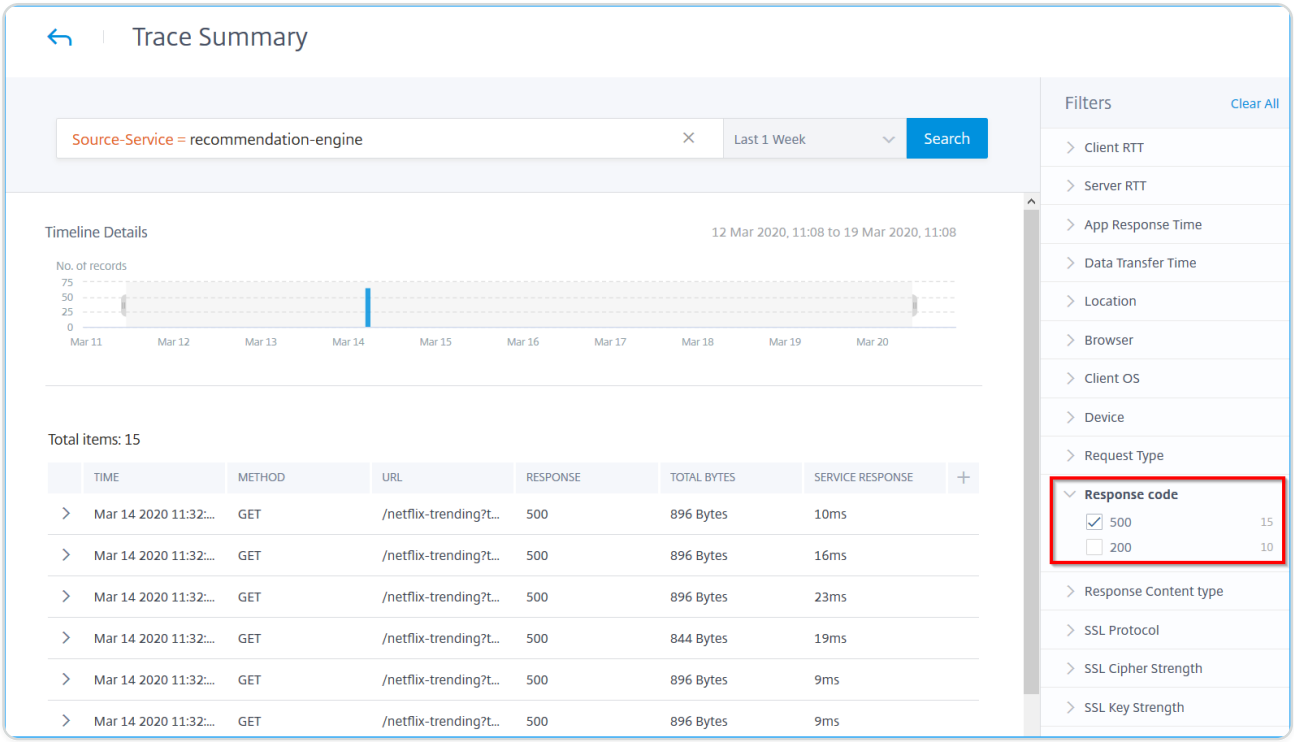
© 1997–2026 Citrix Systems, Inc. All rights reserved.

根据示例图像，`catalogue-store-service` 指示了一个错误。单击 `catalogue-store-service` 可用的事务。



`product-catalogue-service` 和 `catalogue-store-service` 之间的事务详细信息显示 HTTP 响应为 500。通过这些详细信息，作为管理员，您可以分析错误服务并排除 `product-catalogue-service` 作为解决方案。

您还可以通过在“**筛选器**”面板下从每个指标中选择选项来筛选结果。例如，如果要查看所有 5xx 事务，请单击“**响应代码**”并选择“**500**”。



- **客户端 RTT**：数据包从客户端传输所需的时间。
- **服务器 RTT**：数据包从服务器传输所需的时间。

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

- **应用程序响应时间**：应用程序平均响应时间
- **数据传输时间**：数据传输大小以及服务之间传输发生的速度。
- **位置**：客户端位置
- **浏览器**：客户端使用的浏览器类型。例如：Chrome、Firefox。
- **客户端操作系统**：基于浏览器用户代理详细信息的客户端操作系统。
- **设备**：基于浏览器用户代理详细信息的设备。例如：平板电脑、手机。
- **请求类型**：事务请求类型。例如：GET。
- **响应代码**：从服务器接收到的响应代码。例如：501、404、200。
- **响应内容类型**：事务内容类型。如果客户端请求的是 text/html，则服务器的响应也必须是 text/html。
- **SSL 协议**：客户端使用的 SSL 协议版本。例如：SSLv3。
- **SSL 密码强度**：基于 SSL 证书密钥大小的密码强度，例如高、中、低。
- **SSL 密钥强度**：SSL 密码强度是根据 SSL 证书密钥大小计算的。密钥长度定义了 SSL 算法的安全性。例如：2048
- **SSL 前端故障原因**：前端 SSL 握手错误消息。例如：SSL CLIENTAUTH FAILURE

查看服务图中部分数据或无数据的诊断详细信息

完成所需的服务图配置并在 NetScaler Console 中添加 Kubernetes 集群后，服务图开始填充数据。在某些情况下，您可能会发现服务图显示部分数据或无数据。服务图中部分数据或无数据的一些可能原因包括：

- 静态路由未配置
- Kubernetes 集群状态为关闭
- CPX 注册失败
- CPX 虚拟服务器未获得许可
- 所需的分析配置未设置，这会阻止服务图加载所有数据

作为管理员，当您看到服务图显示部分数据或无数据时，您可能会发现很难分析原因。服务图页面中的诊断信息使您能够查看可能的原因和所需的措施，以解决部分数据或无数据问题。

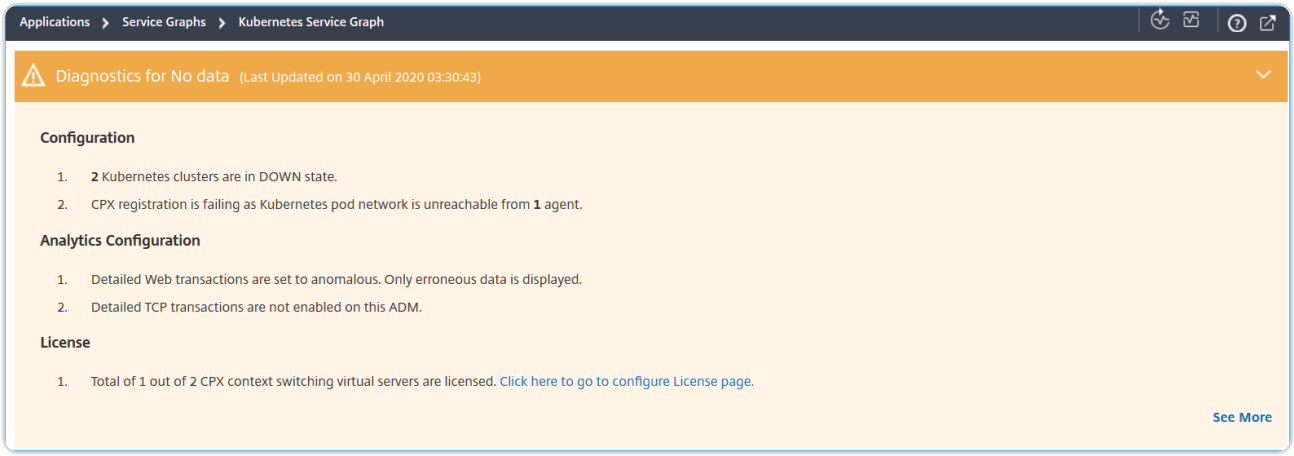
在 NetScaler Console 中，导航到 **应用程序** > **服务图**，然后单击**微服务**选项卡。

无数据诊断

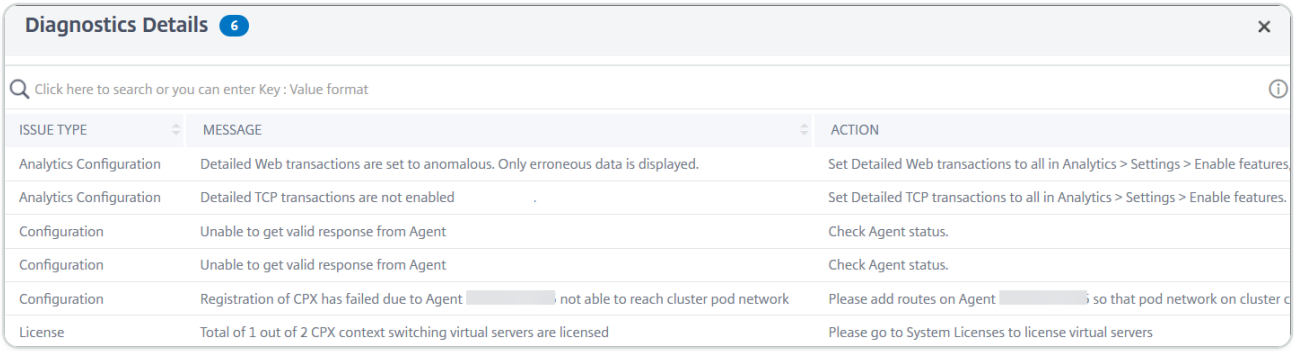
如果服务图未显示任何数据，则会显示以下诊断消息。

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

单击 > 查看详细信息。您可以查看服务图未显示任何数据的可能原因。下图是服务图中无数据的示例。



单击 **查看更多** 以查看问题的详细信息。

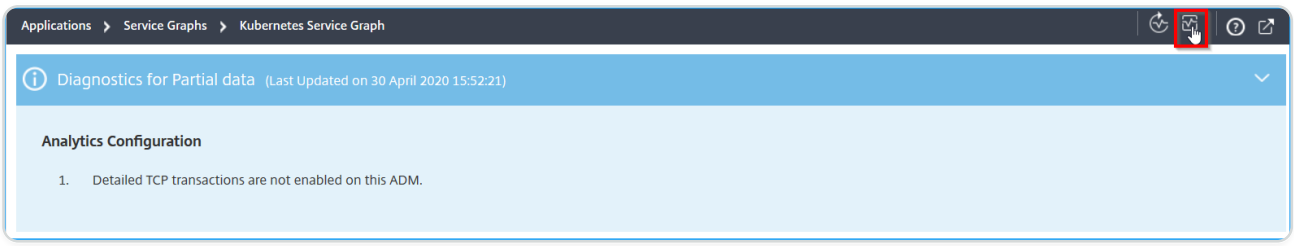


- **问题类型** – 指示问题是否源于配置、分析配置或许可。
- **消息** – 指示导致问题的原因。
- **操作** – 指示为解决问题必须执行的操作。

部分数据的诊断

如果服务图仅显示部分数据，请单击“**显示诊断**”按钮以查看诊断信息。

以下示例表明 TCP 事务已禁用。



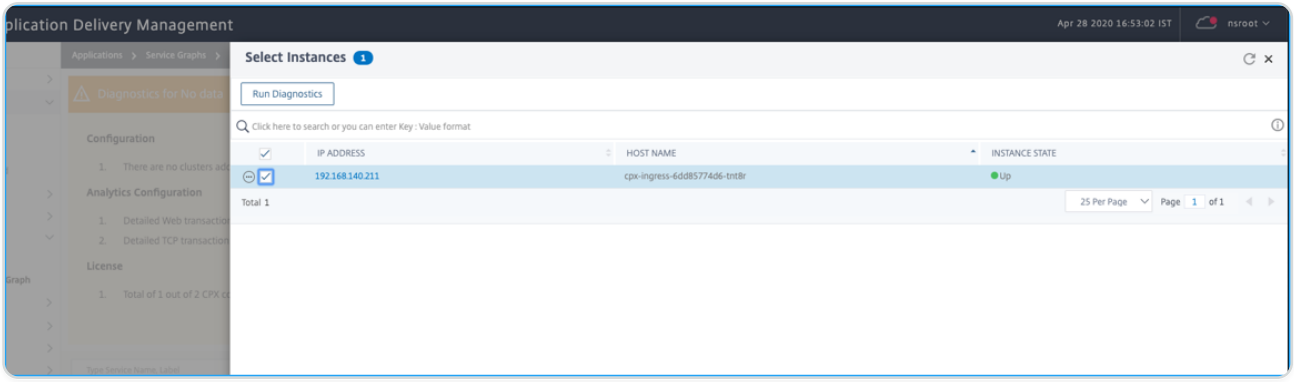
对于此示例，您必须通过导航到“**设置 > 分析设置**”将“**TCP 事务设置**”启用为“**全部**”。

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

故障排除

作为管理员，您可以使用这些诊断消息来验证并尝试解决这些问题。解决问题后，NetScaler Console 会定期自动运行诊断检查。诊断检查完成后，服务图中部分数据或无数据的问题将得到解决。

您还可以单击“**运行诊断**”，选择“**CPX 实例**”，然后单击“**运行诊断**”。



有关更多故障排除方案，请参阅常见问题。

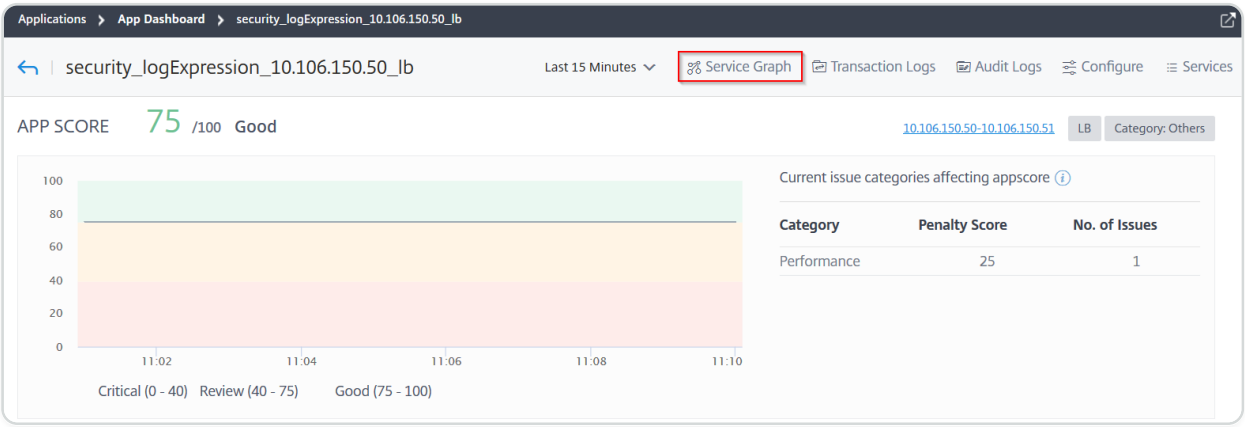
应用程序的服务图

要查看应用程序的服务图：

1. 导航到 **应用程序** > **仪表板**。
2. 选择一个应用程序。

   显示应用程序详细信息页面。

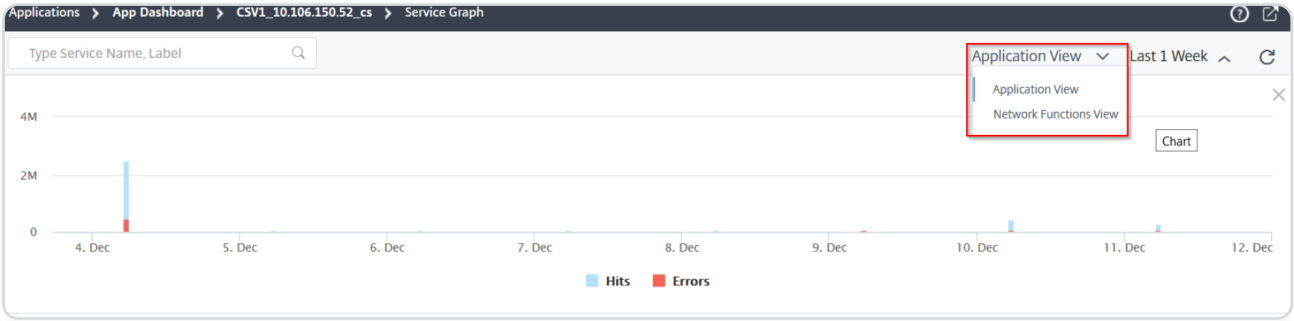
3. 选择时间段，然后单击 **服务图**。



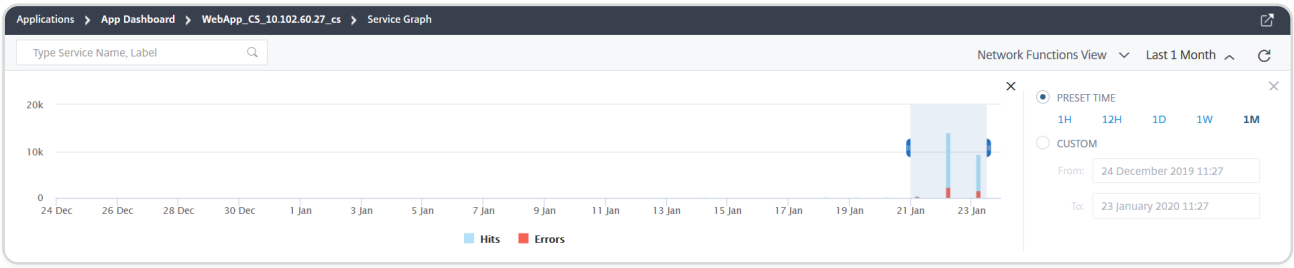
显示所选应用程序的服务图页面。

您可以在 **应用程序视图** 或 **网络功能视图** 中查看服务图。

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

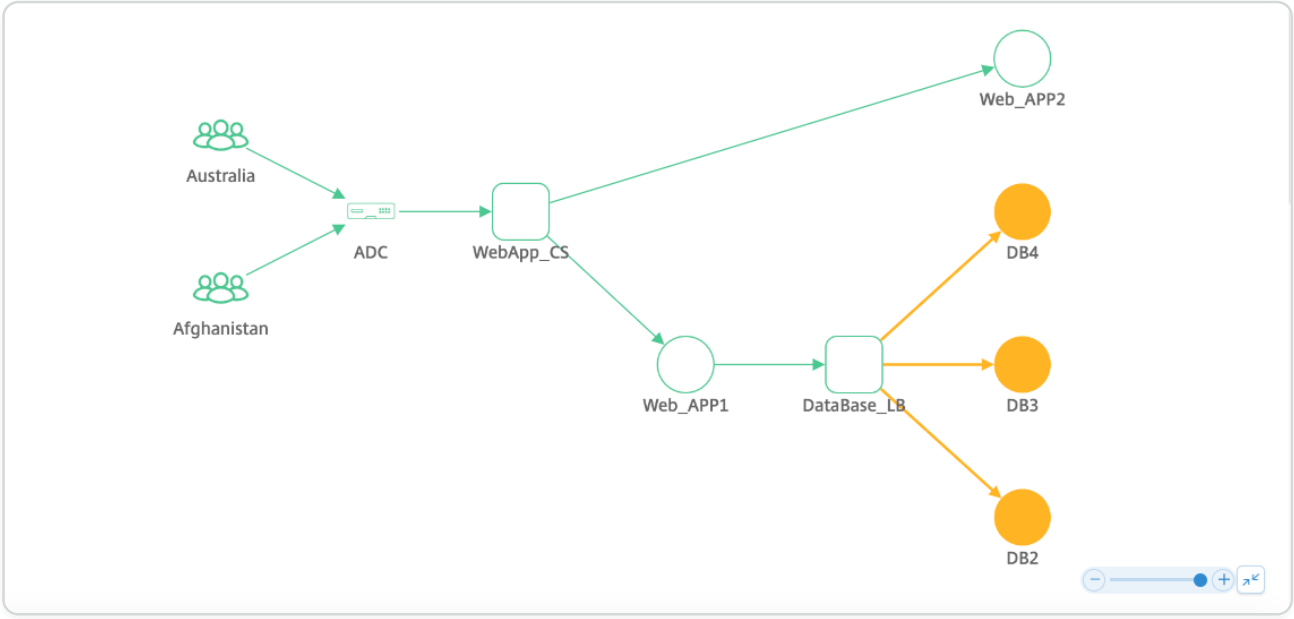


您还可以拖动并选择命中和错误以修改结果。



应用程序视图

显示应用程序配置概述。在此视图中，您可以可视化客户端、NetScaler 和 Web 应用程序之间的通信。



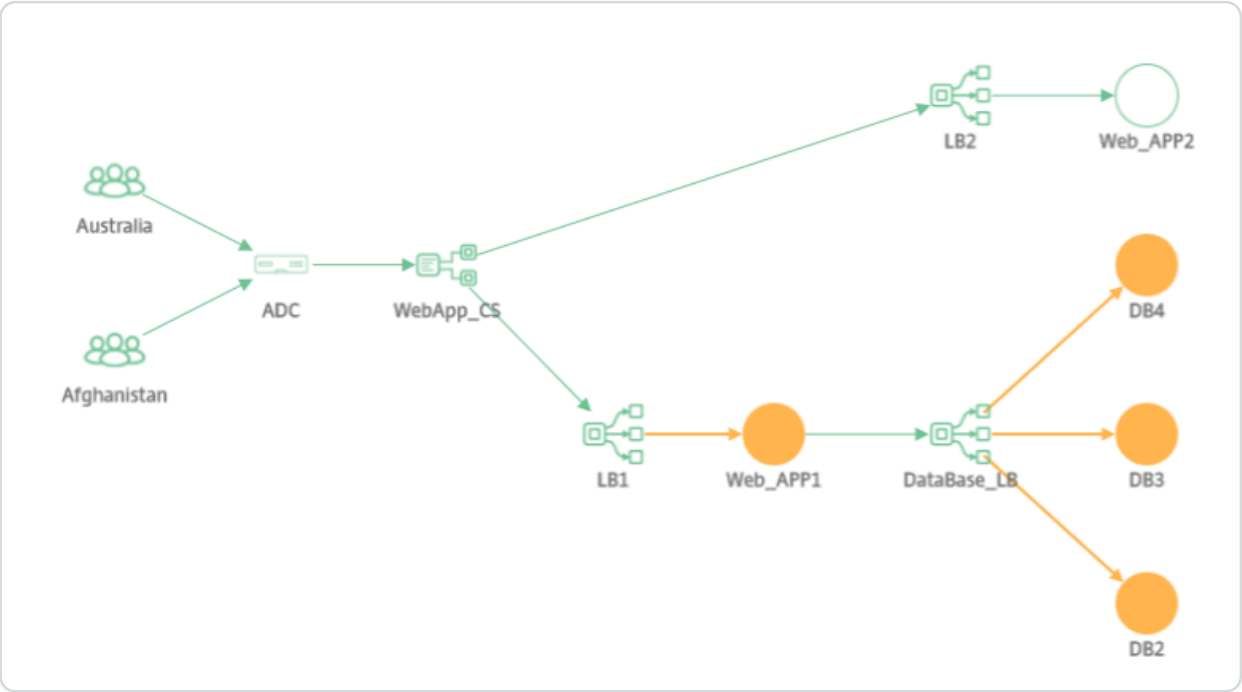
网络功能视图

显示与应用程序关联的虚拟服务器。在此视图中，您可以可视化 NetScaler 是否正在与以下项通信：

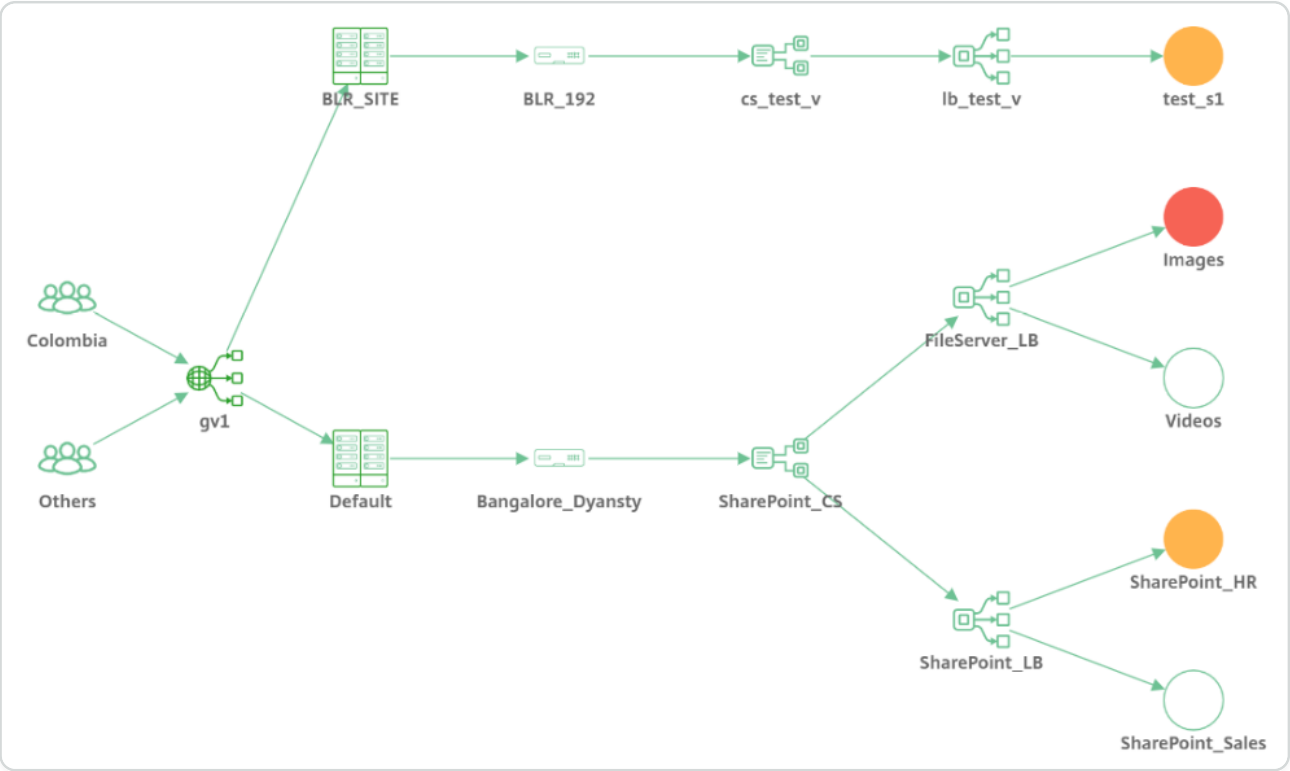
- 内容交换虚拟服务器以访问应用程序
- 负载均衡虚拟服务器以访问应用程序

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

- 内容交换和负载均衡虚拟服务器都用于访问应用程序



对于 GSLB 应用程序，详细信息会与数据中心和 NetScaler 一起显示。

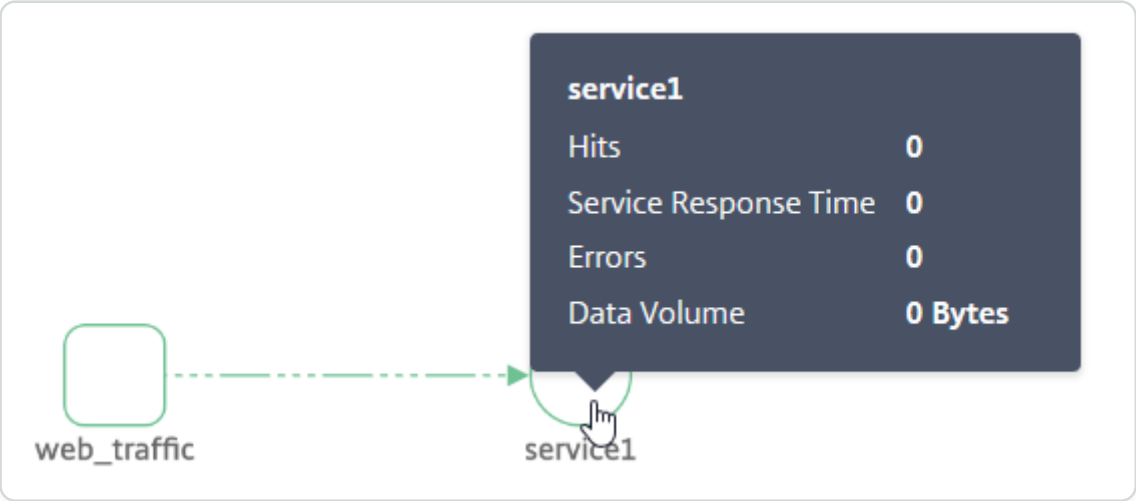


无活动事务的服务图视图

如果 NetScaler 与 Web 应用程序之间没有活动事务发生，服务图将仅显示应用程序的基本配置（不包括客户端和 NetScaler）。

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

当您将鼠标指针悬停在服务或虚拟服务器上时，由于没有事务，所有指标的详细信息都显示为 0。

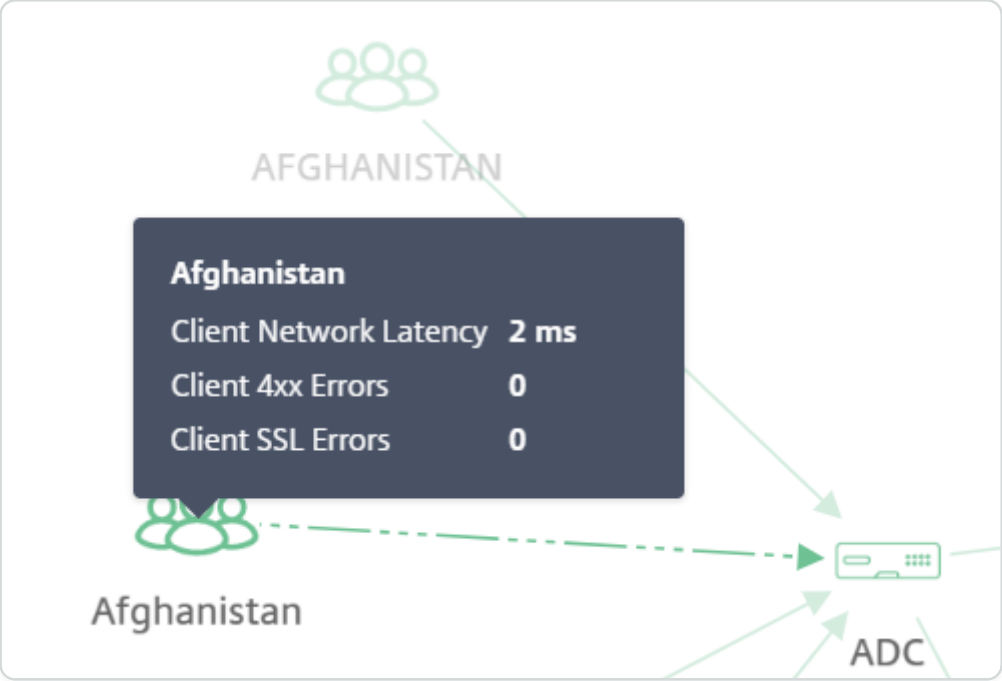


分析指标

将鼠标指针悬停在每个服务上，可在应用程序视图或网络功能视图中查看指标详细信息。

客户端指标

将鼠标指针悬停在客户端上以查看客户端指标。



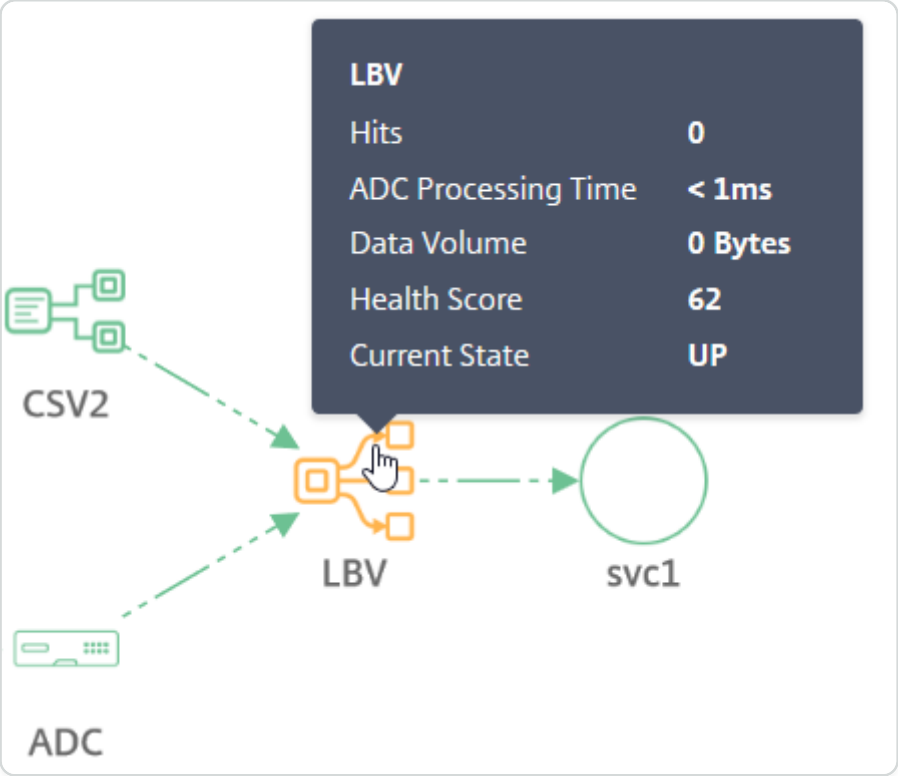
- **客户端网络延迟** – 指示来自客户端的网络延迟。

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

- **客户端 4xx 错误** – 指示来自客户端的 4xx 错误总数。
- **客户端 SSL 错误** – 指示来自客户端的 SSL 错误总数。

网络功能指标

将鼠标指针悬停在负载平衡或内容切换服务上以查看指标详细信息。



- **命中数** – 指示虚拟服务器接收到的总命中数
- **NetScaler 处理时间** – 指示 NetScaler 实例的平均处理时间
- **数据量** – 指示虚拟服务器处理的总数据量
- **健康评分** – 指示应用程序评分
- **当前状态** – 指示虚拟服务器的当前状态

服务指标

将鼠标指针悬停在服务（Web 应用程序）上以查看指标

服务指标(/en-us/netscaler-application-delivery-management-software/media/ga-sg-servicemetrics.png)

- **命中数** – 指示服务收到的总命中数
- **服务响应时间** – 指示服务的平均响应时间
- **错误** – 指示服务发生的总错误数

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

- **数据量** – 指示服务处理的总数据量

NetScaler 指标（仅适用于 GSLB 应用程序）

将鼠标指针悬停在 NetScaler 上以查看指标。

NetScaler 指标(/en-us/netscaler-application-delivery-management-software/media/adc-metrics-gslb.png)

- 显示主机名和当前的 NetScaler 分数。该分数是根据不同的 NetScaler 潜在问题计算得出的。有关更多信息，请参阅实例分数。
- **IP 地址** – 表示 NetScaler IP 地址
- **当前状态** – 表示 NetScaler 状态，例如“正常”、“关闭”或“停止服务”
- **NetScaler 处理时间** – 表示 NetScaler 实例的平均处理时间

注意

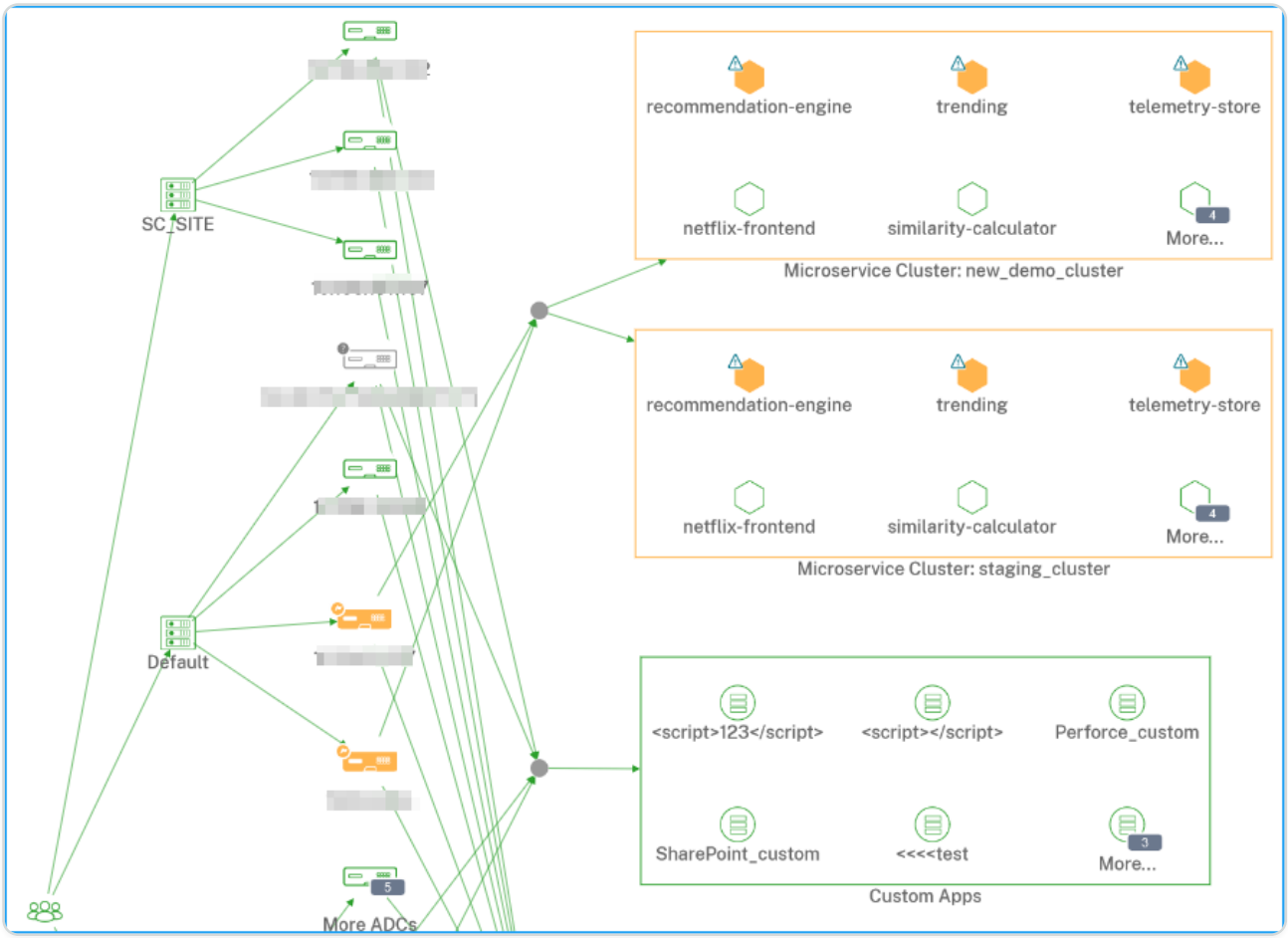
如果未将主机名分配给 NetScaler：

显示的是 NetScaler IP 地址而不是主机名。
在指标中，NetScaler IP 地址信息未显示。
主机名(/en-us/netscaler-application-delivery-management-software/media/hostname-gslb.png)

服务图中所有应用程序的全局视图

导航到**应用程序** > **服务图**，然后点击**全局**。

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



服务图在选定的时间段内显示以下内容：

- 用户访问特定应用程序的区域

托管 NetScaler 实例的数据中心

- 来自所有 NetScaler 实例的总离散应用程序

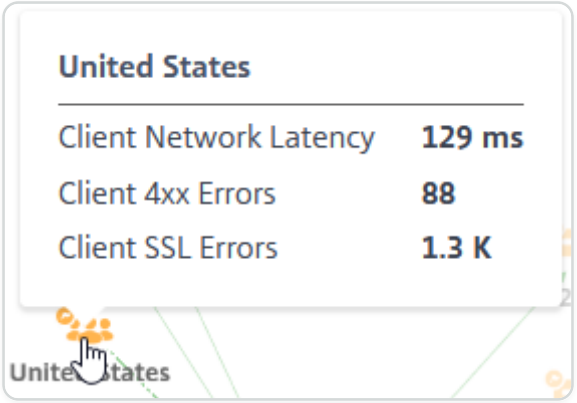
> **注意**
>
> 如果 NetScaler 实例没有离散应用程序，则从 NetScaler 实例指向离散虚拟服务器的箭头边不可见

- 来自所有 NetScaler 实例的总自定义应用程序
- 来自 NetScaler CPX 实例的总微服务应用程序

查看客户端指标

将鼠标指针悬停在客户端区域上以查看指标。

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

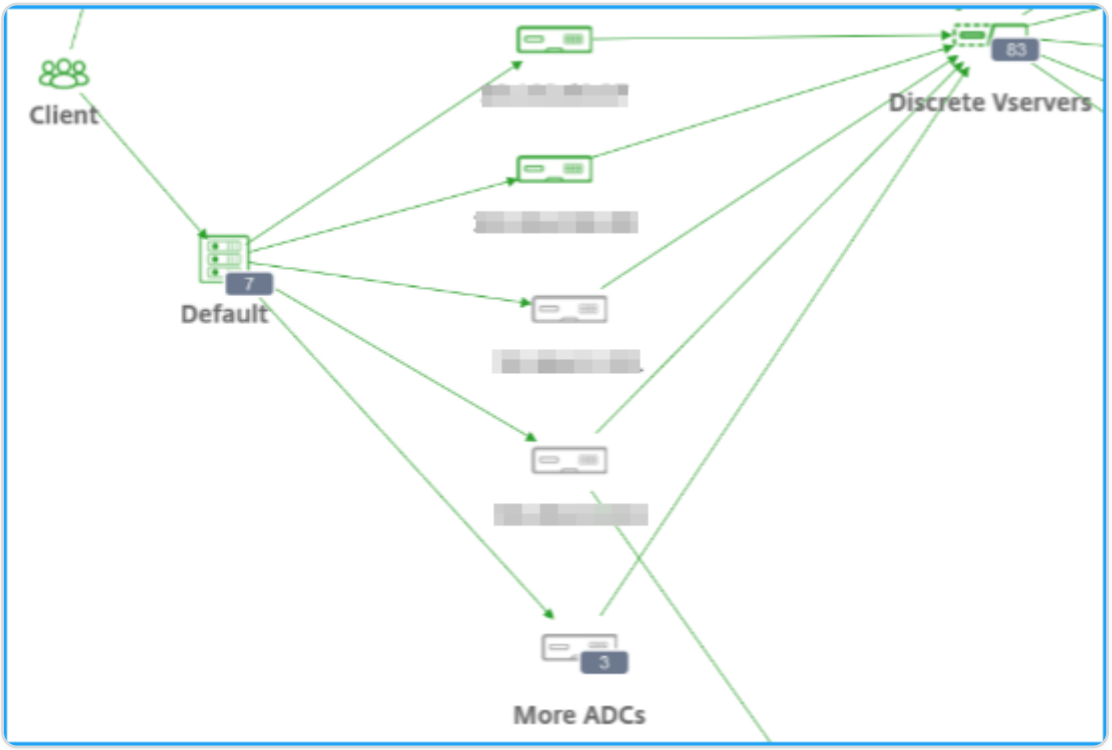


- **客户端网络延迟** - 表示平均客户端网络延迟。
- **客户端 4xx 错误** - 表示客户端 4xx 错误的总数。
- **客户端 SSL 错误** - 表示客户端 SSL 错误的总数。

查看 NetScaler 详细信息

服务图使您能够查看：

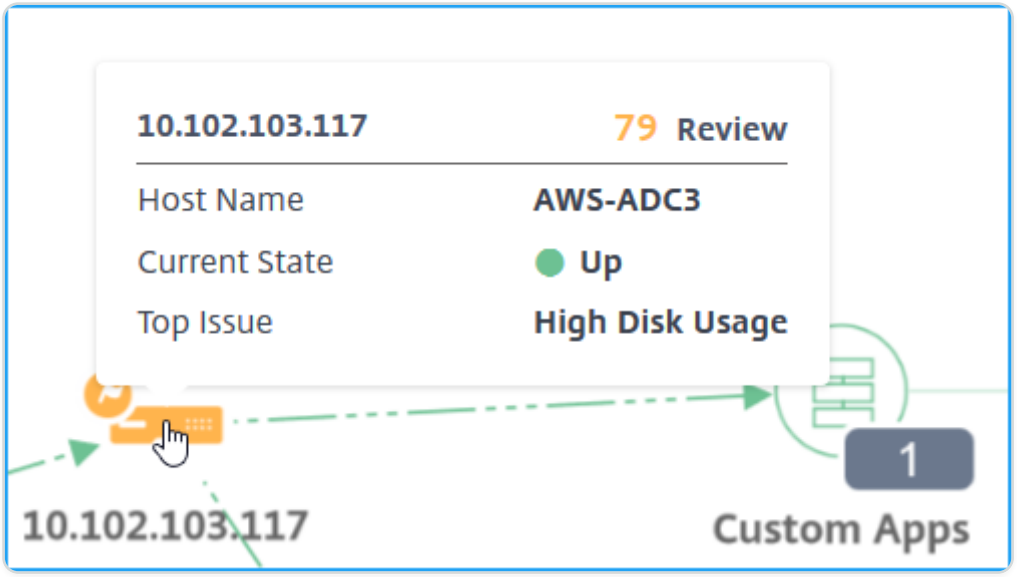
- 数据中心及其分组的总 NetScaler 实例
- 每个数据中心中得分最低的 4 个 NetScaler 实例



单击 **更多 ADC**，通过选择相应的状态（严重、审查、良好和不适用）选项卡来查看所有 NetScaler 实例。

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

将鼠标指针悬停在 NetScaler 实例上以查看指标。



您可以查看：

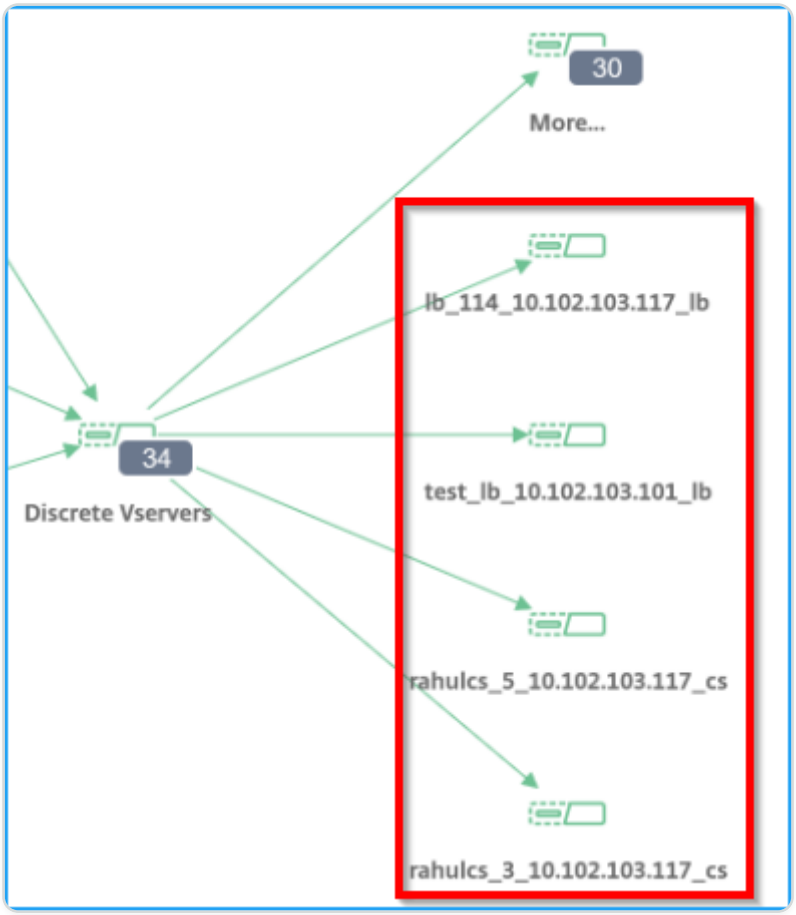
- NetScaler 实例 IP 地址和分数
- **主机名** – 表示分配给 NetScaler 实例的主机名
- **当前状态** – 表示 NetScaler 实例的当前状态，例如“正常”、“关闭”、“停止服务”。
- **主要问题** – 指示影响当前 NetScaler 分数的主要问题

单击 **NetScaler 实例** 以查看实例详细信息，例如实例分数、关键指标以及与 NetScaler 实例相关的问题。有关更多信息，请参阅 在基础架构分析中查看实例详细信息。

查看离散应用程序

服务图显示得分最低的 4 个离散应用程序。

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



假设您有以下离散应用程序：

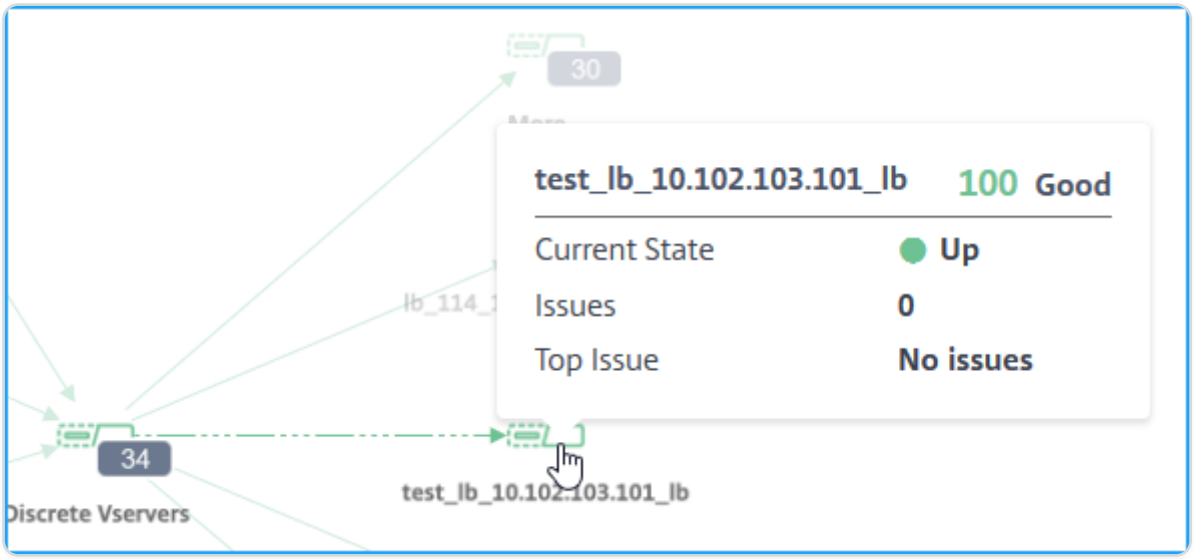
应用程序名称	NETSCALER	应用程序分数	应用程序状态
App1	10.102.29.50	35（严重）	正常运行
App2	10.102.29.90	100 (良好)	宕机
应用 3	10.102.32.40	49 (复查)	运行中
应用 4	10.102.113.208	92 (良好)	宕机
应用 5	10.102.25.25	86 (良好)	运行中
App6	10.102.29.41	77 (良好)	正常
App7	10.102.29.102	41 (待审查)	正常

在此场景中，您可以将 App1、App3、App6 和 App 7 视为服务图中得分最低的 4 个应用程序。

同样，您还可以查看**自定义**和**微服务**应用程序中得分最低的 4 个应用程序。

将鼠标指针悬停在服务上以查看指标信息。

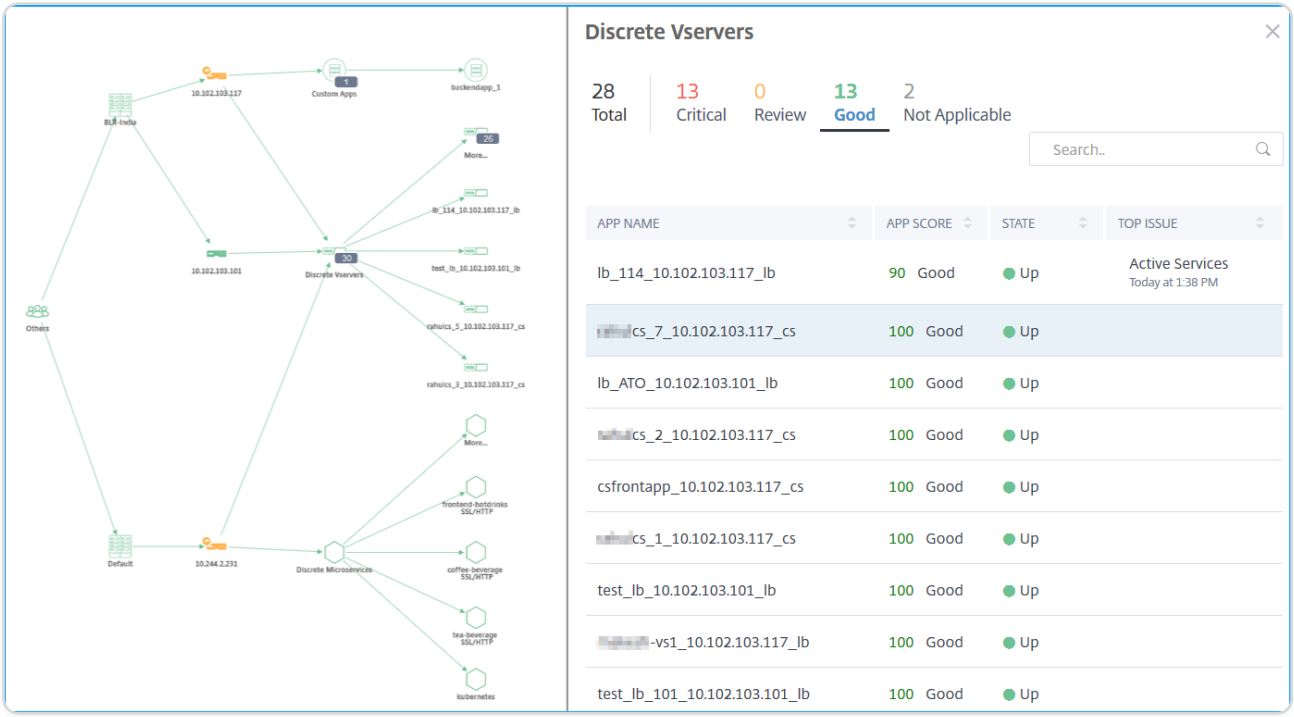
© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以查看：

- 应用程序名称和分数
- **当前状态** – 指示应用程序的当前状态，例如“正常”或“关闭”
- **问题** – 表示适用于该应用程序的总问题数
- **首要问题** – 表示影响整体应用程序得分的首要问题

单击**更多**以查看所有离散应用程序。将显示离散虚拟服务器页面，如下图所示：



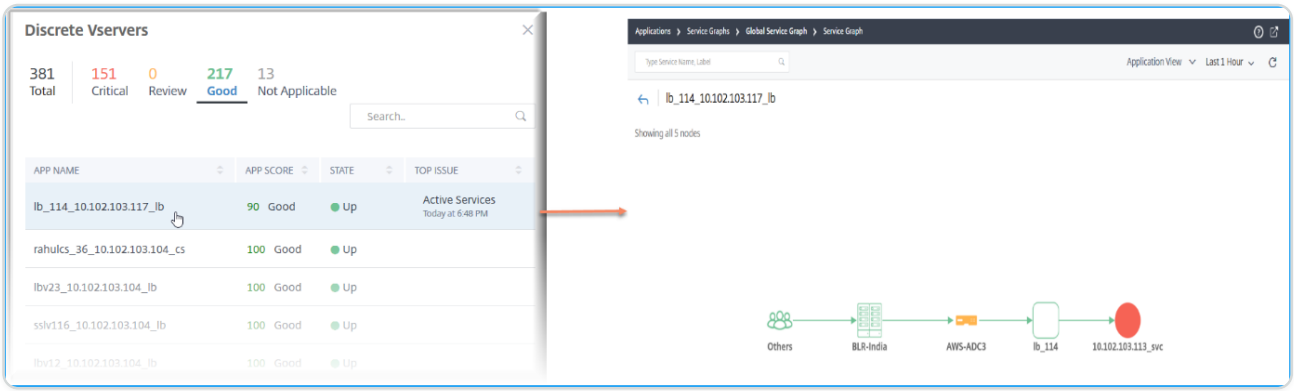
虚拟服务器根据状态显示。

- **总计** – 离散应用程序总数
- **严重** – 应用程序得分在 0 到 < 40 之间

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

- **审查** – 应用程序得分在 40 到 < 75 之间
- **良好** – 应用程序得分 > 75
- **不适用** – 应用程序未绑定到任何虚拟服务器

您可以单击每个选项卡以查看虚拟服务器。当您单击某个应用程序时，将显示所选应用程序的服务图。



有关详细信息，请参阅应用程序服务图。

查看微服务应用程序

服务图还显示属于 Kubernetes 集群的所有微服务应用程序。将鼠标指针悬停在服务上可查看指标详细信息。

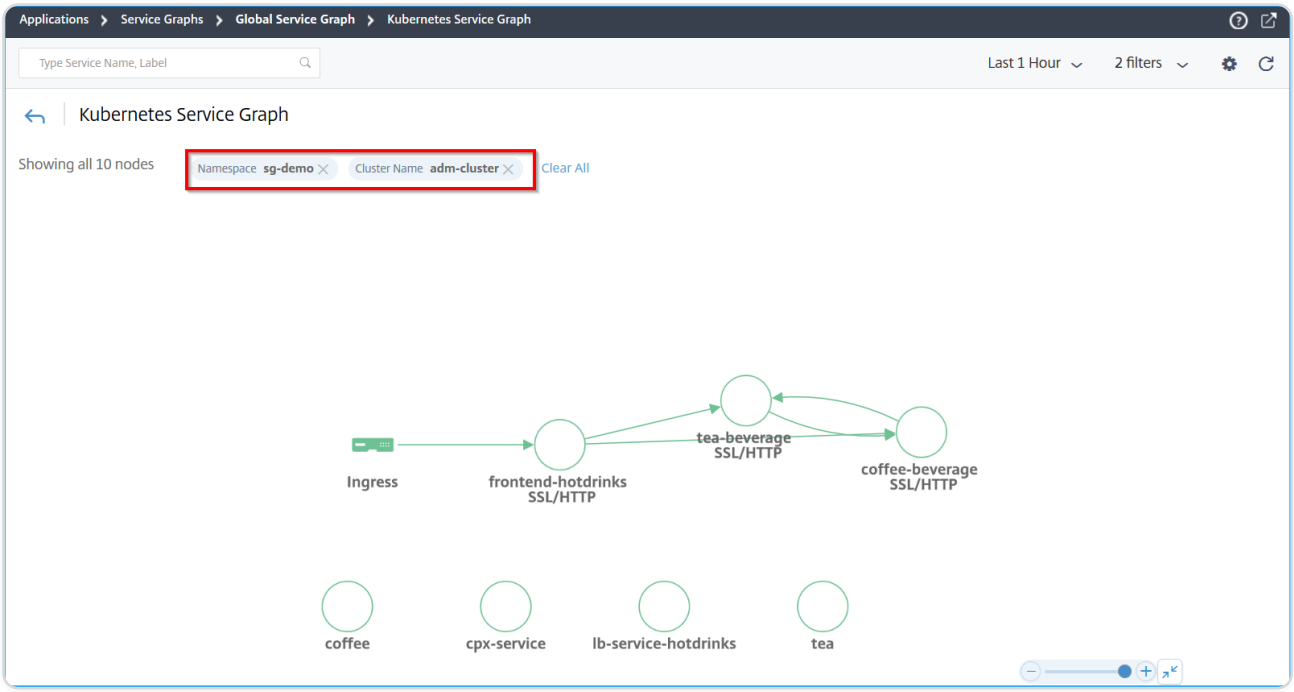
您可以查看：

- 服务名称
- 服务使用的协议，例如 SSL、HTTP、TCP、SSL over HTTP
- **命中数** – 服务收到的总命中数
- **服务响应时间** – 服务平均响应时间。

  （响应时间 = 客户端 RTT + 请求最后一个字节 – 请求第一个字节）
- **错误** – 总错误数，例如 4xx、5xx 等
- **数据量** – 服务处理的数据总量
- **命名空间** – 服务的命名空间
- **集群名称** – 托管服务的集群名称
- **SSL 服务器错误** – 服务中的总 SSL 错误数

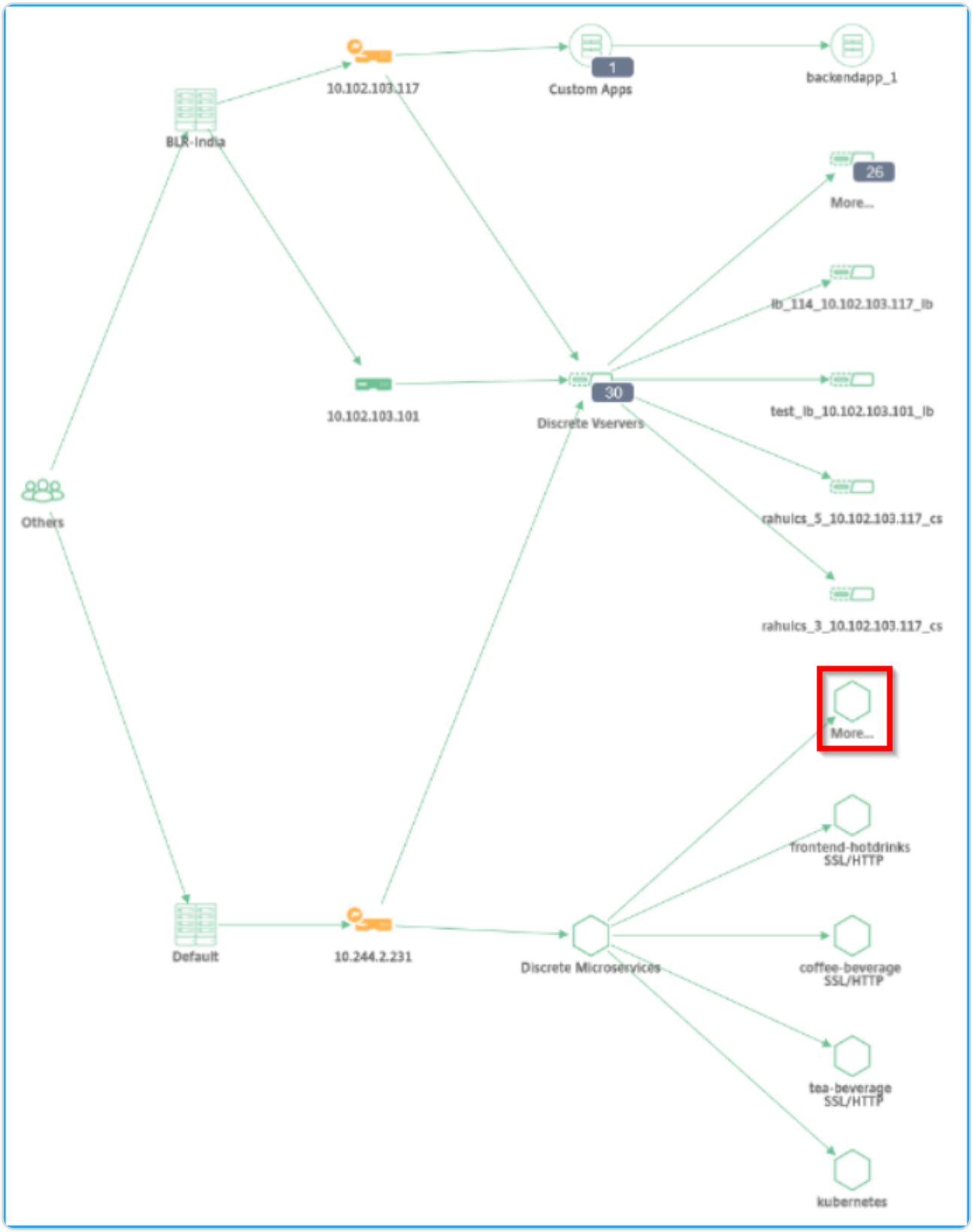
当您单击某个服务时，将显示所选服务的 Kubernetes 服务图，并应用服务命名空间和集群名称筛选器。

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



单击**更多**以查看包含所有服务的 Kubernetes 服务图。有关 Kubernetes 服务图的更多信息，请参阅云原生应用程序的服务图。

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



搜索栏以筛选结果

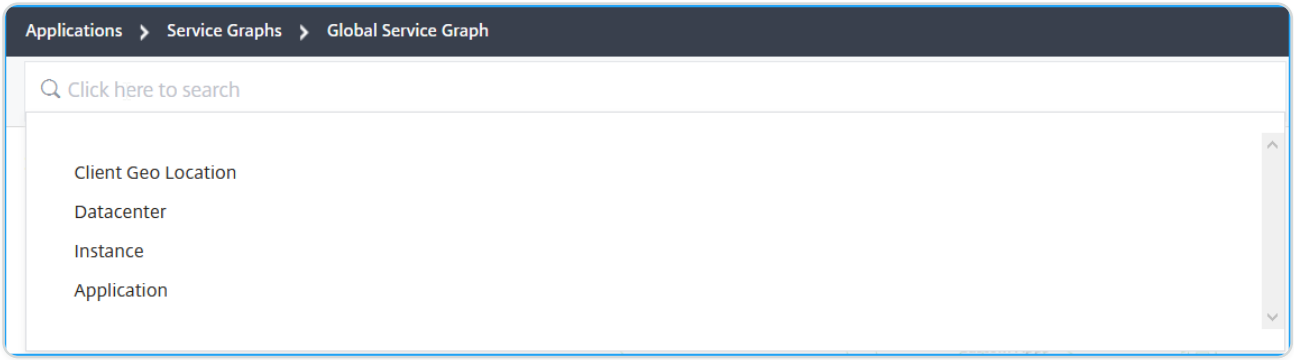
您可以使用搜索栏筛选结果。作为管理员，当您拥有以下情况时，此搜索栏可让您快速缩小范围，定位到特定的实例/客户端/应用程序/数据中心：

- 拥有许多数据中心的大型企业

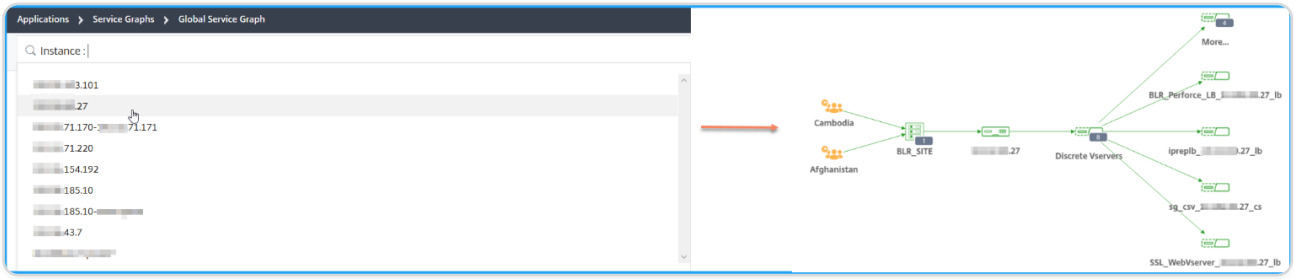
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 为每个数据中心配置了许多 NetScaler 实例
- 配置了通过每个 NetScaler 实例部署或访问的许多应用程序
- 从不同位置访问应用程序的客户端

将鼠标指针放在搜索栏上，然后选择要创建筛选器的类别。



例如，如果您想查看特定的 NetScaler 实例，请从搜索栏中选择**实例**，然后选择实例 IP 地址。全局服务图将显示所选实例及其关联的应用程序、数据中心和客户端位置。



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

StyleBooks

StyleBooks 简化了为您的应用程序管理复杂的 NetScaler 配置的任务。StyleBook 是一种模板，可用于创建和管理 NetScaler 配置。您可以创建一个 StyleBook 来配置 NetScaler 的特定功能，也可以设计一个 StyleBook 来为企业应用程序部署（例如 Microsoft Exchange 或 Lync）创建配置。

StyleBooks 与 DevOps 团队实践的“基础设施即代码”原则非常契合，其中配置是声明性的且受版本控制。这些配置也是可重复的，并且作为一个整体进行部署。StyleBooks 具有以下优势：

- **声明性**：StyleBooks 采用声明性而非命令性语法编写。StyleBooks 允许您专注于描述配置的结果或“所需状态”，而不是在特定 NetScaler 实例上实现它的分步说明。NetScaler Console 计算 NetScaler 上的现有状态与您指定的所需状态之间的差异，并对基础设施进行必要的编辑。由于 StyleBooks 使用以 YAML 编写的声明性语法，因此 StyleBook 的组件可以按任何顺序指定，NetScaler Console 会根据其计算出的依赖关系确定正确的顺序。
- **原子性**：当您使用 StyleBooks 部署配置时，要么部署完整的配置，要么不部署任何配置，这确保了基础设施始终处于一致状态。
- **版本化**：StyleBook 具有名称、命名空间和版本号，可将其与系统中的任何其他 StyleBook 唯一区分开来。对 StyleBook 的任何修改都需要更新其版本号（或其名称或命名空间）以保持此唯一性。版本更新还允许您维护同一 StyleBook 的多个版本。
- **可组合性**：定义 StyleBook 后，该 StyleBook 可以作为一个单元来构建其他 StyleBook。您可以避免重复常见的配置模式。它还允许您在组织中建立标准构建块。由于 StyleBooks 是版本化的，对现有 StyleBooks 的更改会产生新的 StyleBooks，从而确保依赖的 StyleBooks 永远不会被无意破坏。
- **以应用程序为中心**：StyleBooks 可用于定义完整应用程序的 NetScaler 配置。应用程序的配置可以通过使用参数进行抽象。因此，从 StyleBook 创建配置的用户可以通过一个简单的界面进行交互，该界面只需填写几个参数即可创建复杂的 NetScaler 配置。从 StyleBooks 创建的配置不与基础设施绑定。因此，单个配置可以部署在一个或多个 NetScaler 上，并且可以在实例之间移动。
- **自动生成 UI**：当使用 NetScaler Console GUI 完成配置时，NetScaler Console 会自动生成用于填写 StyleBook 参数的 UI 表单。StyleBook 作者无需学习新的 GUI 语言或单独创建 UI 页面和表单。
- **API 驱动**：所有配置操作都通过使用 NetScaler Console GUI 或通过 REST API 支持。API 可以同步或异步模式使用。除了配置任务之外，StyleBooks API 还允许您在运行时发现任何 StyleBook 的架构（参数描述）。

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

您可以使用一个 StyleBook 创建多个配置。每个配置都保存为一个配置包。例如，假设您有一个 StyleBook 定义了典型的 HTTP 负载均衡应用程序配置。您可以创建一个包含负载均衡实体值的配置，并在 NetScaler 实例上执行它。此配置将保存为一个配置包。您可以使用相同的 StyleBook 创建另一个具有不同值的配置，并在相同或不同的 NetScaler 实例上执行它。将为此配置创建一个新的配置包。配置包既保存在 NetScaler Console 上，也保存在执行配置的 NetScaler 实例上。

您可以使用 NetScaler Console 随附的默认 StyleBooks 为您的部署创建配置，也可以设计自己的 StyleBooks 并将其导入 NetScaler Console。您可以使用 StyleBooks 通过 NetScaler Console GUI 或使用 API 来创建配置。

本文档包含以下信息：

- 如何查看 StyleBooks
- 默认 StyleBooks
- 为业务应用程序开发的 StyleBook(/zh-cn/netscaler-application-delivery-management-software/current-release/stylebooks/business-application-stylebooks.html)
- 自定义 StyleBook(/zh-cn/netscaler-application-delivery-management-software/current-release/stylebooks/how-to-create-custom-stylebooks.html)
- StyleBook 中的 API(/zh-cn/netscaler-application-delivery-management-software/current-release/stylebooks/how-to-use-api-to-create-configuration-from-stylebooks.html)
- StyleBook 语法(/zh-cn/netscaler-application-delivery-management-software/current-release/stylebooks/stylebooks-grammar.html)

StyleBook 类别

NetScaler Console 中有两种 StyleBook 类别。它们是默认 StyleBook 和自定义 StyleBook。无论是默认 StyleBook 还是自定义 StyleBook，它都可以是公共 StyleBook 或私有 StyleBook。在 NetScaler Console 中，您可以查看系统中存在的所有 StyleBook，无论其类型或可见性状态如何。您还可以查看 StyleBook 之间如何相互连接的图形显示。

本文档解释了不同类型的 StyleBook。此外，它还解释了您可以在 NetScaler Console 中对 StyleBook 执行的以下操作：

- 下载自定义 StyleBook 并进行修改，或基于现有 StyleBook 创建新的 StyleBook。
- 隐藏默认 StyleBook。
- 从 NetScaler Console 中删除自定义 StyleBook。
- 为 StyleBook 添加标签。

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

默认 StyleBook 和自定义 StyleBook

- **默认 StyleBook** 是随 NetScaler Console 提供的 StyleBook，它们允许您创建可部署到 NetScaler 实例上的配置。您无法删除默认 StyleBook，但可以从 NetScaler Console GUI 中将其隐藏。
- **自定义 StyleBook** 是您导入到 NetScaler Console 中的 StyleBook。

默认 StyleBook 和自定义 StyleBook 都可以是公共的或私有的。

公共 StyleBook 和私有 StyleBook

可用于创建配置包的 StyleBook 可归类为**公共** StyleBook。也就是说，它们都可供您直接使用，通过 NetScaler Console GUI 和 API 创建配置。

但是，有些 StyleBook 用作其他 StyleBook 的构建块。此类 StyleBook 被标记为**私有**。私有 StyleBook 无法直接用于通过 NetScaler Console GUI 创建配置包。但是，您仍然可以在 NetScaler Console 上显示和查看这些 StyleBook。要将任何自定义 StyleBook 标记为**私有**，请将 StyleBook 中的私有属性设置为 **true**。您仍然可以使用私有 StyleBook 通过 NetScaler Console API 创建配置包。

标记为私有的 StyleBook 示例

```
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Configuration

description: |

    This StyleBook defines a simple load balancing configuration and is a
building block to build other load balancing configurations.

schema-version: "1.0"

private: true
```

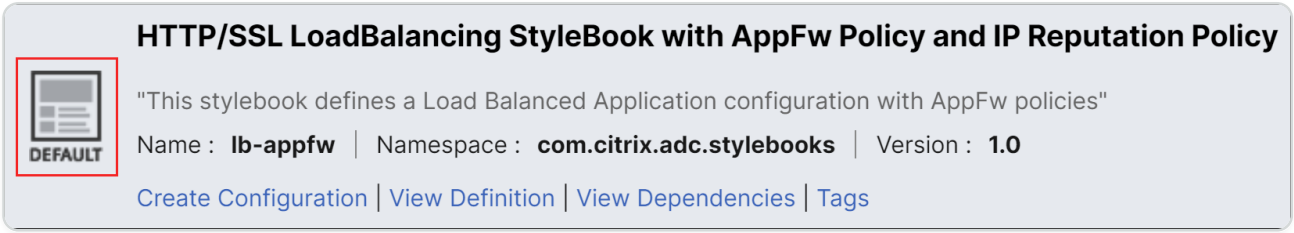
© 1997–2026 Citrix Systems, Inc. All rights reserved.

查看 StyleBook

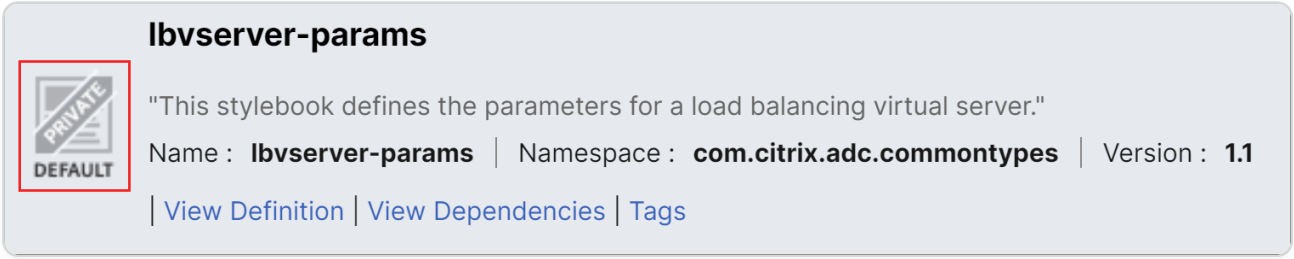
NetScaler Console 中 StyleBook 的数量（包括默认和私有）正在增加。您可能需要搜索要访问的特定 StyleBook。您可能还需要单独查看这两种类型的 StyleBook。

在 NetScaler Console 中，当您导航到 **应用程序** > **StyleBook** 时，您可以查看系统中存在的 StyleBook 列表。

默认公共 StyleBook 的面板上具有以下图标：

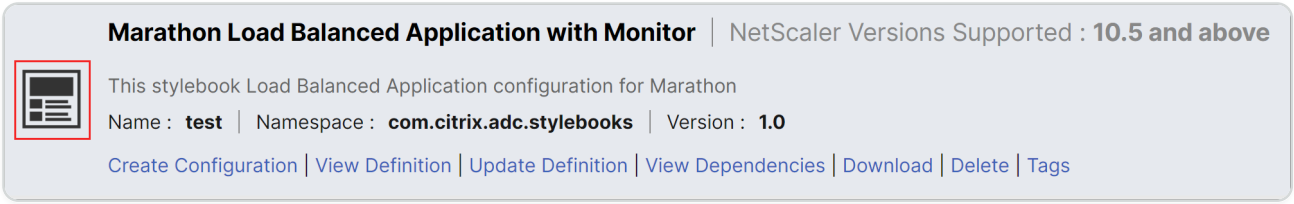


而默认私有 StyleBook 则有一个图标，表明它是私有 StyleBook：



虽然您可以查看私有 StyleBook 的定义和依赖项，但不能使用 GUI 从私有 StyleBook 创建配置包。私有 StyleBook 的主要目的是将其用作另一个 StyleBook 的构建块。使用构建块 StyleBook 有助于鼓励重用常见的配置模式。

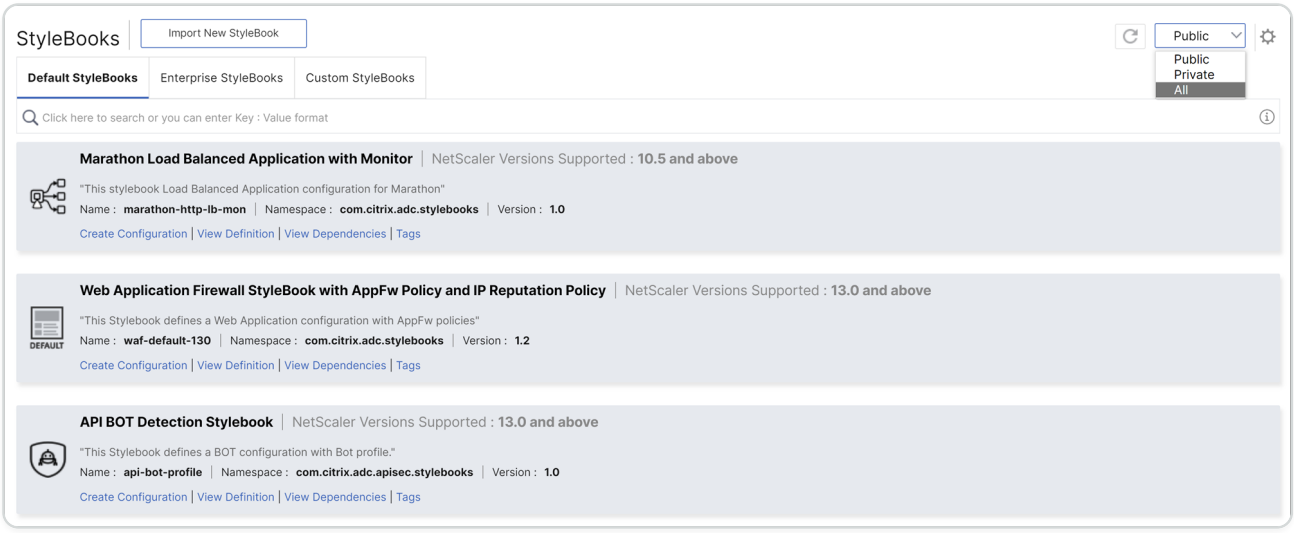
自定义公共 StyleBook 具有不同的图标，如下图所示：



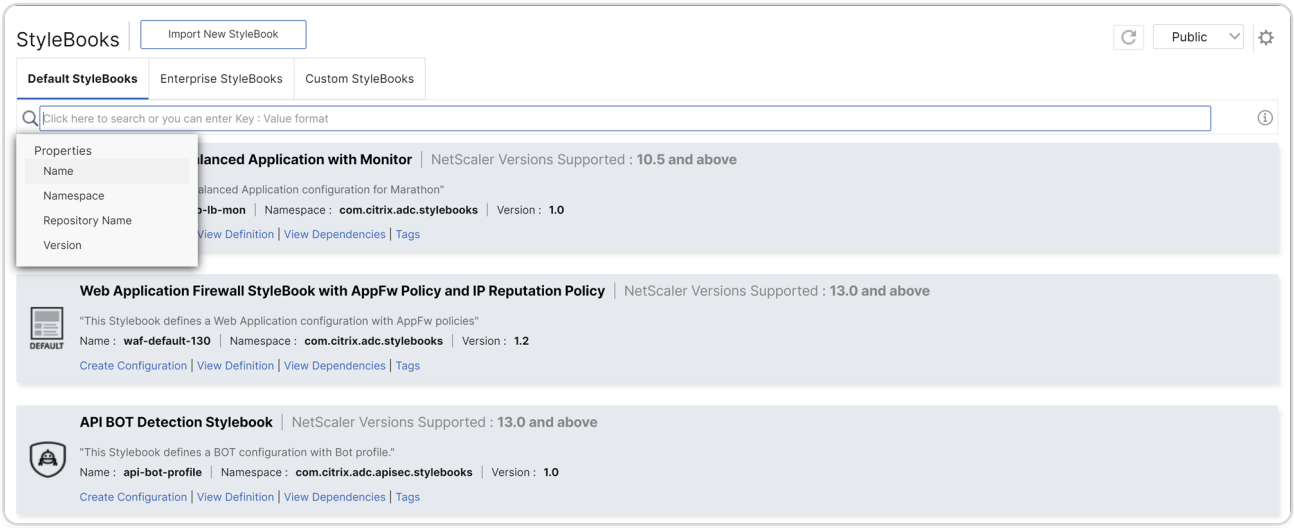
而自定义私有 StyleBook 则显示此图标：

在页面右上角，您可以看到一个选项，用于选择要查看的 StyleBook 类型。有三个选项 - 所有、公共或私有 StyleBook。单击其中一个选项。

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



您还可以通过单击搜索图标来搜索特定的 StyleBook。您可以按名称、命名空间和版本属性或这些选项的组合进行搜索。搜索操作不区分大小写。



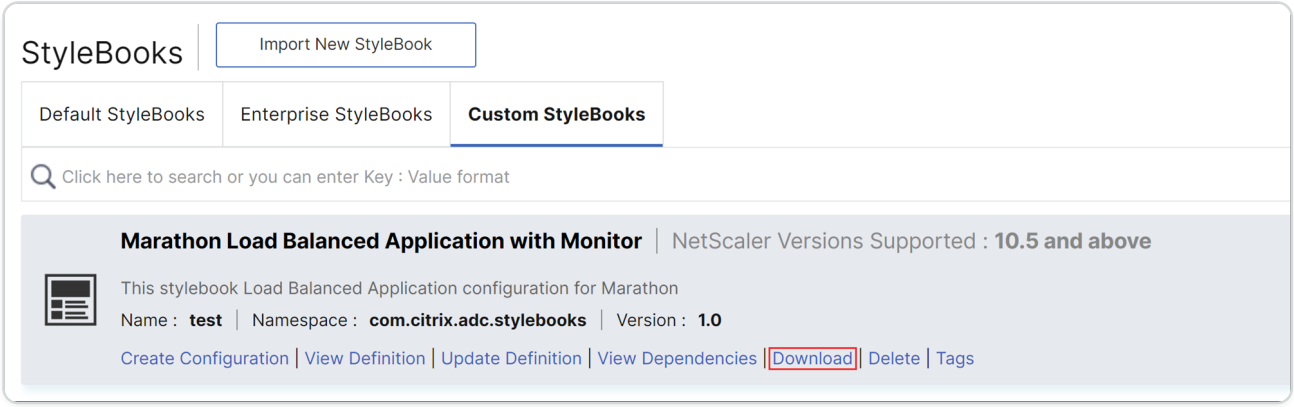
下载自定义 StyleBook

要从 NetScaler Console 下载自定义 StyleBook，请导航到 **Applications** > **StyleBooks** > **Configurations**。在右侧面板上显示的 StyleBook 列表中，选中下载自定义 StyleBook 的选项。单击 **Download**。如果 StyleBook 具有依赖的自定义 StyleBook，则可以在下载的捆绑包中包含这些依赖的 StyleBook。

注意：

您可以下载标记为公共或私有的自定义 StyleBook。

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



注意：

您无法下载默认 StyleBook。您可以查看它们的定义和依赖项。为此，请单击 StyleBook 面板上的 **View Definition** 和 **View Dependencies** 链接。

更新自定义 StyleBook

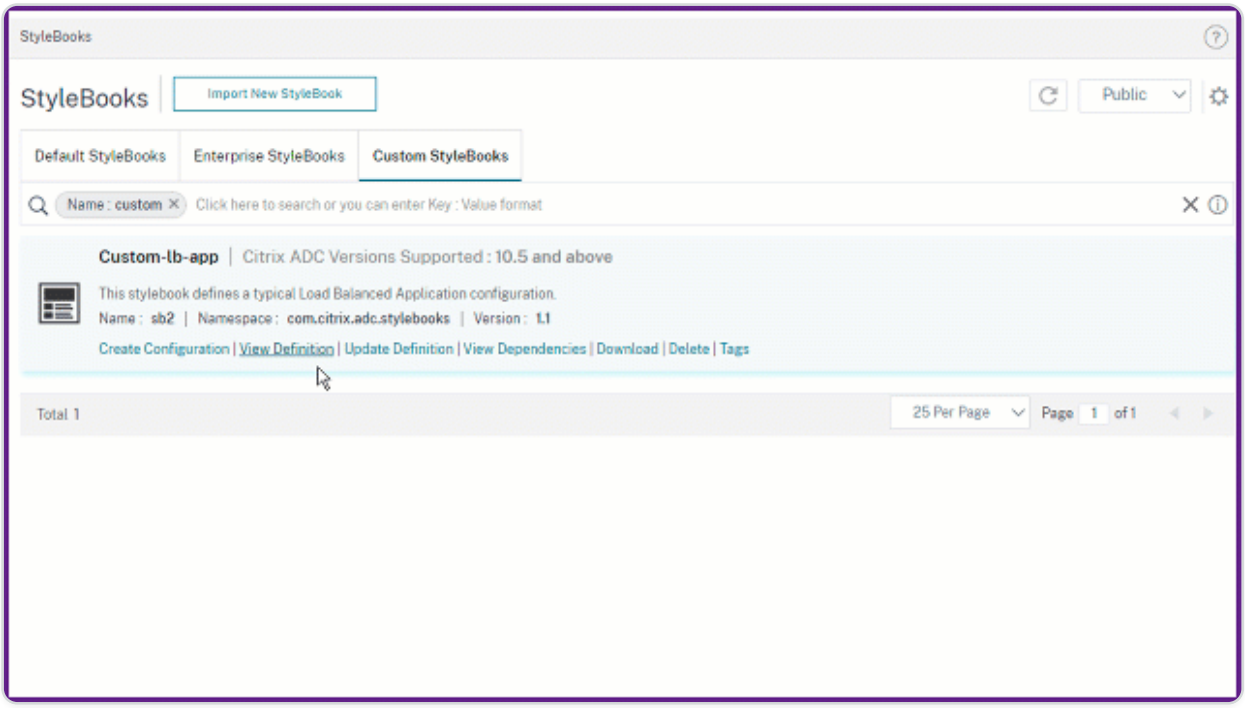
您可以直接从 NetScaler Console GUI 更新自定义 StyleBook 定义。因此，这有助于您在不更改 StyleBook 版本的情况下对其进行更改。您还可以更新从 StyleBook 捆绑包导入的定义。

重要提示：

- 在从 NetScaler Console GUI 更新 StyleBook 定义之前，请确保 StyleBook 定义没有依赖的 StyleBook。
- 您可以更新具有配置包的 StyleBook 定义。
- 确保 StyleBook 定义向后兼容。现有 StyleBook 的所有参数都将保留在更新后的 StyleBook 中，并且添加的参数将显示为可选。

1. 导航到 **应用程序 > 配置 > 样式簿**。
2. 选择**自定义 StyleBook** 选项卡。
3. 在要更新的 StyleBook 上选择**更新定义**。
4. 根据需要更新定义，然后单击**更新**。

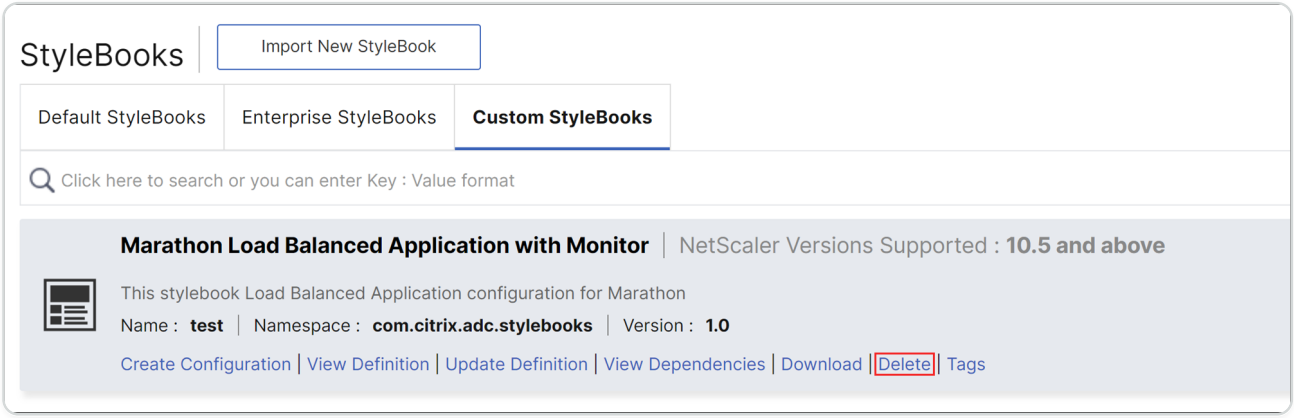
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 刷新页面以查看最新更改。

删除自定义 StyleBook

您还可以通过单击**删除**按钮来删除自定义 StyleBook。一个弹出窗口会提示您确认是否要从 NetScaler Console 中删除 StyleBook。如果 StyleBook 使用其他自定义 StyleBook，您可以通过选中复选框来选择删除这些 StyleBook。



注意：

如果自定义 StyleBook 在 NetScaler Console 中有依赖的 StyleBook，请勿删除它。否则，它将破坏现有的 StyleBook。

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

查看 StyleBook 依赖项

StyleBook 的一个重要而强大的功能是它们可以作为其他 StyleBook 的构建块。您可以将一个 StyleBook 导入到另一个 StyleBook 中。导入的 StyleBook 被声明为一种类型，并由第二个 StyleBook 的组件或参数使用。您可以研究 NetScaler Console 中现有的默认 StyleBook，以了解如何在一个 StyleBook 的基础上构建另一个 StyleBook。

NetScaler Console 允许您查看 StyleBook 之间如何相互连接的图形显示。这种表示对于使用其他 StyleBook 作为构建块构建的复杂 StyleBook 尤其有用。通过查看依赖关系图，可以了解多个 StyleBook 之间的关系和依赖项。

被其他 StyleBook 使用的 StyleBook 无法从系统中删除，因为它会破坏现有的 StyleBook。使用依赖关系图显示，您可以识别哪些 StyleBook 正在阻止删除某个 StyleBook。

查看 StyleBook 依赖项

在 NetScaler Console 中，导航到 **应用程序** > **StyleBooks**。StyleBooks 页面显示了 NetScaler Console 中所有可供您使用的 StyleBooks。向下滚动并找到您的 StyleBook。**StyleBook** 磁贴显示了用于创建配置、查看 StyleBook 定义和查看 StyleBook 依赖项的链接。单击 **查看依赖项**。

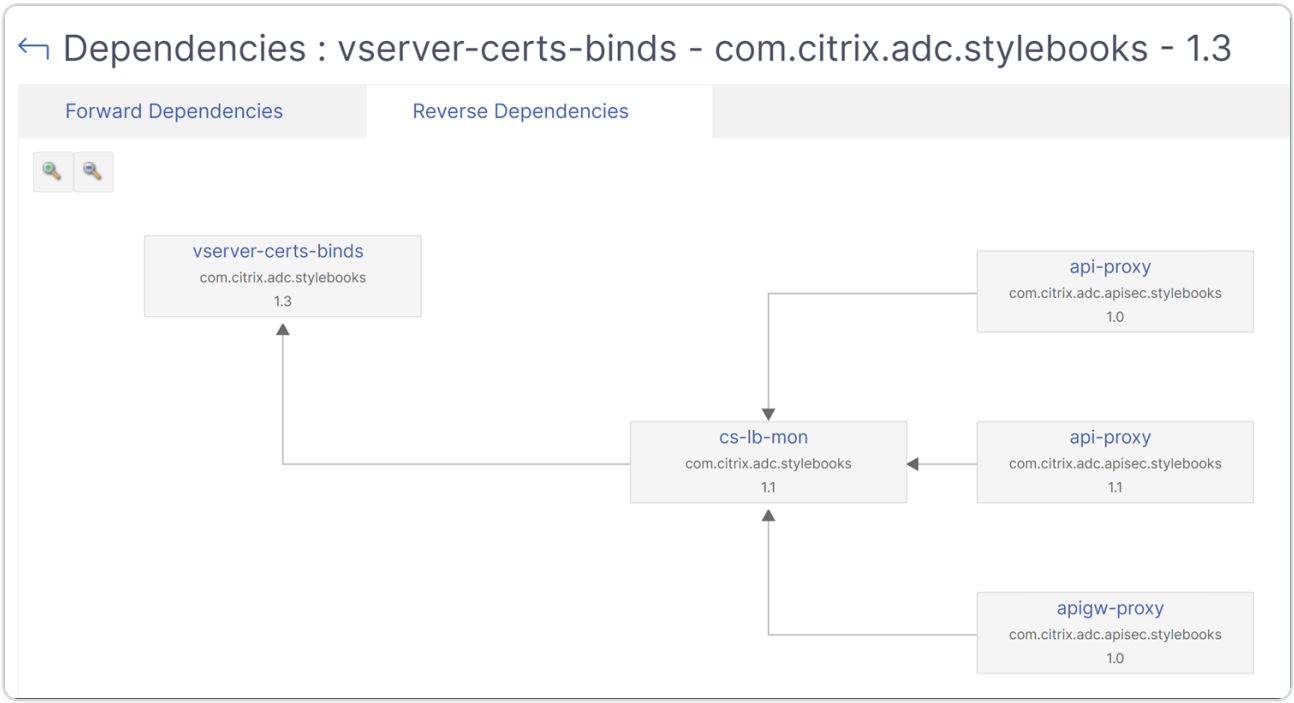
正向依赖项

正向依赖项 选项卡允许您查看您的 StyleBook 正在使用的不同默认 StyleBooks。按照箭头查找 StyleBook 正在使用的 StyleBook。当您将鼠标指向其中一个箭头时，该箭头以及相互连接的 StyleBooks 将突出显示。您还可以单击 StyleBook 名称以查看该 StyleBook 的定义。

反向依赖项

反向依赖项 选项卡允许您以图形方式查看正在使用您的 StyleBook 的 StyleBooks。如果您按照箭头，您可以看到显示中的所有 StyleBooks 都指向您的 StyleBook。有些 StyleBooks 可能直接使用该 StyleBook，有些 StyleBooks 可能通过另一个 StyleBook 使用该 StyleBook。

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



根据配置包审核 NetScaler 配置

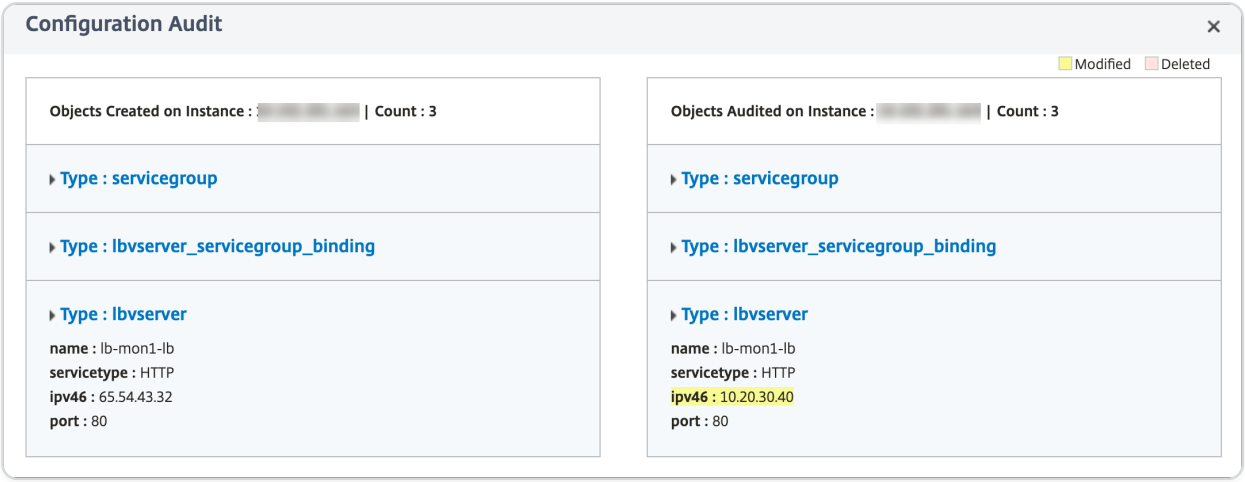
您可以将 StyleBook 配置包所做的更改与当前的 NetScaler 配置进行比较。通过此比较，您可以执行以下操作：

- 检测 StyleBook 配置包与 NetScaler 配置之间的配置漂移。
- 识别 NetScaler 上未反映配置包所做更改的任何已修改和已删除对象。

要将配置包更改与 NetScaler 配置进行比较，请执行以下操作：

1. 导航到 **应用程序** > **StyleBooks** > **配置**。
2. 单击 **配置审核**。

   配置审核 页面显示已创建和已审核的对象。

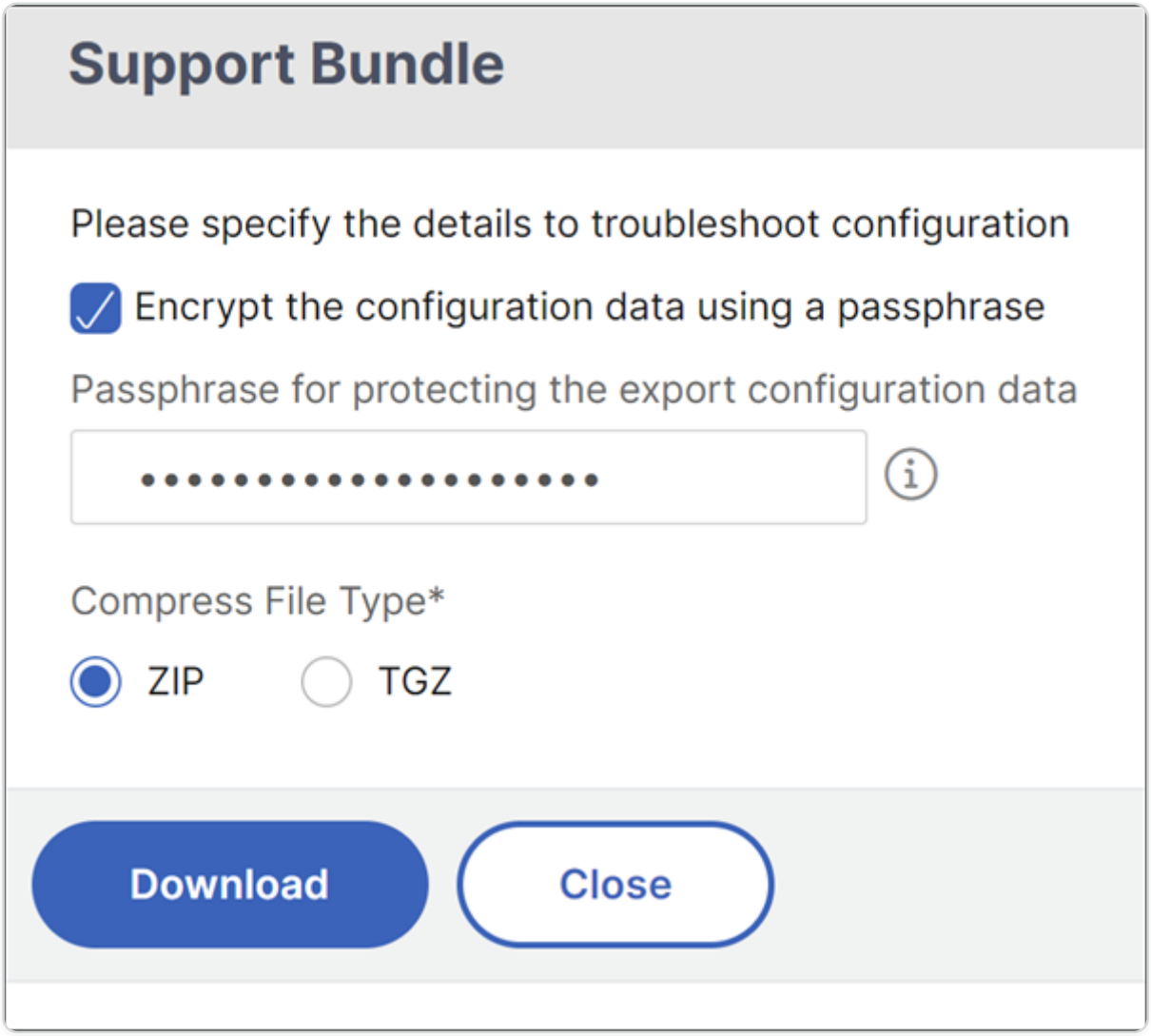


© 1997–2026 Citrix Systems, Inc. All rights reserved.

下载配置包的支持包

配置包的支持包可帮助 NetScaler® 技术支持团队查看、分析和排查配置包问题。

1. 在 **Applications > Configuration > Config Packs > Support Bundles** 中，选择一个配置包。单击 **Download**。
2. 在 **Download Support Bundle** 页面中，指定：
   - **使用密码短语加密配置数据** - 如果要指定密码短语来加密捆绑文件，请选择此选项。
   - **密码短语** - 指定一个密码短语来加密导出捆绑包。此密码短语可保护配置包的敏感数据。密码短语必须至少包含 20 个字符。
   - **压缩文件类型** - 您可以以 ZIP 或 TGZ 文件格式压缩捆绑包。
3. 单击 **Download**。



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

为 StyleBook 创建标签

您可以在 NetScaler Console 中为任何 StyleBook 添加标签。标签是键值对，可让您使用不同的条件对 StyleBook 进行分组。您可以在 NetScaler Console 中搜索或筛选 StyleBook 时使用这些标签。

要为 StyleBook 添加标签：

1. 导航到 **Applications** > **StyleBooks**。
2. 在要添加标签的 StyleBook 上选择 **Tags**。

   StyleBook 标签(/en-us/netscaler-application-delivery-management-software/media/adm-tags-stylebooks-new.png)

   您可以为所有类型的 StyleBook 添加标签。
3. 指定所需的**键**和**值**信息，以帮助您筛选 StyleBook。

   例如，键=team，值=bizdata

   为 StyleBook 创建标签(/en-us/netscaler-application-delivery-management-software/media/adm-create-tags-stylebook.png)

   要添加更多标签，请单击 **+**。
4. 单击**创建**。

要在搜索栏中使用标签筛选 StyleBook，请单击**标签**并从列表中选择一个键和值。将显示与指定标签匹配的 StyleBook。

如何使用标签(/en-us/netscaler-application-delivery-management-software/media/use-tags-stylebook.png)

以下是搜索具有标签的 StyleBook 的示例，其中 `key=team` 和 `value=bizdata`：

标签示例(/en-us/netscaler-application-delivery-management-software/media/example-adm-tag.png)

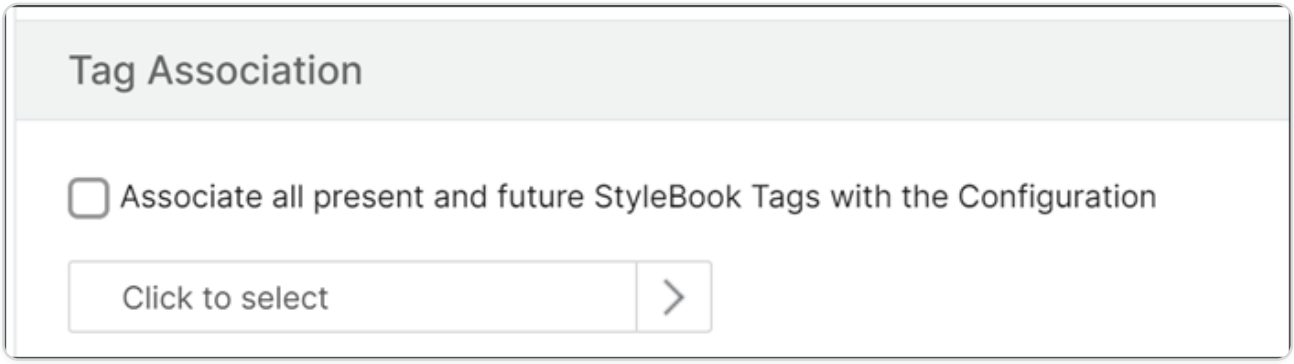
您可以将 StyleBook 标签与其配置包关联。因此，您可以使用 StyleBook 标签本身搜索配置包。

创建配置包时，请在**标签关联**部分使用以下选项之一：

- **将所有当前和未来的 StyleBook 标签与配置关联** – 此选项将所有 StyleBook 标签与配置包关联。它还确保关联您将来可能添加到 StyleBook 的新标签。

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

- **选择标签** – 此选项显示所选 StyleBook 的标签。您可以选择所需的 StyleBook 标签并将其与配置包关联。



使用 CLI 命令配置 StyleBook

如果要使用 CLI 命令配置任何 StyleBook，请执行以下操作：

- 在 NetScaler 中运行 `show ns runningConfig` 命令。
- 在 NetScaler Console 中，使用 默认 StyleBook、业务应用程序 StyleBook 或 自定义 StyleBook 创建配置。
- 再次在 NetScaler 中运行 `show ns runningConfig` 命令。

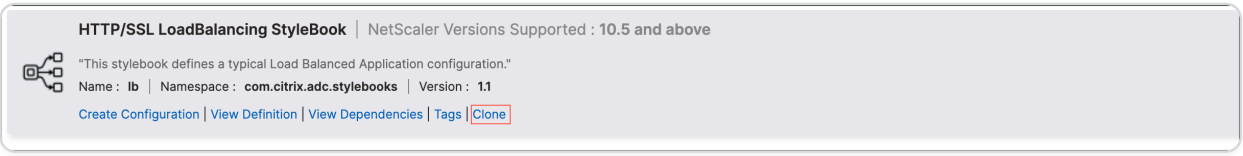
两次输出之间的差异显示了可用于使用 NetScaler CLI 配置任何 StyleBook 的 CLI 命令。

克隆 StyleBook

作为管理员，您可以创建 StyleBook 及其依赖 StyleBook 的副本。然后，您可以使用此捆绑包进行自定义，例如更新 `parameters` 和 `components` 部分。

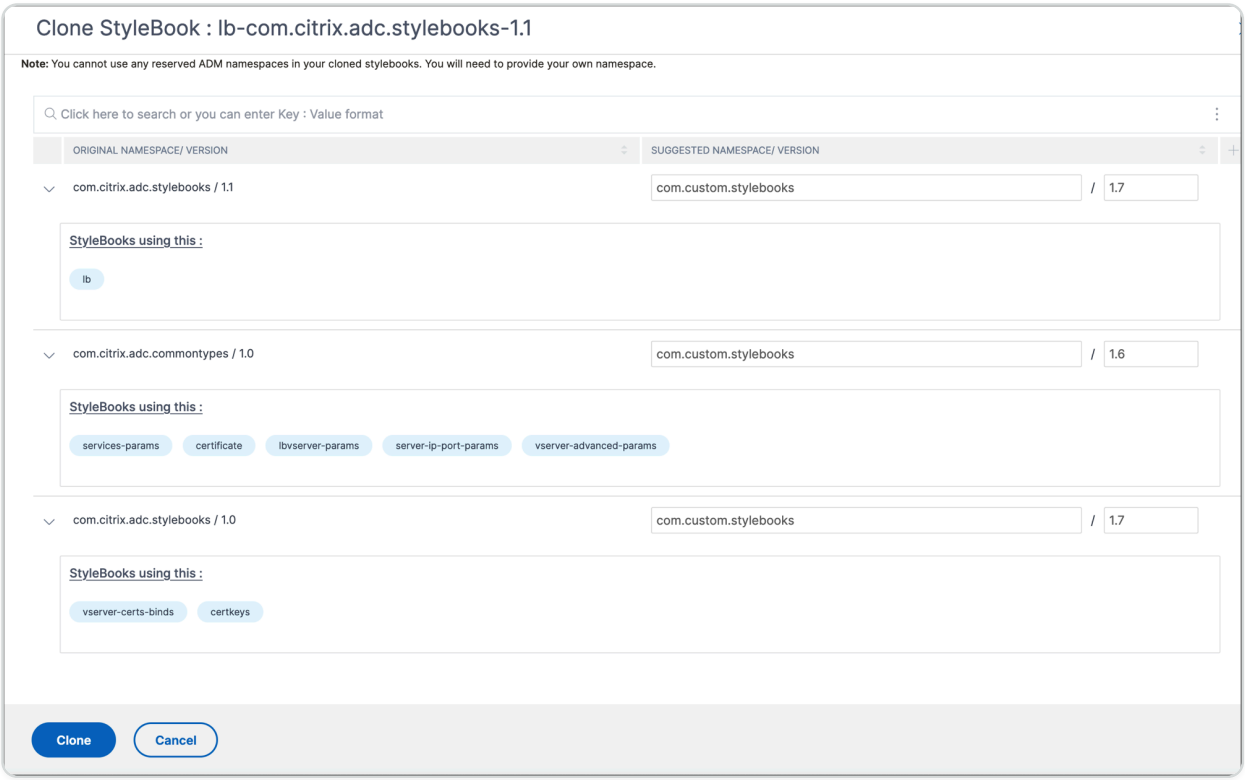
要克隆 StyleBook：

1. 导航到 **应用 > 配置 > 样式簿**。
2. 在要复制的默认或自定义 StyleBook 上选择 **Clone**。



3. 在 **Clone StyleBook** 页面中，输入 StyleBook 和依赖 StyleBook 的命名空间和版本。您还可以选择建议的命名空间和版本。

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



注意：

克隆的 StyleBook 及其依赖的 StyleBook 必须具有不同的命名空间和版本，以将其与现有 StyleBook 区分开来。您不能将任何保留的 NetScaler Console 命名空间用于克隆的 StyleBook。

4. 单击 **Clone**。克隆的 StyleBook 包将导入到 NetScaler Console 并显示在 **StyleBooks** 页面中。

从外部存储库导入和同步 StyleBook

设想一个场景，其中您正在开发中使用 CI/CD 流程。或者，设想一个场景，其中您正在 GitHub/GitLab 中管理所有应用程序源代码和部署对象。

在 GitHub/GitLab 存储库中，您可能已经创建了多个 StyleBook，用于部署 NetScaler 配置和管理这些 StyleBook。NetScaler Console 中也需要这些 StyleBook。现在，您可以直接将这些 StyleBook 导入到 NetScaler Console 中。您无需手动将它们从 GitHub/GitLab 复制，然后上传到 NetScaler Console，也无需手动同步 NetScaler Console 和 GitHub/GitLab 中的文件。

要导入 StyleBook 和配置包，请在 NetScaler Console 中定义一个存储库，该存储库代表一个 GitHub/GitLab 存储库。提供 GitHub/GitLab 存储库 URL 以及您在 GitHub/GitLab 中创建的用户名和 API 或个人访问 (PA) 令牌。这意味着，只有在 GitHub/GitLab 中拥有有效帐户的授权用户才能导入和同步 StyleBook。

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

您可以导入和同步以下类型的存储库：

- **可公开访问的存储库** - 指向公众开放且可通过互联网访问的存储库。
- **本地或私有 GitLab/GitHub 存储库** - 指私有托管且通常只能在企业内网中访问的存储库。对于这些存储库，您必须在注册过程中选择一个 NetScaler 代理。NetScaler 代理充当代理，用于访问企业内网中的存储库。

创建存储库后，您可以将 NetScaler Console 与您的 GitHub/GitLab 存储库同步。NetScaler Console 连接到 GitHub/GitLab 并导入在该存储库中找到的 StyleBook。然后，NetScaler Console 验证这些 StyleBook 并将其添加到 NetScaler Console 中的 StyleBook 列表中。如果 StyleBook 验证失败，则不会将其添加到 NetScaler Console 中。更正错误并将更新的版本提交到您的 GitHub/GitLab 存储库中。稍后，您可以尝试将它们再次导入或同步到 NetScaler Console 中。

注意

- StyleBook 文件可以从 GitHub/GitLab 存储库的任何分支导入和同步。
- 您也可以导入和同步具有关联的依赖 StyleBook 的 StyleBook。
- 从 GitHub/GitLab 存储库同步 StyleBook 必须从 NetScaler Console GUI 或 API 手动启动。也就是说，目前 StyleBook 的导入和同步不会根据 GitHub/GitLab 提交活动自动进行。

添加存储库并从外部存储库导入 StyleBook

在开始之前，请确保您在 GitHub/GitLab 中拥有有效帐户。

您可以将 StyleBook 文件从 GitHub/GitLab 存储库中的任何文件夹导入到 NetScaler Console。

1. 在 NetScaler Console 中，导航到 **应用程序** > **StyleBooks** > **存储库**。
2. 单击 **添加**。在 **添加存储库** 窗口中，输入以下参数：

   - **名称**。键入存储库的名称。此名称可以与 GitHub/GitLab 中的存储库名称相同，也可以不同。
   - **存储库 URL** - 键入 GitHub/GitLab 存储库 URL。

     您可以指定 GitHub/GitLab 企业版 URL。它有助于您从 GitHub/GitLab 企业版帐户导入或同步 StyleBooks 和配置包。
   - **是否为私有 URL？** - 如果存储库是本地或私有 GitLab/GitHub 存储库，请选中此复选框，然后选择一个 **代理**。

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

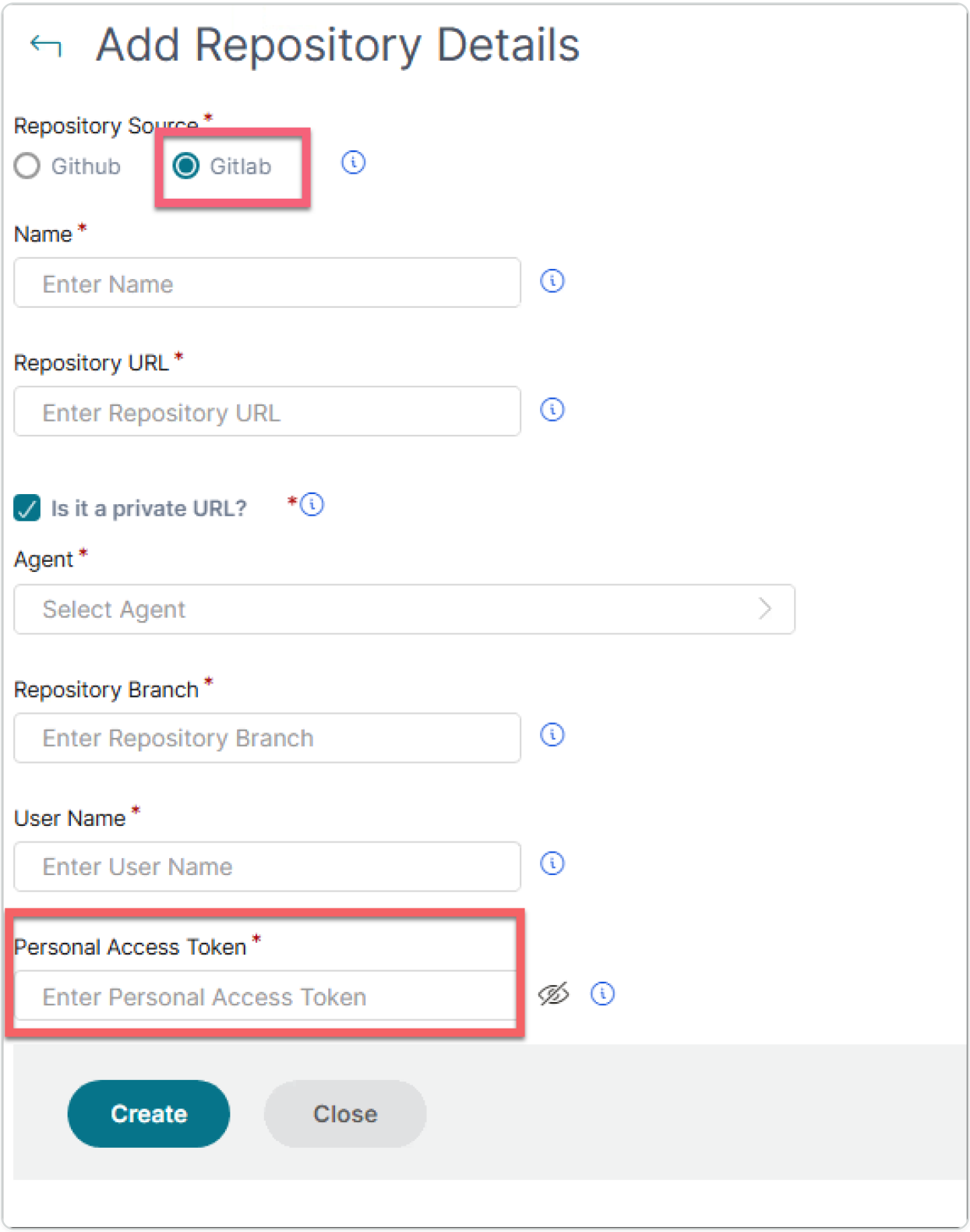
- **用户名和密码**。键入用于访问 GitHub/GitLab 帐户的用户名和密码。

注意

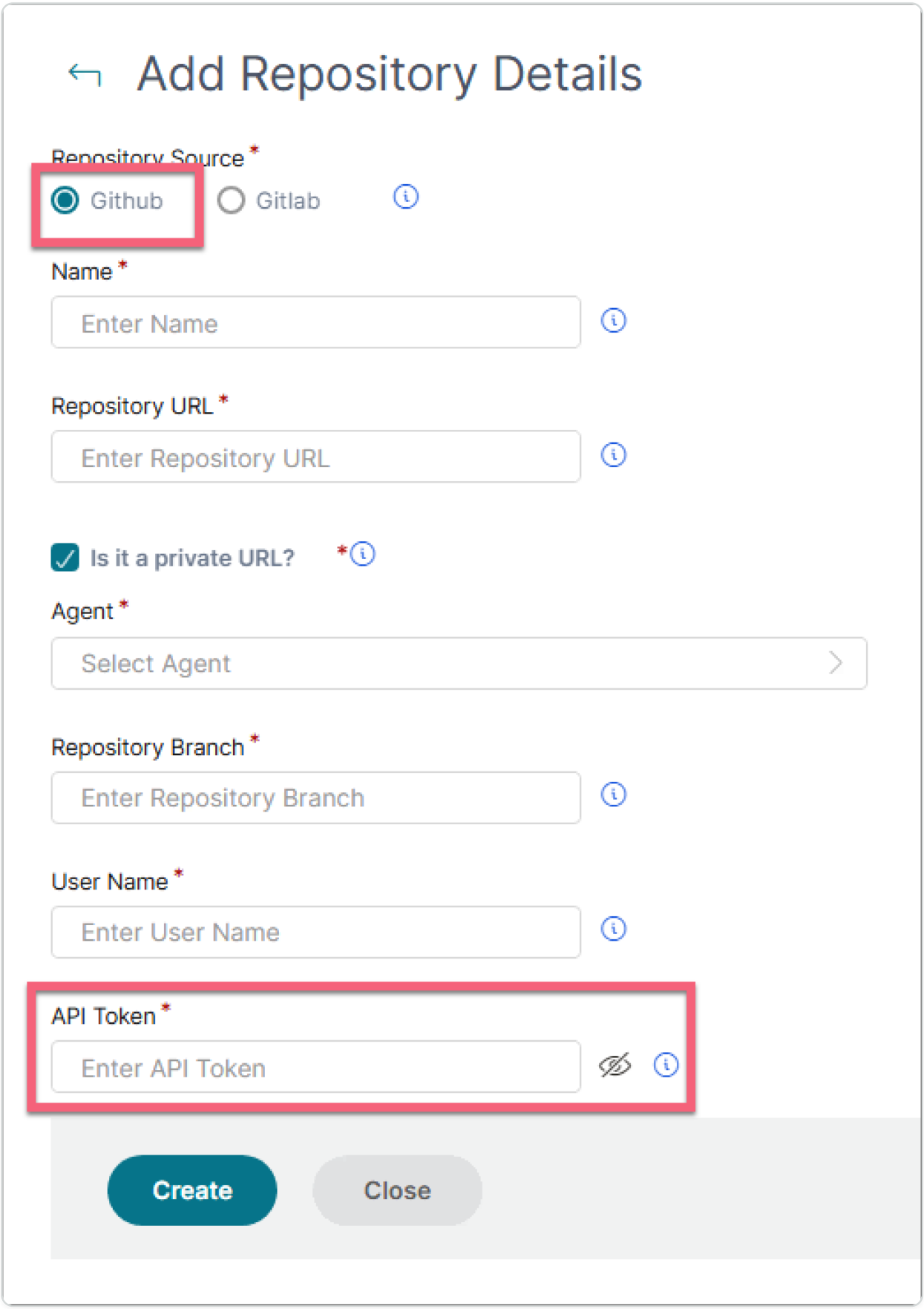
您还可以提供 API 令牌来代替密码。API 令牌可用于通过 HTTPS 访问 GitHub/GitLab，以代替密码。有关如何为 GitHub/GitLab 存储库创建 API/PA 令牌的信息，请参阅 GitHub/GitLab 文档中的创建个人访问令牌。

3. 单击 **创建**。

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



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



存储库已在 NetScaler Console 中创建。

4. 要导入或同步 StyleBooks，请在 **存储库** 页面中选择存储库，然后单击 **同步**。

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

您可以在此处使用的其他操作包括：

- **编辑**。您可以编辑存储库 URL、用户名和密码（或 API 令牌）。
- **删除**。您可以删除存储库以及 NetScaler Console 中所有先前从该 GitHub/GitLab 存储库导入的 StyleBook。

> **注意**
>
> 如果存储库中包含任何关联了 ConfigPack 的 StyleBook，则无法从 NetScaler Console 中删除该存储库。首先，删除这些 StyleBook 的所有配置包。之后，您可以从 NetScaler Console 中删除该存储库，以清理该存储库中的 StyleBook。

- **重置**。您可以删除 NetScaler Console 中从该存储库同步的所有 StyleBook，而无需实际删除 NetScaler Console 中的存储库条目。
- **列出文件**。您可以查看 NetScaler Console 中源自 GitHub/GitLab 存储库的所有 StyleBook 的列表。

从 GitHub/GitLab 导入 StyleBook 和配置包的步骤

完成先决条件后，请按照以下步骤从 GitHub/GitLab 存储库导入 StyleBook 和配置包：

1. 可选：如果您尚未添加存储库，请添加一个。
2. 在“存储库”页面中选择存储库。
3. 单击**同步**。

使用默认样式簿

NetScaler Console 提供了默认样式簿。使用默认样式簿时，您必须指定样式簿中参数的值，并选择要执行配置的 NetScaler 实例的 IP 地址。提交配置后，NetScaler Console 会验证您指定的参数值，创建配置图，连接到 NetScaler 实例，并在这些实例上执行配置。

从默认样式簿创建配置

1. 导航到 **应用程序** > **配置 > 样式簿**。样式簿页面显示 NetScaler Console 中的所有样式簿。此列表包括默认样式簿和自定义样式簿。您可以在搜索字段中键入样式簿的名称，然后按 **Enter** 键。或者，您可以向下滚动列表以查找样式簿。
2. 单击 **创建配置**。指定参数的所需值。

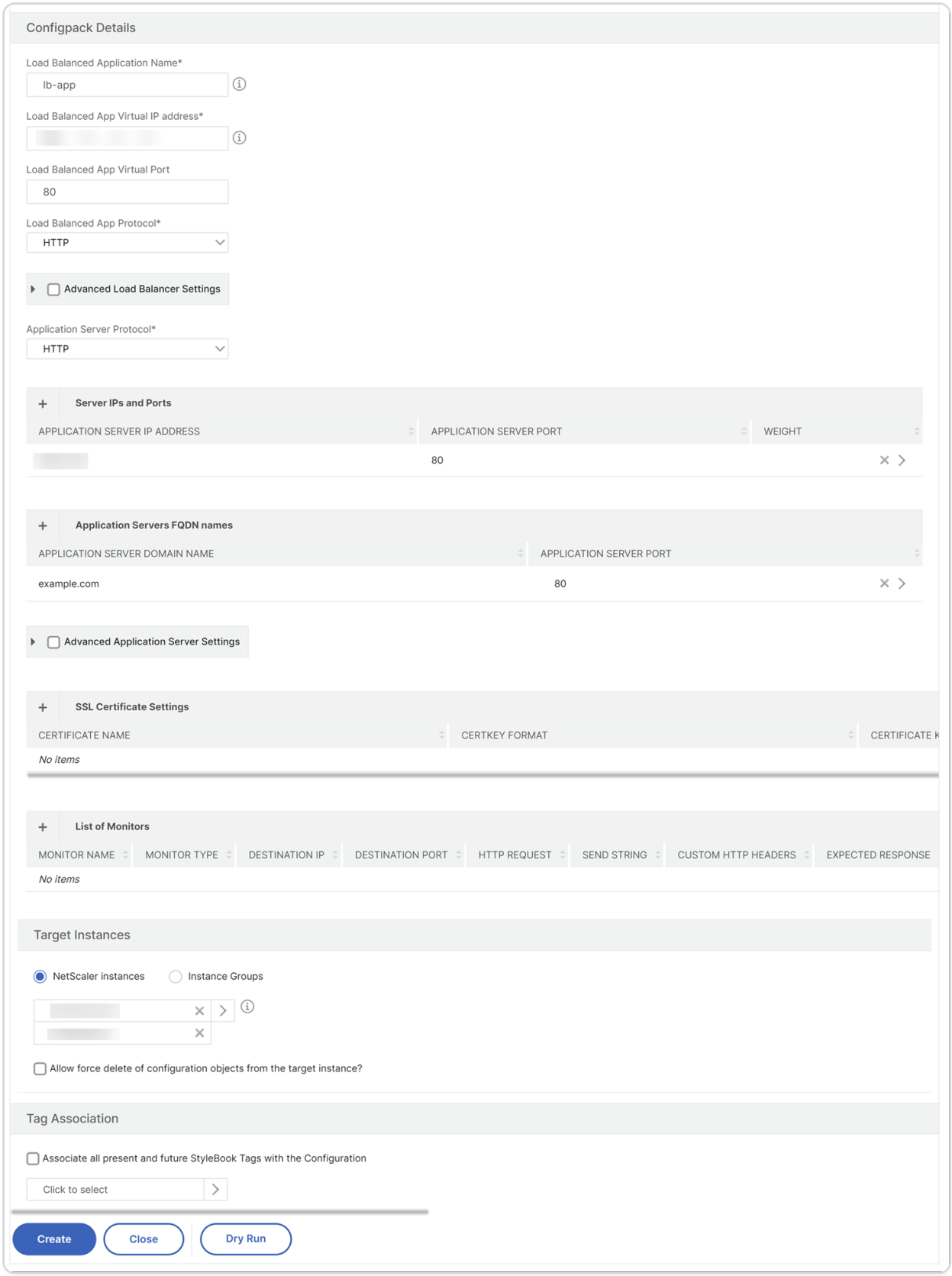
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

配置参数和值可能有所不同，具体取决于所选的样式簿。

3. 在 **目标实例** 下，单击并选择要执行配置的 NetScaler 实例的 IP 地址。如果要在多个实例上执行此配置，请单击“+”添加更多实例。

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



如果在 **NetScaler Console** > **设置 > 更改系统设置** > **修改系统设置** 中启用了 **提示实例登录凭据** 选项，当您在选定的 NetScaler 实例上执行配置时，系统会提示您输入 NetScaler 实例凭据。否则，NetScaler Console 将使用实例配置文件中存储的实例凭据登录到实例。

要启用 **提示样式簿操作凭据**，请按照以下步骤操作：

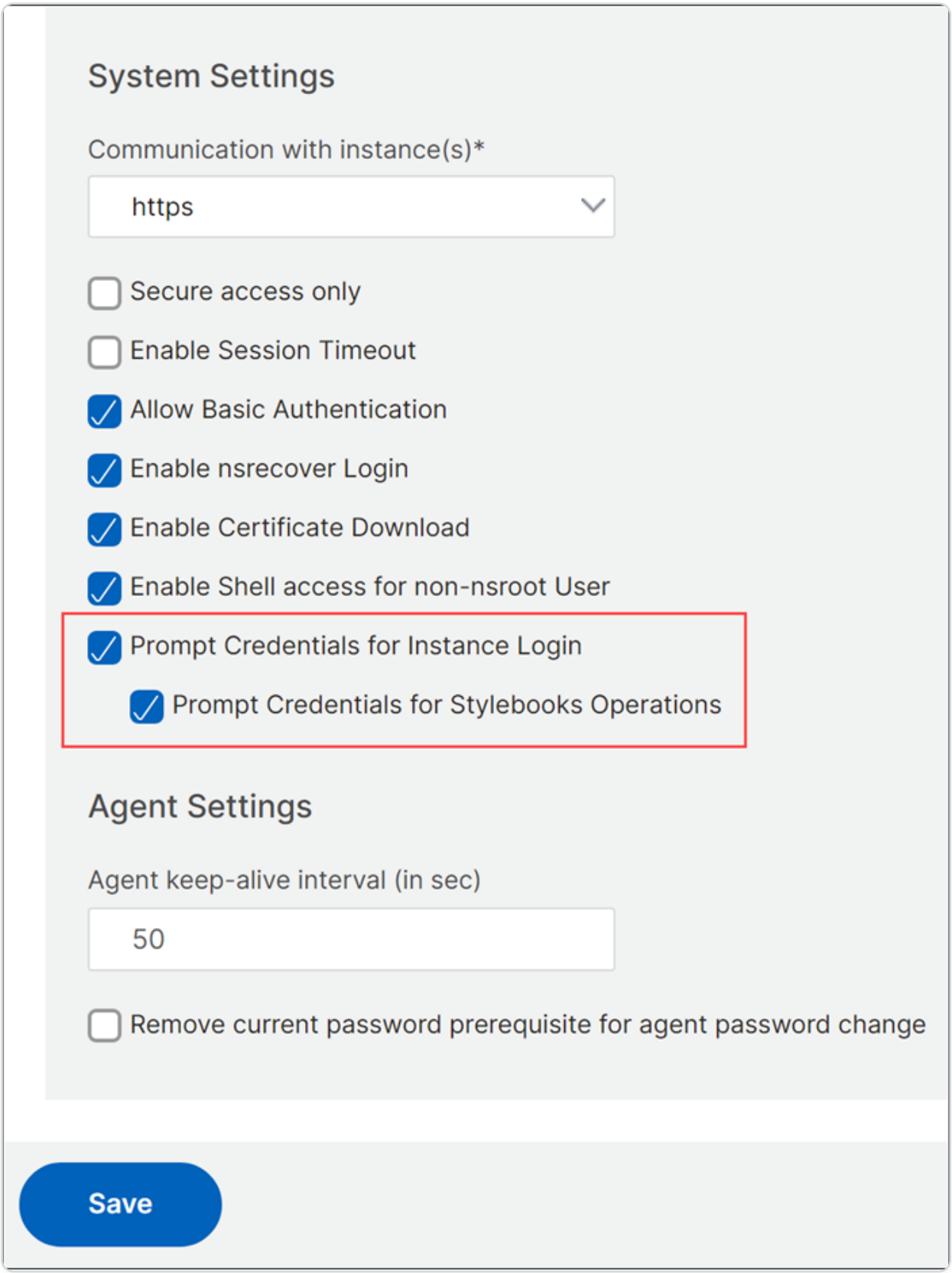
© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 导航到 **设置 > 管理**。

b. 在 **系统管理** 页面上，在 **系统配置** 下，选择 **系统、时区、允许的 URL 和代理设置**。

c. 在 **系统配置** 页面上，在 **系统设置** 下，选择 **提示实例登录凭据** 和 **提示样式簿操作凭据**。

d. 单击 **保存**。

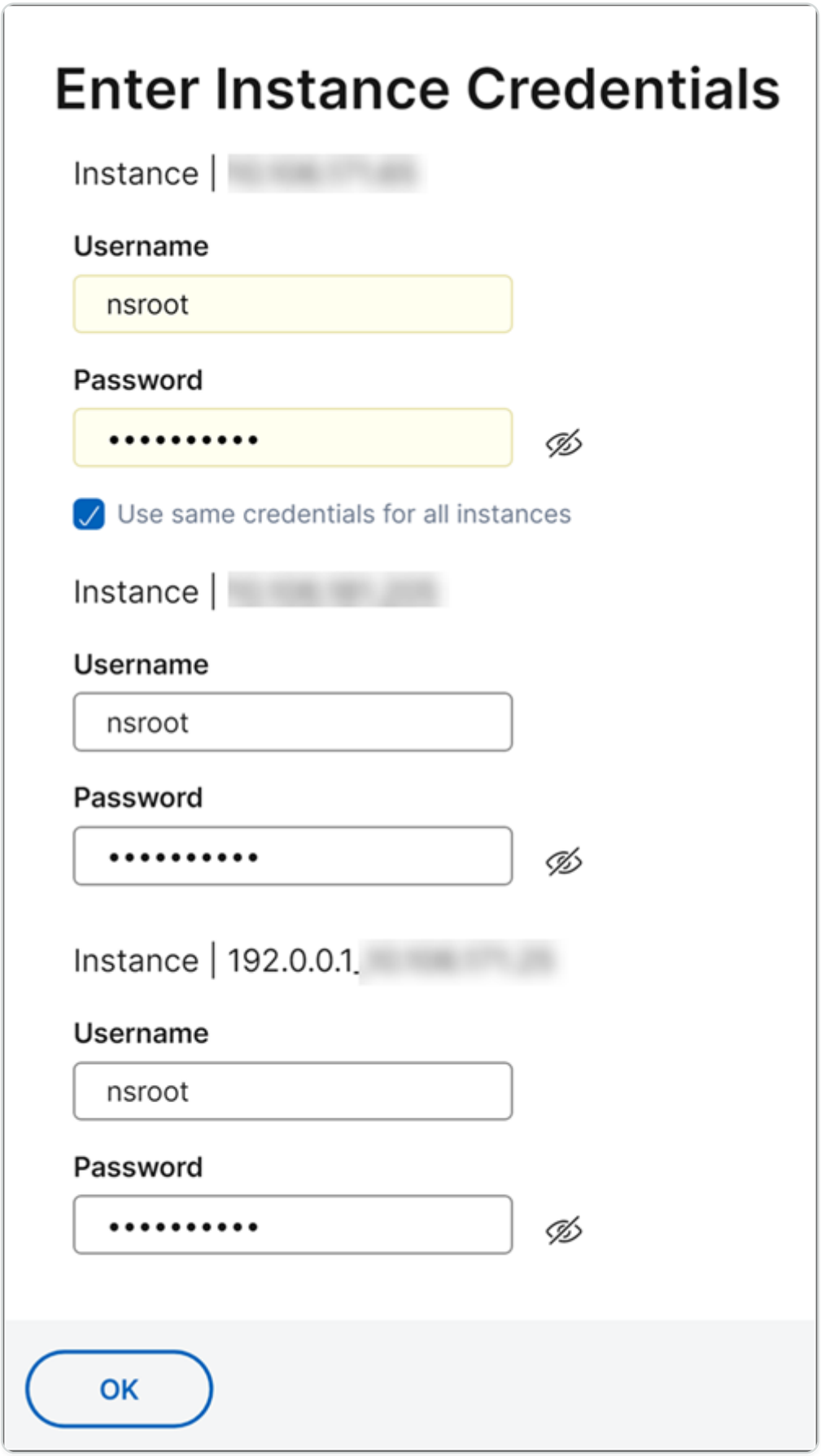


© 1997–2026 Citrix Systems, Inc. All rights reserved.

从版本 14.1 build 25.x 开始，您可以为所有选定的 NetScaler 实例提供凭据。

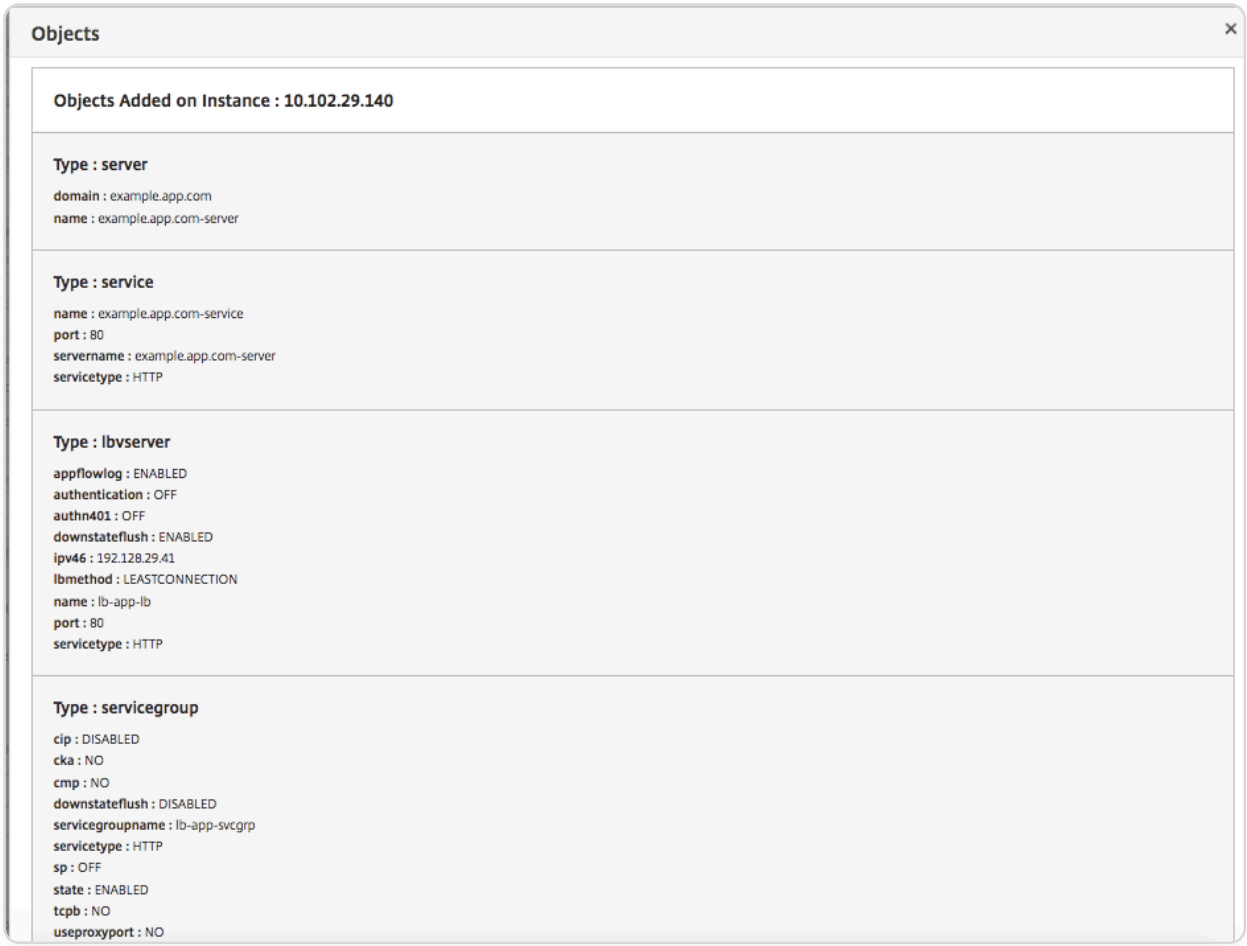
当您选择两个或更多 NetScaler 实例并选择 **对所有实例使用相同的凭据** 时，您可以将相同的凭据应用于选定的 NetScaler 实例。

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



如果您想在 NetScaler 实例上执行配置之前对其进行测试或验证，请选择 **试运行**，然后单击 **创建**。如果您的配置有效，则会显示根据您提供的值创建的对象。

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



4. 清除 **试运行** 复选框，然后单击 **创建** 以创建配置并在 NetScaler 实例上执行配置。您创建的 StyleBook 配置将显示在配置列表中，如下所示。

> **注意：**
>
> 您还可以单击刷新图标，将 NetScaler Console 中最近发现的 NetScaler 实例添加到此窗口中可用的实例列表中。

您现在可以使用 NetScaler Console 检查、更新或删除此配置包。

Web 应用防火墙 StyleBook

NetScaler Web 应用防火墙是一种 Web 应用防火墙 (WAF)，可保护 Web 应用程序和站点免受已知和未知攻击，包括所有应用层和零日威胁。

NetScaler Console 现在提供了一个默认的 StyleBook，您可以使用它更方便地在 NetScaler 实例上创建应用程序防火墙配置。

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

部署应用程序防火墙配置

以下任务可帮助您在业务网络中的 NetScaler 实例上部署负载平衡配置以及应用程序防火墙和 IP 信誉策略。

创建带有应用程序防火墙设置的 LB 配置：

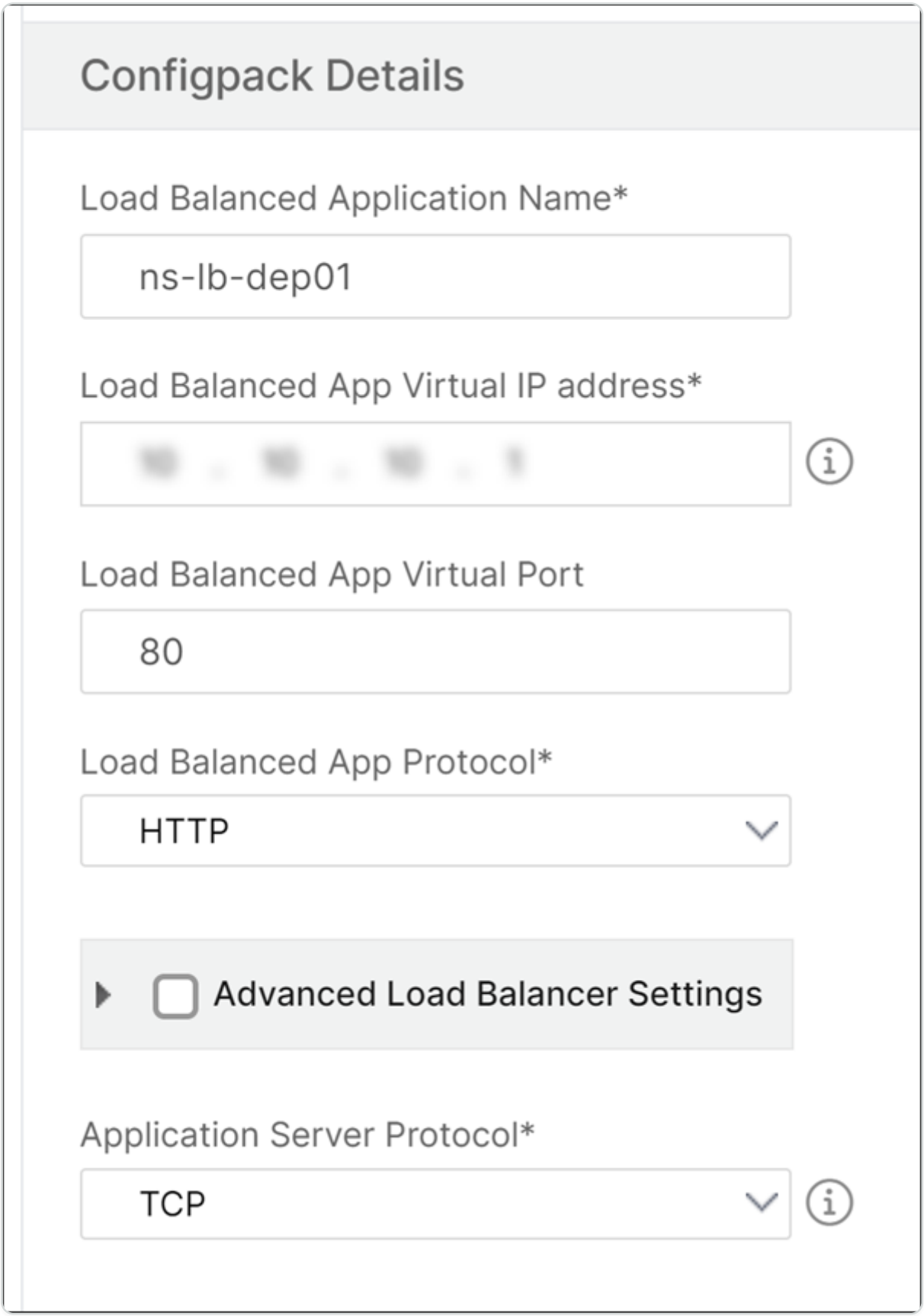
1. 在 NetScaler Console 中，导航到“**应用程序**”>“**配置**”>“**StyleBooks**”。StyleBooks 页面显示了 NetScaler Console 中所有可供您使用的 StyleBook。向下滚动并找到带有应用程序防火墙策略和 IP 信誉策略的 HTTP/SSL 负载平衡 StyleBook。您还可以通过输入名称 `lb-appfw` 来搜索 StyleBook。单击“**创建配置**”。

   StyleBook 将作为用户界面页面打开，您可以在其中输入此 StyleBook 中定义的所有参数的值。

2. 输入以下参数的值：

   - **负载平衡应用程序名称**。要在您的网络中部署的带有应用程序防火墙的负载平衡配置的名称。
   - **负载平衡应用程序虚拟 IP 地址**。NetScaler 实例接收客户端请求的虚拟 IP 地址。
   - **负载平衡应用程序虚拟端口**。用户访问负载平衡应用程序时要使用的 TCP 端口。
   - **负载平衡应用程序协议**。从列表中选择前端协议。
   - **应用程序服务器协议**。选择应用程序服务器的协议。

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



3. 作为选项，您可以启用和配置**高级负载均衡器设置**。

   指定高级负载均衡器设置(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-2.png)

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

4. 您还可以选择设置身份验证服务器，用于对负载均衡虚拟服务器的流量进行身份验证。

   可选，高级负载均衡器虚拟服务器(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-3.png)

5. 在“服务器 IP 和端口”部分中单击“+”以创建应用程序服务器及其可访问的端口。

   指定 IP 和端口详细信息(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-4.png)

6. 您还可以为应用程序服务器创建 FQDN 名称。

   为应用程序服务器创建 FQDN 名称(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-5.png)

7. 您还可以指定 SSL 证书的详细信息。

   指定应用程序服务器的 SSL 证书详细信息(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-6.png)

8. 您还可以在目标 NetScaler 实例中创建监视器。

   在目标实例中创建监视器(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-7.png)

9. 要在虚拟服务器上配置应用程序防火墙，请启用 WAF 设置。

   如果要将应用程序防火墙设置应用于该 VIP 上的所有流量，请确保应用程序防火墙策略规则为 true。否则，请指定 NetScaler 策略规则以选择要应用应用程序防火墙设置的请求子集。接下来，选择要应用的配置文件类型 - HTML 或 XML。

   启用 WAF 设置(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-8.png)

10. 您可以选择通过启用应用程序防火墙配置文件设置复选框来配置详细的应用程序防火墙配置文件设置。

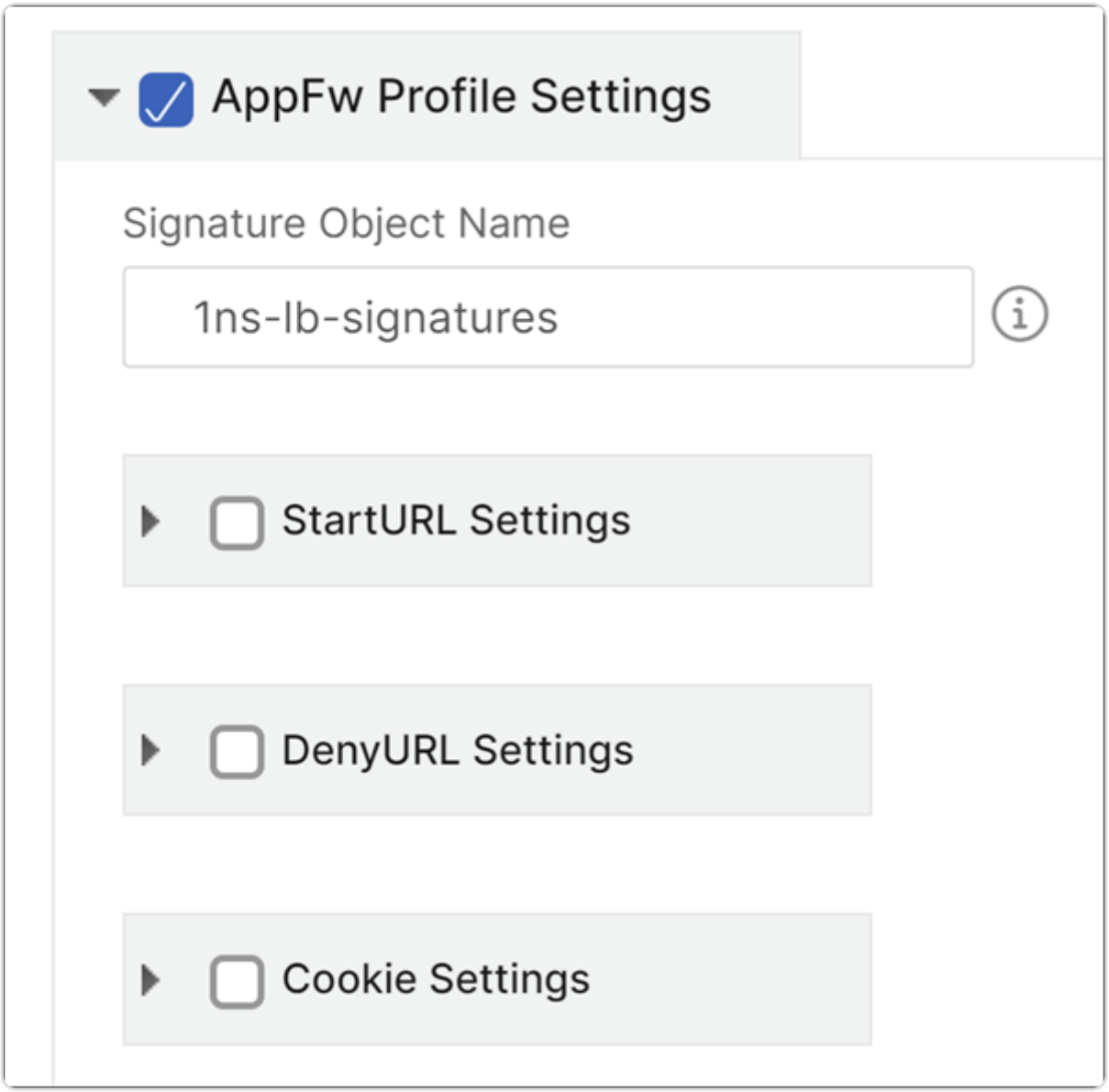
11. 或者，如果您想配置应用程序防火墙签名，请输入在要部署虚拟服务器的 NetScaler 实例上创建的签名对象的名称。

    注意：

    您不能使用此 StyleBook 创建签名对象。

12. 接下来，您还可以配置任何其他应用程序防火墙配置文件设置，例如 StartURL 设置、DenyURL 设置等。

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



有关应用程序防火墙和配置设置的更多信息，请参阅应用程序防火墙。

13. 在**目标实例**部分中，选择要部署带有应用程序防火墙的负载平衡虚拟服务器的 NetScaler 实例。

> **注意：**
>
> 您还可以单击刷新图标，将 NetScaler Console 中最近发现的 NetScaler 实例添加到此窗口中可用的实例列表中。

14. 您还可以启用**IP 信誉检查**来识别发送不需要请求的 IP 地址。您可以使用 IP 信誉列表来抢先拒绝来自信誉不佳的 IP 的请求。
15. 单击**创建**以在选定的 NetScaler 实例上创建配置。

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

> **提示**
>
> 我们建议您选择**试运行**，以在实例上运行实际配置之前检查必须在目标实例上创建的配置对象。

成功创建配置后，StyleBook 将创建所需的负载平衡虚拟服务器、应用程序服务器、服务、服务组、应用程序防火墙标签、应用程序防火墙策略，并将它们绑定到负载平衡虚拟服务器。

下图显示了在每个服务器中创建的对象：

WAF 在 NetScaler 实例上创建的对象(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-12.png)

16. 要查看在 NetScaler Console 上创建的配置包，请导航到 **应用程序** > **配置**。

    WAF 配置包(/en-us/netscaler-application-delivery-management-software/media/waf-stylebook-13.png)

隐藏所有默认 StyleBook

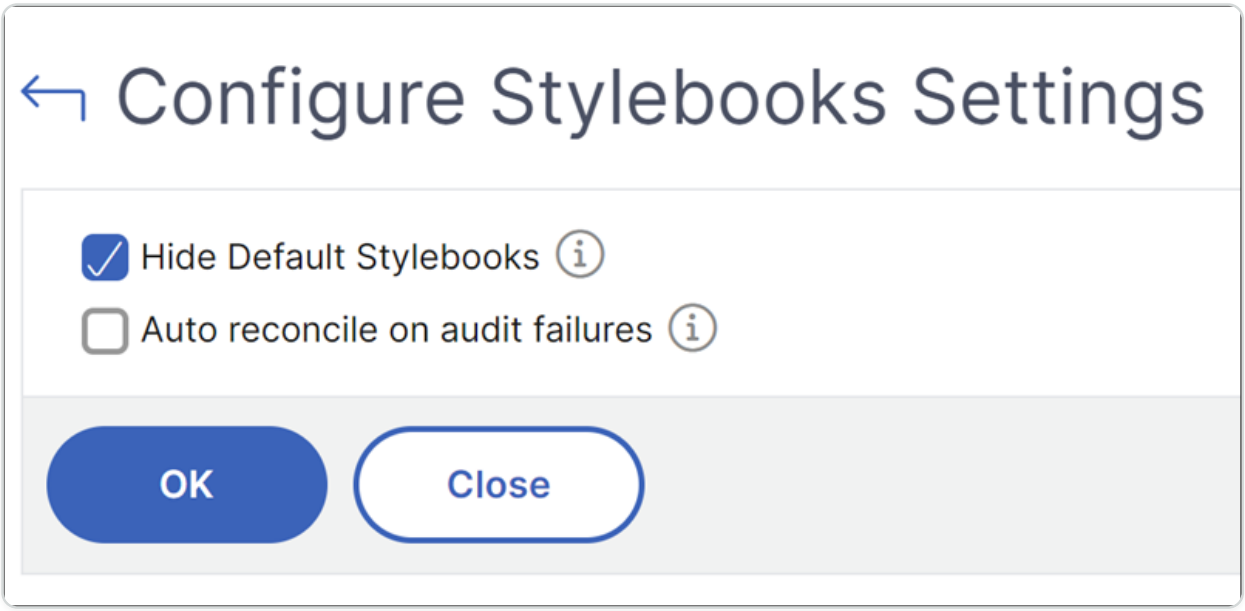
NetScaler Console 列出了 NetScaler Console 文件夹系统中存在的所有 StyleBook。StyleBook 列表包括默认 StyleBook 和自定义 StyleBook，它们可以是私有的，也可以是公共的。作为管理员，您可能希望隐藏所有默认 StyleBook。您可以允许用户仅查看和访问您或用户构建的自定义 StyleBook。

NetScaler Console 允许您显示自定义 StyleBook 并隐藏 NetScaler Console 附带的所有默认 StyleBook。提供了一个新的 GUI 选项，您可以在其中隐藏所有默认 StyleBook。

隐藏所有默认 StyleBook：

1. 在 NetScaler Console 中，导航到 **应用程序** > **配置 > 设置**。
2. **Settings** 页面显示默认 StyleBook 是否对用户可见的信息。
3. 要隐藏默认 StyleBook，请单击右上角的编辑图标。
4. 在 **Configure StyleBook Settings** 页面上，选择 **Hide Default StyleBooks** 选项。
5. 单击 **OK**。

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



如果您没有选择使用 RBAC 功能隐藏该页面，则用户仍然可以看到 **Configure StyleBook Settings** 页面。用户可能仍然可以选择取消隐藏默认 StyleBook。

要隐藏 **Configure StyleBook Settings** 页面，您必须创建一个策略，并将该策略分配给不应看到默认 StyleBook 的用户。

创建 RBAC 策略：

1. 在 NetScaler Console 中，导航到 **帐户** \> **用户管理** \> **访问策略**。
2. 单击 **Add** 以创建策略。
3. 输入策略名称。
4. 在**权限**部分中，确保未选择**所有** > **应用程序** > **配置** > **设置**，然后单击**确定**。

创建策略后，您必须创建角色，将每个角色绑定到一个或多个策略，并将角色分配给用户组。要了解有关如何将策略与用户关联的更多信息，请参阅配置基于角色的访问控制。

Prometheus 分析 StyleBook

您可以通过在 NetScaler 中创建分析配置文件并指定架构文件，将指标从 NetScaler 导出到 Prometheus。在 StyleBooks 中，您可以使用 `Prometheus TimeSeries Analytics Configuration` StyleBook 并将配置运行到所有托管实例。

先决条件

确保托管的 NetScaler 实例为 **13.1 build 39-27 或更高版本**。

要使用 `Prometheus TimeSeries Analytics Configuration` StyleBook 进行配置：

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

1. 导航到 **Applications** > **Configurations** > **StyleBooks**，通过键入名称 `Prometheus TimeSeries Analytics Configuration` 搜索 StyleBook，然后单击 **Create Configuration**。
2. 在 **配置包详情** 中：
   a. 指定分析配置文件名称。有关更多信息，请参阅 配置指标收集器。
   b. **计数器架构文件**：
      - 如果要继续使用默认架构，可以跳过此步骤。
      - 如果要继续使用自定义架构，请上传已使用参数修改的架构文件。在 NetScaler 中，包含所有受支持计数器的参考文件 `reference_schema.json` 位于路径 `/var/metrics_conf/` 下。您可以使用 FTP 客户端将文件复制到本地。
3. 在 **Target Instances** 中，选择要运行配置的实例或实例组。
4. 在 **Tag Assosiation** 中，将所有当前和未来的 StyleBook 标签与配置关联。

   此选项将所有 StyleBook 标签与配置包关联。它还确保关联您将来可能添加到 StyleBooks 的新标签。

   注意：

   点击 **试运行** 以查看在 NetScaler® 实例中创建、修改或删除的结果。

5. 点击 **创建** 以运行配置。

使用 StyleBooks 配置构建器迁移 NetScaler® 应用程序配置

StyleBooks 配置构建器用于从现有 NetScaler 配置创建应用程序配置 StyleBook。此功能还可自动将应用程序配置从一个 NetScaler 实例迁移到另一个实例。

使用配置构建器，您可以简化创建自定义 StyleBook 的过程，即使您对 StyleBook 语法和构造缺乏深入了解，也能轻松完成。否则，创建 StyleBook 需要熟悉 StyleBook 语法和构造。

配置构建器还会创建一个配置包，其中一个 NetScaler 实例的配置可以复制到另一个 NetScaler 实例。初始配置源可以是以下之一：

- **NetScaler 实例：** 指定要复制的应用程序配置所在的实例。

  即使您未指定目标实例，配置构建器也会将 NetScaler 配置转换为 StyleBook 和配置包。您以后可以使用此配置包将 NetScaler 配置迁移到其他 NetScaler 实例。

- **一组 CLI 命令：** 从 `ns.conf` 或 `Application config` 粘贴配置。

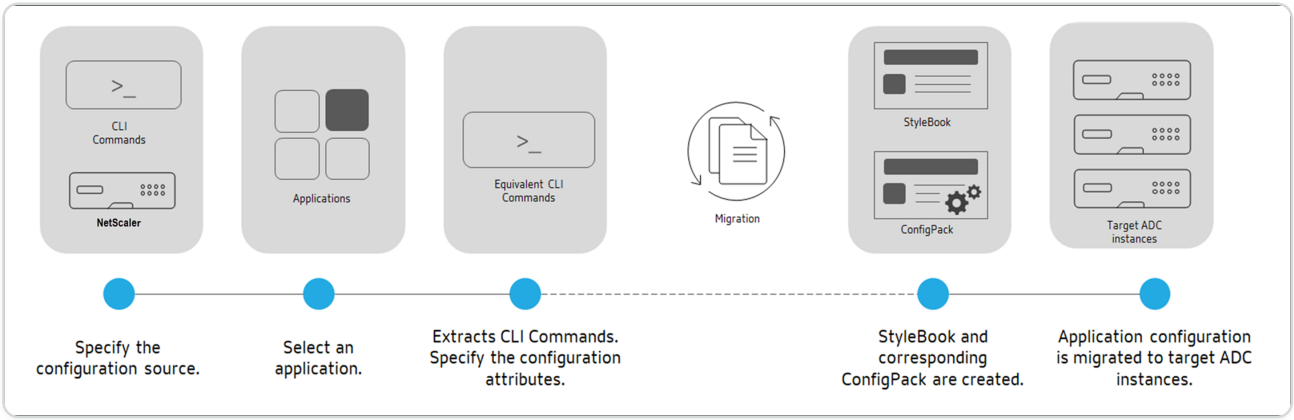
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **上传配置文件：** 从本地计算机上传配置。

配置构建器会识别源配置中嵌入的独立应用程序列表。当您选择感兴趣的应用程序配置时，配置构建器会提取所选应用程序的 CLI 命令集。这些 CLI 命令是从源配置中提取的。它还会识别可能需要您输入的部署和配置属性。

- **应用程序部署信息** - 您可以查看和编辑原始配置中虚拟服务器、服务、服务组成员的 IP 地址和端口。您还可以查看和编辑虚拟服务器的状态和 ARP。
- **配置属性** - 这些属性可以是源配置中指定的密码或证书。

指定必要信息后，开始在目标 NetScaler 实例上迁移或复制应用程序配置。



完成应用程序创建和迁移后，NetScaler Console 中会创建一个配置包及其对应的 StyleBook。此配置包表示目标 NetScaler 实例上的应用程序配置。要查看创建的配置包，请导航到 **应用程序** > **StyleBooks** > **配置**。

在迁移的配置之间共享配置实体

使用配置迁移实用程序迁移配置时，可以重用配置实体。后续迁移成功重用现有配置实体。以前，当迁移共享某些配置实体的两个配置时，配置迁移会因错误“**资源已存在**”而失败。此选项通过允许在多个配置中重用配置实体来简化迁移工作流。

支持的 NetScaler 功能

StyleBook 配置构建器可识别并支持源配置中的以下 NetScaler 功能：

- 分析
- AppFlow®
- 应用程序级体验质量配置 (AppQoE)
- 身份验证和授权
- 审计

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

- 僵尸程序管理
- 缓存重定向
- 内容交换
- DNS
- 前端优化
- HTTP 压缩
- 集成缓存
- 负载均衡
- 监控
- QUIC 协议
- 速率限制
- 响应器
- 重写
- SSL 卸载
- 溢出
- 流量管理
- URL 转换
- Web 应用程序防火墙 (WAF)

创建 StyleBook 以迁移 NetScaler 应用程序配置

以下过程用于创建 StyleBook，以在 NetScaler Console 中迁移 NetScaler 应用程序：

1. 导航到 **应用程序** > **配置** > **配置包**。
2. 单击 **迁移 NetScaler 配置**。
3. 点击“**开始**”。
4. 在“**指定配置**”中，选择以下配置源之一：
   - “**从 NetScaler 导入**”：
     - “**源 NetScaler 实例**” - 选择要从中迁移或复制应用程序配置的 NetScaler 实例。单击“**确定**”。
   - “**使用 CLI 命令导入**” - 从配置文件粘贴配置。

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

- “**上传配置文件**” - 单击“**浏览**”从本地计算机选择配置文件。

“**目标实例**” - 选择要迁移或复制应用程序配置的 NetScaler 实例或自动扩缩组。单击“**确定**”。

点击“**下一步**”。

5. 在“**高级策略配置**”中，根据您的配置，会出现以下情况：

   - 配置中所有现有的经典策略都已成功转换为高级策略，没有错误。查看更新的配置并选择确认。点击“**下一步**”。
   - 配置中所有现有的经典策略都已成功转换为高级策略，但存在错误。查看并修复错误。点击“**上一步**”。
   - 如果没有经典策略，则配置不会更新。点击“**确定**”继续。

6. 在“**定义应用程序**”中，

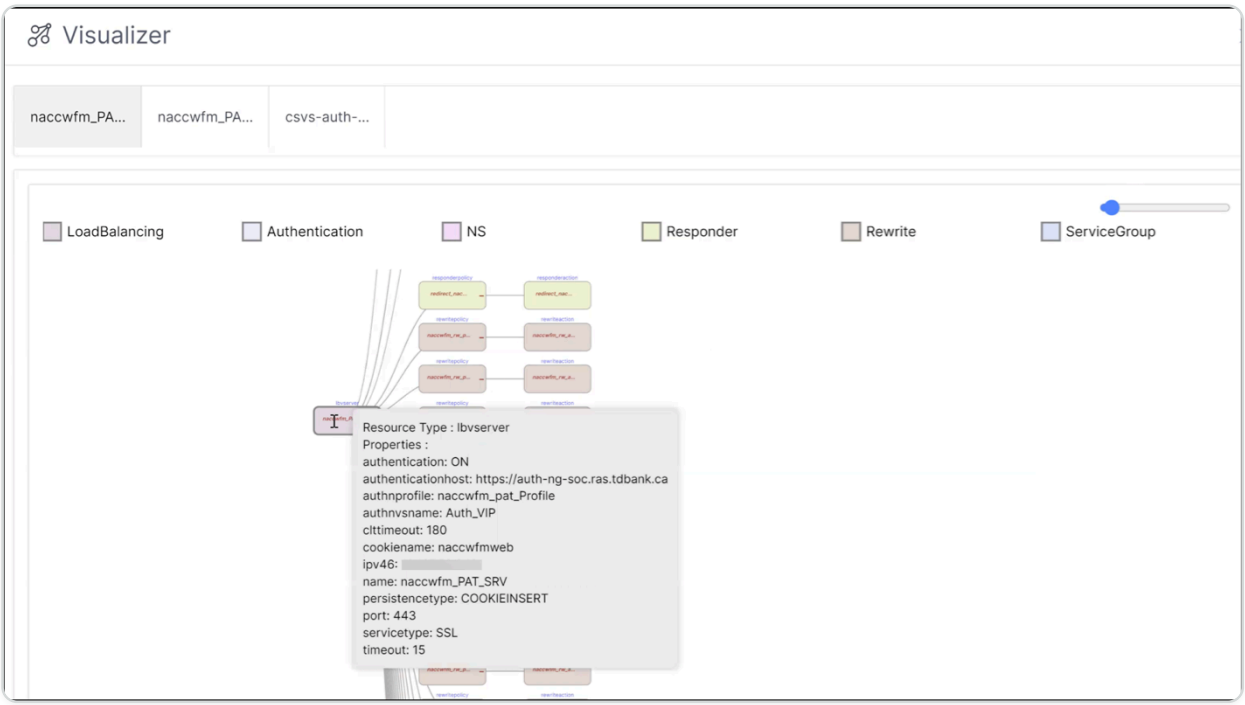
   a. 在“**应用程序名称**”中，指定应用程序的名称。

   b. 选择要迁移的虚拟服务器。

   c. 单击 **下一步**。

7. 在 **应用程序配置** 中，查看应用程序的命令。这些命令特定于所选的应用程序配置。

   启用 **可视化工具** 以查看应用程序配置及其关联的实体。可视化工具允许您查看不同组件的连接方式，并有助于您在迁移过程中进行理解和决策。



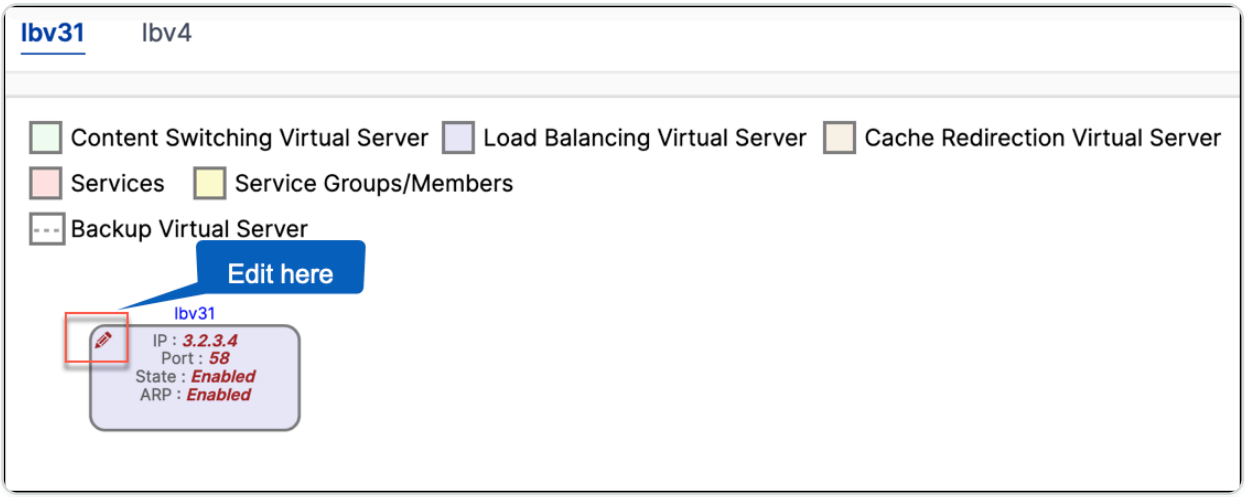
使用可视化工具，您可以：

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

- 查看与服务器关联的操作和策略的层次结构
- 将鼠标悬停在服务器上，以获取服务器的详细描述，包括绑定到服务器的策略和操作
- 使用缩放滑块放大和缩小视图
- 通过单击实体上的减号 (-) 或加号 (+) 符号来折叠或展开层次结构

单击 **下一步**。

8. 在 **应用程序部署信息** 中，您可以查看和编辑虚拟服务器、服务和服务组成员的 IP 地址、端口、状态和 ARP。



在 **详细信息** 页面中，您可以编辑 NSIP 实体的 IP 地址、端口、状态和 ARP 状态。

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

注意：

- 虚拟服务器 IP 的 NSIP 实体状态决定了 ARP 的初始状态。
- 如果虚拟服务器 IP 的 NSIP 实体已在目标 NetScaler 上配置，则无法修改虚拟服务器的 ARP 状态。
- 修改虚拟服务器的 ARP 状态会更改所有具有相同 IP 地址的虚拟服务器的 ARP 状态。修改虚拟服务器的状态仅影响关联的虚拟服务器。
- ARP 不适用于基于 IP 模式的虚拟服务器。
- 如果源配置中虚拟服务器 IP 的 NSIP 状态已禁用，则 ARP 也会自动禁用，并且您无法修改 ARP。

如果源实例和目标实例相同，则不会显示“**应用程序部署信息**”选项卡。

9. 在“**身份验证/网络部署信息**”中，您可以查看和编辑身份验证服务器和网络配置文件的属性（如果可用）。

   a. 在“**身份验证部署信息**”中，选择所需的身份验证服务器，并编辑服务器的 IP 地址、服务器 IP、服务器名称和端口号。

   b. 在“**网络配置文件信息**”中，选择所需的网络配置文件，并编辑“**网络配置文件**”和“**IPSET**”详细信息。

   注意：

   此步骤中进行的 NSIP 地址更改将用于最终迁移，并且会更新上一步中的配置以反映这些更改。

10. 在“**资源文件/密钥**”中，上传用于解密密码和证书的证书和密钥。单击“**下一步**”。
11. 在“**全局配置**”中，查看源和目标之间的全局配置设置差异。查看要应用于目标的配置并选择确认。单击“**下一步**”。
12. 在“**迁移**”中，查看 StyleBook 详细信息。单击“**迁移**”。

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

注意：

默认情况下，NetScaler Console 管理在将应用程序或虚拟服务器迁移到 NetScaler 时创建的配置包。如果您不想将配置包与生成的配置关联，请清除**通过 NetScaler Console 管理配置**复选框。

13. 在**不支持的配置**中，查看任何遗漏或不支持的配置。要成功迁移这些配置，您必须在目标实例上单独应用遗漏或不支持的配置。单击**下一步**。

限制

- 源实例中提及的命名表达式和 `responderhtmlpages` 未被识别。请确保在迁移之前在目标实例上配置命名表达式和 `responderhtmlpages`。
- 如果源具有 `servicegroup` 的配置和监视器绑定，如下所示：

  `bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>`

  出现以下错误：

  ```
  CLI Command conversion failed: 100 - No such command [{ "errorcode":
  1090, "message": "No such argument [XXX]", "severity": "ERROR" }]
  ```

  出现此错误是因为 NetScaler 以无效格式保存服务组和监视器之间的绑定。此问题已在 NetScaler 12.1.52.15 版本中修复。

业务应用程序样式书

NetScaler Console 提供样式书，可帮助您部署用于特定业务应用程序的 NetScaler 配置。有关此类样式书的更多信息，请参阅以下主题：

- SSO Google Apps 样式书
- SSO Office 365 样式书
- 微软 Skype 企业版 样式书
- Microsoft Exchange 样式书
- Microsoft SharePoint 样式书
- Microsoft ADFS 代理样式书
- Oracle 电子商务样式书

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

SSO Google 应用样式簿

Google Apps 是由 Google 开发的云计算、生产力与协作工具、软件和产品的集合。单点登录 (SSO) 允许用户使用其企业凭据一次性登录所有服务，从而访问其所有企业云应用程序，包括管理员登录到管理控制台。

NetScaler Console SSO Google Apps StyleBook 允许您通过 NetScaler 实例为 Google Apps 启用 SSO。此 StyleBook 将 NetScaler 实例配置为 SAML 身份提供程序，用于对访问 Google Apps 的用户进行身份验证。

使用此 StyleBook 在 NetScaler 实例中为 Google 应用启用 SSO 会执行以下步骤：

1. 配置身份验证虚拟服务器
2. 配置 SAML IdP 策略和配置文件
3. 将策略和配置文件绑定到身份验证虚拟服务器
4. 在实例上配置 LDAP 身份验证服务器和策略
5. 将 LDAP 身份验证服务器和策略绑定到在实例上配置的身份验证虚拟服务器

配置详细信息：

下表列出了此集成成功运行所需的最低软件版本。此集成过程也支持更高版本。

产品	最低要求版本
NetScaler	版本 11.0，高级/高级版许可证

以下说明假定您已创建了适当的外部或内部 DNS 条目，以将身份验证请求路由到 NetScaler 监控的 IP 地址。

部署 SSO Google 应用 StyleBook 配置：

以下任务可帮助您在业务网络中部署 Microsoft SSO Google Apps StyleBook。

部署 SSO Google 应用 StyleBook

1. 在 NetScaler Console 中，导航到 **Applications** > **Configurations** > **StyleBooks**。StyleBooks 页面显示了 NetScaler Console 中所有可用的 StyleBook。向下滚动并找到 **SSO Google Apps StyleBook**。单击 **Create Configuration**。
2. StyleBook 将作为用户界面页面打开，您可以在其中输入此 StyleBook 中定义的所有参数的值。
3. 输入以下参数的值：

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

a. **应用程序名称**。要在您的网络中部署的 SSO Google 应用配置的名称。

b. **身份验证虚拟 IP 地址**。身份验证、授权和审计虚拟服务器使用的虚拟 IP 地址，Google 应用 SAML IdP 策略绑定到该虚拟服务器。

c. **SAML 规则表达式**。默认情况下，使用以下 NetScaler 策略 (PI) 表达式：HTTP.REQ.HEADER("Referrer").CONTAINS("google")。如果您的要求不同，请使用其他表达式更新此字段。此策略表达式匹配应用这些 SAML SSO 设置的流量，并确保 Referrer 标头来自 Google 域。

4. SAML IdP 设置部分允许您通过创建在步骤 3 中创建的身份验证、授权和审计虚拟服务器使用的 SAML IdP 配置文件和策略，将您的 NetScaler 实例配置为 SAML 身份提供程序。

a. **SAML 颁发者名称**。在此字段中，输入您的身份验证虚拟服务器的公共 FQDN。示例：`https://<NetScaler Auth VIP>/saml/login`

b. **SAML 服务提供商 (SP) ID**。（可选）NetScaler 身份提供程序接受来自与此 ID 匹配的颁发者名称的 SAML 身份验证请求。

c. **断言消费者服务 URL**。输入服务提供商的 URL，NetScaler 身份提供程序在用户成功身份验证后需要将 SAML 断言发送到该 URL。断言消费者服务 URL 可以在身份提供程序服务器站点或服务提供商站点启动。

d. 本节中还有其他可选字段可供您输入。例如，您可以设置以下选项：

i. SAML 绑定配置文件（默认为“POST”配置文件）。

ii. 用于验证/签署 SAML 请求/响应的签名算法（默认为“RSA-SHA1”）。

iii. 用于对 SAML 请求/响应进行哈希摘要的方法（默认为“SHA-1”）。

iv. 加密算法（默认为 AES256）和其他设置。

> **注意**
>
> 我们建议您保留默认设置，因为这些设置已经过测试，与 Google Apps 兼容。

e. 您还可以启用“用户属性”复选框以输入用户详细信息，例如：

i. 用户属性的名称

ii. 用于评估以提取属性值的 NetScaler PI 表达式

iii. 属性的用户友好名称

iv. 选择用户属性的格式。

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

这些值包含在颁发的 SAML 断言中。您可以使用此 StyleBook 在 NetScaler 颁发的断言中包含最多五组用户属性。

5. 在“LDAP 设置”部分中，输入以下详细信息以对 Google Apps 用户进行身份验证。为了使域用户能够使用其公司电子邮件地址登录 NetScaler 实例，您必须配置以下内容：

   a. **LDAP (Active Directory) 基本 DN**。输入要允许身份验证的 Active Directory (AD) 中用户帐户所在域的基本域名。例如，`dc=netscaler`, `dc=com`

   b. **LDAP (Active Directory) 绑定 DN**。添加一个具有浏览 AD 树权限的域帐户（为便于配置，请使用电子邮件地址）。例如，`cn=Manager,dc=netscaler,dc=com`

   c. **LDAP (Active Directory) 绑定 DN 密码**。输入用于身份验证的域帐户密码。

   d. 您需要在此部分输入的其他一些字段如下：

      i. NetScaler 用于用户身份验证的 LDAP 服务器 IP 地址

      ii. LDAP 服务器的 FQDN 名称

      > **注意**
      >
      > 您必须指定上述两者中的至少一个 - 即 LDAP 服务器 IP 地址或 FQDN 名称。

      iii. NetScaler 用于用户身份验证的 LDAP 服务器端口（默认为 389）。

      iv. LDAP 主机名。如果启用了验证（默认情况下已禁用），则此项用于验证 LDAP 证书。

      v. LDAP 登录名属性。用于提取登录名的默认属性是“sAMAccountName”。

      vi. 其他可选的杂项 LDAP 设置

6. 在 SAML IdP SSL 证书部分，您可以指定 SSL 证书的详细信息：

   a. **证书名称**。输入 SSL 证书的名称。

   b. **证书文件**。从本地系统或 NetScaler Console 上的目录中选择 SSL 证书文件。

   c. **证书密钥格式**。从下拉列表中选择证书和私钥文件的格式。支持的格式为 .pem 和 .der 扩展名。

   d. **证书密钥名称**。输入证书私钥的名称。

   e. **证书密钥文件**。从本地系统或 NetScaler Console 中选择包含证书私钥的文件。

   f. **私钥密码**。如果您的私钥文件受密码保护，请在此字段中输入密码。

   g. 您还可以启用“高级证书设置”复选框，以输入证书过期通知期、启用或禁用证书过期监视器等详细信息。

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

7. （可选）如果上面输入的 SAML IdP 证书需要在 NetScaler 上安装 CA 公共证书，则可以选择 IdP SSL CA 证书。请确保在高级设置中选择“是 CA 证书”。
8. （可选）您可以选择 SAML SP SSL 证书来指定用于验证来自 Google Apps (SAML SP) 的身份验证请求的 Google SSL 证书（公钥）。
9. 单击**目标实例**，然后选择要部署此 Google Apps SSO 配置的 NetScaler 实例。单击**创建**以创建配置并在选定的 NetScaler 实例上部署配置。

> **注意**
>
> 您还可以单击刷新图标，将 NetScaler Console 中最近发现的 NetScaler 实例添加到此窗口中的可用实例列表中。

此外，

> **提示**
>
> 我们建议，在运行实际配置之前，您选择**试运行**，以直观地确认 StyleBook 在目标 NetScaler 实例上创建的配置对象。

SSO Office 365 样式簿

Microsoft Office 365 是一套基于云的生产力和协作应用程序，由 Microsoft 以订阅方式提供。它包括 Microsoft 热门的基于服务器的应用程序，例如 Exchange、SharePoint、Office 和 Skype for Business。单点登录 (SSO) 使户能够访问其所有企业云应用程序：

- 包括登录到管理控制台的管理员
- 使用其企业凭据一次性登录所有 Microsoft Office 365 服务。

SSO Office 365 StyleBook 允许您通过 NetScaler 实例为 Microsoft Office 365 启用 SSO。您现在可以将 NetScaler 配置为 SAML 身份提供程序 (IdP)，将 Microsoft Office 365 配置为 SAML 服务提供程序，从而配置 SAML 身份验证。

使用此 StyleBook 在 NetScaler 实例中为 Microsoft Office 365 启用 SSO 涉及以下步骤：

1. 配置身份验证虚拟服务器
2. 配置 SAML IDP 策略和配置文件
3. 将策略和配置文件绑定到身份验证虚拟服务器
4. 在实例上配置 LDAP 身份验证服务器和策略

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

5. 将 LDAP 身份验证服务器和策略绑定到在实例上配置的身份验证虚拟服务器。

下表列出了此集成成功运行所需的最低软件版本。此集成过程也应适用于更高版本。

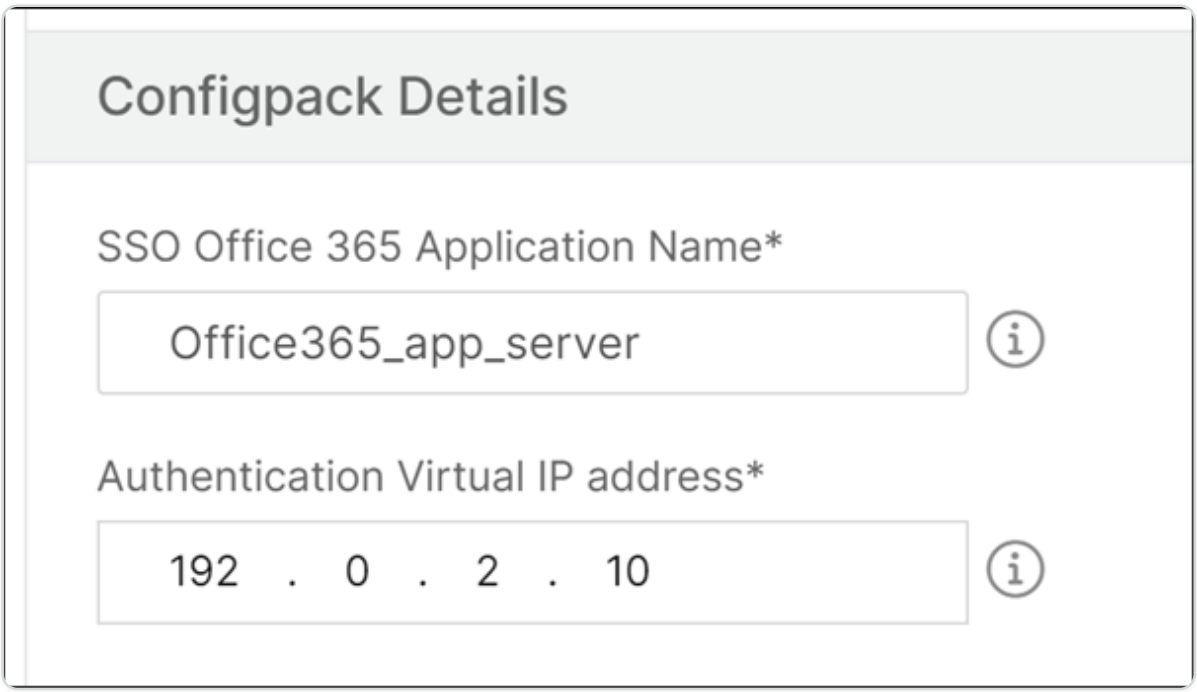
产品	最低要求版本
NetScaler	11.0，高级/高级版许可证

以下说明假定您已创建相应的外部和内部 DNS 条目。这些条目对于将身份验证请求路由到 NetScaler 监控的 IP 地址至关重要。

以下说明可帮助您在业务网络中实施 SSO Office 365 StyleBook。

部署 SSO Microsoft Office 365 样式簿

1. 在 NetScaler Console 中，导航到 **应用程序** > **样式簿**。**样式簿** 页面显示了 NetScaler Console 中所有可用的样式簿。向下滚动并找到 **SSO Office 365 样式簿**。单击 **创建配置**。
2. 样式簿将作为用户界面页面打开，您可以在其中输入此样式簿中定义的所有参数的值。
3. 输入以下参数的值：
   a. **应用程序名称**。要在您的网络中部署的 SSO Microsoft Office 365 配置的名称。
   b. **身份验证虚拟 IP 地址**。AAA 虚拟服务器将使用的虚拟 IP 地址，Microsoft Office 365 SAML IdP 策略将绑定到该虚拟服务器。



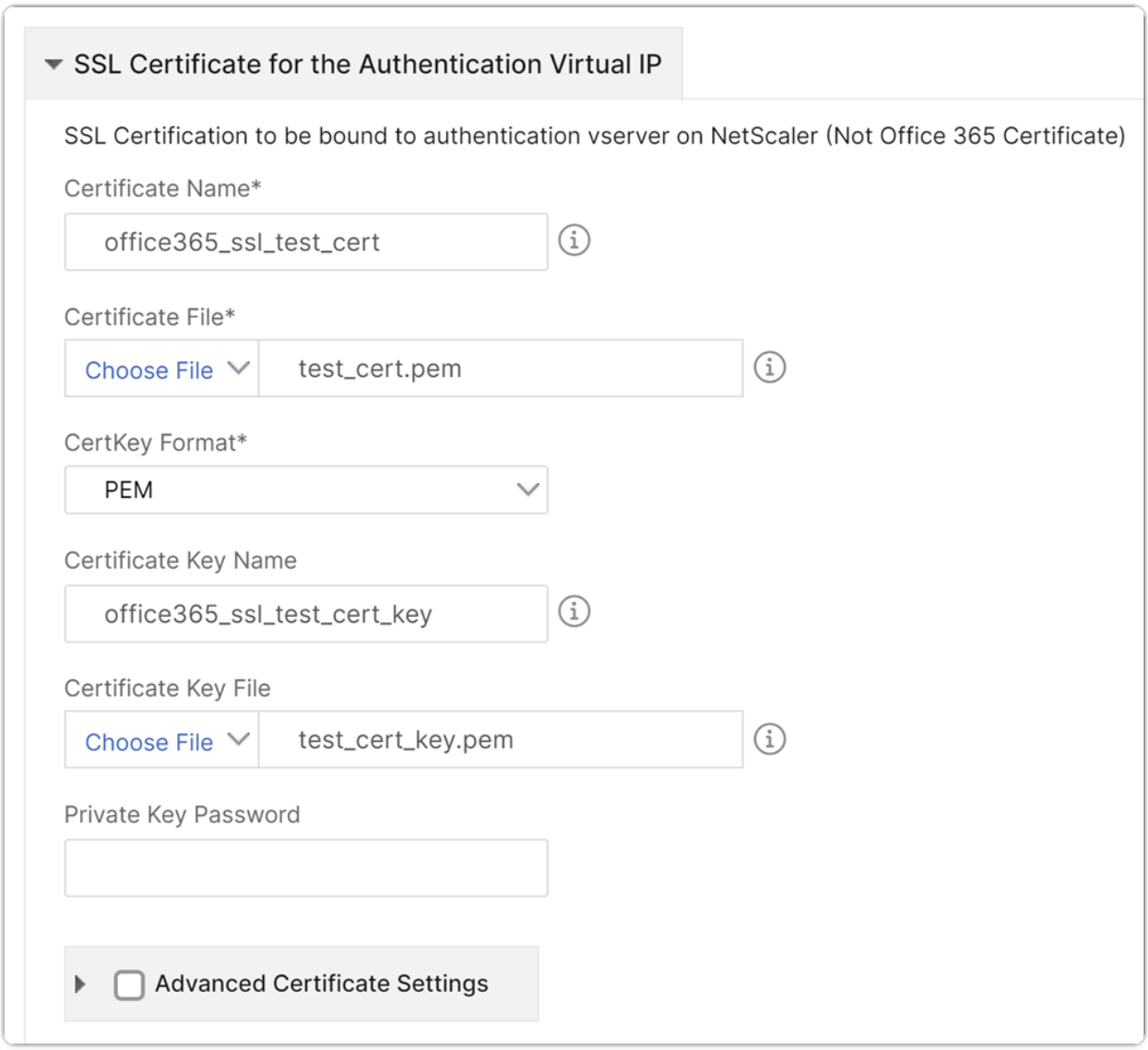
4. 在 **SSL 证书 设置** 部分中，输入 SSL 证书和证书密钥的名称。

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

注意

这不是 Office 365 服务提供商证书。此 SSL 证书绑定到 NetScaler 实例上的虚拟身份验证服务器。

5. 从本地存储文件夹中选择相应的文件。您还可以输入私钥密码以加载 PEM 格式的加密私钥。



6. 您还可以启用 **高级证书设置** 复选框。在此处，您可以输入证书过期通知期限、启用或禁用证书过期监视器等详细信息。
7. 如果 SSL 证书需要在 NetScaler 上安装 CA 公共证书，您可以选择 **用于身份验证虚拟 IP 的 SSL CA 证书** 复选框。请确保在上述 **高级证书设置** 部分中选择“是 CA 证书”。
8. 在 **SSO Office 365 的 LDAP 设置** 部分中，输入以下详细信息以对 Office 365 用户进行身份验证。要允许域用户使用其公司电子邮件地址登录到 NetScaler 实例，请配置以下内容：

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

- **LDAP (Active Directory) 基本**。输入用户帐户在 Active Directory (AD) 中所在的域的基本域名以允许身份验证。例如，dc=netscaler®,dc=com
- **LDAP (Active Directory) 绑定 DN**。添加一个域帐户（为便于配置，请使用电子邮件地址），该帐户具有浏览 AD 树的权限。例如，cn=Manager,dc=netscaler,dc=com
- **LDAP (Active Directory) 绑定 DN 密码**。输入用于身份验证的域帐户密码。
- 您需要在此部分中输入的其他一些字段如下：
  - NetScaler 用于对用户进行身份验证的 LDAP 服务器 IP 地址。
  - LDAP 服务器的 FQDN 名称。

    注意

    您必须指定上述两者中的至少一个 - LDAP 服务器 IP 地址或 FQDN 名称。

  - NetScaler 用于对用户进行身份验证的 LDAP 服务器端口（默认为 389）。LDAPS 使用 636。
  - LDAP 主机名。如果启用了验证（默认情况下处于关闭状态），则主机名用于验证 LDAP 证书。
  - LDAP 登录名属性。用于提取登录名的默认属性是“samAccountname”。
  - 其他可选的杂项 LDAP 设置。

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

Active Directory (LDAP) Settings for SSO Office 365

LDAP Settings for SSO Office 365

LDAP (Active Directory) Base*

dc=netscaler,dc=com

LDAP (Active Directory) Bind DN*

cn=Manager,dc=netscaler,dc=con

LDAP (Active Directory) Bind DN Password*

•••••

LDAP Server (Active Direcory) IP

192 . 0 . 2 . 10

LDAP Server FQDN name

LDAP Server (Active Directory) Port

389

LDAP Host name

office365_ldap_hostname

☐ Active Directory LDAP

☐ Validate LDAP Certificate

LDAP (Active Directory) Login username

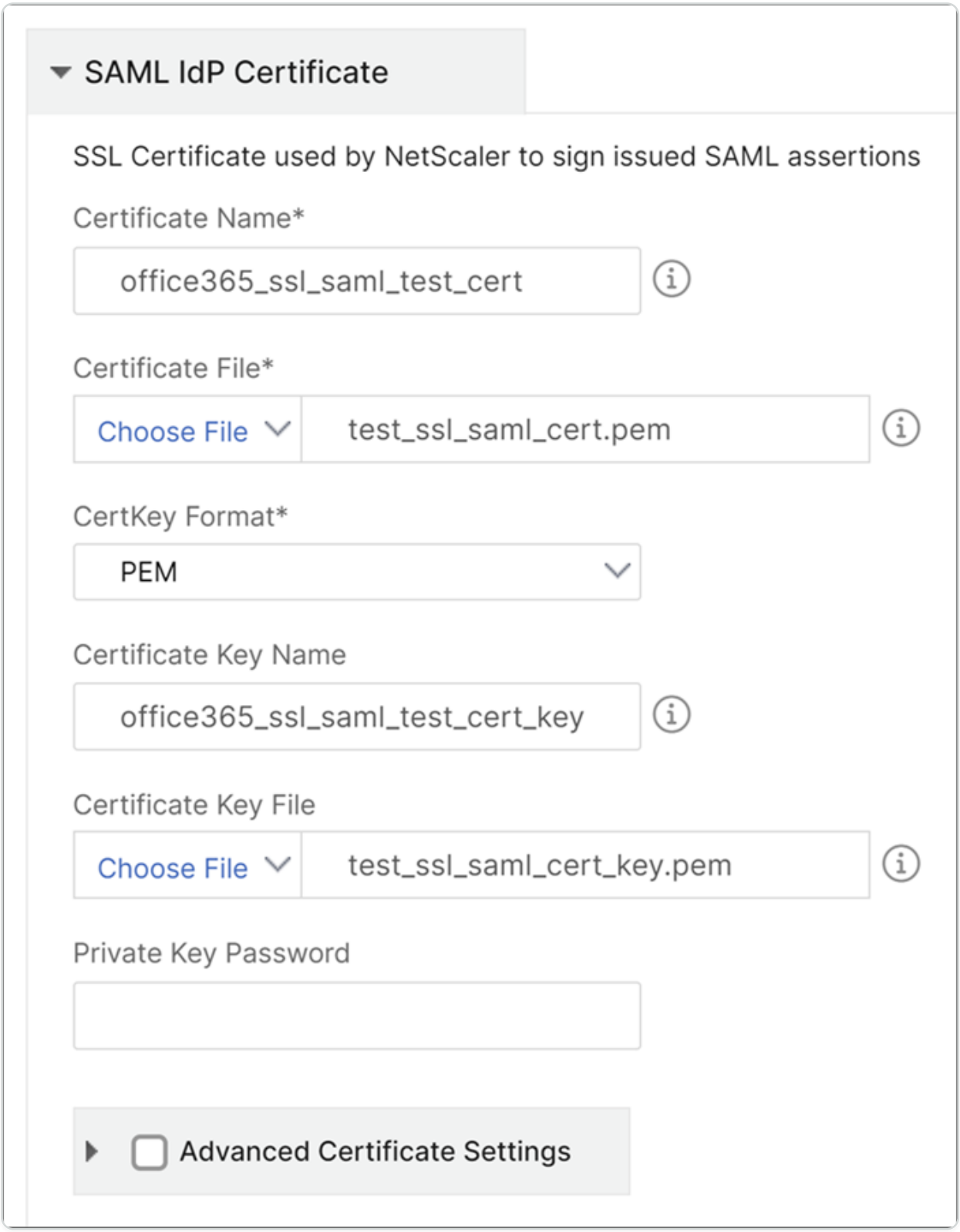
samAccountname

9. 在**SAML IdP 证书**部分中，您可以指定用于 SAML 断言的 SSL 证书的详细信息。

   - **证书名称**。输入 SSL 证书的名称。
   - **证书文件**。从本地系统上的目录中选择 SSL 证书文件。
   - **证书密钥格式**。从下拉列表框中选择证书和私钥文件的格式。支持的格式为 .pem 和 .der 文件扩展名。
   - **证书密钥名称**。输入证书私钥的名称。
   - **证书密钥文件**。从本地系统中选择包含证书私钥的文件。
   - **私钥密码**。输入保护私钥文件的密码。

   您还可以启用**高级证书设置**复选框。在此处，您可以输入证书过期通知期限、启用或禁用证书过期监视器等详细信息。

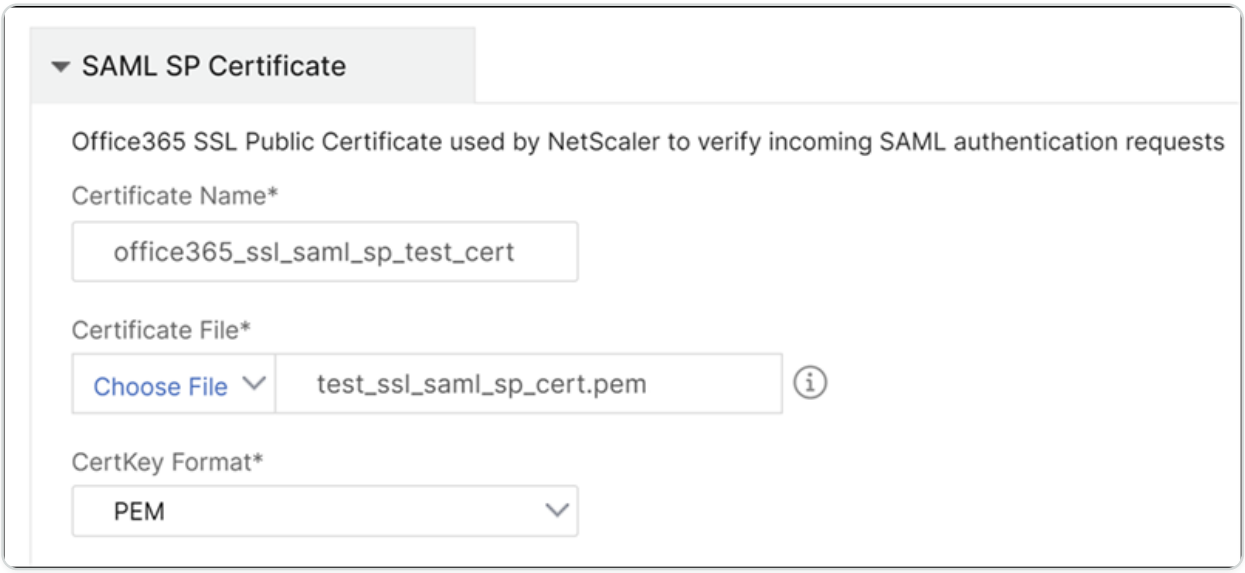
© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. 如果上面输入的 SAML IdP 证书需要在 NetScaler 上安装 CA 公共证书，则可以选择 **SAML IdP CA 证书**。请确保在上述**高级证书设置**部分中选择**是 CA 证书**。
11. 在**SAML SP 证书**部分中，输入 Office 365 SSL 公共证书的以下详细信息。此证书由 NetScaler 实例用于验证传入的 SAML 身份验证请求。
    - **证书名称**。键入 SSL 证书的名称。

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

- **证书文件**。从本地系统上的目录中选择 SSL 证书文件。
- **证书密钥格式**。从下拉列表框中选择证书和私钥文件的格式。支持的格式为 .pem 和 .der 文件扩展名。
- 您还可以启用**高级证书设置**复选框。在此处，您可以输入证书过期通知期限、启用或禁用证书过期监视器等详细信息。



12. **SAML Idp 设置**部分允许您通过创建步骤 3 中 AAA 虚拟服务器使用的 SAML IDP 配置文件和策略，将 NetScaler 实例配置为 SAML 身份提供程序。

    - **SAML 颁发者名称**。在此字段中，键入身份验证虚拟服务器的公共 FQDN。示例：`https://<NetScaler Auth VIP>/saml/login`
    - **名称标识符表达式**。键入用于提取 SAML 断言中发送的 SAML NameIdentifier 的 NetScaler 表达式。示例：`"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`
    - **签名算法**：选择用于验证/签名 SAML 请求/响应的算法（默认为“RSA-SHA256”）。
    - **摘要方法**。选择用于对 SAML 请求/响应进行哈希摘要的方法（默认为“SHA256”）。
    - **受众名称**。键入表示服务提供商的实体名称或 URL (Microsoft Office 365)。
    - **SAML 服务提供商 (SP) ID**。（可选）NetScaler 身份提供商接受来自与此 ID 匹配的颁发者名称的 SAML 身份验证请求。
    - **断言使用者服务 URL**。输入服务提供商的 URL，NetScaler 身份提供商需要在用户成功身份验证后将 SAML 断言发送到该 URL。断言使用者服务 URL 可以在身份提供商服务器站点或服务提供商站点启动。
    - 本节中还有其他可选字段可供输入。例如，您可以设置以下选项：
        - **SAML 属性名称**。SAML 断言中发送的用户属性的名称。
        - **SAML 属性友好名称**。SAML 断言中发送的用户属性的友好名称。

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

- **SAML 属性的 PI 表达式**。默认情况下，使用以下 NetScaler 策略 (PI) 表达式：HTTP.REQ.USER.ATTRIBUTE(1)。此字段将从 LDAP 服务器发送的第一个用户属性（邮件）指定为 SAML 身份验证属性。
- 选择用户属性的格式。

这些值包含在颁发的 SAML 断言中。

提示

建议您保留默认设置，因为这些设置已经过测试，可与 Microsoft Office 365 应用程序配合使用。

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

Saml issuer name

https://nssaml.citrix.com/saml/log

Name Identifier Expression

HTTP.REQ.USER.ATTRIBUTE(2).B6

Signature Algorithm

RSA-SHA256

Digest Method

SHA256

Audience name or url

urn:federation:MicrosoftOnline

☐ Option to Reject unsigned SAML Requests

SAML Attribute Name

IDPEmail

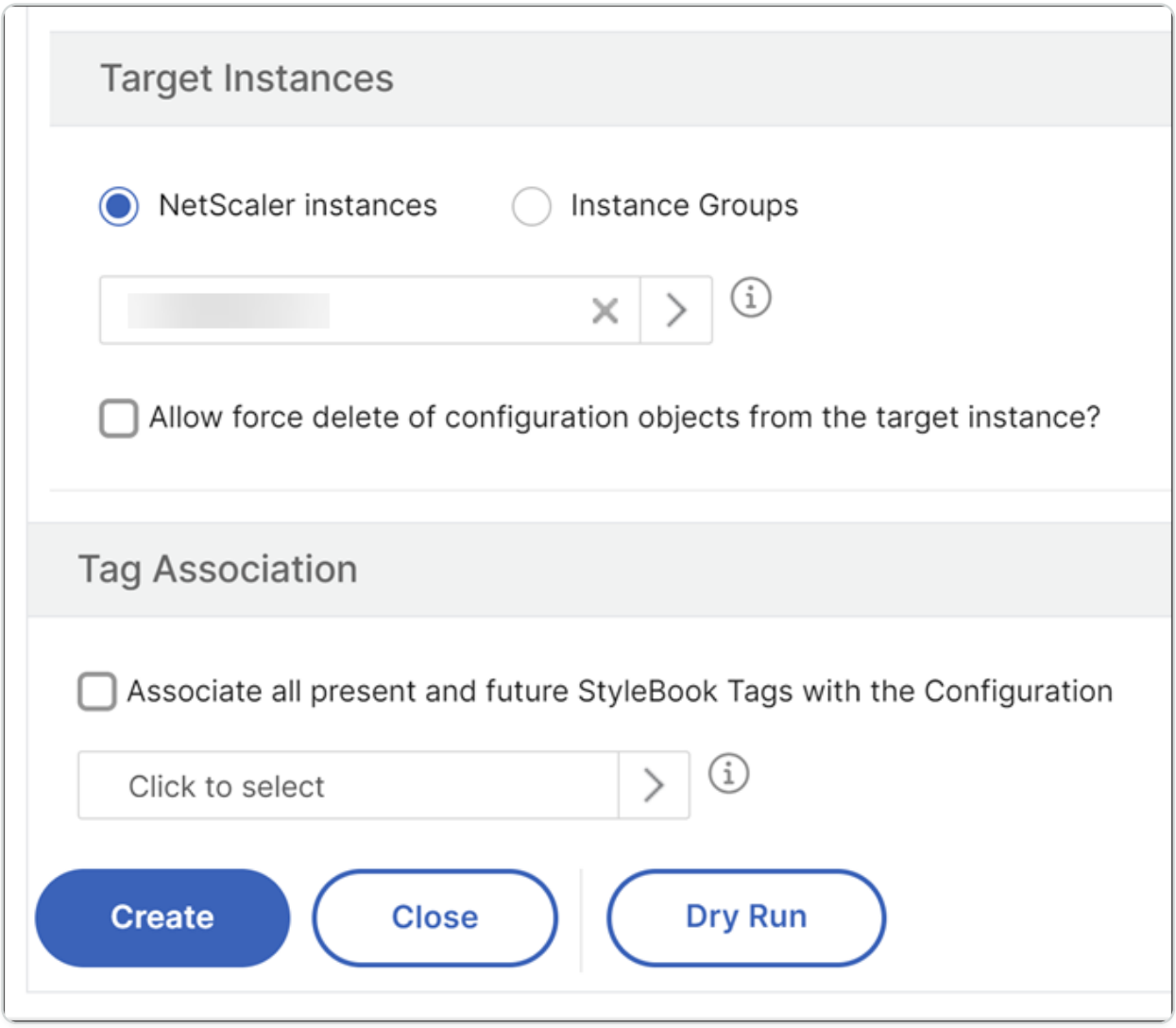
SAML Attribute Friendly Name

UserID

PI Expression for SAML Attribute

HTTP.REQ.USER.ATTRIBUTE(1)

13. 单击 **目标实例** 并选择要部署此 Microsoft Office 365 SSO 配置的 NetScaler 实例。单击 **创建** 以创建配置并在所选 NetScaler 实例上部署配置。



提示

我们建议在执行实际配置之前，选择**试运行**以查看 StyleBook 在目标 NetScaler 实例上创建的配置对象。

微软商务版 Skype 样式簿

Skype for Business 2015 应用程序依赖于多个外部组件才能运行。Skype for Business 网络由各种系统组成，例如服务器及其操作系统、数据库、身份验证和授权系统、网络系统和基础设施以及电话 PBX 系统。Skype for Business Server 2015 有两个版本：标准版和企业版。主要区别在于对高可用性功能的支持，这些功能仅包含在企业版中。为了实现高可用性，必须将多个前端服务器部署到池中，并且必须对 SQL 服务器进行镜像。

企业版部署能够创建具有不同角色的多个服务器。

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

主要组件

Skype for Business 2015 应用程序中的主要组件包括：

- 前端服务器
- 边缘服务器
- 导播服务器
- 数据库 (SQL) 服务器

前端服务器

在 Skype for Business 应用程序中，前端服务器是您网络中的核心服务器。它提供用户身份验证、注册、在线状态、地址簿、音视频会议、应用程序共享、即时消息和 Web 会议的链接和服务。如果您正在部署 Skype for Business 2015 企业版，则拓扑通常由至少两个前端服务器组成，这些服务器在前端池中进行负载均衡，并带有一个数据库服务器，该服务器托管着包含 Skype for Business 数据库的 SQL Server 实例。

边缘服务器

如果未登录到您组织内部网络的外部用户需要能够与内部用户进行交互，则需要部署 Skype for Business 的边缘服务器。这些外部用户可以是经过身份验证的匿名远程用户、联合合作伙伴或其他移动客户端。

Skype For Business 边缘服务器中有四种类型的角色：

- 访问边缘，它处理 SIP 流量并验证外部连接，允许远程连接并允许联合连接
- Web 会议，处理数据会议包，并允许外部用户访问 Skype for Business
- A/V 会议，处理 A/V 会议包，并将音频和视频、应用程序共享和文件传输扩展到外部用户
- XMPP 代理，处理 XMPP 包，并允许基于 XMPP 的服务器或客户端连接到 Skype for Business。

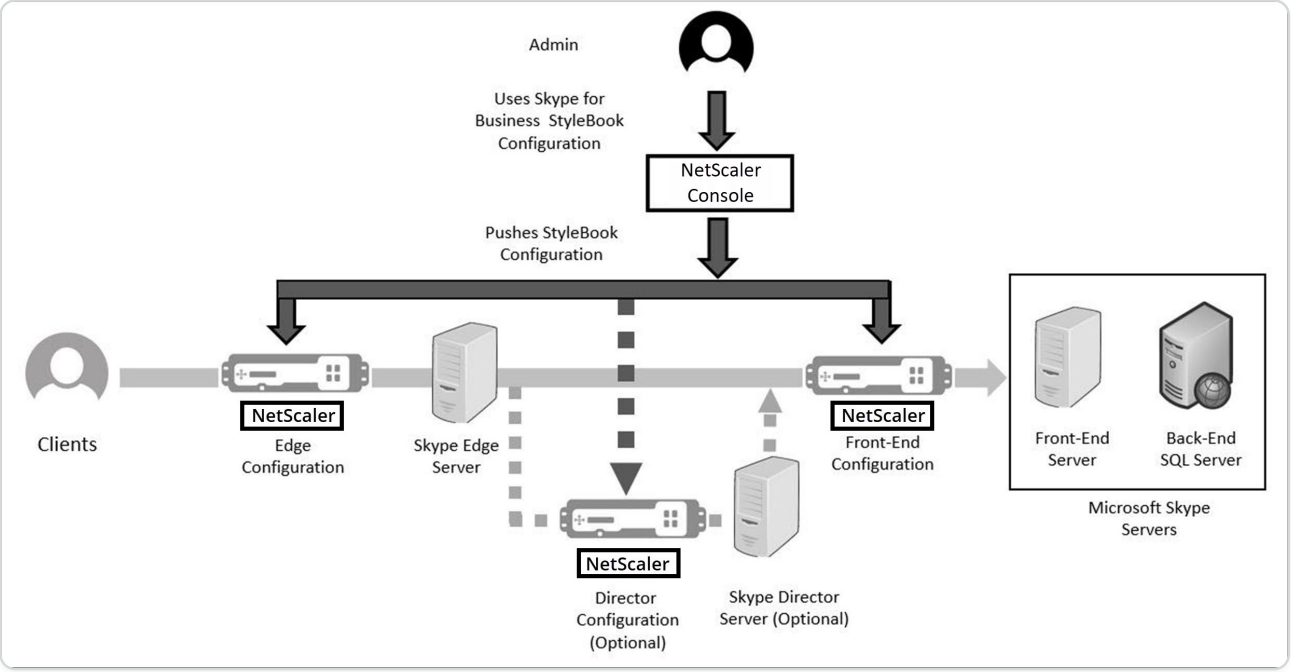
Director 服务器

Director 服务器在 Skype for Business 2015 中的主要功能是验证端点并将用户“引导”到包含其帐户的池中。在 Skype for Business 2015 中，尽管 Director 是独立服务器上一个完全专用且特定的角色，但它是一个可选服务器。这通过简化配置的部署或删除来增强安全性。

当存在多个池时，Director 最有用，因为它们为验证端点提供了单一联系点。此外，对于远程用户，Director 在 Edge 池和 Front-End 池之间充当额外的跳点，增加了额外的攻击防护层。

下图以图示方式表示网络中 Skype 服务器的部署：

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



在企业中配置 NetScaler 实例

下表列出了以下说明中包含的示例配置中使用的 IP 地址：

SKYPE FOR BUSINESS 服务器	虚拟 IP 地址	服务器 IP 地址	NETSCALER 实例
Edge 服务器	外部 VIP - 192.20.20.20	192.20.20.21; 192.20.20.22	10.102.29.141
	内部 VIP - 10.10.10.20	10.10.10.21; 10.10.10.22	
前端服务器	10.10.10.10	10.10.10.11; 10.10.10.12	10.102.29.60
总监服务器	10.10.10.30	10.10.10.31; 10.10.10.32	10.102.29.93

配置前端服务器

1. 在 NetScaler Console 中，导航到“**应用程序**”>“**配置**”，然后单击“**新建**”。“**选择样式簿**”页面显示 NetScaler Console 中可供使用的所有样式簿。向下滚动并选择“**Microsoft Skype for Business 2015 样式簿**”。样式簿将作为用户界面页面打开，您可以在其中输入此样式簿中定义的所有参数的值。
2. 在**边缘服务器**部分，输入以下虚拟 IP (VIP) 地址以及网络中所有边缘服务器的 IP 地址。

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

a. 外部 VIP 地址和 IP 地址，用于将用于访问边缘、Web 会议边缘和 A/V 边缘的边缘服务器。

b. 内部 VIP 地址和 IP 地址，用于将连接到内部网络的边缘服务器。

c. 您的网络中有两个外部边缘服务器和两个内部边缘服务器。

3. 在**前端服务器**部分，输入将为 Skype for Business 前端服务器创建的虚拟前端服务器 (VIP) 的 IP 地址。此外，输入网络中所有 Skype for Business 前端服务器的 IP 地址。
4. 在**导播服务器**部分，输入将为 Skype for Business 应用程序创建的导播服务器的虚拟 IP 地址 (VIP)。此外，输入网络中所有 Skype for Business 导播服务器的 IP 地址。创建至少两个导播服务器以实现高可用性。
5. **高级设置**部分列出了在 NetScaler 实例上为三个 Skype 服务器配置的所有默认端口。

下表提供了所有默认端口和协议的列表：

标签	端口	协议	描述
HTTP 端口	80	HTTP	当不使用 HTTPS 时，用于从前端服务器到 Web 场 FQDN 的通信。
HTTPS 端口	443	HTTPS	用于从前端服务器到 Web 场 FQDN 的通信。
AutoDiscover 内部端口	4443	HTTPS	用于 AutoDiscover 登录的 HTTPS（来自反向代理）和 HTTPS 前端池间通信。
RPC 端口	135	DCOM 和远程过程调用 (RPC)	用于基于 DCOM 的操作，例如移动用户、用户复制器同步和地址簿同步。
SIP 端口	5061	TCP (TLS)	供前端服务器用于所有内部 SIP 通信。
SIP 焦点端口	444	HTTPS, TCP	用于焦点（管理 Skype 会议状态的组

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

标签	端口	协议	描述
			件）与各个服务器之间的 HTTPS 通信。
SIP 组端口	5071	TCP	用于响应组应用程序的传入 SIP 请求。
SIP 应用程序共享端口	5065	TCP	用于应用程序共享的传入 SIP 侦听请求。
SIP 助理端口	5072	TCP	用于服务员的传入 SIP 请求（即用于拨入式会议）。
SIP 会议公告端口	5073	TCP	用于 Skype for Business 服务器会议公告服务的传入 SIP 请求（即用于拨入式会议）。
SIP 呼叫驻留端口	5075	TCP	用于呼叫驻留应用程序的传入 SIP 请求。
SIP 呼叫准入端口	448	TCP	由 Skype for Business 服务器带宽策略服务用于呼叫准入控制。
SIP 呼叫准入 TURN 端口	5080	TCP	由带宽策略服务用于音频/视频边缘 TURN 流量的呼叫准入控制。
SIP 音频测试端口	5076	TCP	用于音频测试服务的传入 SIP 请求。
HTTPS 外部端口	443	HTTPS	用于远程用户访问的 SIP/TLS 通信、访问内部 Web 会议以及用于访问内部媒体和 A/V 会话的 STUN/

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

标签	端口	协议	描述
			TCP 入站和出站媒体通信的外部端口。
HTTPS 内部端口	443	HTTPS	用于内部端口，实现远程用户访问的 SIP/TLS 通信、访问内部 Web 会议以及访问内部媒体和 A/V 会话的 STUN/TCP 入站和出站媒体通信。
SIP 外部远程访问端口	5061	TCP	用于外部端口，实现远程用户访问或联合的 SIP/MTLS 通信。
SIP 内部远程访问端口	5061	TCP	用于内部端口，实现远程用户访问或联合的 SIP/MTLS 通信。
SIP 外部 STUN UDP 端口	3478	UDP	用于外部端口，实现 STUN/UDP 入站和出站媒体通信。
SIP 内部 STUN UDP 端口	3478	UDP	用于 STUN/UDP 入站和出站媒体通信的内部端口。
SIP 内部即时消息端口	5062		用于通过内部防火墙出站的即时消息通信的 SIP/MTLS 身份验证的内部端口。
HTTP 端口	80	TCP	用于 Directors 与 Web 场 FQDN 之间的初始通信。
HTTPS 端口	443	HTTPS	用于 Directors 与 Web 场 FQDN 之间的通信。

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

标签	端口	协议	描述
自动发现内部端口	4443	HTTPS	用于 HTTPS（来自反向代理）和 HTTPS Director 池间通信以进行 AutoDiscover 登录。
SIP 内部端口	5061	TCP	用于服务器之间的内部通信和客户端连接。

6. 在“**目标实例**”部分中，选择要部署三个 Skype for Business 服务器的三个不同 NetScaler 实例。

注意

您还可以单击刷新图标，将 NetScaler Console 中最近发现的 NetScaler 实例添加到此窗口中可用的实例列表中。

7\. 单击**创建**以在选定的 NetScaler 实例上创建配置。

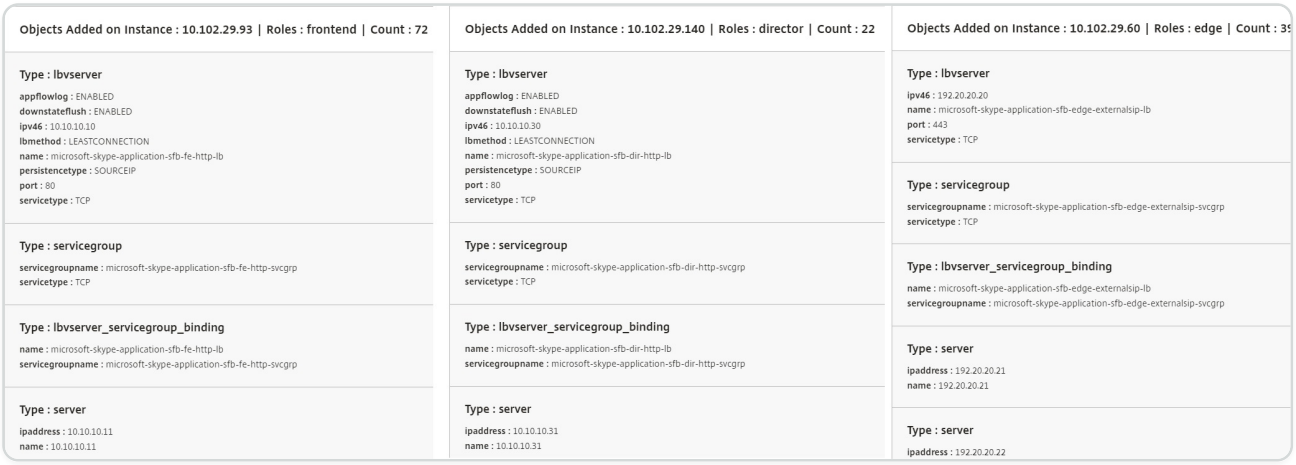
提示

建议您选择“**试运行**”以检查在实例上执行实际配置之前必须在目标实例上创建的配置对象。

成功创建配置后，StyleBook 将创建 25 个负载平衡虚拟服务器。也就是说，对于每个端口，都会定义一个负载平衡虚拟服务器以及一个服务组，并且该服务组绑定到负载平衡虚拟服务器。该配置还将前端服务器添加为服务组成员，并将其绑定到服务组。创建的服务组成员数量等于创建的前端服务器数量。

下图显示了在每个服务器中创建的对象：

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



Microsoft Exchange 样式簿

您可以使用 Microsoft Exchange 2016 StyleBook 部署 NetScaler 配置，以优化和保护网络中的 Microsoft Exchange 2016 企业应用程序。Microsoft Exchange 2016 是为您的员工和其他利益相关者提供电子邮件、个人信息管理和消息服务的关键企业应用程序。

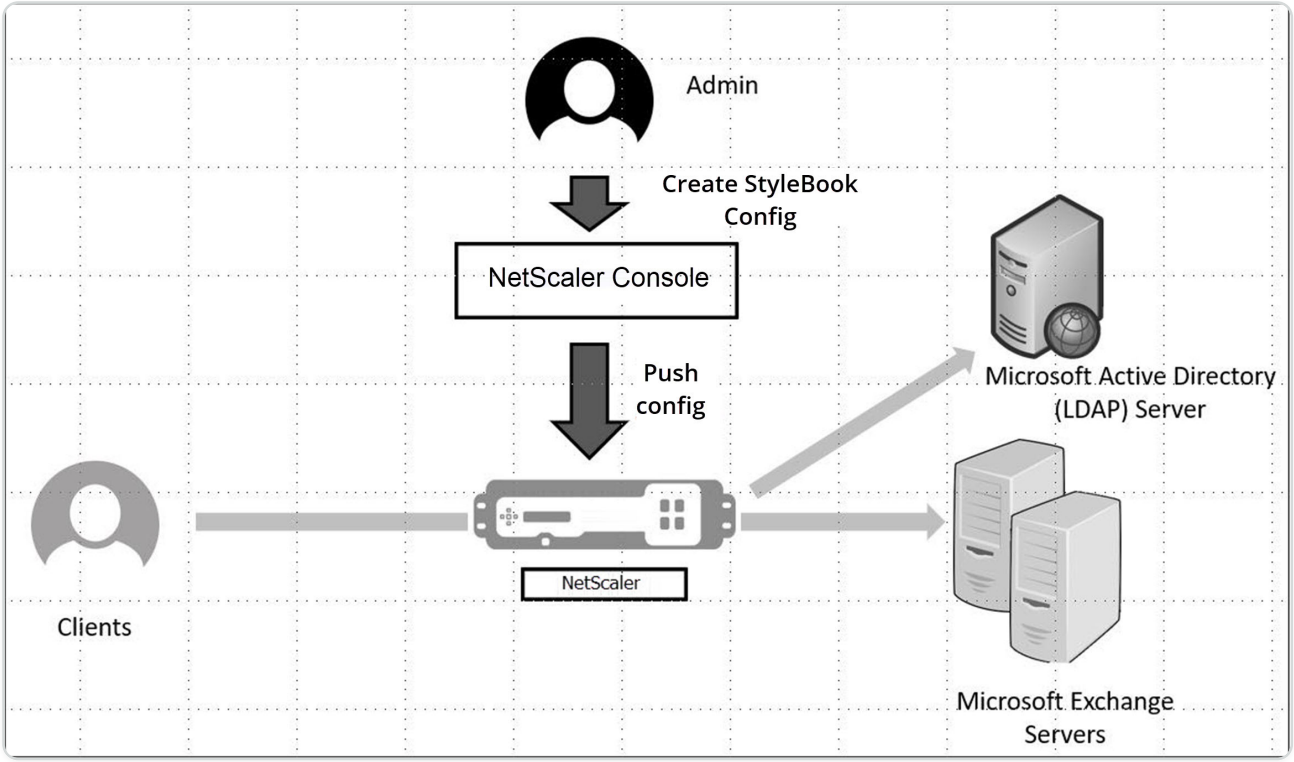
使用 Microsoft Exchange StyleBook 配置的 NetScaler 功能

Microsoft Exchange 2016 StyleBook 为 Microsoft Exchange 2016 服务器启用并配置以下 NetScaler 功能：

- 负载平衡 - 启用多个 Exchange 服务器负载平衡的基本负载平衡
- 内容切换 - 启用单 IP 访问并将查询重定向到正确的负载平衡虚拟服务器的内容切换
- 重写 - 将用户重定向到安全页面
- SSL 卸载 - 将 SSL 处理卸载到 NetScaler，从而减轻 Exchange 服务器的负载

下图以图表形式表示网络中 Exchange 服务器的部署：

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



先决条件

- 对于基于证书的身份验证，网络设置中所有可寻址的主机都必须具有可解析的域名，而不仅仅是 IP 地址。
- 确保 Microsoft Exchange 2016 服务器中 SIP 端口可访问。

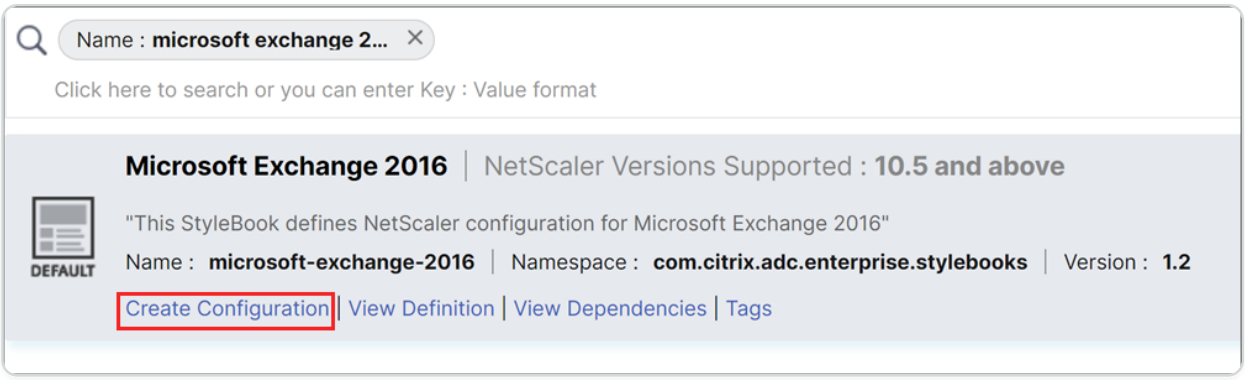
配置 Microsoft Exchange 样式簿

在您的企业中配置 Microsoft Exchange StyleBook 以部署 NetScaler 配置。

在 NetScaler Console 中配置 Microsoft Exchange 应用程序

1. 在 NetScaler Console 中，导航到 **Applications** > **StyleBooks**。
2. 搜索 **Microsoft Exchange 2016 StyleBook**，然后单击 **创建配置**。

   StyleBook 显示为用户界面表单，您可以在其中输入此 StyleBook 中定义的所有参数的值。



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

3. 输入以下参数的详细信息：

   - **Exchange Application Name** - 网络中 Microsoft Exchange 应用程序的名称
   - **Exchange VIP** - NetScaler 上接收 Microsoft Exchange 应用程序客户端请求的虚拟 IP 地址
   - **Exchange Server IPs** - 网络中所有 Exchange 服务器的 IP 地址。

     如果要添加更多 IP 地址，请单击加号 (**+**) 图标。通常，网络中会配置两台 Exchange 服务器。

4. 在 **Exchange Certificates** 部分中，将 Exchange 证书上传到 NetScaler Console。输入证书和密钥文件的名称，然后从本地存储上传。您还可以提供私钥密码来加密密钥文件。

   注意

   确保证书文件为“.pem”或“.der”格式。NetScaler Console 拒绝其他格式的文件。

   如果要指定证书过期详细信息或任何高级设置，请选择 **Advanced Certificate Settings**。

5. 在 **Exchange Active Directory Authentication config** 部分中，通过输入数据来配置 AD 设置。

   - **Active Directory 身份验证 VIP** - 用于在 NetScaler 设备上创建和配置 AD (LDAP) 虚拟服务器的虚拟 IP 地址。
   - **Active Directory 服务器 IP** - 您的 Active Directory 域控制器的 IP 地址。
   - **Active Directory 基本字符串** - Active Directory 中的 LDAP 基本字符串。例如，CN=Users,DC=CTXNSSFB,DC=COM。
   - **Active Directory LDAP 绑定可分辨名称 (DN)** - LDAP 绑定可分辨名称 (DN) 用于将此对象绑定到 LDAP 服务器 (AD)。例如，“cn=Administrator,cn=Users,dc=acme,dc=com”
   - **Active Directory LDAP 绑定可分辨名称 (DN) 密码** - LDAP 绑定可分辨名称 (DN) 是 AD 身份验证的密码
   - **Active Directory 用户名属性** - 用于用户名的 AD 属性。NetScaler 使用 LDAP 属性查询外部 Active Directory 服务器。例如，“sAMAccountName”
   - **Active Directory 组属性名称** - 在 LDAP 服务器上配置的 LDAP 组属性名称。例如，LDAP 中组属性的“memberOf”。
   - **Active Directory 子属性名称** - 在 LDAP 服务器上配置的 LDAP 子属性名称。例如，LDAP 中子属性的“cn”。
   - **Active Directory 身份验证域** - 用于身份验证的 AD/LDAP 域名。例如，ctxnssfb.com。

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

6. 在“**目标实例**”部分中，选择要部署此 Exchange 配置的 NetScaler 实例。

   注意

   如果要查看最近发现的 NetScaler 实例，请单击刷新图标。

7. 单击“**创建**”以创建配置文件并在选定的 NetScaler 实例上运行配置。

   建议您首先选择“**试运行**”以检查在目标实例上创建的配置对象，然后再在该实例上运行实际配置。

成功创建配置后，StyleBook 已创建一个内容交换虚拟服务器、五个负载平衡虚拟服务器以及一个绑定到一个 LDAP 身份验证虚拟服务器的 LDAP 策略。此外，还创建了相应的服务组并将其绑定到负载平衡虚拟服务器。

Microsoft SharePoint 样式簿

Microsoft SharePoint 2016 是一个关键的企业应用程序，主要提供文档管理和存储系统，该系统高度可配置并受所有主流浏览器支持。

您可以使用 Microsoft SharePoint 2016 样式簿部署 NetScaler 配置，以优化和保护您网络中的 Microsoft SharePoint 2016 企业应用程序。

先决条件

- 微软 SharePoint 2016
- NetScaler Console，版本 12.0 及更高版本
- NetScaler，版本 10.5 及更高版本

由 Microsoft SharePoint 2016 样式簿配置的 NetScaler 功能

您可以使用 Microsoft SharePoint 2016 样式簿为 Microsoft SharePoint 2016 启用和配置以下 NetScaler 功能：

- 负载平衡
- 内容切换
- 响应器
- 重写
- 压缩
- 集成缓存

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

负载均衡

NetScaler 负载均衡将请求均匀地分发到后端 SharePoint 服务器。对后端服务器的智能监控可防止请求发送到出现故障的服务器。

SharePoint StyleBook 配置了 12 个负载均衡虚拟服务器，每个服务器都专门用于对特定类型的内容（例如文档、图像、音频、视频和其他文件类型）的请求进行负载均衡。

SharePoint StyleBook 现在通过配置基于 SSL 的 LB 虚拟服务器来支持 SharePoint 应用程序的 SSL 模式。请确保选择 SSL 作为前端协议。请注意，虚拟端口默认设置为 443。您还可以选择 SSL 将服务组（SharePoint 应用程序服务器）绑定到目标负载均衡虚拟服务器。请注意，后端协议默认设置为 HTTP。

内容切换

内容切换功能用于根据特定类型的请求 SharePoint 内容（例如文档、图像以及音频或视频文件）将客户端请求分发到多个负载均衡虚拟服务器。内容切换模块将传入流量定向到能够处理该类型内容的最优匹配负载均衡虚拟服务器。因此，您可以对不同类型的流量应用不同的优化策略。例如，您可能希望对视频使用与文本文档不同的压缩或缓存策略。

响应程序

NetScaler 实例的响应程序功能可用于将用户从 HTTP 无缝重定向到 HTTPS。响应程序还可以配置为提供自定义错误页面。响应程序策略确定需要采取操作的请求（流量），并将每个策略绑定到负载均衡虚拟服务器。SharePoint StyleBook 包含一个将用户从 HTTP 重定向到 HTTPS URL 的配置。

重写

重写模块用于即时修改请求/响应标头、URL 或内容。此模块与流量处理内联工作，因此可以根据特定用例适当地更改流量流。例如，重写可以在不暴露有关网站服务器的不必要细节的情况下提供对请求内容的访问。

在 SharePoint StyleBook 中，重写功能用于从用户请求中删除不必要的标头。

压缩

NetScaler 压缩引擎识别并压缩可压缩内容。此过程可缩短数据传输时间，降低客户端的网络带宽要求，同时节省 SharePoint 内容服务器上的 CPU 周期。NetScaler 实例可以压缩静态和动态生成的数据。它应用 GZIP 或 DEFLATE 压缩算法从服务器响应中删除多余和重复的信息，并以更紧凑高效的格式表示原始信息。客户端浏览器解压缩数据的能力取决于它支持哪种或哪些算法：GZIP、DEFLATE 或两者都支持。

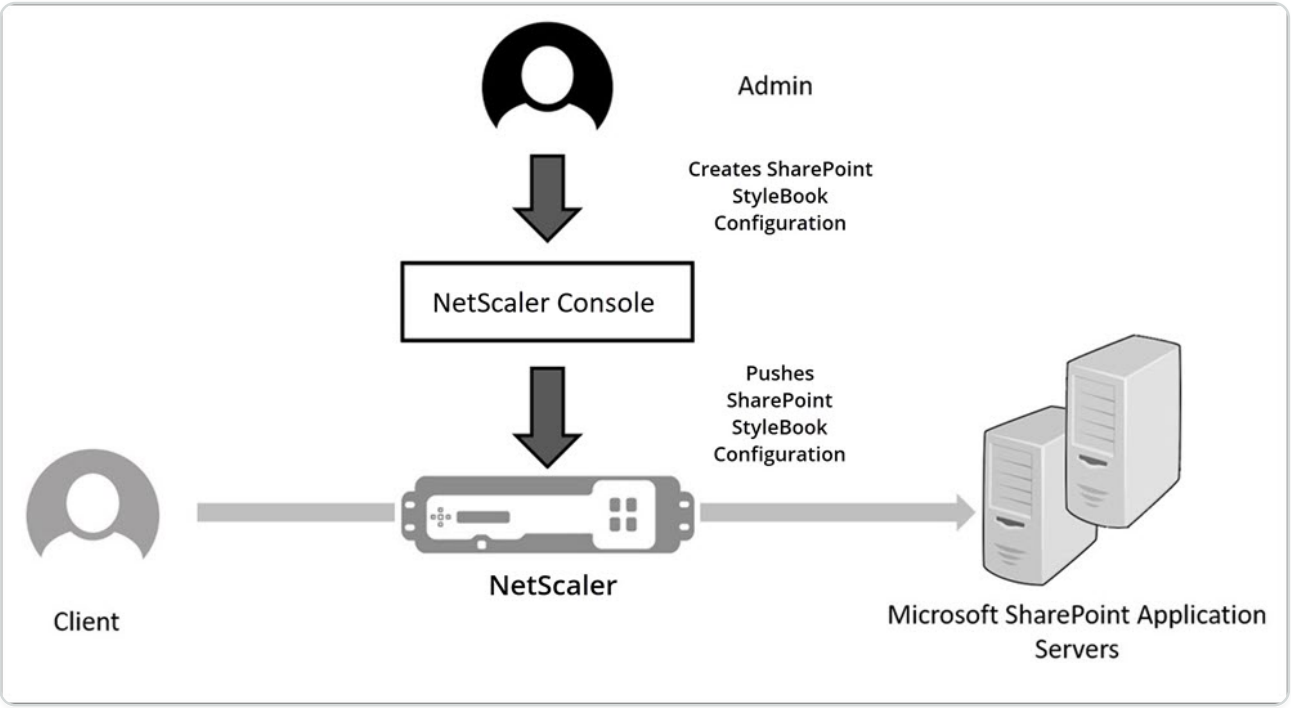
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler 实例配置为压缩 HTML、XML、纯文本、层叠样式表 (CSS) 和 Microsoft Office 文档中的文本，但不压缩 GIF 或 JPG 格式的图像。压缩流量的主要优势包括降低带宽成本、减少 WAN 延迟和提高服务器性能。

集成缓存

NetScaler 内存缓存可以存储 SharePoint 对象，以便快速向用户提供频繁请求的内容。缓存内容包括下载的文档以及音频、视频和图像文件。

下图以图示方式表示了 SharePoint 服务器在网络中的部署，该网络由 NetScaler 实例作为前端，并在该实例上使用 NetScaler Console 部署 SharePoint StyleBook 配置。



部署 SharePoint StyleBook 配置

以下任务将帮助您在业务网络中部署 Microsoft SharePoint 2016 StyleBook。

部署 Microsoft SharePoint 2016 StyleBook：

1. 在 NetScaler Console 中，导航到 **应用程序** > **管理** > **配置**，然后单击 **新建**。

   Choose StyleBook 页面显示了 NetScaler Console 中所有可供您使用的 StyleBook。

2. 向下滚动并选择 **Microsoft SharePoint 2016 StyleBook**。

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

注意

在 NetScaler Console 中，导航到 **Applications** > **Configurations** > **StyleBooks**。向下滚动以找到 **Microsoft SharePoint 2016 StyleBook**，然后单击 **Create Configuration**。

StyleBook 将作为用户界面表单打开，您可以在其中输入此 StyleBook 中定义的所有参数的值。

输入以下参数的值：

a. **SharePoint 应用程序名称**。要在网络中部署的 SharePoint 配置的名称。

b. **SharePoint 虚拟 IP**。NetScaler 实例接收 Microsoft SharePoint 应用程序客户端请求的虚拟 IP 地址。

c. **SharePoint 虚拟端口**。用户访问 SharePoint 应用程序时使用的 TCP 端口

d. **SharePoint 前端协议**。从下拉列表中选择 SharePoint 前端协议。可用选项为 HTTP 或 SSL。

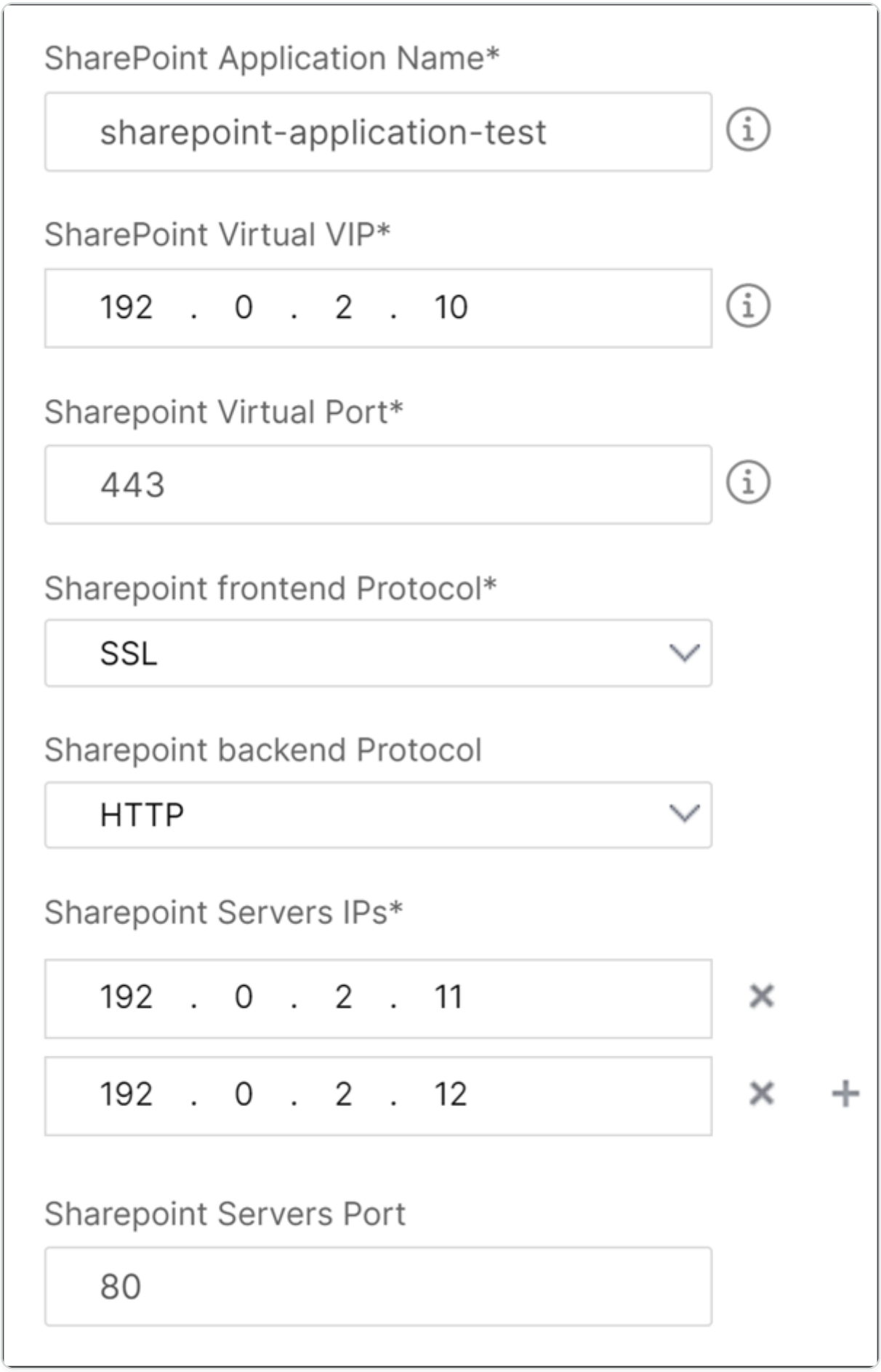
   注意

   如果选择 SSL，请确保在此 StyleBook 的 SharePoint 高级设置部分中启用了“重写配置”参数。

e. **SharePoint 服务器 IP**。网络中所有 SharePoint 服务器的 IP 地址。

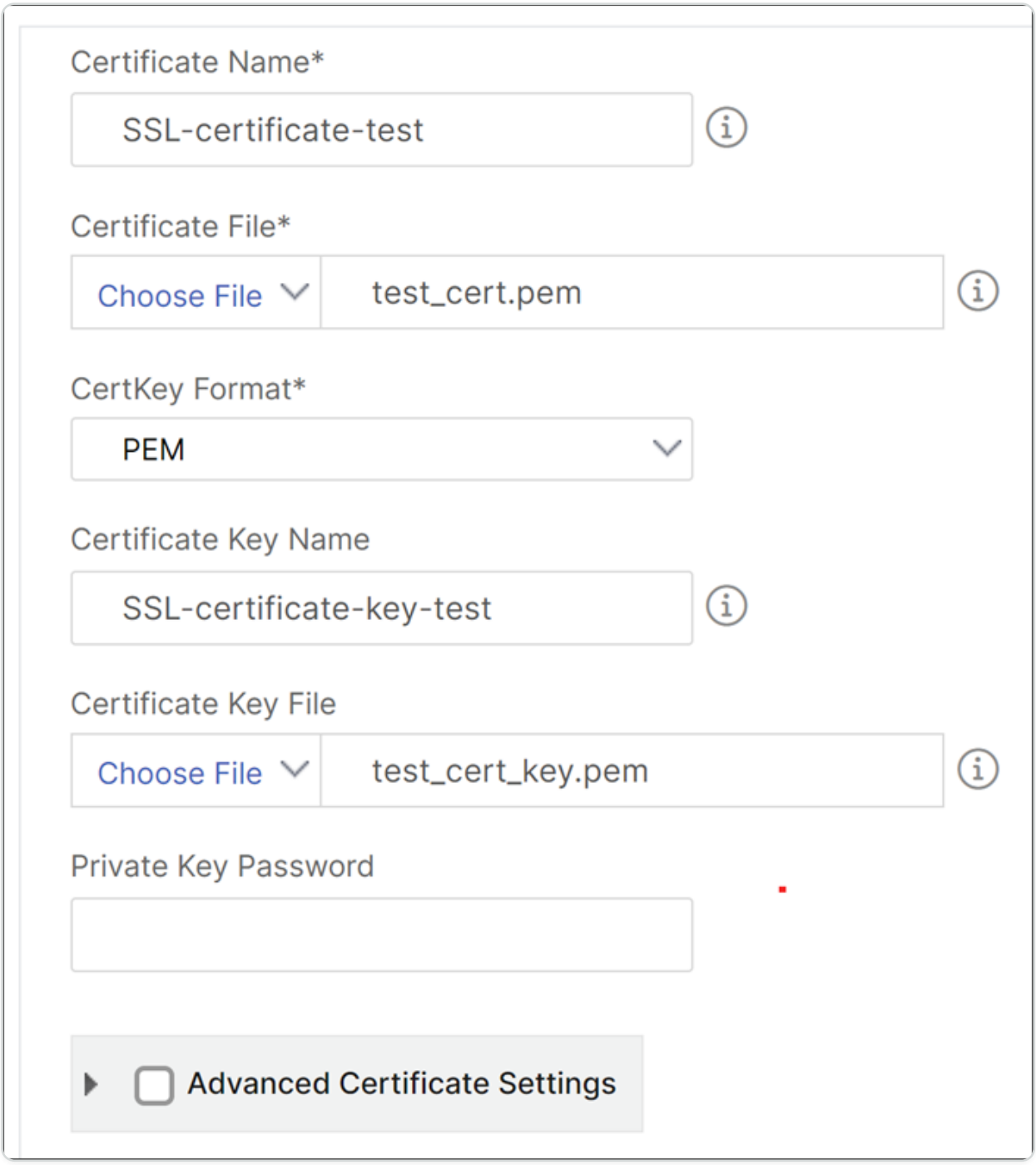
f. **SharePoint 服务器端口**。SharePoint 服务器使用的 TCP 端口号。默认情况下，此值为 80。如果需要，可以编辑此值，但请确保 Microsoft SharePoint 2016 服务器上可访问此端口。

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



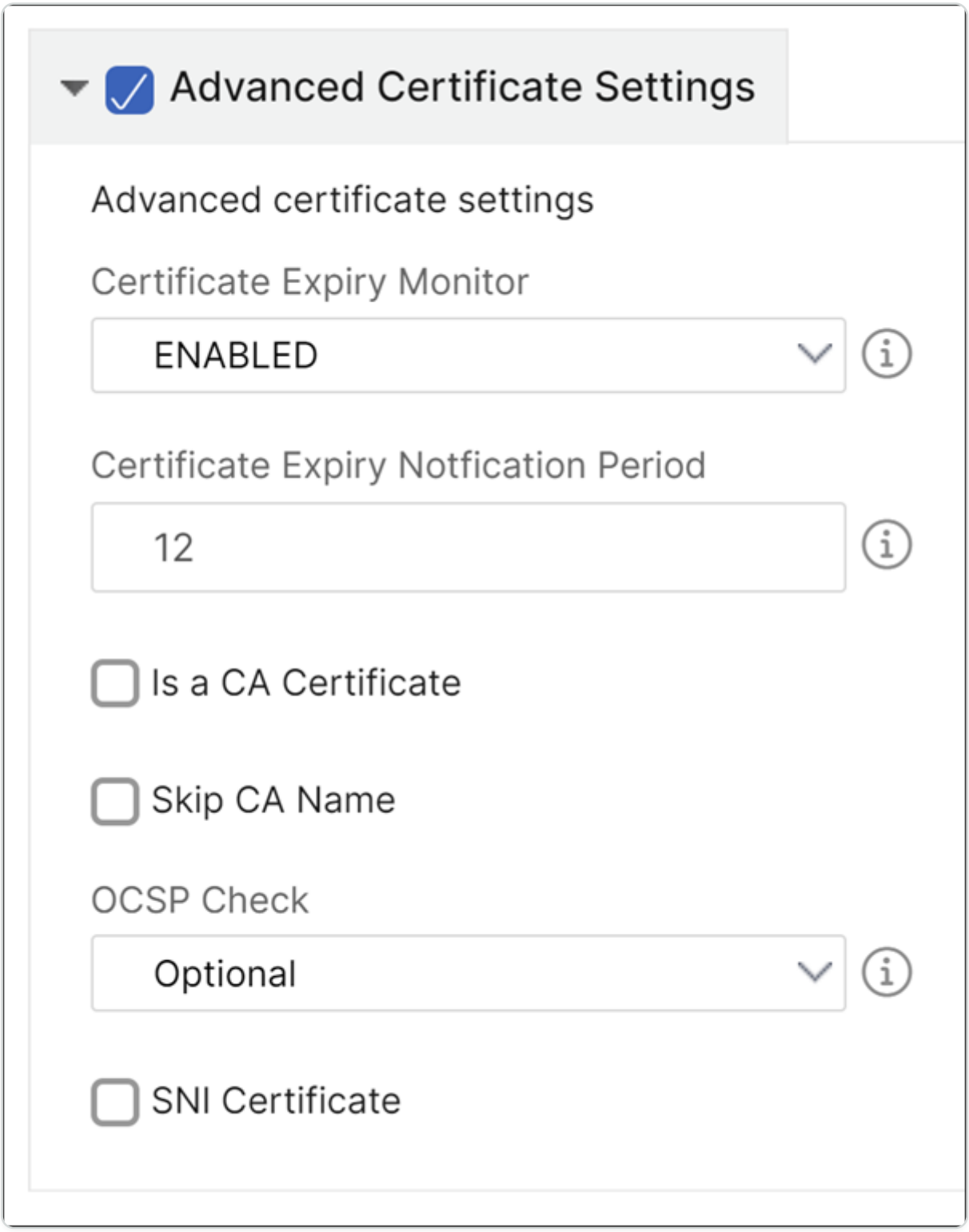
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在“**SSL 证书设置**”部分中，单击“+”输入 SSL 证书名称、证书密钥，并从本地存储文件夹中选择相应文件。



4. （可选）单击“**高级证书设置**”以启用或禁用 SSL 证书过期监控。如果启用证书过期监控，请设置天数，以便 NetScaler Console 在证书即将过期后的这些天数后发出警报。您还可以选择将 OCSP 检查作为可选功能或强制功能。

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

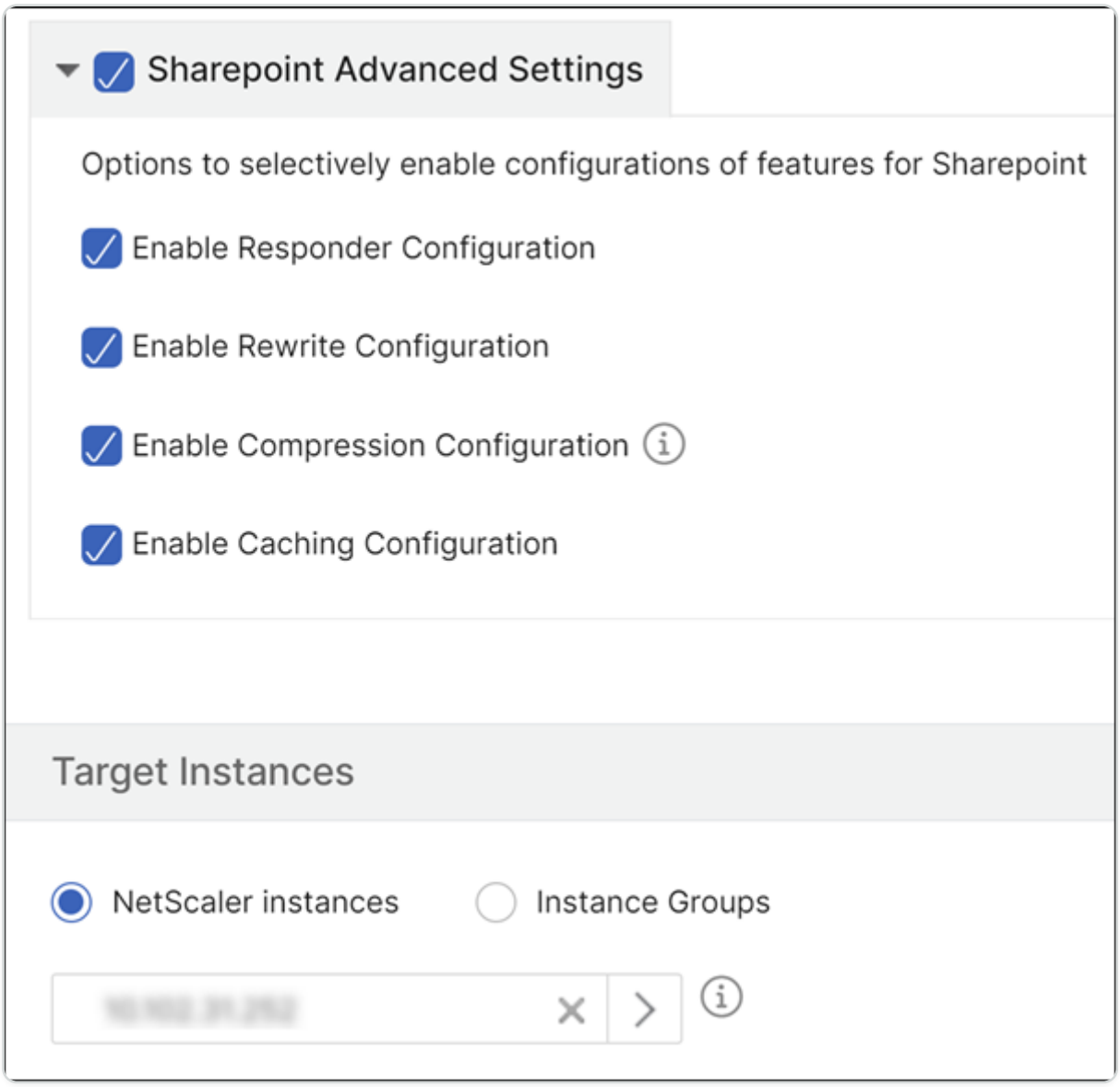


5. SharePoint“**高级设置**”部分允许您启用将在 NetScaler 实例上配置的 NetScaler 功能。虽然负载平衡和内容切换功能默认在实例上配置，但您可以选择要在实例上配置的其他功能，即响应程序配置、重写配置、压缩配置和集成缓存配置。
6. 单击“**目标实例**”，然后选择要部署此 SharePoint 配置的 NetScaler 实例。单击“**创建**”以创建配置并将其部署到所选的 NetScaler 实例上。

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

注意

您还可以单击刷新图标，将 NetScaler Console 中最近发现的 NetScaler 实例添加到此窗口中可用的实例列表中。



注意

我们建议您在执行实际配置之前，选择**试运行**以检查将在目标实例上创建的配置对象。

当配置创建并成功部署后，SharePoint StyleBook 会创建一个内容交换虚拟服务器和 12 个负载均衡虚拟服务器。它还会创建策略和服务组，并将它们绑定到负载均衡虚拟服务器。创建哪些策略取决于在创建配置包时在 StyleBook 中选择的功能。

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

查看 NetScaler 实例上定义的对象

在 NetScaler Console 上创建配置包后，您可以查看为 SharePoint StyleBook 在 NetScaler 实例上创建的所有对象。导航到 **Applications** > **Administration** > **Configuration**，然后单击 **View Objects Created**。下图显示了一些已创建的对象，其中包含“从 NetScaler Console 部署 SharePoint StyleBook 配置”示例中指定的 IP 地址。

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

Type : lbvserver

appflowlog : DISABLED
backuppersistencetimeout : 20
downstateflush : DISABLED
ipv46 : 0.0.0.0
lbmethod : LEASTCONNECTION
name : sharepoint application test frontpage services lb
persistencebackup : SOURCEIP
persistencetype : COOKIEINSERT
port : 0
servicetype : HTTP
timeout : 20

Type : servicegroup

cip : DISABLED
cka : YES
cmp : NO
downstateflush : DISABLED
healthmonitor : NO
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp
servicetype : HTTP
sp : ON
state : ENABLED
tcpb : NO
useproxyport : NO
usip : NO

Type : lbvserver_servicegroup_binding

name : sharepoint-application-test-frontpage-services-lb
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.11
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

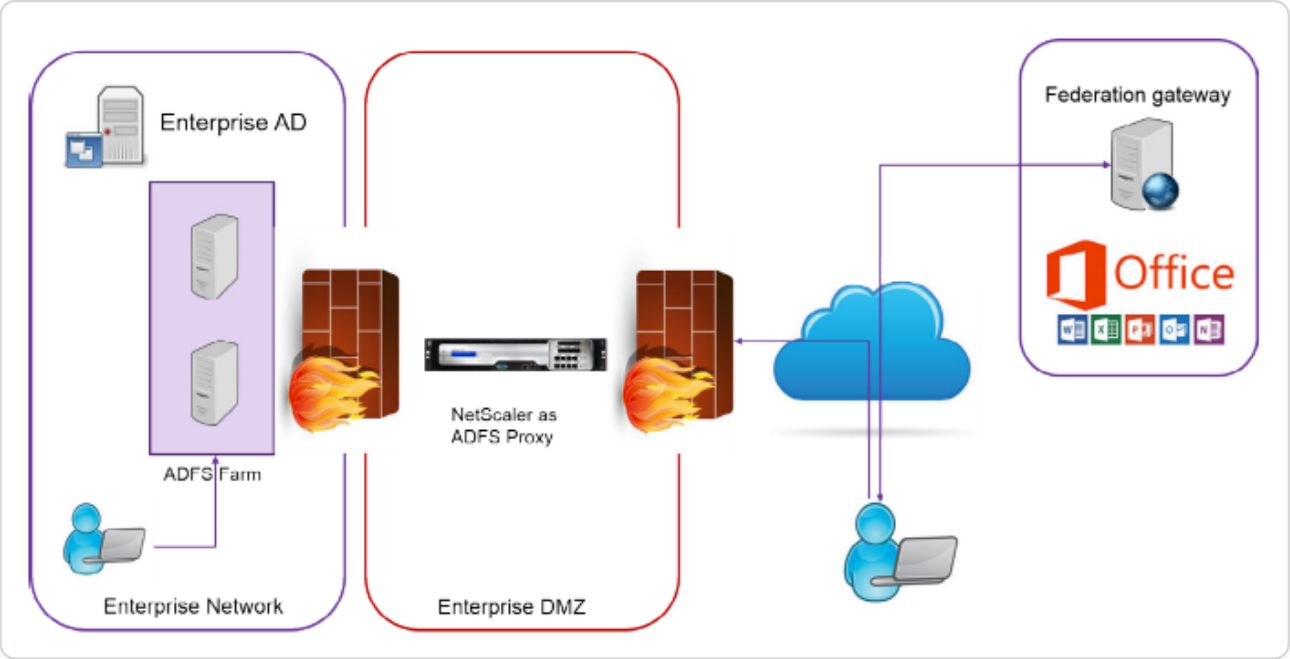
Microsoft ADFS 代理 StyleBook

Microsoft ADFS 代理通过为内部联合资源和云资源提供单点登录访问发挥着重要作用。云资源的一个示例是 Office 365。ADFS 代理服务器的目的是接收请求并将其转发到无法从 Internet 访问的 ADFS 服务器。ADFS 代理是反向代理，通常位于您组织的边界网络 (DMZ) 中。ADFS 代理在远程用户连接和应用程序访问中起着关键作用。

NetScaler 拥有精确的技术，可实现安全连接、身份验证和联合身份处理。使用 NetScaler 作为 ADFS 代理可避免在 DMZ 中部署额外组件。

NetScaler Console 中的 Microsoft ADFS 代理 StyleBook 允许您在 NetScaler 实例上配置 ADFS 代理服务器。

下图显示了在企业 DMZ 中将 NetScaler 实例部署为 ADFS 代理服务器。



使用 NetScaler 作为 ADFS 代理的优势

1. 满足负载平衡和 ADFS 代理需求
2. 支持内部和外部用户访问场景
3. 支持丰富的预身份验证方法
4. 为用户提供单点登录体验
5. 支持主动和被动协议
    a. 主动协议应用程序的示例包括 – Microsoft Outlook、Microsoft Skype for Business
    b. 被动协议应用程序的示例包括 – Microsoft Outlook Web 应用程序、Web 浏览器

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

6. 用于基于 DMZ 部署的强化设备
7. 通过使用额外的核心 NetScaler 功能增加价值
    a. 内容交换
    b. SSL 卸载
    c. 重写
    d. 安全 (NetScaler AAA)

对于基于活动协议的场景，您可以连接到 Office 365 并提供您的凭据。Microsoft Federation Gateway 代表活动协议客户端联系 ADFS 服务（通过 ADFS 代理）。然后，网关使用基本身份验证 (401) 提交凭据。NetScaler 在访问 ADFS 服务之前处理客户端身份验证。身份验证后，ADFS 服务向 Federation Gateway 提供 SAML 令牌。Federation Gateway 随后将令牌提交给 Office 365 以提供客户端访问。

对于被动客户端，ADFS 代理 StyleBook 会创建 Kerberos 约束委派 (KCD) 用户帐户。KCD 帐户对于 Kerberos SSO 身份验证连接到 ADFS 服务器是必需的。StyleBook 还会生成 LDAP 策略和会话策略。这些策略随后绑定到处理被动客户端身份验证的 NetScaler AAA 虚拟服务器。

StyleBook 还可以确保 NetScaler 上的 DNS 服务器已为 ADFS 配置。

下面的配置部分描述了如何设置 NetScaler 以处理基于活动和被动协议的客户端身份验证。

配置详情

下表列出了成功部署此集成所需的最低软件版本。

产品	最低要求版本
NetScaler	11.0，高级/高级版许可证

以下说明假定您已创建了相应的外部和内部 DNS 条目。

从 NetScaler Console 部署 Microsoft ADFS 代理 StyleBook 配置

以下说明将帮助您在业务网络中实施 Microsoft ADFS 代理 StyleBook。

部署 Microsoft ADFS 代理 StyleBook

1. 在 NetScaler Console 中，导航到 **Applications** \> **StyleBooks**。**StyleBooks** 页面显示了 NetScaler Console 中所有可供您使用的 StyleBook。
2. 向下滚动并找到 **Microsoft ADFS 代理 StyleBook**。单击 **Create Configuration**。 StyleBook 将作为用户界面页面打开，您可以在其中输入此 StyleBook 中定义的所有参数的值。

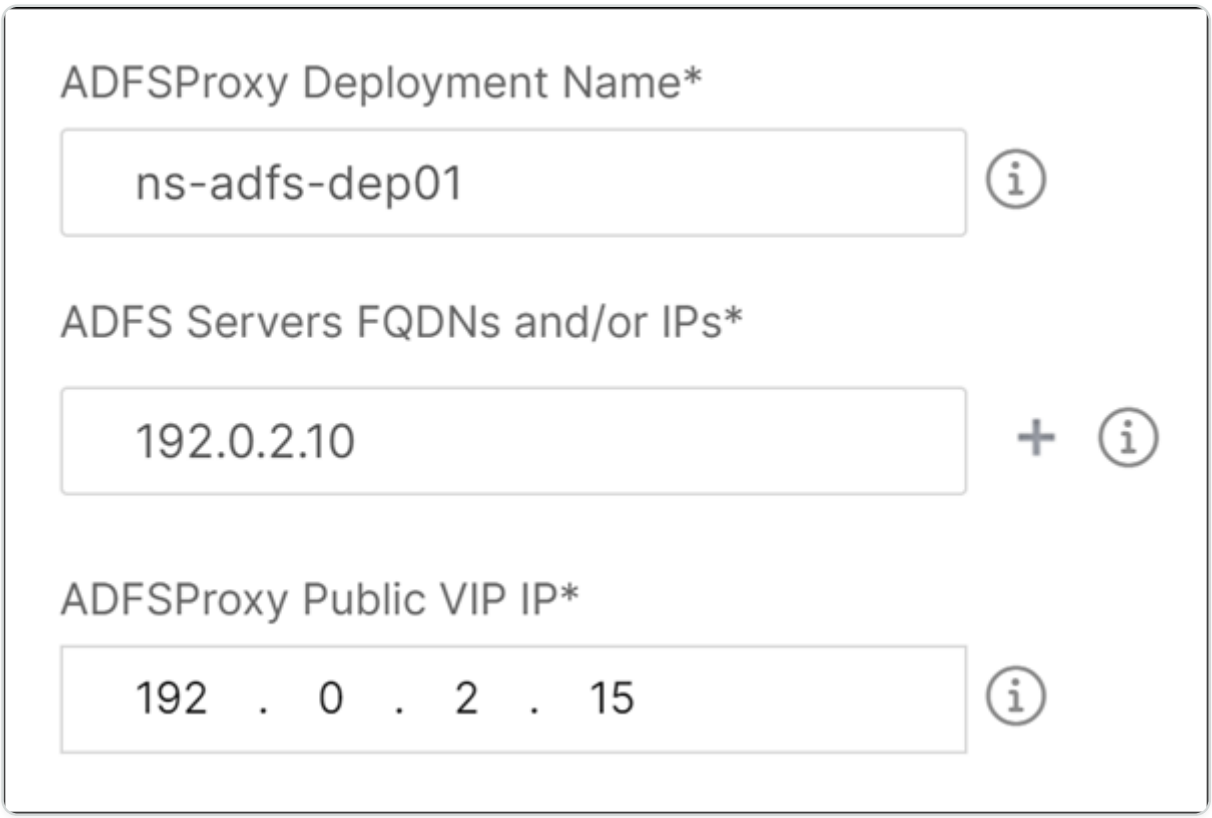
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 输入以下参数的值：

   a. **ADFS 代理部署名称**。为部署在您网络中的 ADFS 代理配置选择一个名称。

   b. **ADFS 服务器 FQDN 或 IP**。输入网络中所有 ADFS 服务器的 IP 地址或 FQDN（域名）。

   c. **ADFS 代理公共 VIP IP**。输入 NetScaler 上用作 ADFS 代理服务器的公共虚拟 IP 地址。

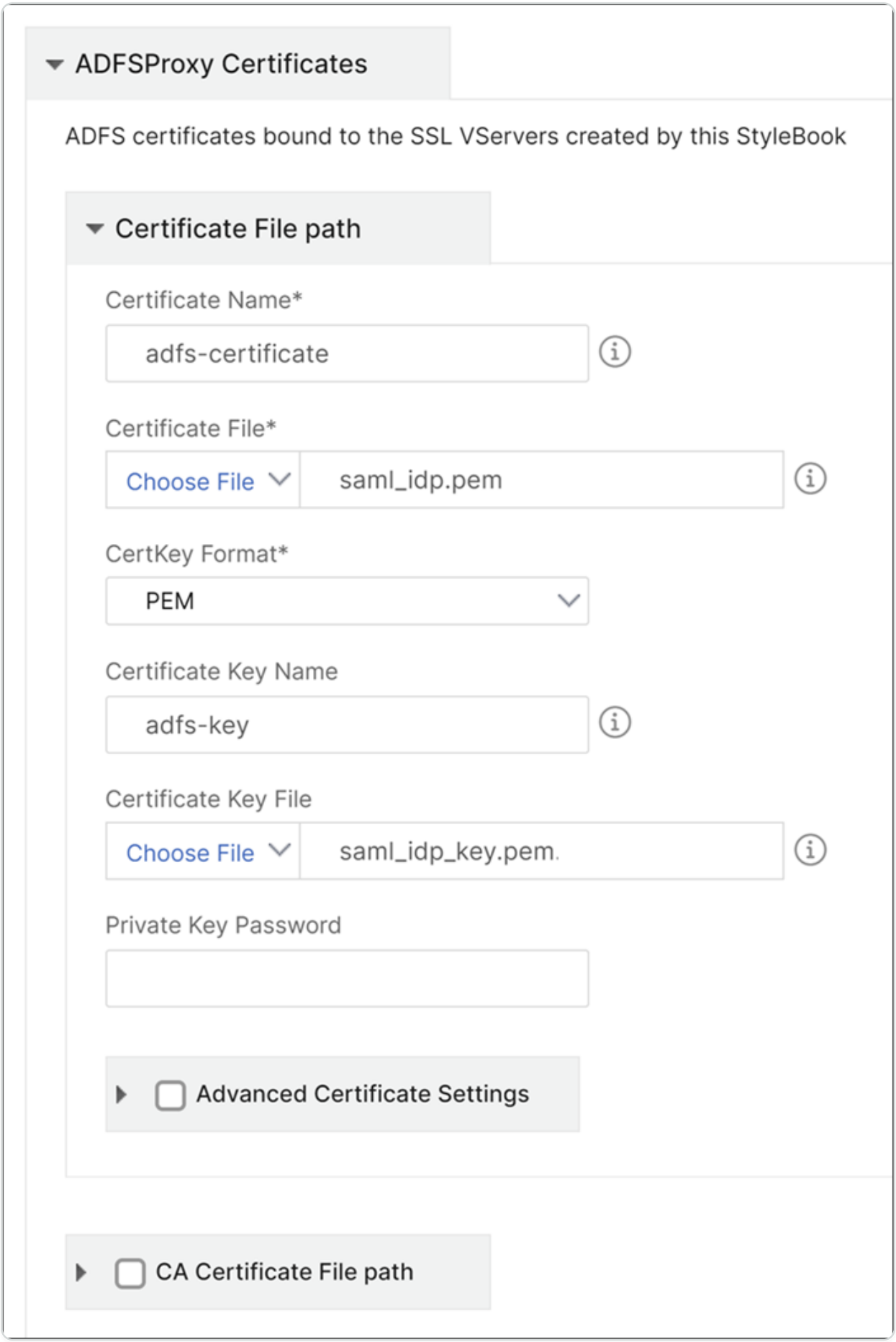


4. 在 **ADFS 代理证书**部分中，输入 SSL 证书和证书密钥的详细信息。

   此 SSL 证书绑定到 NetScaler 实例上创建的所有虚拟服务器。

   从本地存储文件夹中选择相应的文件。您还可以输入私钥密码以加载 .pem 格式的加密私钥。

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



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

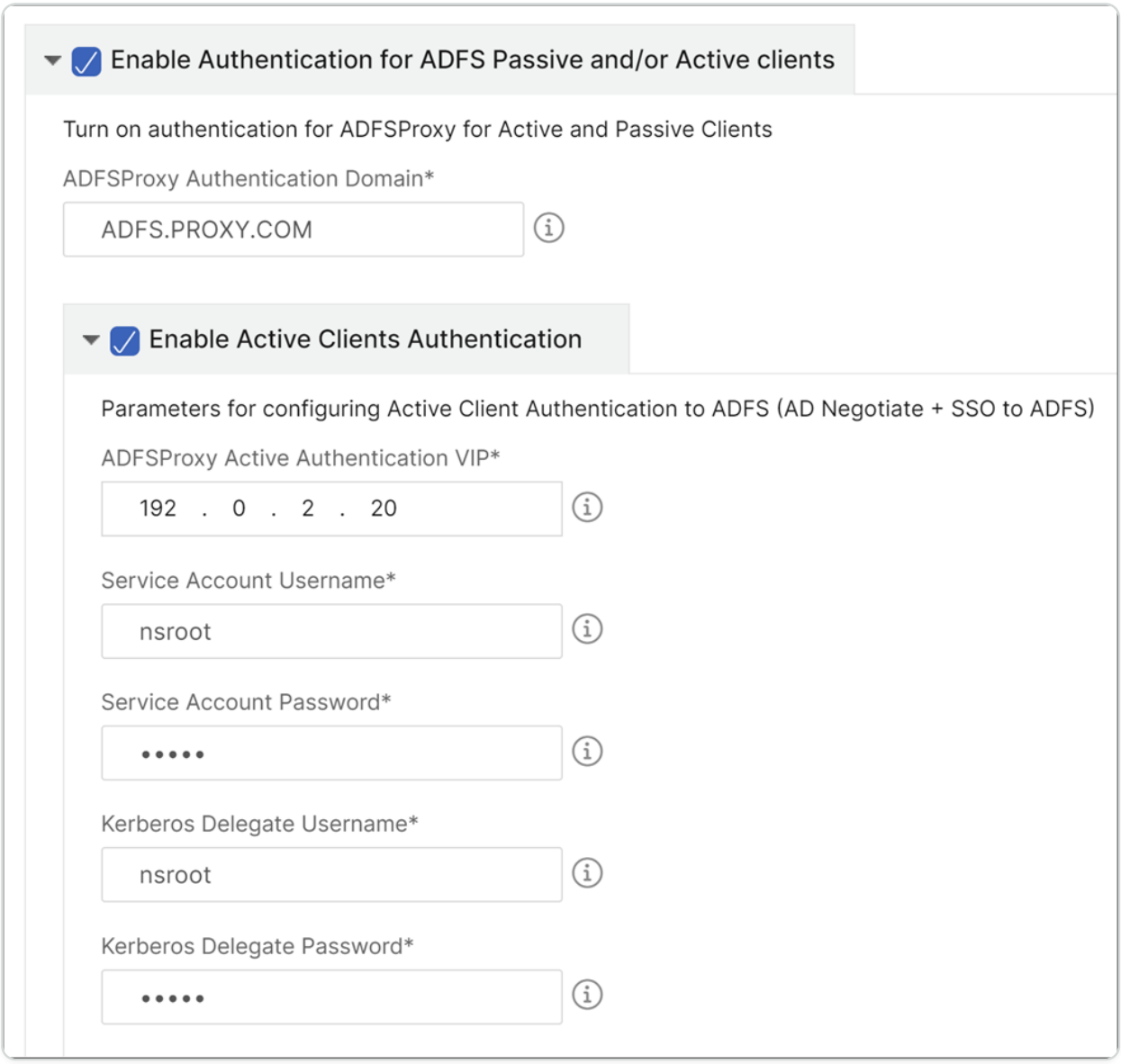
您还可以启用**高级证书设置**复选框。在此处，您可以键入证书过期通知期限、启用或禁用证书过期监视器等详细信息。

5. 如果 SSL 证书需要将 CA 公共证书安装在 NetScaler 上，您可以选择性地选中 **SSL CA 证书**复选框。确保在**高级证书设置**部分中选择**是 CA 证书**。
6. 为活动客户端和被动客户端启用身份验证。键入用于用户身份验证的 Active Directory 中的 DNS 域名。然后，您可以为活动客户端、被动客户端或两者配置身份验证。
7. 键入以下详细信息以启用活动客户端的身份验证：

> **注意**
>
> 配置对活动客户端的支持是可选的。

   a. **ADFS 代理活动身份验证 VIP**。键入 NetScaler 实例上虚拟身份验证服务器的虚拟 IP 地址，活动客户端将重定向到该实例进行身份验证。
   b. **服务帐户用户名**。键入 NetScaler 用于将您的用户身份验证到 Active Directory 的服务帐户用户名。
   c. **服务帐户密码**。键入 NetScaler 用于将您的用户身份验证到 Active Directory 的密码。

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



8. 通过启用相应选项并配置 LDAP 设置来配置被动客户端的身份验证。

> **注意**
>
> 配置对被动客户端的支持是可选的。

键入以下详细信息以启用被动客户端的身份验证：

a. **LDAP (Active Directory) 基本**。键入 Active Directory (AD) 中用户帐户所在域的基本域名，以允许身份验证。例如，dc=netscaler®，dc=com

b. **LDAP (Active Directory) 绑定 DN**。添加一个具有浏览 AD 树权限的域帐户（为便于配置，请使用电子邮件地址）。例如，cn=Manager,dc=netscaler,dc=com

c. **LDAP (Active Directory) 绑定 DN 密码**。键入用于身份验证的域帐户密码。

本节中您必须填写的其他一些字段如下：

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

d. **LDAP 服务器 (Active Directory) IP**。键入 Active Directory 服务器的 IP 地址，以便 AD 身份验证正常工作。

e. **LDAP 服务器 FQDN 名称**。键入 Active Directory 服务器的 FQDN 名称。FQDN 名称是可选的。提供步骤 1 中的 IP 地址或 FQDN 名称。

f. **LDAP 服务器 Active Directory 端口**。默认情况下，LDAP 协议的 TCP 和 UDP 端口为 389，而安全 LDAP 的 TCP 端口为 636。

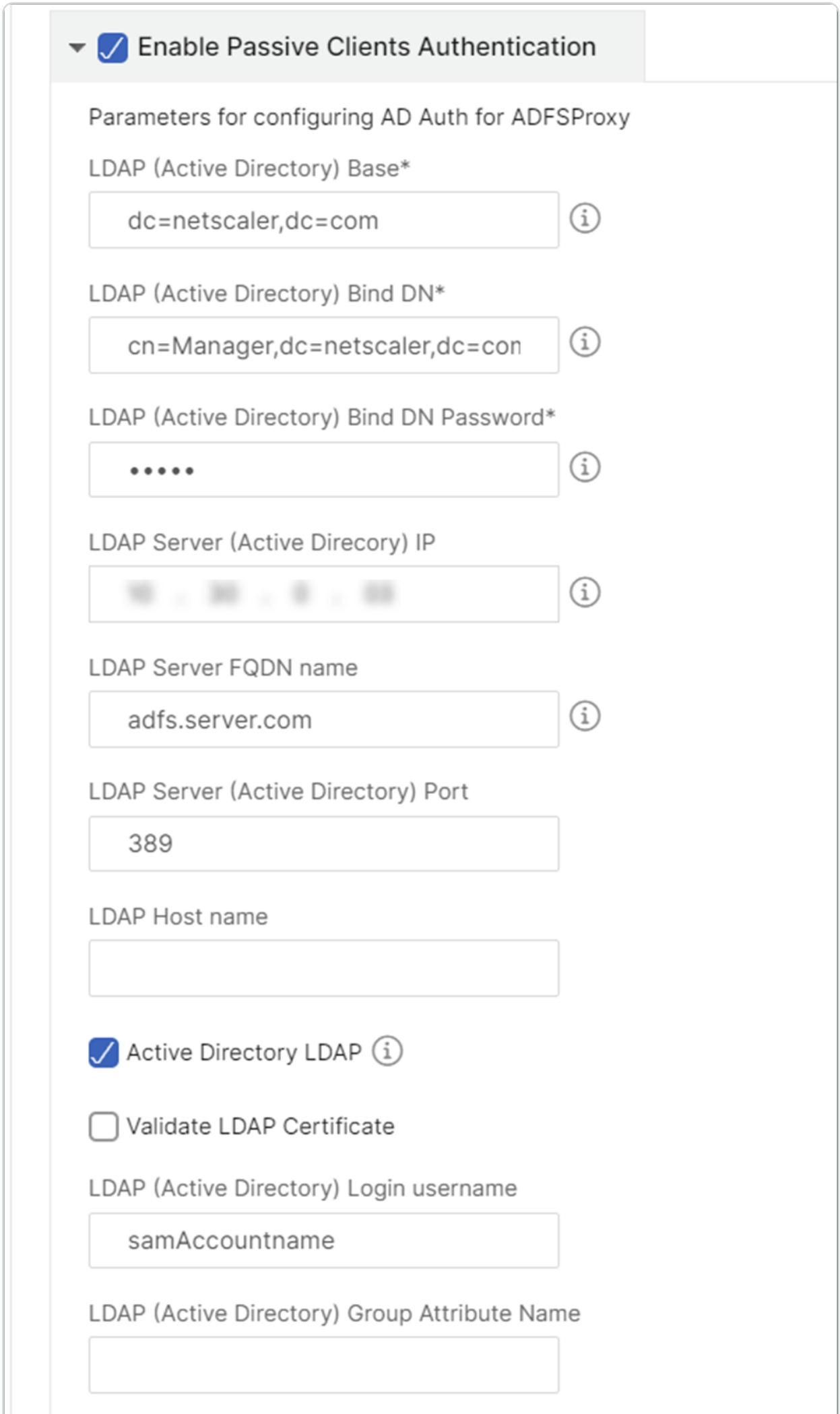
g. **LDAP (Active Directory) 登录用户名**。键入用户名，格式为“sAMAccountName”。

h. **ADFS 代理被动身份验证 VIP**。键入用于被动客户端的 ADFS 代理虚拟服务器的 IP 地址。

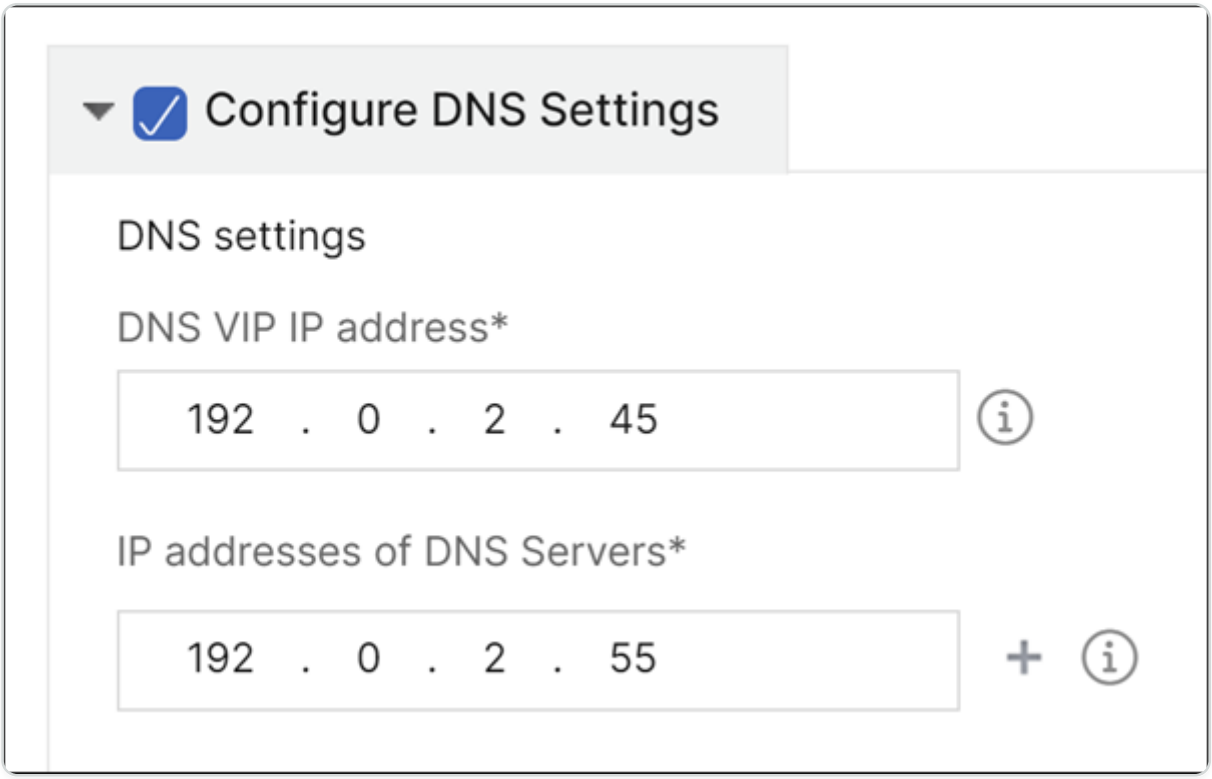
注意

标有“*”的字段为必填项。

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

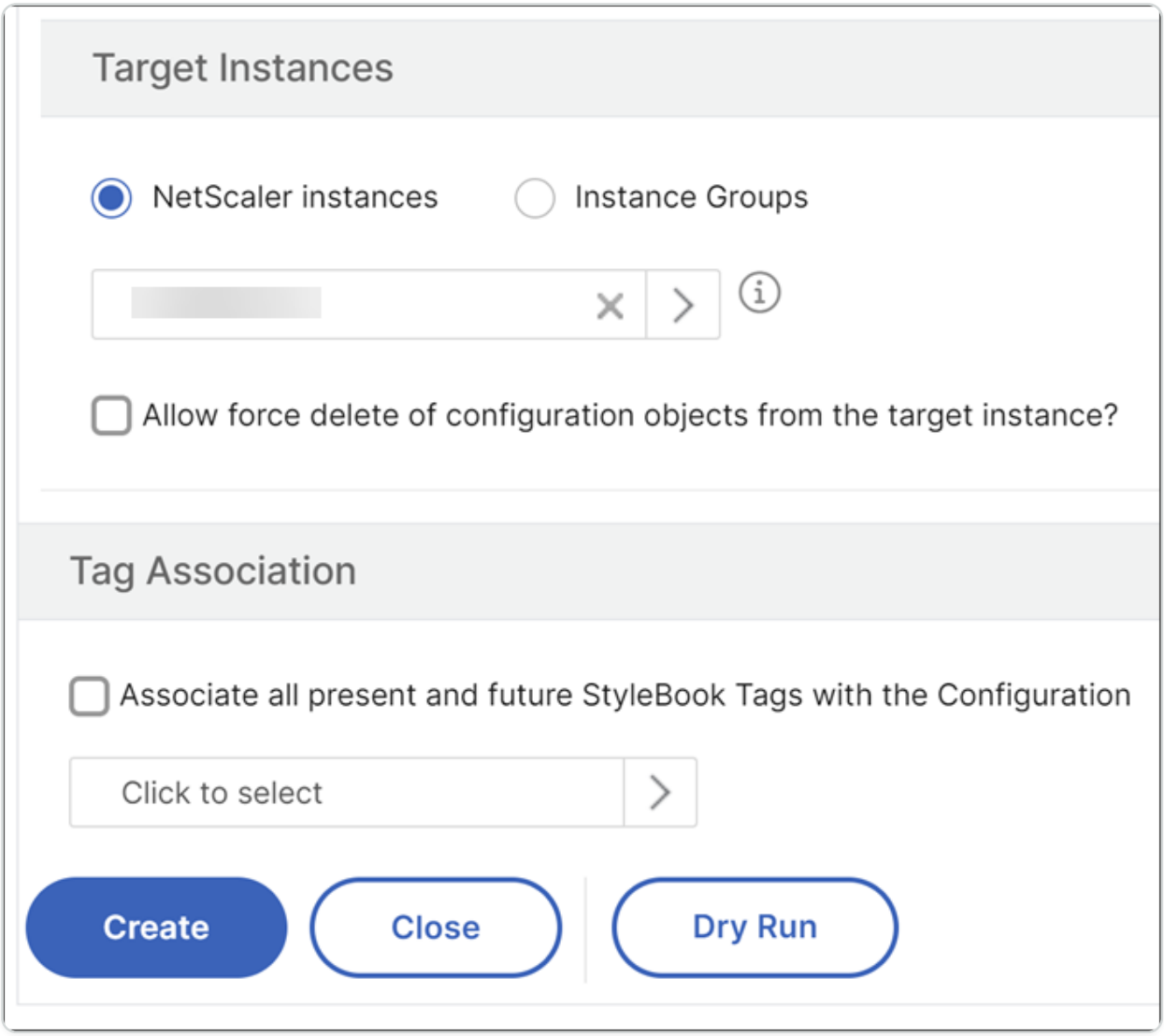

Enable Passive Clients Authentication
Parameters for configuring AD Auth for ADFSProxy
LDAP (Active Directory) Base*
dc=netscaler,dc=com
LDAP (Active Directory) Bind DN*
cn=Manager,dc=netscaler,dc=con
LDAP (Active Directory) Bind DN Password*
•••••
LDAP Server (Active Direcory) IP
LDAP Server FQDN name
adfs.server.com
LDAP Server (Active Directory) Port
389
LDAP Host name
Active Directory LDAP
Validate LDAP Certificate
LDAP (Active Directory) Login username
samAccountname
LDAP (Active Directory) Group Attribute Name

9. 或者，您也可以为 DNS 服务器配置 DNS VIP。



10. 单击**目标实例**并选择要部署此 Microsoft ADFS 代理配置的 NetScaler 实例。单击**创建**以创建配置并将其部署到选定的 NetScaler 实例上。

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



注意

建议您在执行实际配置之前，选择“**试运行**”。您可以首先查看 StyleBook 在目标 NetScaler 实例上创建的配置对象。然后，您可以单击“**创建**”以在选定的实例上部署配置。

创建的对象

当 ADFS 代理配置部署在 NetScaler 实例上时，会创建多个配置对象。下图显示了创建的对象列表。

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

Type : systemfile

filecontent :
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURtVENDQW9HZ0F3SUJBZ0lCQXpBTkJna3Foa2lHOXcwQkFRc0ZBI
VFHRXdKVlV6RW1NQ1FHQ1NxR1NjYjNEUUVKQVJZWApIVzkxWTJWbUxXTmhRR0ZqYldVdFkyOXljQzVqYjIweEZEQV
1URXlPVEExTVRrd05Wb1hEVEI5TVRFeU9EQTFNVGt3TlZvd2dZZ3gKR0RBV0JnTlZCQU1NRDNsdmRXTmxaaTF6WVcx
FRa0JGaGw1YjNWalpXWXRjMkZ0YkVCaFkyMWxMV052Y25BdVkyOXRNUkl3CkVBWURWUVFLREFsQlEwMUZMVU5
GQUFPQ0FROEFNSUlCQ2dLQ0FRRUF5L1gza0VCd2F0SEpoQmFXR2Z6WmwxQ1FkZ2jtbDFlYgpZT3hadG4xOHNpS
9kNXJCOHNmeG56K2RvbjJyaUhHaktEazVPYkFScmd2NVNHaGhmL3pvQVpDa3MybkVocjh6UElxOWoKQm8wc3NlTl
HV3VlpBakQxVitnNTVHSkdXMW9ubndyTlc0Q3ViTzMyRTFDNjh1WG1TZnIwdUlzTzIvRDF2ZnovSDh0QlM4CjFlV0VIa
0RBSkJnTlZIUk1FQWpBQU1Bc0dBMVVkRHdRRUF3SUY0REFOQmdrcWhraUc5dzBCQVFzRkFBT0NBUUVBbk1RSQpz
KOGc3CjNlUzlkbE15UkUveXh4N3V5SXpqR0ZaV1VBclMxL09PcUxGRHR2NEFZWXZ6UVhGL0pWM2phWjZnUkdMS0
zFRclNHdVYrdgoxRW1tMlNNcWxrbGVVclN5QXBuSlVWNHA0QTVDbTh6UTRVVDhtZjZQRkU2TFhRTHZCYzhWdUJvR
NBVEs1azE1NVZSd2UKaWt3OFYzR082MmdRc0hvV05RPT0KLS0tLS1FTkQgQ0VSVElGSUNBVEUtLS0tLQo=

fileencoding : BASE64

filelocation : /nsconfig/ssl

filename : saml-idp.pem

Type : systemfile

filecontent :
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFcEFJQkFBS0NBUUVBeS9YM2tFQndhdEhKaEJhV0dmelpsM
Q2eWJWY1NzajFiT0JEdU9CbVpnRS9LQS9kNXJCOHNmeG4Keitkb24ycmlIR2pLRGs1T2JBUnJndjVTR2hoZi96b0FaQ2t
BhTU1tV3dyQmN0OUhKdEJxcEpVUHV3VlpBakQxVitnNTVHCkpHVzFvbm53ck5XNEN1Yk8zMkUxQzY4dVhtU2ZyMH
h0bW1YT2tLb0JWaXdJREFRQUJBb0lCQUVtS1FGOEV2UVBtN0cveAo3T0VsNkJiRTk3RjJ2NEhtRnFJVjFpc1VoL2Q2Y2h2
WTUdnTHBZcDYvRS9DcFFQdkhyNEJSS3hiVXBvQkpaZ0g0eloKRHZjT1dadIjtc0hXYVBkUmoxVDNaaHdsd21aMEQ4U
wrSXBBRHJybkdOdUNHMId4NUorNHM3VG9aMXYzc1NtRThaK2pqdWtYCk5DTFBKcnh3dFJlSXc3ajRTenlDNWFCR1M
1RrZHhTc2ZPblF6THgwYUNQWnFWNCtQVkoycThzbkpvMXhJOWI1dE9mRlBNVApGRHZNYXZwKytHQnpWTyszRWI
wWDA2NWlSTnZVYnVrQklqWDgvYkhTNIlITjFWR2o2RVFYQmtrNmJmSXNDZ1lFQXpNQ2kKMkFhd0FTY3htT0Q1Zm
1PZTNPU2dVMWh4WmNDdjlUMGhNNEdWVVQyVFhqWkZNWWFBWk8yNjFwdWVKbTRkMXZqdDY3CjJrN0tVclhpY
iMzgxNW5tUmpyZTFrK21QN2tuL0xFQk1pVUVXV0tybXpFanRsbzhRTFhXVjZzU3ltVXJCVU11bnVLWgo1Y1B5bFdFTE
VCcUwwQjh5a0djUGVUbkRlS3dLQmdRQ0tBME1BMkNrazdkVkpsa08xb05jTDhrUGNYL0ZzckJURi8xL0QKRTcva1AxT
GR1Blb3NJK3FxQWw1aktiY3AxMFZYNUJ1cS9xbm9vREVkN2d0NGNFcEM0RTUvQW85VThGWVVGR3ZpcC9wdGwxC
EeloKUmllWXlWUnRkbkU5TE5kYU5STXdpTWFCYkhFazF4R1IxSDByQnFEYUE0M1B4Zm9FYjdndEdCaHE2azRUempa
otLS0tLUVORCBSU0EgUFJJVkFURSBLRVktLS0tLQo=

fileencoding : BASE64

filelocation : /nsconfig/ssl

filename : saml-idp.key

Type : sslcertkey

cert : saml-idp.pem

certkey : adfs-certificate

inform : PEM

key : saml-idp.key

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

Objects Added on Instance : 192.168.153.160 | Count : 57

Type : nsfeature

Meta Properties
action : **enable**

feature : cs lb ssl rewrite aaa

Type : lbvserver

ipv46 : 192.50.50.12
name : ns-adfs-dep01-adfs-dns
port : 53
servicetype : DNS

Type : service

ip : 10.30.30.5
name : ns-adfs-dep01-dns-svc-1
port : 53
servicetype : DNS

Type : lbvserver_service_binding

name : ns-adfs-dep01-adfs-dns
servicename : ns-adfs-dep01-dns-svc-1

Type : authenticationnegotiateaction

domain : ADFS.CITRIX.COM
domainuser : nsroot
domainuserpasswd : nsroot
name : ns-adfs-dep01-negotiate-action

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

Type : authenticationpolicy

action : ns-adfs-dep01-negotiate-action
name : ns-adfs-dep01-negotiate-policy
rule : true

Type : aaakcdaccount

delegateduser : nsroot
kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
kcdpassword : nsroot
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
name : ns-adfs-dep01-adfs-auth401-tmsession-action
persistentcookie : ON
persistentcookievalidity : 3
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-auth401-tmsession-action
name : ns-adfs-dep01-adfs-auth401-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.40
maxloginattempts : 255
name : ns-adfs-dep01-adfs-auth401-auth-vserver
port : 443
servicetype : SSL

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

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-auth401-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-negotiate-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-adfs-auth401-tmsession-policy
priority : 10

Type : authenticationldapaction

authentication : ENABLED
authtimeout : 30
followreferrals : OFF
ldapbase : dc=netscaler,dc=com
ldapbinddn : cn=Manager,dc=netscaler,dc=com
ldapbinddnpassword : nsroot
ldaploginname : samAccountname
name : ns-adfs-dep01-ldap-action
passwdchange : DISABLED
sectype : PLAINTEXT
serverip : 10.30.30.3
serverport : 389
ssonameattribute : userPrincipalName
svrtype : AD
validateservercert : NO

Type : authenticationpolicy

action : ns-adfs-dep01-ldap-action
name : ns-adfs-dep01-ldap-policy
rule : true

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

Type : aaakcdaccount

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
name : ns-adfs-dep01-adfs-ldap-tmsession-action
persistentcookie : OFF
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-ldap-tmsession-action
name : ns-adfs-dep01-adfs-ldap-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.30
maxloginattempts : 255
name : ns-adfs-dep01-adfs-ldap-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-ldap-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-ldap-policy
priority : 10

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

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-adfs-ldap-tmsession-policy
priority : 10

Type : csvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-cs
port : 443
servicetype : SSL

Type : lbvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
port : 445
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : server

ipaddress : 192.30.30.30
name : 192.30.30.30

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

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

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
priority : 9800

Type : lbvserver

appflowlog : ENABLED
authentication : ON
authenticationhost : ADFS.CITRIX.COM
authn401 : OFF
authnvsname : ns-adfs-dep01-adfs-ldap-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
port : 446
servicetype : SSL

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

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/ls/auth/integrated") || HTTP.REQ.URL.CONTAINS("/adfs/ls/wia")

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
priority : 9900

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

Type : lbvserver

appflowlog : ENABLED
authentication : OFF
authn401 : ON
authnvsname : ns-adfs-dep01-adfs-auth401-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
port : 444
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

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

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
rule : true

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
priority : 10000

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-cs

Type : rewritepolicylabel

labelname : ns-adfs-dep01-request-rewritepolicylabel
transform : HTTP_REQ

Type : rewritepolicylabel

labelname : ns-adfs-dep01-response-rewritepolicylabel
transform : HTTP_RES

Type : rewriteaction

name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
stringbuilderexpr : "/adfs/services/trust/proxymex"
target : HTTP.REQ.URL
type : REPLACE

Type : rewritepolicy

action : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") && (!HTTP.REQ.URL.CONTAINS("/trust/proxymex"))

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

Type : rewritepolicylabel_rewritepolicy_binding

gotopriorityexpression : END
labelname : ns-adfs-dep01-request-rewritepolicylabel
policyname : ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
priority : 10

Type : lbvserver_rewritepolicy_binding

bindpoint : REQUEST
gotopriorityexpression : END
invoke : true
labelname : ns-adfs-dep01-request-rewritepolicylabel
labeltype : policylabel
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
policyname : NOPOLICY-rewrite
priority : 10

Oracle 电子商务 StyleBook

Oracle E-Business Suite 是最全面的集成式全球业务应用程序套件。此套件可帮助组织做出更好的决策、降低成本、提高绩效，并包含以下应用程序。

- 企业资源规划 (ERP)
- 客户关系管理 (CRM)
- 供应链管理 (SCM)

这些计算机应用程序由 Oracle 开发或收购。Oracle E-Business Suite 12.2 StyleBook 允许您在选定的 NetScaler 实例上部署配置。

此 StyleBook 创建一个负载平衡配置，其中包含一个负载平衡虚拟服务器、一个服务组和一系列服务。它还将服务绑定到服务组，并将服务组绑定到虚拟服务器。您可以通过选择 SSL 并从本地系统提供 SSL 文件和密钥文件来选择加密通信。

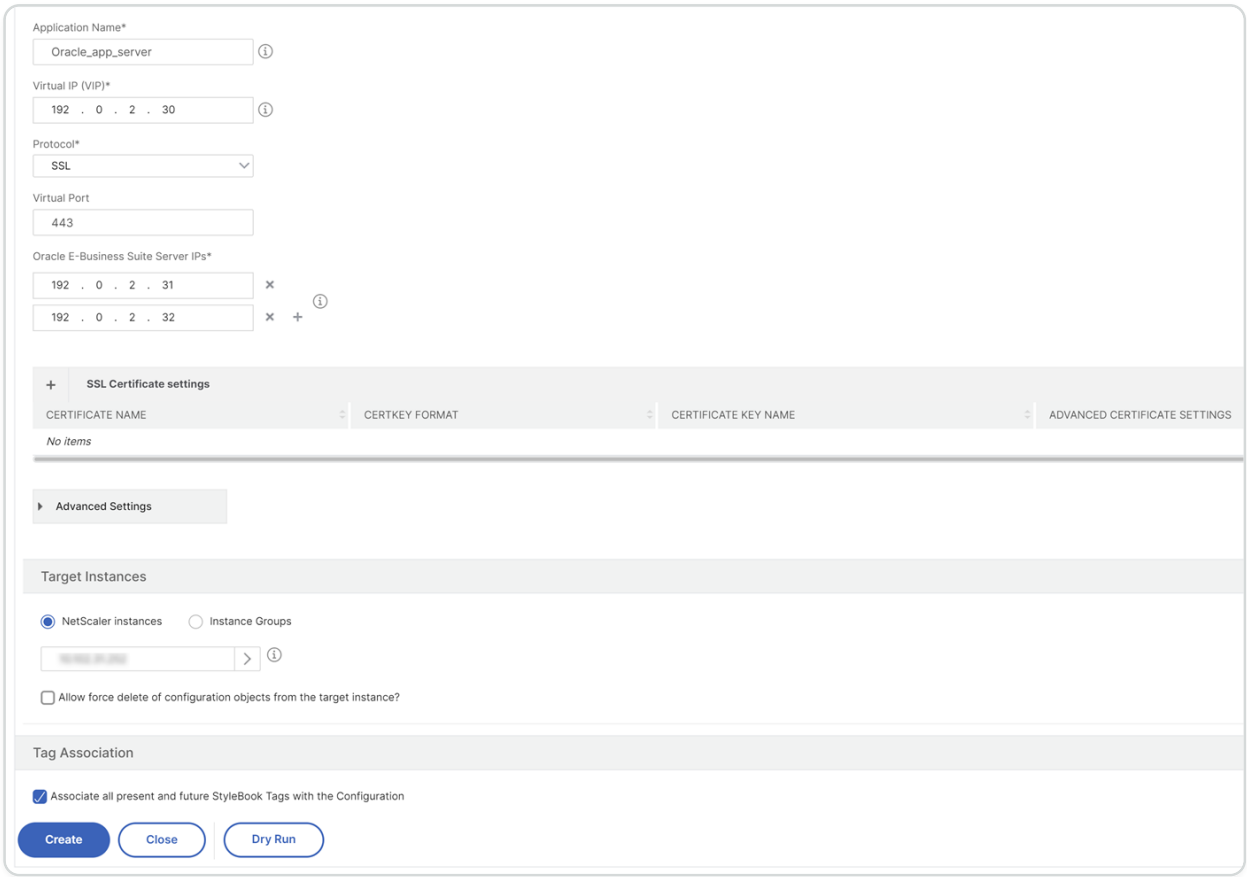
为 Oracle E-Business Suite 12.2 创建配置

1. 在 NetScaler Console 中，导航到 **Applications** > **Configuration > StyleBooks**。**StyleBooks** 页面显示 NetScaler Console 中所有可用的 StyleBook。向下滚动并选择 **Oracle E-Business Suite 12.2**。您还可以使用搜索选项来搜索 StyleBook。
2. 在 StyleBook 面板中，单击 **Create Configuration**。
3. 在负载平衡器设置部分中，键入负载平衡器应用程序的名称和虚拟 IP 地址。

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

4. 选择所需的协议。您有两个选项：HTTP 和 HTTPS/SSL。您还可以键入端口号。
5. 键入网络中所有需要进行负载平衡的 Oracle E-Business Suite 应用程序服务器的 IP 地址。单击 **+** 以添加更多服务器 IP 地址。
6. 在 **SSL Certificates Settings** 部分中，从本地存储中选择相应的文件。您还可以启用 **Advanced Certificate Settings** 复选框。在此处，您可以配置更多详细信息，例如证书过期通知期限。您还可以启用或禁用证书过期监视器。

   选择必须创建配置的目标 NetScaler 实例，然后单击 **Create**。



提示

您还可以单击刷新图标，将 NetScaler Console 中最近发现的 NetScaler 实例添加到此窗口中可用的实例列表。刷新图标目前仅在 NetScaler Console 上可用。

Citrix StoreFront™ 样式簿

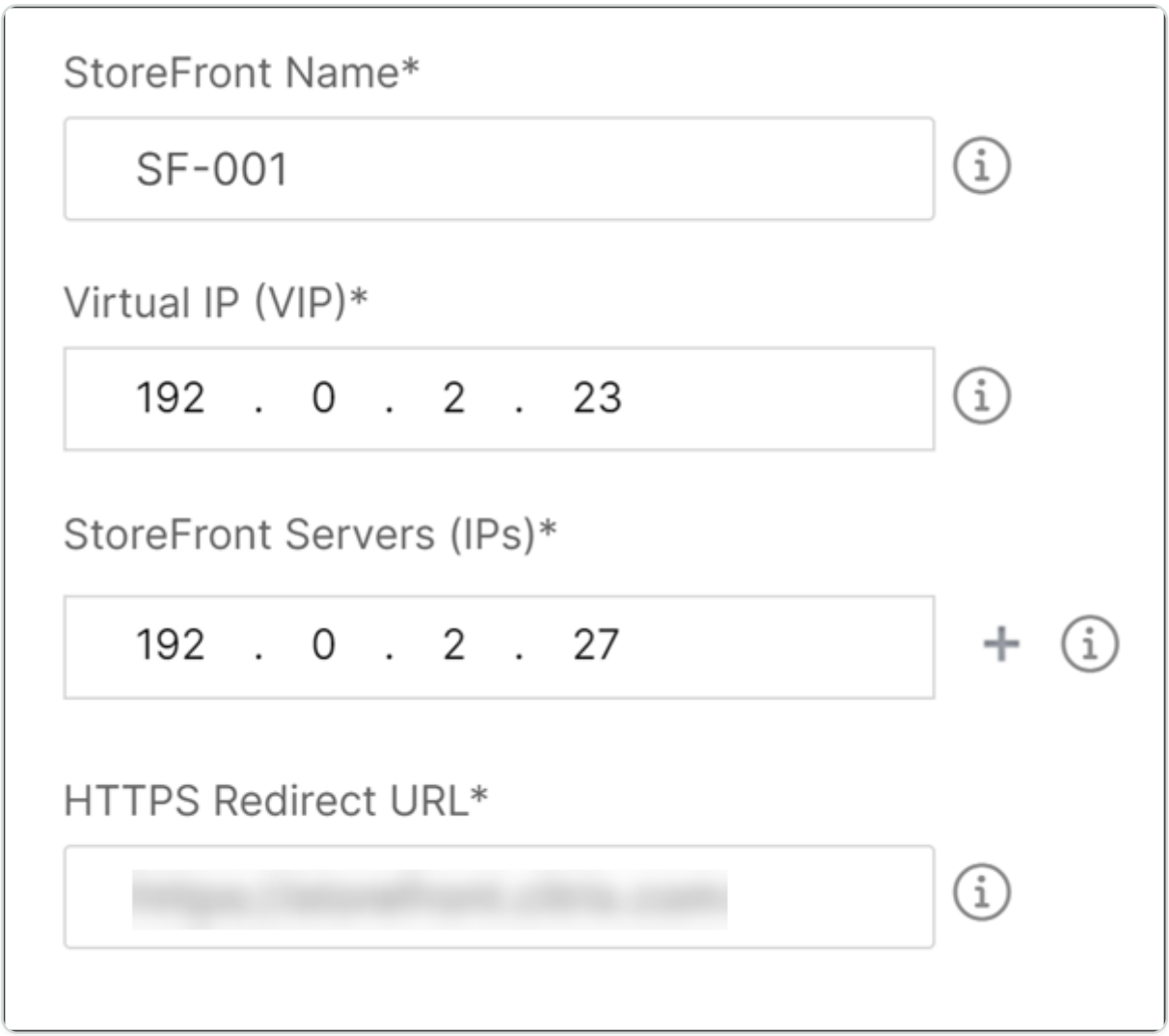
StoreFront 是一个企业应用商店，它将来自 Citrix Virtual Apps and Desktops 站点的应用程序和桌面聚合到一个商店中供用户使用。StoreFront 对托管资源的站点进行用户身份验证，并管理用户访问的应用程序商店和桌面。它托管您的企业应用程序商店，允许用户自助访问您提供给他们的应用程序和桌面。

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

此样式簿定义了 StoreFront 服务器的 NetScaler 配置。借助此样式簿，您可以将 StoreFront 服务器配置到所需的 NetScaler 实例。您可以通过选择 SSL 并从本地系统提供 SSL 文件和密钥文件来选择加密通信。

为 Citrix StoreFront 应用程序创建配置

1. 在 NetScaler Console GUI 中，导航到“**应用程序 > 样式簿**”。
2. 在搜索栏中，使用“**名称**”属性并搜索 `Citrix StoreFront`。
3. 在 Citrix StoreFront 样式簿上，单击“创建配置”。
4. 指定以下详细信息：
   - **StoreFront 名称**：指定 StoreFront 名称。StoreFront 配置包将使用相同的 StoreFront 名称创建。
   - **虚拟 IP (VIP)**：指定 NetScaler 实例接收客户端请求的虚拟 IP 地址。
   - **StoreFront 服务器**：指定要使用 NetScaler 实例配置的 StoreFront 服务器的 IP 地址。
   - **HTTPS 重定向 URL**：指定 HTTPS 请求重定向到的 HTTPS URL。



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

5. 在“**SSL 证书设置**”部分中，输入 SSL 证书和证书密钥的名称。
6. 从本地存储文件夹中选择相应的文件。您还可以键入私钥密码以指定 PEM 格式的加密私钥。

   指定 StoreFront StyleBooks 的 SSL 证书设置(/en-us/netscaler-application-delivery-management-software/media/ssl-cert-sf-stylebooks.png)
7. 您还可以启用**高级证书设置**复选框。在此处，您可以输入证书过期通知期限、启用或禁用证书过期监视器等详细信息。
8. 可选，如果 SSL 证书需要将 CA 公共证书安装在 NetScaler 上，请选择**用于身份验证虚拟 IP 的 SSL CA 证书**复选框。请确保在**高级证书设置**部分中选择**是 CA 证书**。
9. 单击**创建**。
10. 单击**目标实例**，然后选择要配置 StoreFront 服务器的 NetScaler 实例。
11. 单击**创建**以创建配置并在选定的 NetScaler 实例上部署配置。

创建和使用自定义 StyleBook

您可以为您的部署编写自己的 StyleBook，将其导入 NetScaler Console，并创建配置对象。您还可以使用 API 从您的 StyleBook 创建配置。

本文档包含以下信息：

开始之前

在开始创建 StyleBook 之前，请确保您了解以下内容：

- NITRO API。有关更多信息，请参阅 Nitro API 文档
- YAML

StyleBook 文件使用 YAML 格式。有关 YAML 格式的信息，请参阅 YAML 语法。

以下是创建 StyleBook 时必须注意的 YAML 准则列表：

- YAML 区分大小写。
- YAML 需要正确的缩进
- 使用 `<spacebar>` 键创建正确的缩进。请勿使用 `<tab>` 键。在将 StyleBook 导入 MA 服务时，使用 `<tab>` 键会导致编译错误。
- 请勿在引号内使用字符串。仅当字符串包含标点符号（破折号、冒号等）时，才将字符串包含在引号内。如果您想将数字解释为字符串，请将数字包含在引号内，或使用 StyleBook 的 str() 内置函数。

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

- 诸如 YES/Yes/yes/Y/y/NO/no/No/n/N、ON/On/on/OFF/Off/off 和 TRUE/true/truthy/FALSE/False/false/falsely 等字面量被视为布尔值，分别等同于 true 和 false。要将它们解释为字符串，请将它们包含在引号内。例如：
  - "YES"
  - "否"
  - "真"
  - "假"等。

注意

在将您的 StyleBook 文件导入 NetScaler Console 之前，建议您验证文件是否符合 YAML 格式。我们建议您使用 StyleBooks 中内置的 YAML 验证器来验证和导入 YAML 内容。

配置 StyleBooks 时，您只能使用支持 **创建** 和 **删除** 操作（POST 和 DELETE HTTP 方法）的 Nitro 配置资源。有关更多信息，请参阅 Nitro API 文档。

StyleBook 的结构

编写 StyleBooks 需要您了解 StyleBooks 的语法、句法和结构。典型的 StyleBook 包含以下部分：

- **标头**：此部分允许您定义 StyleBook 的标识并描述其功能。这是必填部分。
- **导入 StyleBooks**：此部分允许您声明要从当前 StyleBook 引用哪些其他 StyleBook。编写 StyleBook 需要导入 NetScaler NITRO 配置 StyleBooks 或其他 StyleBooks。这是必填部分。
- **参数**：此部分允许您定义 StyleBook 中创建配置所需的参数。它描述了 StyleBook 接受的输入。这是可选部分。
- **组件**：此部分允许您定义 StyleBook 为特定配置创建的实体（配置对象）。此部分被视为 StyleBook 的核心。组件通常使用参数部分中提供的输入来调整 StyleBook 生成的配置。这是可选部分。

  StyleBook 可以包含参数部分、组件部分或两者兼有。仅包含参数部分的 StyleBook 可用于定义可供其他 StyleBooks 使用的参数列表。这促进了参数组在 StyleBooks 集合中的可重用性。仅包含组件部分的 StyleBook 可用于在 StyleBook 中指定属性值，而不是定义参数来获取用户输入。
- **输出**：参数部分定义了 StyleBook 的输入，而此可选部分定义了其输出。在此可选输出部分中，您可以指定要向从该 StyleBook 创建配置的用户以及导入该 StyleBook 的其他 StyleBooks 公开的组件。用户和导入的 StyleBooks 随后可以引用公开组件的属性。

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

- **操作**：StyleBook 可以包含一个可选部分，用于在 NetScaler Console 中对作为 StyleBook 一部分的任何虚拟服务器启用分析。

下图显示了 StyleBook 的简单大纲。

```
name: lb-vserver
description: "This stylebook defines a load balancing virtual server configuration."
display-name: "Load Balancing Virtual Server (HTTP)"
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: name
    type: string
    required: true
  -
    name: ip
    type: ipaddress
    required: true
  -
    name: lb-alg
    type: string
    allowed-values:
      - ROUNDROBIN
      - LEASTCONNECTION
    default: ROUNDROBIN
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.name
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
```

Header

Import StyleBooks

Parameters

Components

以下示例可帮助您了解 StyleBook 的语法和结构，以及如何编写复杂程度不断提高的 StyleBook。

- 用于创建负载平衡虚拟服务器的 StyleBook
- 用于创建基本负载平衡配置的 StyleBook
- 创建复合 StyleBook
- 使用 GUI 属性自定义您的 StyleBook

用于创建负载均衡虚拟服务器的样式簿

在此示例中，您设计一个基本的样式簿，用于创建 HTTP 协议类型并侦听端口 80 的负载均衡虚拟服务器。虚拟服务器名称、IP 地址和负载均衡方法参数接受用户定义的值，也就是说，它们是样式簿的参数。

标头

样式簿的前六行构成标头部分。在此示例中，标头部分编写如下：

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

```
name: lb-vserver

description: This StyleBook defines a load balancing virtual server
configuration.

display-name: Load Balancing Virtual Server (HTTP)

namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"
```

标头部分包括以下详细信息：

- **name**：此样式簿的名称。
- **description**：描述此样式簿的功能。此描述显示在 NetScaler Console 上。
- **display-name**：样式簿的描述性名称，显示在 NetScaler Console 上。
- **namespace**：命名空间是样式簿唯一标识符的一部分，以避免名称冲突。
- **schema-version**：在此版本中始终取值“1.0”。
- **version**：样式簿的版本号。更新样式簿时可以更改版本号。

name、**namespace** 和 **version** 的组合在系统中唯一标识一个样式簿。在 NetScaler Console 中，不能有两个样式簿具有相同的 name、namespace 和 version 组合。但是，您可以有两个样式簿具有相同的 name 和 version 但不同的 namespace，或者具有相同的 namespace 和 version 但不同的 name。

注意

假设您已更新样式簿并拥有更新的版本号。现在，如果您在其他样式簿中引用（即导入）此样式簿，请务必同时更新其他样式簿中的版本号，以便它们使用导入样式簿的正确版本。

导入样式簿

标头后面的部分称为“import-stylebooks”。在此部分中，您必须声明要在当前样式簿中引用的任何其他样式簿的命名空间和版本号。这使您能够导入并重用其他样式簿，而不是在自己的样式簿中重新构建相同的配置。

在此示例中，import-stylebooks 部分编写如下：

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

```
import-stylebooks:

 -

  namespace: netscaler.nitro.config

  prefix: ns

  version: "10.5"
```

如果任何样式簿直接使用 NITRO 配置对象，则必须引用 netscaler.nitro.config 命名空间。此命名空间包含所有 NetScaler NITRO 类型，例如 lbvserver。由于支持 10.5 及更高版本的软件，您可以使用您的样式簿在运行 10.5 及更高版本的任何 NetScaler 实例上创建并运行配置。

import-stylebooks 部分中使用的前缀是引用命名空间和版本组合的速记。在此示例中，ns 指的是 netscaler.nitro.config 的 10.5 版本。在样式簿的后续部分中，您无需使用命名空间和版本来引用导入的样式簿，而是可以使用所选的前缀字符串，例如上面示例中的 ns。

样式簿中使用的版本是 NetScaler NITRO 版本。基于 Nitro X 版本的样式簿可用于配置任何版本为 X 或更高版本的 NetScaler。

注意

为确保您的样式簿可用于配置任何 10.5 或更高版本的 NetScaler 实例，为实现最大兼容性，我们建议您在直接使用 Nitro 内置样式簿（命名空间：netscaler.nitro.config，版本：10.5）的样式簿中导入 Nitro 10.5 命名空间。

重要的是，导入其他样式簿的样式簿需要基于与其导入的样式簿相同或更高版本的 Nitro 版本。例如，基于 Nitro 10.5 版本的样式簿不能依赖、使用或导入基于 11.1 版本的样式簿。但基于 11.1 版本的样式簿可以导入基于任何低于 11.1 版本的样式簿。

也可能存在根本不导入 Nitro 命名空间的样式簿。这意味着样式簿无需直接定义 Nitro 组件，但可以导入（依赖）定义 Nitro 组件的样式簿。导入其他样式簿的样式簿总是获取其依赖项层次结构中的最高 Nitro 版本，因此可用于配置该版本或更高版本的 NetScaler。

参数

参数部分允许您声明样式簿中所需的所有参数。作为样式簿开发人员，您必须决定希望样式簿用户指定哪些输入。在此示例中，您已构建样式簿，要求其用户提供虚拟服务器的名称、其 IP 地址以及负载均衡方法。

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

参数部分如下所示：

```
parameters:

 -

  name: name

  type: string

  label: Application Name

  description: Name of the application configuration.

  required: true



 -

  name: ip

  type: ipaddress

  label: Application Virtual IP (VIP)

  description: Application VIP that the clients access.

  required: true



-

  name: lb-alg

  type: string

  label: LoadBalancing Algorithm

  description: Choose the load balancing algorithm (method) used for load
balancing client request between the application servers.
```

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

```
allowed-values:

 - ROUNDROBIN

 - LEASTCONNECTION

 default: ROUNDROBIN
```

注意

如果您不提供参数的标签，则 NetScaler Console 会在显示此参数时使用名称属性。您必须始终为参数定义标签，以便您可以控制它们在 NetScaler Console 中的显示方式。

但是，在使用 API 时，参数由其名称指定。
在本节中，您已声明了三个参数，这些参数由其 **name** 属性值指示 - **name** 用于虚拟服务器名称，**ip** 用于虚拟服务器的 IP 地址，**lb-alg** 用于负载平衡方法。

- **type**。这些参数可以采用的值类型。例如，name 和 lb-alg 可以采用字符串值，而 ip 值必须是 IP 地址类型。StyleBook 中的参数可以是以下任何内置类型：
- **string**。一个字符数组。如果未指定长度，则字符串值可以包含任意数量的字符。但是，您可以使用 min-length 和 max-length 属性来限制字符串类型的长度。
- **number**。一个整数。您可以使用 min-value 和 max-value 属性来指定此类型可以采用的最小值和最大值。
- **boolean**。可以是 true 或 false。另请注意，YAML 将所有字面量视为布尔值（例如，Yes 或 No）。
- **ipaddress**。表示有效 IPv4 或 IPv6 地址的字符串。
- **tcp-port**。一个介于 0 到 65535 之间的数字，表示 TCP 或 UDP 端口。
- **password**。一个不透明/秘密字符串值。当 NetScaler Console 显示此参数的值时，它会显示为星号 (*****)。
- **certfile**。证书文件。
- **keyfile**。证书私钥文件。
- **file**。此类型的参数要求用户上传文件，例如证书或密钥文件。
- **object**。由多个元素组成，每个元素都是一个参数。此类型可用于将多个相关参数分组到一个父参数下。

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

- **required**。指示参数是强制性的还是可选的。如果设置为 true，则参数是强制性的，用户在使用此 StyleBook 创建配置时必须为此参数提供值。默认情况下，所有参数都是可选的。在此示例中，**name** 和 **ip** 是强制参数，而 **lb-alg** 是可选参数，其默认值为“ROUNDROBIN”。

使用 **default** 属性为可选参数分配默认值。在创建配置时，如果用户未指定值，则使用默认值。例如，对于 **lb-alg** 参数，默认值为 ROUNDROBIN。

使用 **allowed-values** 属性定义用户在创建配置时可以选择的特定值。在此示例中，您为 **lb-alg** 参数指定了两个值 - ROUNDROBIN 和 LEASTCONNECTION。

导入并使用 StyleBook 时，NetScaler Console 会显示一个包含这三个参数的表单。为 name 和 ip 显示的字段允许输入字符串和 ipaddress 类型的值，lb-alg 字段显示为下拉列表，其中 ROUNDROBIN 选作默认值。

注意

除了内置类型之外，参数还可以将另一个 StyleBook 作为其类型。这是一种重用其他 StyleBook 中定义的参数的方法。

组件

此 StyleBook 中的最后一个部分称为组件部分，被认为是 StyleBook 中最重要的部分。在此部分中，您定义必须由 StyleBook 创建的配置对象。

对于此示例，您必须按如下方式编写组件部分：

```
components:

 -

  name: lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name

   servicetype: HTTP

   ipv46: $parameters.ip
```

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

```
    port: 80

    lbmethod: $parameters.lb-alg
```

此示例仅包含一个组件。组件的主要属性是名称、类型和属性。组件的类型决定了此组件提供的属性。组件分为两种类型：

- **内置类型**。此类型由系统提供，您无需定义它，例如 NITRO 实体类型“lbvserver”或“servicegroup”。在此示例中，您使用的是内置组件类型。
- **复合类型**。此类型是您创建并导入到 NetScaler Console 中的 StyleBook，或者是 NetScaler Console 随附的默认 StyleBook。您可以在创建复合 StyleBook 中了解有关复合 StyleBook 的更多信息。

在此示例中，您定义了一个名为 **lbvserver-comp** 的组件。此组件的类型为 **ns::lbvserver**（一种内置 Nitro 类型），其中“ns”是引用您在 import-stylebooks 部分中指定的命名空间 netscaler.nitro.config 和版本 10.5 的前缀，“lbvserver”是此命名空间中的 Nitro 资源。

此处定义的 **properties** 是“lbvserver”资源的属性。要了解有关所有可用的 NetScaler Nitro 资源及其属性的更多信息，请参阅 NetScaler NITRO REST API 文档。

此部分中的属性包括“lbvserver”资源的强制属性，并允许您为这些属性指定值。在此示例中，您为 servicetype 和 port 指定静态值，而 name、ipv46 和 lbmethod 属性的值则来自输入参数。在 StyleBook 的其余部分中，您可以使用 **$parameters.\<parameter-name\>** 表达式（例如 **$parameters.ip**）引用参数部分中定义的参数名称。

注意

按照惯例，“ns”前缀始终用于在“import-stylebooks”部分中指定 NetScaler Nitro 命名空间。虽然这不是强制性的，但 Citrix 建议您在自己的 StyleBook 中使用相同的约定以保持一致性。

构建您的 StyleBook

既然您已经定义了此 StyleBook 的所有必需部分，请将它们组合起来构建您的第一个 StyleBook。将 StyleBook 内容复制并粘贴到文本编辑器中，然后将文件保存为 **lb-vserver.yaml**。我们建议您使用 StyleBooks 中内置的 YAML 验证器来验证和导入 YAML 内容。

文件 lb-vserver.yaml 的完整内容如下所示：

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

```
name: lb-vserver

namespace: com.example.stylebook

version: "1.0"

display-name: Load Balancing Virtual Server (HTTP)

description: "This stylebook defines a very simple load balancing HTTP
virtual server configuration"

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  version: "10.5"

  prefix: ns

 -

  namespace: com.citrix.adc.stylebooks

  version: "1.0"

  prefix: stlb



parameters:

 -

  name: name

  label: "Application Name"
```

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

```
    description: "Give a name to the application configuration."
    type: string
    required: true
  -
    name: vip-ipaddress
    label: "Load Balancer IP Address"
    description: "The Application VIP that clients access"
    type: ipaddress
    required: true
  -
    name: lb-alg
    label: LB Algorithm
    description: Load Balancing Algorithm
    type: string
    default: ROUNDROBIN
    allowed-values:
     - ROUNDROBIN
     - LEAST-CONNECTION


  components:
   -
    name: lbvserver-comp
```

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

```
  description: This StyleBook component (a Builtin Nitro StyleBook) builds
a NetScaler load balancing virtual server configuration object.

  type: ns::lbvserver

  properties:

   name: $parameters.name

   ipv46: $parameters.vip-ipaddress

   lbmethod: $parameters.lb-alg

   servicetype: HTTP

   port: 80
```

要开始使用您的 StyleBook 创建配置，您必须将其导入 NetScaler Console，然后才能使用它。有关更多信息，请参阅如何使用用户定义的 StyleBook。

您还可以将此 StyleBook 导入其他 StyleBook（使用 import-stylebooks 构造）。或者，您可以修改此 StyleBook 以包含更多参数和组件，如下一节所述。

用于创建基本负载均衡配置的 StyleBook

在前面的示例中，您已经构建了一个用于创建负载均衡虚拟服务器的基本 StyleBook。您可以将此 StyleBook 另存为其他名称，然后更新它以包含用于基本负载均衡配置的附加参数和组件。将此 StyleBook 文件保存为 **basic-lb-config.yaml**。

在本节中，您将设计一个新的 StyleBook，用于创建负载均衡配置，该配置包含负载均衡虚拟服务器、服务组和服务列表。它还将服务绑定到服务组，并将服务组绑定到虚拟服务器。

标头

要构建此 StyleBook，您必须首先更新标头部分。此部分与您为负载均衡虚拟服务器 StyleBook 创建的部分类似。在标头部分中，将 **name** 的值更改为 basic-lb-config。此外，更新 **description** 和 **display-name** 以适当描述此 StyleBook。您无需更改 **namespace** 和 **version** 值。因为您已更改名称，所以名称、命名空间和版本的组合会在系统中为此 StyleBook 创建一个唯一标识符。

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

```
name: basic-lb-config

description: This StyleBook defines a simple load balancing configuration.

display-name: Load Balancing Configuration

namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"
```

导入 StyleBook

import-stylebooks 部分保持不变。它引用 netscaler.nitro.config 命名空间以使用 Nitro 配置对象。

```
import-stylebooks:

 -

 namespace: netscaler.nitro.config

 prefix: ns

 version: "10.5"
```

参数

您必须更新参数部分，以添加两个附加参数来定义服务或服务器列表以及服务侦听的端口。前三个参数 name、ip 和 lb-alg 保持不变。

```
parameters:

 -

 name: name

 type: string

 label: Application Name

 description: Name of the application configuration
```

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

```
 required: true

  -

   name: ip

   type: ipaddress

   label: Application Virtual IP (VIP)

   description: Application VIP that the clients access

   required: true

  -

   name: lb-alg

   type: string

   label: LoadBalancing Algorithm

   description: Choose the load balancing algorithm used for load
balancing client requests between the application servers.

     allowed-values:

     - ROUNDROBIN

     - LEASTCONNECTION

      default: ROUNDROBIN

  -

   name: svc-servers

   type: ipaddress\[\]

   label: Application Server IPs

   description: The IP addresses of all the servers of this application
```

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

```
    required: true

   -

    name: svc-port

    type: tcp-port

    label: Server Port

    description: The TCP port open on the application servers to receive
requests.

    default: 80
```

在此示例中，添加了参数 **svc-servers** 以接受表示应用程序后端服务器的服务 IP 地址列表。这是一个强制参数，由 **required: true** 指示。第二个参数 **svc-port** 表示服务器侦听的端口号。如果用户未指定，svc-port 参数的默认端口号为 80。

组件

您还必须更新组件部分，以定义附加组件，使其使用这两个新参数并构建完整的负载均衡配置。

在此示例中，您必须按如下方式编写组件部分：

```
components:

 -

  name: lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name + "-lb"

   servicetype: HTTP

   ipv46: $parameters.ip

   port: 80
```

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

```
    lbmethod: $parameters.lb-alg



  components:

   -

    name: svcg-comp

    type: ns::servicegroup

    properties:

     name: $parameters.name + "-svcgrp"

     servicetype: HTTP



  components:

   -

    name: lbvserver-svg-binding-comp

    type: ns::lbvserver\_servicegroup\_binding

    properties:

     name: $parent.parent.properties.name

     servicegroupname: $parent.properties.name

   -

    name: members-svcg-comp

    type: ns::servicegroup\_servicegroupmember\_binding

    repeat: $parameters.svc-servers

    repeat-item: srv
```

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

```
properties:

 ip: $srv

 port: str($parameters.svc-port)

 servicegroupname: $parent.properties.name
```

在此示例中，原始组件 **lbvserver-comp**（来自前面的示例）现在有一个名为 **svcg-comp** 的子组件。并且，**svcg-comp** 组件内部有两个子组件。将一个组件嵌套在另一个组件中，允许嵌套组件通过引用父组件中的属性来创建配置对象。嵌套组件可以为父组件中创建的每个对象创建一个或多个对象。

svcg-comp 组件用于在 NetScaler 实例上创建服务组，方法是使用为资源“servicegroup”的属性提供的值。在此示例中，您为 servicetype 指定了静态值，而 name 的值则来自输入参数。您通过使用 **$parameters.name + "-svcgrp"** 符号来引用参数部分中定义的参数 **name**，其中 **-svcgrp** 附加（连接）到用户定义的名称。

组件 **svcg-comp** 有两个子组件：**lbvserver-svg-binding-comp** 和 **members-svcg-comp**。

第一个子组件 **lbvserver-svg-binding-comp** 用于在其父组件创建的服务组与父组件的父组件创建的负载平衡虚拟服务器 (lbvserver) 之间绑定配置对象。$parent 符号（也称为父引用）用于引用父组件中的实体。例如，**servicegroupname: $parent.properties.name** 引用由父组件 **svcg-comp** 创建的服务组，而 **name: $parent.parent.properties.name** 引用由父组件的父组件 **lbvserver-comp** 创建的虚拟服务器。

组件 **members-svcg** 用于在服务列表与父组件创建的服务组之间绑定配置对象。通过使用 StyleBook 的 **repeat** 构造迭代参数 **svc-servers** 中指定的服务器列表，可以创建多个绑定配置对象。在迭代过程中，此 StyleBook 组件会为服务组中的每个服务（在 **repeat-item** 构造中称为 srv）创建一个类型为 **servicegroup_servicegroupmember_binding** 的 Nitro 配置对象，并将每个 Nitro 配置对象中的 **ip** 属性设置为相应服务器的 IP 地址。

通常，您可以在组件中使用 **repeat** 和 **repeat-item** 构造，使该组件构建多个相同类型的配置对象。您可以为 **repeat-item** 构造分配一个变量名，例如 srv，以指定迭代中的当前值。此变量名在同一组件的属性或子组件中引用为 **$\<varname\>**，例如 $srv。

在上面的示例中，您使用了组件的相互嵌套来轻松构建此配置。在这种特定情况下，组件嵌套并不是构建配置的唯一方法。您可以在不嵌套的情况下实现相同的结果，如下所示：

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

```
components:

 -

  name: members-svcg-comp

  type: ns::servicegroup\_servicegroupmember\_binding

  repeat: $parameters.svc-servers

  repeat-item: srv

  properties:

   ip: $srv

   port: str($parameters.svc-port)

   servicegroupname: $components.svcg-comp.properties.name

 -

  name: lbvserver-svg-binding-comp

  type: ns::lbvserver\_servicegroup\_binding

  properties:

   name: $components.lbvserver-comp.properties.name

   servicegroupname: $components.svcg-comp.properties.name

 -

  name: lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name + "-lb"

   servicetype: HTTP
```

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

```
    ipv46: $parameters.ip

    port: 80

    lbmethod: $parameters.lb-alg

  -

   name: svcg-comp

   type: ns::servicegroup

   properties:

   name: $parameters.name + "-svcgrp"

   servicetype: HTTP
```

在这里，所有组件都处于同一级别（即它们没有嵌套），但所实现的结果（生成的 NetScaler 配置）与之前使用的嵌套组件的结果相同。此外，StyleBook 中组件的声明顺序不影响配置对象的创建顺序。在此示例中，组件 **svcg-comp** 和 **lbvserver-comp** 即使最后声明，也必须在构建第二个组件 **lbvserver-svg-binding-comp** 之前构建，因为第二个组件中存在对这些组件的前向引用。

注意

按照惯例，StyleBook、参数、替换、组件和输出的名称都使用小写。当它们包含多个单词时，用“ - ”字符分隔。例如，“lb-bindings”、“app-name”、“rewrite-config”等。另一个惯例是组件名称以“-comp”字符串作为后缀。

输出

您可以添加到新 StyleBook 的最后一个部分是输出部分，您可以在其中指定此 StyleBook 在用于创建配置后向其用户（或在其他 StyleBook 中）公开的内容。例如，您可以在输出部分中指定公开将由此 StyleBook 创建的 lbvserver 和服务组配置对象。

```
 outputs:

  -

   name: lbvserver-comp
```

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

```
  value: $components.lbvserver-comp

  description: The component that builds the Nitro lbvserver configuration
object

 -

  name: servicegroup-comp

  value: $components.svcg-comp

  description: The component that builds the Nitro servicegroup
configuration object
```

StyleBook 的输出部分是可选的。StyleBook 不需要返回输出。但是，通过将一些内部组件作为输出返回，它允许导入此 StyleBook 的任何 StyleBook 具有更大的灵活性，这在创建复合 StyleBook 时可以看到。

注意

最佳实践是在输出部分公开 StyleBook 的整个组件，而不仅仅是组件的单个属性（例如，公开整个 $components.lbvserver-comp 而不是仅公开名称 $components.lbvserver-comp.properties.name）。此外，还要为输出添加描述，解释特定输出所代表的内容。

构建您的 StyleBook

现在您已经定义了此 StyleBook 的所有必需部分，将它们组合在一起以构建您的第二个 StyleBook。您已将此 StyleBook 文件保存为 **basic-lb-config.yaml**。我们建议您使用 StyleBooks 页面中内置的 YAML 验证器来验证和导入 YAML 内容。

文件 **basic-lb-config.yaml** 的完整内容如下所示：

```
name: basic-lb-config

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Configuration

description: This StyleBook defines a simple load balancing configuration.
```

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

```
schema-version: "1.0"


import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
```

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

```
  type: string

  label: LoadBalancing Algorithm

  description: Choose the loadbalancing algorithm (method) used for
loadbalancing client requests between the application servers.

  allowed-values:

     - ROUNDROBIN

     - LEASTCONNECTION

  default: ROUNDROBIN

 -

  name: svc-servers

  type: ipaddress[]

  label: Application Server IPs

  description: The IP addresses of all the servers of this application

  required: true



components:

 -

  name: lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name + "-lb"

   servicetype: HTTP
```

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

```
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
  -
   name: svcg-comp
   type: ns::servicegroup
   properties:
     servicegroupname: $parameters.name + "-svcgrp"
     servicetype: HTTP


  -
   name: lbvserver-svg-binding-comp
   type: ns::lbvserver_servicegroup_binding
   properties:
    name: $components.lbvserver-comp.properties.name
    servicegroupname: $components.svcg-comp.properties.servicegroupname
  -
   name: members-svcg-comp
   type: ns::servicegroup_servicegroupmember_binding
   repeat: $parameters.svc-servers
   repeat-item: srv
   properties:
```

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

```
    ip: $srv

    port: 80

    servicegroupname: $components.svcg-comp.properties.servicegroupname

outputs:

-

  name: lbvserver-comp

  value: $components.lbvserver-comp

  description: The component that builds the Nitro lbvserver configuration
object

-

  name: servicegroup-comp

  value: $components.svcg-comp

  description: The component that builds the Nitro servicegroup
configuration object
```

要开始使用您的 StyleBook 创建配置，您必须将其导入到 NetScaler Console，然后才能使用它。有关更多信息，请参阅如何使用用户定义的 StyleBook。

您还可以将此 StyleBook 导入到其他 StyleBook 中，并使用其属性，如下一节所述。

创建复合 StyleBook

StyleBook 的一个重要且强大的功能是它们可以作为其他 StyleBook 的构建块。一个 StyleBook 可以导入到另一个 StyleBook 中，并且可以将其称为第二个 StyleBook 的组件所使用的**类型**，类似于 Nitro 内置 StyleBook。

例如，您可以使用在上一节中构建的 **basic-lb-config** StyleBook 来构建另一个名为 **composite-example** 的 StyleBook。要使用“basic-lb-config”StyleBook，您必须在新的 StyleBook 的 import-stylebooks 部分中导入它。

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

构建您的 StyleBook

新的 StyleBook 如下所示：

```
name: composite-example

namespace: com.example.stylebooks

version: "0.1"

display-name: Load Balancing Virtual Server (HTTP/RoundRobin)

description: This StyleBook defines a RoundRobin load balancing
configuration with a monitor.

schema-version: "1.0"

import-stylebooks:

  -

   namespace: netscaler.nitro.config

   version: "10.5"

   prefix: ns

  -

   namespace: com.example.stylebooks

   version: "0.1"

   prefix: stlb

parameters:

  -

    name: name

    type: string

    label: Application Name
```

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

```
    description: Give a name to the application configuration.

    required: true

  -

    name: ip

    type: ipaddress

    label: Application Virtual IP (VIP)

    description: The Application VIP that clients access

    required: true

  -

    name: svc-servers

    type: ipaddress[]

    label: Application Server IPs

    description: The IP addresses of all the servers of this application

    required: true



  -

    name: response-code

    type: string[]

    label: List of Response Codes

    description: List of Response Codes - Provide a list of response codes
in integer.
```

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

```
components:

  -

    name: basic-lb-comp

    type: stlb::basic-lb-config

    description: This component's type is another StyleBook that builds
the NetScaler lbvserver, servicegroups and services configuration objects.

    properties:

     name: $parameters.name

     ip: $parameters.ip

     svc-servers: $parameters.svc-servers

  -

     name: monit-comp

     type: ns::lbmonitor

     description: This component is a basic Nitro type (a Builtin
StyleBook) that builds the NetScaler monitor configuration object.

     properties:

       monitorname: $parameters.name + "-mon"

       type: HTTP

       respcode: $parameters.response-code

       httprequest: "'GET /'"

       lrtm: ENABLED

       secure: "YES"
```

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

```
    components:

      -

        name: monit-svcgrp-bind-comp

        type: ns::servicegroup_lbmonitor_binding

        properties:

          servicegroupname: $components.basic-lb-
comp.outputs.servicegroup-comp.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

在 import-stylebooks 部分中，您通过使用其命名空间和版本（前缀为“stlb”）来导入 basic-lb-config StyleBook。

在 components 部分中，定义了两个组件。第一个组件的类型为 **stlb::basic-lb-config**，其中“basic-lb-config”是您在 StyleBook to create a basic load balancing configuration 中创建的 StyleBook 的名称。为此组件定义的属性对应于 basic-lb-config StyleBook 中声明的强制参数。但是，您可以使用 StyleBook 的任何参数（包括必需参数和可选参数）。您无需重新构建 lbvserver、服务组以及服务和服务组绑定，而是将执行所有这些操作的 StyleBook 作为组件导入，并使用它在新 StyleBook 中创建这些配置对象。

StyleBook 添加了第二个组件“monit-comp”，它使用 Nitro 资源“lbmonitor”（一个内置 StyleBook）的属性来创建监视器配置对象。它还有一个子组件“monit-svcgrp-bind-comp”，用于创建将监视器绑定到第一个组件中创建的服务组的绑定配置对象。由于在“basic-lb-config”StyleBook 中创建的服务组组件作为输出公开，因此此 StyleBook 可以使用表达式 **$components.basic-lb-comp.outputs.servicegroup-comp** 访问它。这是一个示例，说明导入 StyleBook 如何使用 outputs 部分来访问导入 StyleBook 中的组件，否则它们将无法访问这些组件。

接下来，将 StyleBook 内容复制并粘贴到文本编辑器中，然后将文件另存为 **composite-example.yaml**。在将文件导入 NetScaler Console 之前，请务必验证 YAML 内容。然后，将其导入 NetScaler Console 并使用此 StyleBook 创建一个或多个配置。

我们建议您使用 StyleBook 中内置的 YAML 验证器来验证和导入 YAML 内容。

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

在自定义 StyleBook 中使用 GUI 属性

您可以在 StyleBook 的参数部分添加 GUI 属性，以便在 NetScaler Console 上显示时使字段更直观。

示例。您可以使用 label 属性为参数添加描述性名称，并使用 description 属性为此参数添加工具提示。

```
name: ip

label: Virtual Server IP Address

description: IP address of the virtual server that represents the load
balanced application.

type: ipaddress

required: true
```

示例。如果您的参数是对象类型，您可以使用 **gui** 属性定义布局。在此示例中，布局是一个可折叠对象，其中字段以两列显示。

```
name: svcg-advanced

label: Advanced Application Server Settings

type: object

required: false

gui:

 collapse_pane: true

 columns: 2
```

示例。NetScaler Console 上的一些 StyleBook 仅用作其他 StyleBook 的构建块。而且，您可能不希望用户直接从这些 StyleBook 创建配置。因为这些 StyleBook 将作为其他 StyleBook 的一部分使用。将 StyleBook 标记为私有，以确保 StyleBook 不会直接用于在 NetScaler Console GUI 中创建配置。

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

```
name: basic-lb-config

description: This stylebook defines a simple load balancing configuration.

display-name: Load Balancing Configuration

namespace: com.example.stylebooks

private: true

schema-version: "1.0"

version: "0.1"
```

导入自定义 StyleBook

构建 StyleBook 后，您必须将其导入 NetScaler Console 才能使用。NetScaler Console 允许您以 YAML 形式导入单个 StyleBook，或以 .zip、.tgz 或 .gz 形式的捆绑包导入多个 StyleBook YAML 文件。NetScaler Console 系统会在导入时验证您的 StyleBook。现在，该 StyleBook 已可用于创建配置。

NetScaler Console 还内置了一个 YAML 编辑器，您可以使用它来编写 StyleBook YAML 内容。YAML 编辑器允许您直接从 NetScaler Console GUI 验证您的 YAML 构造。您无需使用单独的工具进行这些验证检查。内容会根据 YAML 标准进行验证，任何偏差都会突出显示。然后，您可以更正内容并尝试将 StyleBook 导入 NetScaler Console。内置 YAML 编辑器在编写您自己的 StyleBook 时提供两个优势。

- **颜色编码**。编辑器会根据 YAML 准则显示解析后的 StyleBook 内容，颜色编码有助于您轻松区分 YAML 内容中定义的键和值。
- **YAML 验证**。在您键入时，内容会验证是否存在任何 YAML 错误，任何偏差都会立即突出显示。此验证允许您在将 StyleBook 导入 NetScaler Console 之前编写符合 YAML 准则的文本。

注意：

目前，编辑器根据 YAML 准则验证内容。它不验证代码正确性和排版错误。

导入您的 StyleBook

1. 在 NetScaler Console 中，导航到 **Applications** > **Configuration** > **StyleBooks**，然后单击 **Import New StyleBook**。

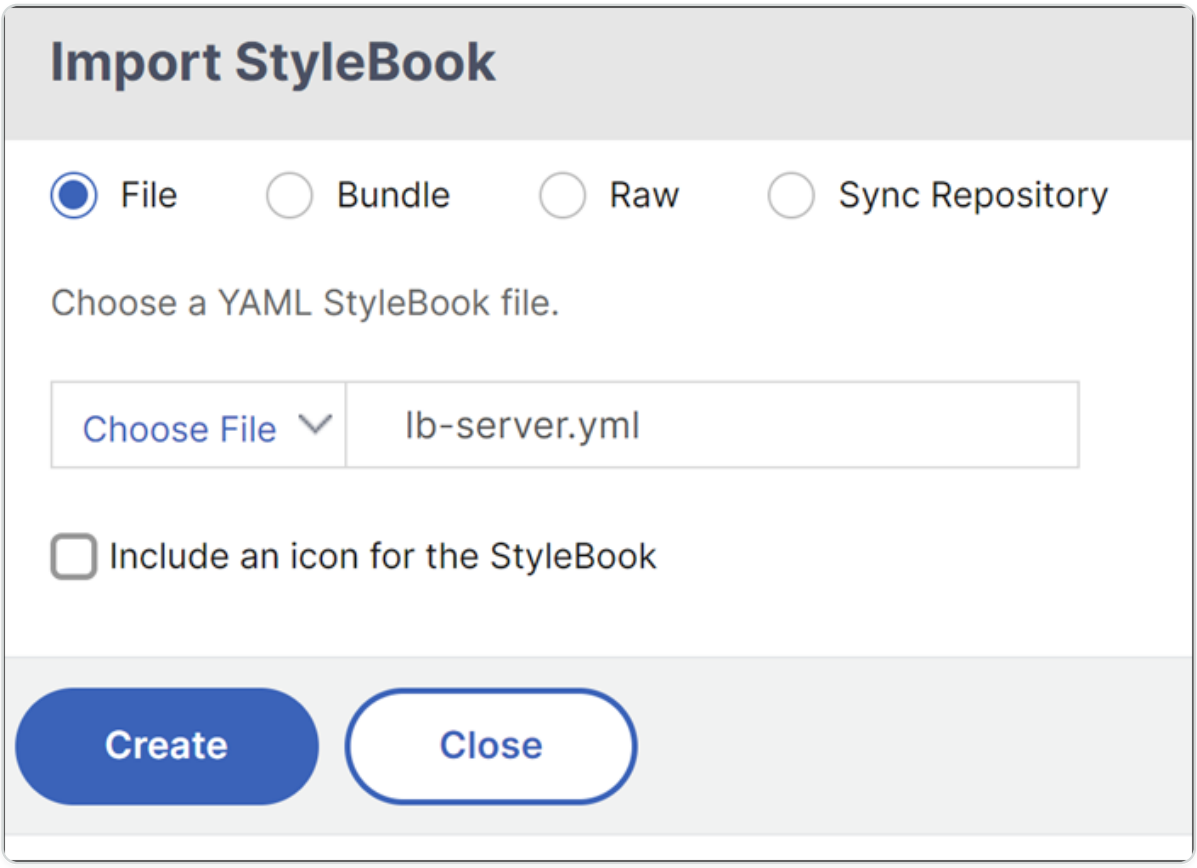
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 单击以下选项之一导入 StyleBook。

   - **文件** - 从本地存储中选择所需文件或文件捆绑包。

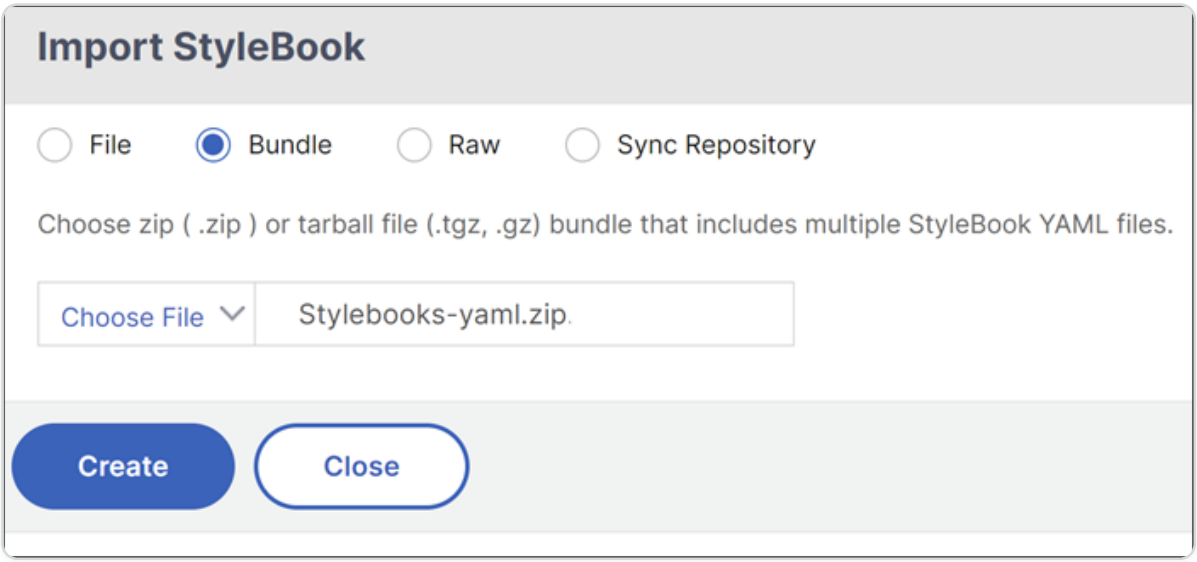
     注意：

     在此示例中，导入您在 StyleBook to Create a Load Balancing Virtual Server 中创建的 `lb-vserver.yml` StyleBook。



   - **捆绑包** - NetScaler Console 允许您以 YAML 格式导入多个 StyleBook。您可以导入多个以 zip (.zip) 格式或 tarball (.tgz, .gz) 格式压缩的 YAML StyleBook 文件。

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



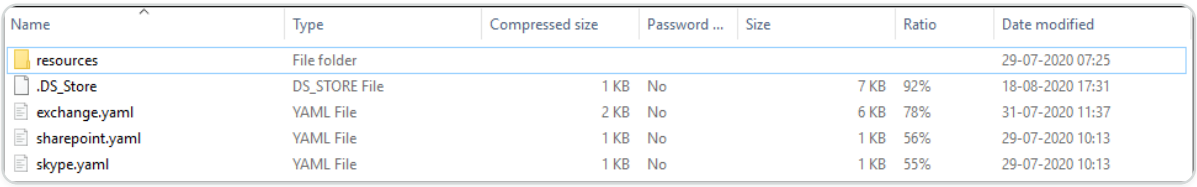
您现在可以将图标包含到捆绑包中的每个 StyleBook。请确保拥有包含 PNG、GIF 或 JPEG 格式图标的 resources 文件夹。如果图标文件名与 StyleBook 名称匹配，则图标会自动映射到 StyleBook。否则，请执行以下操作：

a. 将 `icon_mapping.json` 文件添加到 resources 文件夹中。

b. 在 `icon_mapping.json` 文件中按如下方式映射 StyleBook 和图标：

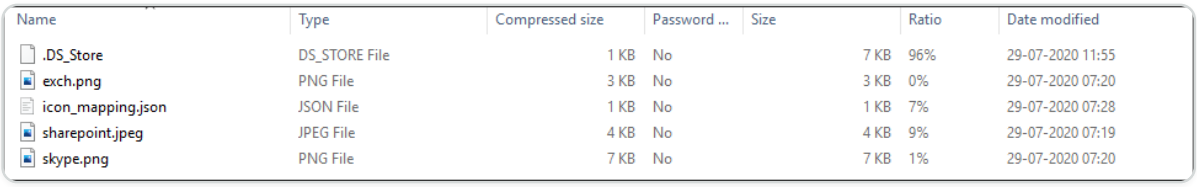
```
<StyleBook file name> : <icon file name>
```

以下是一个 StyleBook 捆绑包示例：



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
resources	File folder					29-07-2020 07:25
.DS_Store	DS_STORE File	1 KB	No	7 KB	92%	18-08-2020 17:31
exchange.yaml	YAML File	2 KB	No	6 KB	78%	31-07-2020 11:37
sharepoint.yaml	YAML File	1 KB	No	1 KB	56%	29-07-2020 10:13
skype.yaml	YAML File	1 KB	No	1 KB	55%	29-07-2020 10:13

`resources` 文件夹包含所需的图标。



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
.DS_Store	DS_STORE File	1 KB	No	7 KB	96%	29-07-2020 11:55
exch.png	PNG File	3 KB	No	3 KB	0%	29-07-2020 07:20
icon_mapping.json	JSON File	1 KB	No	1 KB	7%	29-07-2020 07:28
sharepoint.jpeg	JPEG File	4 KB	No	4 KB	9%	29-07-2020 07:19
skype.png	PNG File	7 KB	No	7 KB	1%	29-07-2020 07:20

在此示例中，`sharepoint.yaml` 和 `skype.yaml` 文件分别自动映射到 `sharepoint.jpeg` 和 `skype.png`。

要将 `exchange.yaml` 映射到 `exch.png`，请在 `icon_mapping.json` 文件中指定以下内容：

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

```
{

"exchange.yaml":"exch.png"

}
```

如果您指定 `defaulticon` 条目，则 StyleBook 将映射到默认图标，除非它们已映射到其他图标。

```
defaulticon: <icon file name>
```

在 **Applications > StyleBooks** 中，导入的 StyleBook 将显示映射的图标。

- **Raw** - 在 YAML 编辑器中编写 StyleBook 的内容。

  您可以验证 StyleBook 内容以检查 StyleBook 语法错误。要验证 StyleBook 内容，请单击 **Validate Contents**。

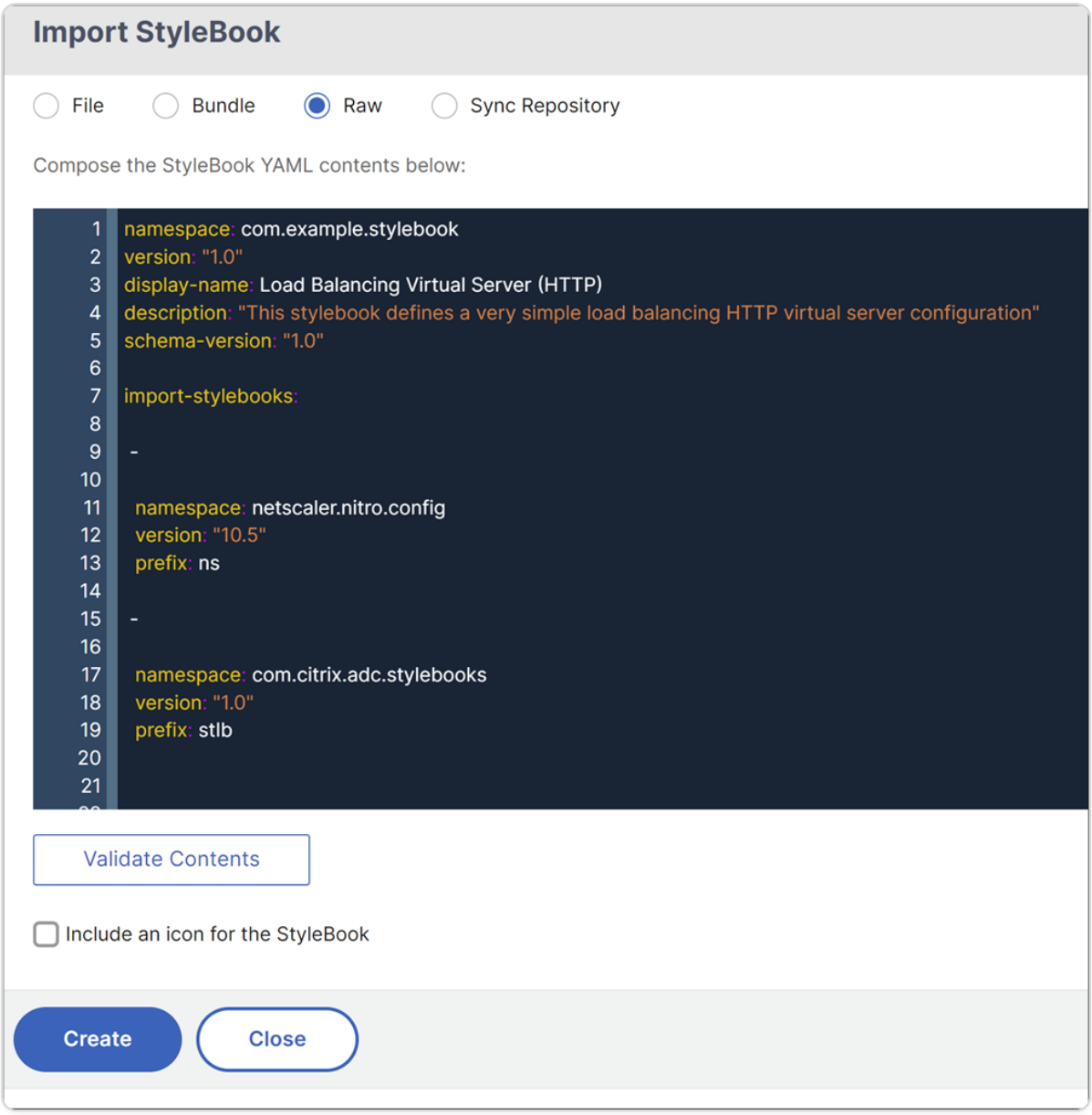
  注意：

  在编写 StyleBook 时，请确保了解以下概念：

  - NITRO API
  - YAML

  有关如何编写自己的 StyleBook 的更多信息，请参阅 如何创建自己的 StyleBook。

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



- **同步存储库** - 此选项列出了添加到 NetScaler Console 的存储库。选择要与 NetScaler Console 同步的存储库。

> **注意：**
>
> 您还可以将 StyleBook YAML 文件的内容复制并粘贴到 YAML 编辑器中。

3. 可选，为 StyleBook 选择一个图标。

   在 **应用程序 > StyleBook** 中，导入的 StyleBook 将显示此图标。

4. 单击**创建**。

   NetScaler Console 现在会根据 StyleBook 语法验证您的 StyleBook 是否存在所有语法和语义错误。如果存在任何错误，您的 StyleBook 将不会导入到 NetScaler Console 中。

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

如果没有错误，StyleBook 将成功导入并列在**StyleBooks**页面上。您可以通过在 StyleBook 的标头部分中定义的显示名称来识别 StyleBook。

> **注意：**
>
> 如果您正在导入文件包，NetScaler Console 会解压缩压缩文件夹并验证所有 StyleBook。即使一个 StyleBook 文件未能通过验证测试，该文件包也不会被导入。

有关 StyleBook 语法以及不同构造和属性的语法的更多信息，请参阅 StyleBook 语法。

5. 单击“**创建配置**”链接，从此 StyleBook 创建配置。

   StyleBook 将作为用户界面页面打开，您可以在其中输入此 StyleBook 中定义的所有参数的值。

6. 为参数指定所需的值。

   在以下示例中，

   a. 指定“**应用程序名称**”和“**负载均衡器 IP 地址**”必填字段。

   b. 从列表中选择“**负载均衡算法**”。默认情况下，选择“**ROUNDROBIN**”。

7. 在“**目标实例**”下，选择要部署配置的 NetScaler 实例的 IP 地址。

   您还可以通过指定所需数量的目标实例，将配置部署到多个 NetScaler 上。

8. 如果要在部署配置之前测试 NetScaler (NITRO) 配置对象，请单击“**试运行**”。

   如果配置有效，则会根据指定值创建配置对象。

   在此示例中，StyleBook 仅创建类型为 `lbvserver` 的一个对象。此负载均衡服务器是此基本示例 StyleBook 中定义的唯一组件。

   稍后，单击“**创建**”以将配置部署到选定的 NetScaler 实例上。

成功部署配置后，新的配置包将显示在“**配置**”页面中。

> **注意：**
>
> 您还可以单击刷新图标，将 NetScaler Console 中最近发现的 NetScaler 实例添加到此窗口中可用的实例列表中。

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

搜索自定义 StyleBook

NetScaler Console 现在允许您根据 StyleBook 的类型进行搜索。也就是说，您现在可以搜索默认 StyleBook 或自定义 StyleBook。当您需要在众多默认 StyleBook 中搜索用户定义的 StyleBook 时，此选项特别有用。

搜索自定义 StyleBook

1. 在 NetScaler Console 中，导航到 **应用程序** > **配置** > **StyleBook**。
2. 单击右上角的搜索图标。
3. 在搜索栏中，选择 **类型**，然后从子列表中选择 **自定义**。
4. NetScaler Console 仅显示用户定义的 StyleBook。

创建和编辑配置包

在 NetScaler Console 中，您可以从 StyleBook 创建配置包。配置包与其创建的 StyleBook 绑定。配置包的更新通过其绑定的 StyleBook 进行。

创建配置包

执行以下操作以从 StyleBook 创建配置包：

1. 导航到 **应用程序 > StyleBooks > 配置**。
2. 单击 **添加**。
3. 在 **选择 StyleBooks** 中，选择要从中创建配置包所需的 StyleBooks。

   此页面将 StyleBooks 分为默认 StyleBooks 和自定义 StyleBooks。选择相应的选项卡以查找所需的 StyleBooks。
4. 指定所需详细信息，例如应用程序名称、IP 地址、端口或协议类型。

   GUI 字段因 StyleBook 而异。
5. 在 **目标实例** 中，选择要运行配置的实例或实例组。

   > **注意：**
   >
   > 您可以通过指定所需数量的目标实例，将配置部署到多个 NetScaler 上。

6. 单击 **试运行**。

   对象 页面显示从 NetScaler 实例创建、修改或删除的对象。
7. 点击 **创建**

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

配置包显示在 **StyleBook > Configurations** 页面中。

如果要编辑现有配置包，请选择配置包，然后点击 **编辑**。

重用在 StyleBooks 外部创建的配置并在 ConfigPacks 之间共享配置

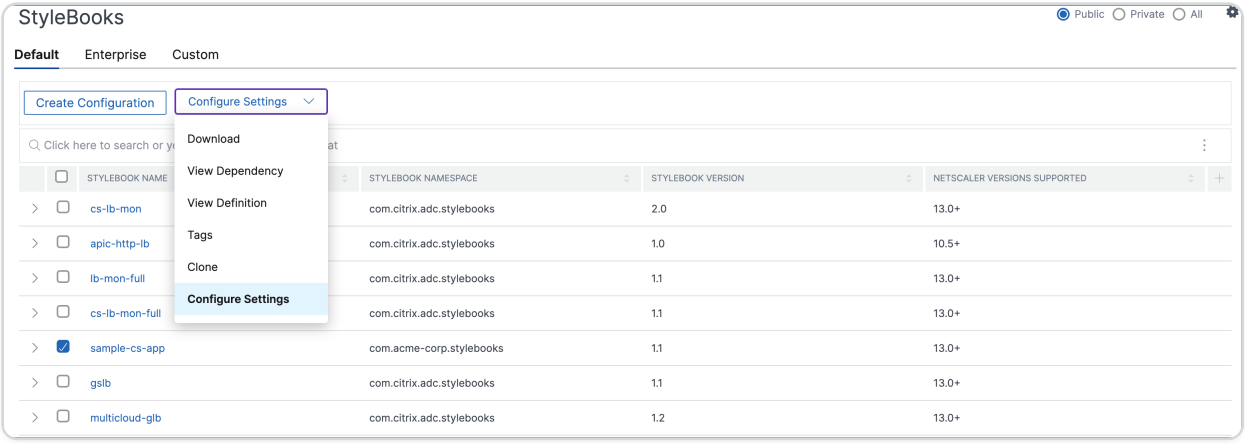
有时，您可能在 Stylebooks 之外创建了 NetScaler® 配置，无论是由于特定的操作需求还是旧版设置。您现在可以将这些以前存在的配置作为 Stylebook 配置包的一部分进行集成和管理，从而实现更灵活和集中的管理。

例如，在此功能之前，如果 NetScaler 已配置 SSL 配置文件，并且 StyleBook 的配置包操作尝试创建同名的 SSL 配置文件，则配置包操作将因“资源已存在”错误而失败。现在，启用此功能后，配置包操作会成功，并且同名的现有 SSL 配置文件可以在新配置包中重用。

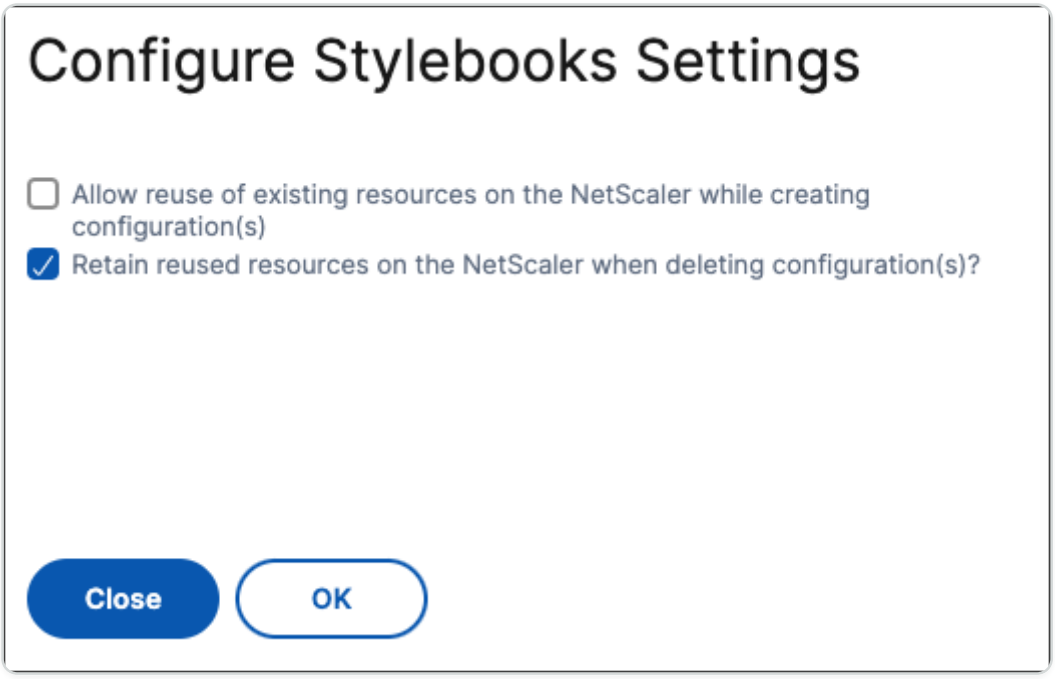
同样，您可能还会遇到网络设置、安全策略或部分应用程序配置等资源在多个应用程序或配置中都需要的情况。此功能使您能够在多个配置包之间共享配置。

要启用此功能，请按照以下步骤操作：

1. 导航到 应用程序 > 配置 > Stylebooks。
2. 在 Stylebooks 页面上，选择您将用于创建新配置包的 Stylebook，或与您正在编辑的配置包关联的 Stylebook。
3. 在“选择操作”中，点击“配置设置”。



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



4. 通过选择以下一个或两个选项来调整设置：

   - 要在创建配置时启用 NetScaler 上现有资源的重用，请选择选项 **允许在创建配置时重用 NetScaler 上的现有资源**。
   - 要在删除配置时保留 NetScaler 上重用的资源，请选择选项 **删除配置时是否保留 NetScaler 上重用的资源？**。此选项会在 NetScaler 上保留最初在 Stylebooks 之外创建的资源，即使引用它们的最后一个配置包被删除，从而确保其持续可用性。

5. 点击 **确定**。

更改配置包的 StyleBook

有时，您需要更新 StyleBook 以添加功能或修复问题。如果您已经使用旧的 StyleBook 创建了配置包，您可能希望更新它们以使用新的更新后的 StyleBook。要使用新的 StyleBook，请更改配置包的现有 StyleBook。

考虑一个示例 StyleBook **example-lb**，它在 NetScaler 实例上部署基本的负载均衡器配置。然后，您从此 StyleBook 创建一个配置包 CP1。

当您想要使用基本的负载均衡器配置来配置监视器时，您需要一个新的 StyleBook。因此，创建 **example-lb-mon** StyleBook，它包含配置监视器以及基本负载均衡器配置的功能。

创建 StyleBook 后，更新现有配置包 CP1 以添加一些监视器。为此，请执行以下操作：

1. 导航到 **应用程序 > StyleBooks > 配置**。
2. 选择您要更改其 StyleBook 的配置包。

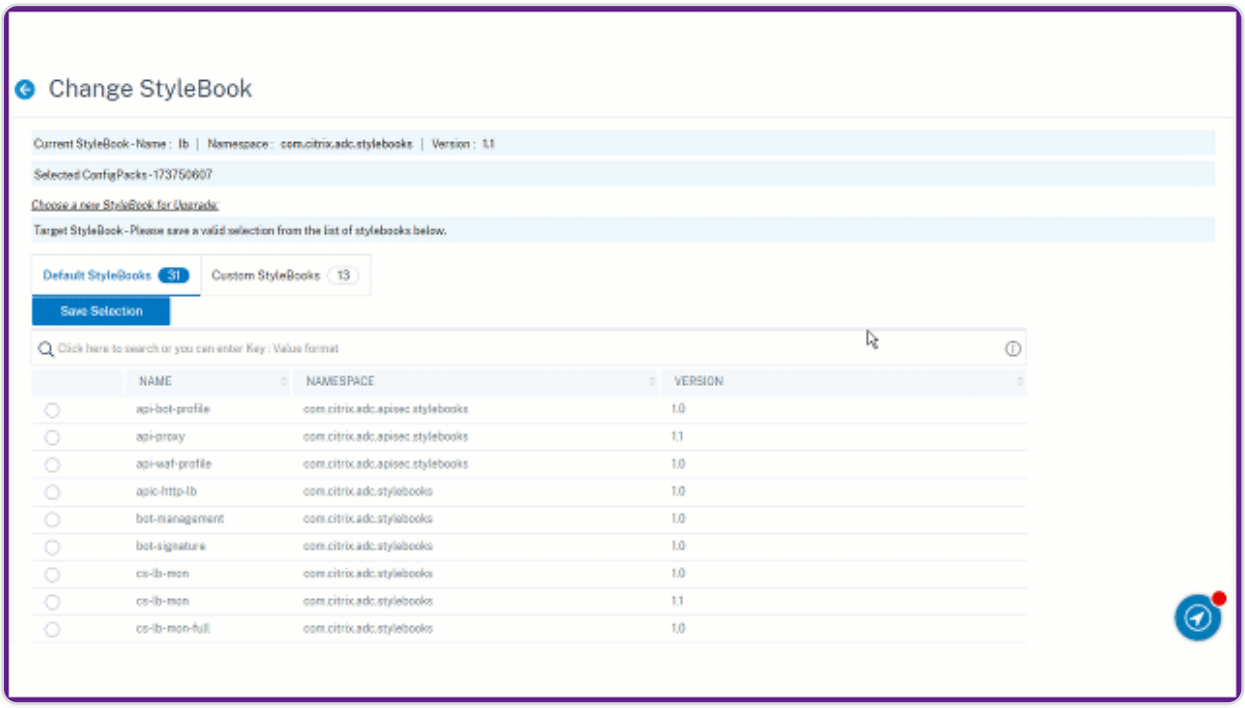
   在此示例中，从列表中选择 CP1。

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

3. 点击 **更改 StyleBook**。
4. 从列表中选择所需的 StyleBook。然后，点击 **保存选择**。
5. 点击 **更改**。

   在此示例中，从列表中选择 **example-lb-mon**。

   当您更改配置包的 StyleBook 时，新 StyleBook 中的参数结构可能与现有 StyleBook 不同。如果参数结构与之前的 StyleBook 相似，参数值将自动保留在其各自的字段中。否则，只有在两个 StyleBook 之间具有相同结构的参数才会被传输。例如，相同的参数名称、类型、参数父级等。



   如果在新 StyleBook 中添加了新的必需参数，更改 StyleBook 后，您必须手动指定这些参数的值。

   在此示例中，**example-lb** StyleBook 的配置页面上显示的参数如下：

   负载均衡配置包示例(/en-us/netscaler-application-delivery-management-software/media/nmas-migrate-configpack-3.png)

   新的 **example-lb-mon** StyleBook 的配置页面上显示的参数如下：

   配置包迁移后的参数示例(/en-us/netscaler-application-delivery-management-software/media/nmas-migrate-configpack-4.png)

   在这种情况下，StyleBook 会保留基本负载均衡器配置的旧值，因为新的 StyleBook 未更改现有参数。它只添加了新参数。对于监视器参数，请手动指定所需值。
6. 在**目标实例**中，查看所选实例并在必要时更新列表。

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

7. 单击**试运行**。

   对象页面显示从 NetScaler 实例创建、修改或删除的对象。

8. 单击**确定**。

   在**StyleBook > 配置**页面中，**StyleBook 名称**列显示所选配置包的新 StyleBook 名称。在此示例中，它显示 **example-lb-mon**。

更改具有多个配置包的 StyleBook

更改具有多个配置包的现有 StyleBook 时，请执行以下操作：

1. 将新的 StyleBook 导入 NetScaler Console。

   通常，新的 StyleBook 具有与现有 StyleBook 相同的名称和命名空间，但版本更高。但是，如果名称、命名空间或版本不同，则可以跳过此步骤。

2. 更改与现有 StyleBook 关联的配置包的 StyleBook。

   仅当所选配置包与同一 StyleBook 关联时，才能选择“**更改 StyleBook**”。

   对于所选配置包，当满足以下条件时，NetScaler Console 会成功更改 StyleBook：

   - 现有 StyleBook 的所有配置参数都必须存在于所选 StyleBook 中。
   - 所选 StyleBook 中的新参数是可选的。

   要查看所选配置包的进度，请在“**配置**”页面中选择“**正在进行/失败的配置**”。

3. 一旦所有配置包都绑定到新的 StyleBook，请从 NetScaler Console 中删除旧的 StyleBook。

导出或导入配置包

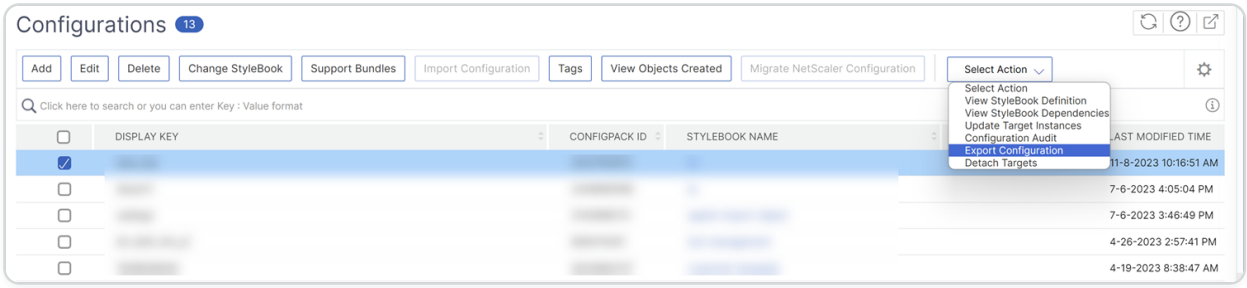
您可以像 StyleBook 一样导出或导入配置包。借助此功能，您可以轻松地将 StyleBook 配置共享到另一个 NetScaler Console。导出配置包时，`tgz` 或 `zip` 捆绑包会下载到您的本地计算机。此捆绑包包含一个 JSON 文件，其中包含配置包中定义的所有参数。

导出配置

要导出配置包，请执行以下操作：

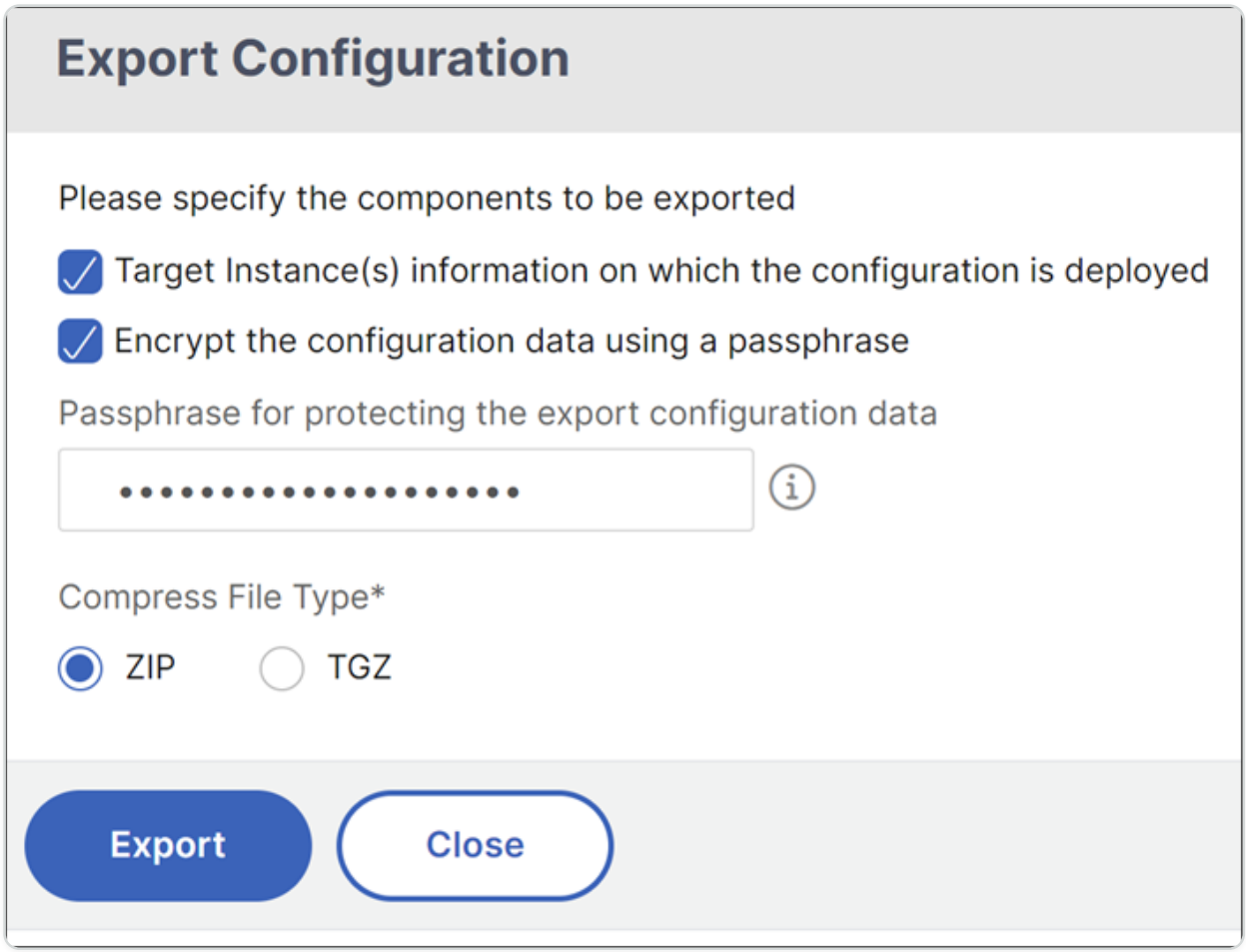
1. 导航到“**应用程序 > StyleBooks > 配置**”。
2. 选择要导出的配置包。
3. 在“**选择操作**”中，选择“**导出配置**”。

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



4. 在“**导出配置**”窗格中，指定以下内容：

   - **部署配置的目标实例信息**：选择此选项可将目标实例的信息包含在导出包中。
   - **与配置关联的 StyleBook**：选择此选项可将 StyleBook 包含在导出包中。
   - **用于保护导出配置数据的密码**：指定一个密码来加密导出包。此密码可保护配置包的敏感数据。
   - **压缩文件类型**：选择 **ZIP** 或 **TGZ** 文件类型。



5. 单击“**导出**”。

   将导出包保存到本地计算机上。

导入配置

您可以将配置包从本地计算机导入到其他 NetScaler Console。要导入配置包，请执行以下操作：

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

1. 导航到“**应用程序 > StyleBooks > 配置**”。
2. 选择“**导入配置**”。
3. 从计算机中选择导入文件包。
4. 使用您在导出期间指定的密码。
5. 可选，在“高级选项”中，选择“**仅当所有配置对象已存在于 NetScaler 上时才允许创建新配置**”。

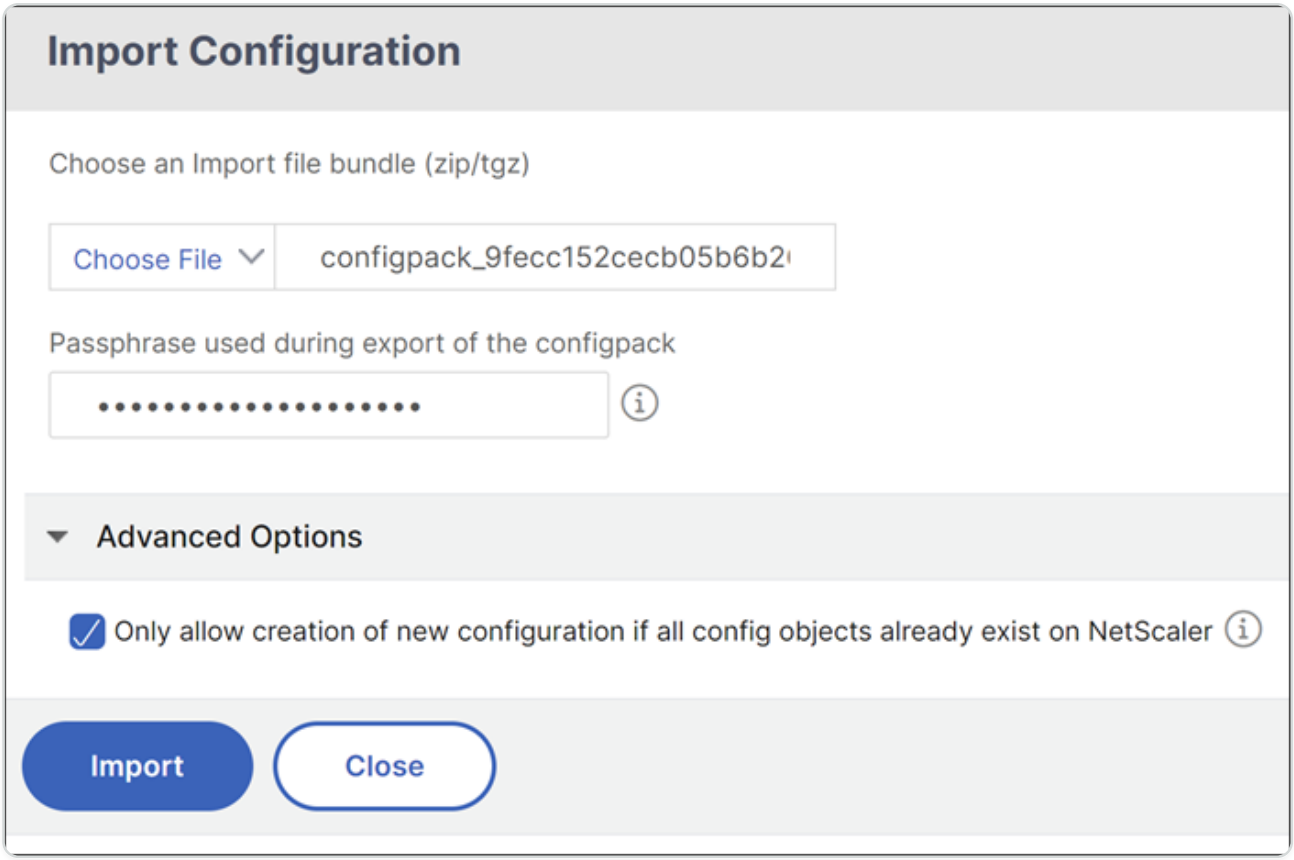
   此选项不会更改已在 NetScaler 实例上创建的对象。

   假设您在两个 NetScaler Console 服务器中添加了相同的 NetScaler 实例。并且，您想要将配置包从一个 NetScaler Console 服务器迁移到另一个服务器。使用此选项可以导入配置包，而无需更改其在 NetScaler 实例上的配置对象。

   重要

   要使用此选项，请确保指定的配置包包含目标实例信息。请参阅导出配置。

   仅当所有对象都存在于目标实例上时，此选项才会迁移配置。
6. 单击“**导入**”。



导入配置包时，NetScaler Console 会验证以下内容：

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

- **关联的 StyleBook**：如果关联的 StyleBook 不在 NetScaler Console 中，它会随配置包一起导入 StyleBook。
- **目标实例**：检查目标实例并在指定的目标实例上部署配置。如果 NetScaler Console 中不存在提及的 NetScaler 实例，则导入配置包时不会包含目标实例。
- **源 NetScaler Console**：如果您在同一 NetScaler Console 服务器上导入配置包，则所选捆绑包会更新现有配置包。

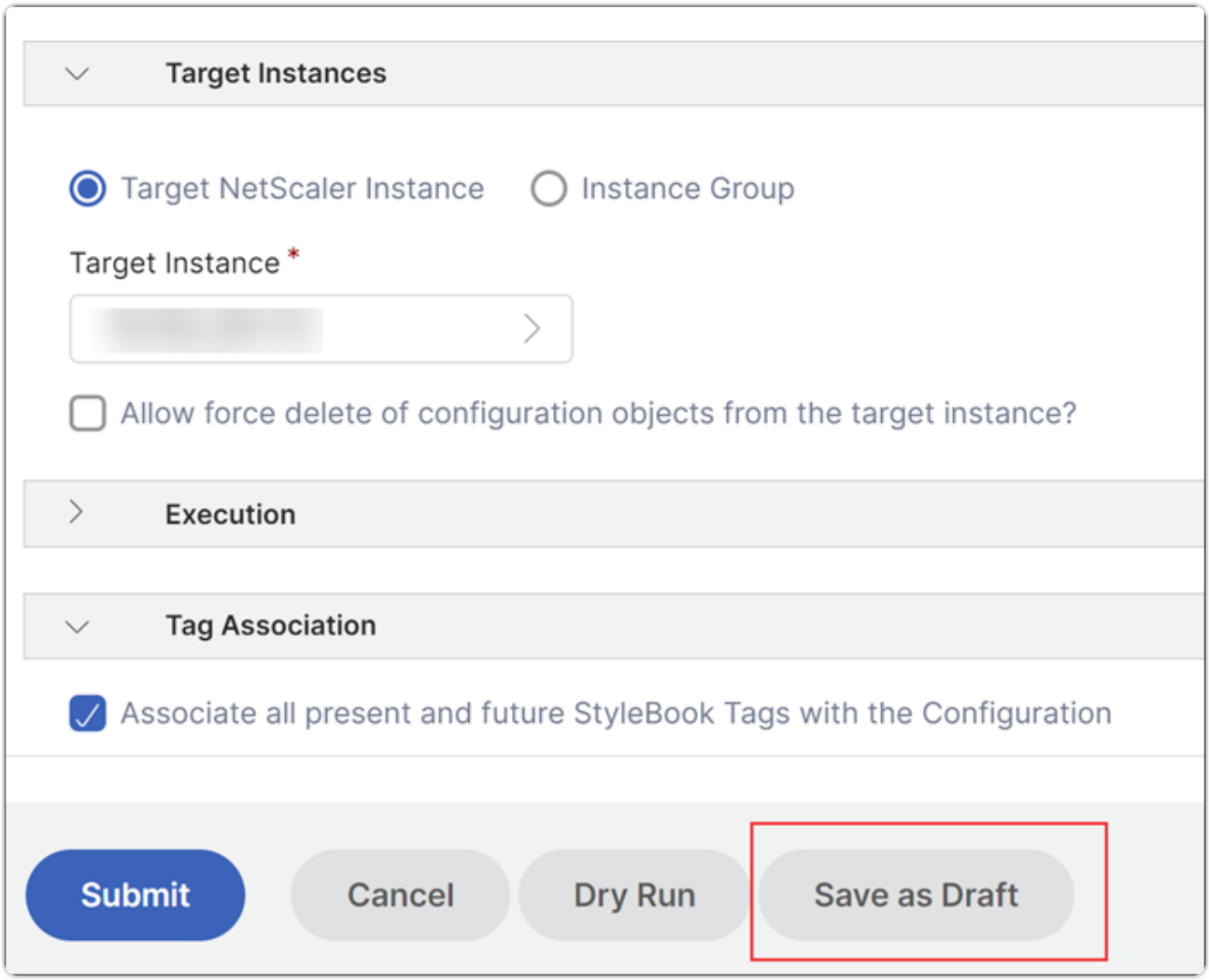
将配置包另存为草稿

配置包中的“**另存为草稿**”选项允许您将配置更改另存为草稿。此功能会保存更改，而不会立即将其部署到 NetScaler 实例。

要将配置包另存为草稿：

1. 导航到“**应用程序 > 配置 > 配置包**”。
2. 在“**配置**”页面上，单击“**添加**”。
3. 选择所需的样式簿，然后单击“**选择**”。
4. 在“**创建配置**”页面上，单击“**另存为草稿**”。

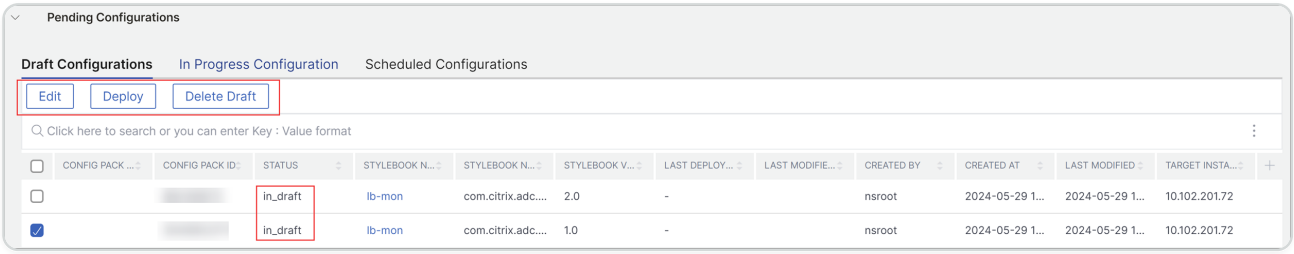
© 1997–2026 Citrix Systems, Inc. All rights reserved.



将配置包另存为草稿后，您的配置更改不会直接部署到 NetScaler 实例。相反，配置包将作为草稿存储在“**待处理配置**”下的“**草稿配置**”选项卡中。

在“**草稿配置**”选项卡中，选择配置包以执行以下操作：

- 编辑配置包的配置。
- 将配置部署到 NetScaler 实例。
- 删除草稿以在不部署的情况下移除配置。



您还可以安排何时部署已保存的草稿。

有关详细信息，请参阅安排配置包。

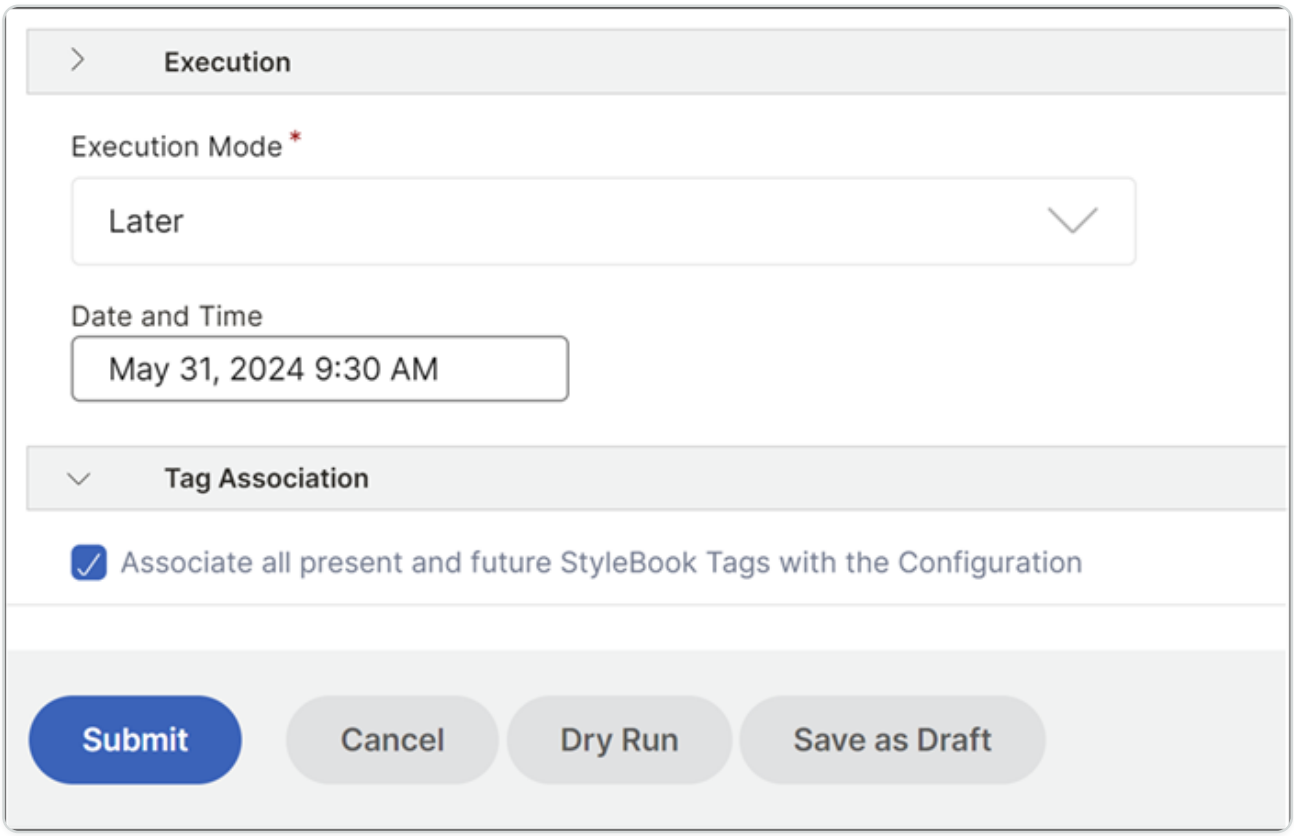
© 1997–2026 Citrix Systems, Inc. All rights reserved.

为配置包创建计划

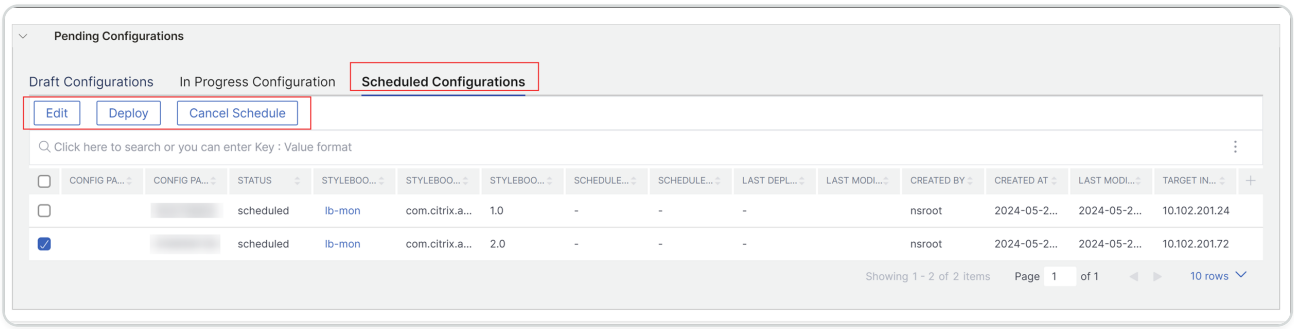
创建配置包时，配置包默认会自动部署到 NetScaler 实例。借助此功能，您可以安排何时部署配置包。

要为配置包创建计划：

1. 导航到 **应用程序 > 配置 > 配置包**。
2. 在 **配置** 页面上，单击 **添加**。
3. 选择 StyleBook 并单击 **选择**。
4. 在 **创建配置** 页面上，在 **执行** 下，从 **执行模式** 列表中选择 **稍后**。
5. 选择所需的调度时间和日期，然后单击 **提交**。



所有计划的配置都存储在 **待处理配置** 下的 **计划的配置** 选项卡中。您可以选择已创建的计划来编辑、部署或取消该计划。



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

对于已部署的配置包

您还可以创建计划以编辑和删除已部署的配置包。

计划配置包的编辑操作

要创建编辑已部署配置包的计划：

1. 导航到 **应用程序 > 配置 > 配置包**。
2. 在 **配置** 页面上，选择一个 StyleBook 并单击 **编辑**。
3. 在 **编辑配置** 页面上，编辑配置包。
4. 在“**执行模式**”列表中，选择“**稍后**”。
5. 选择所需的计划时间和日期，然后单击“**提交**”。

计划配置包的删除操作

要创建计划以删除已部署的配置包：

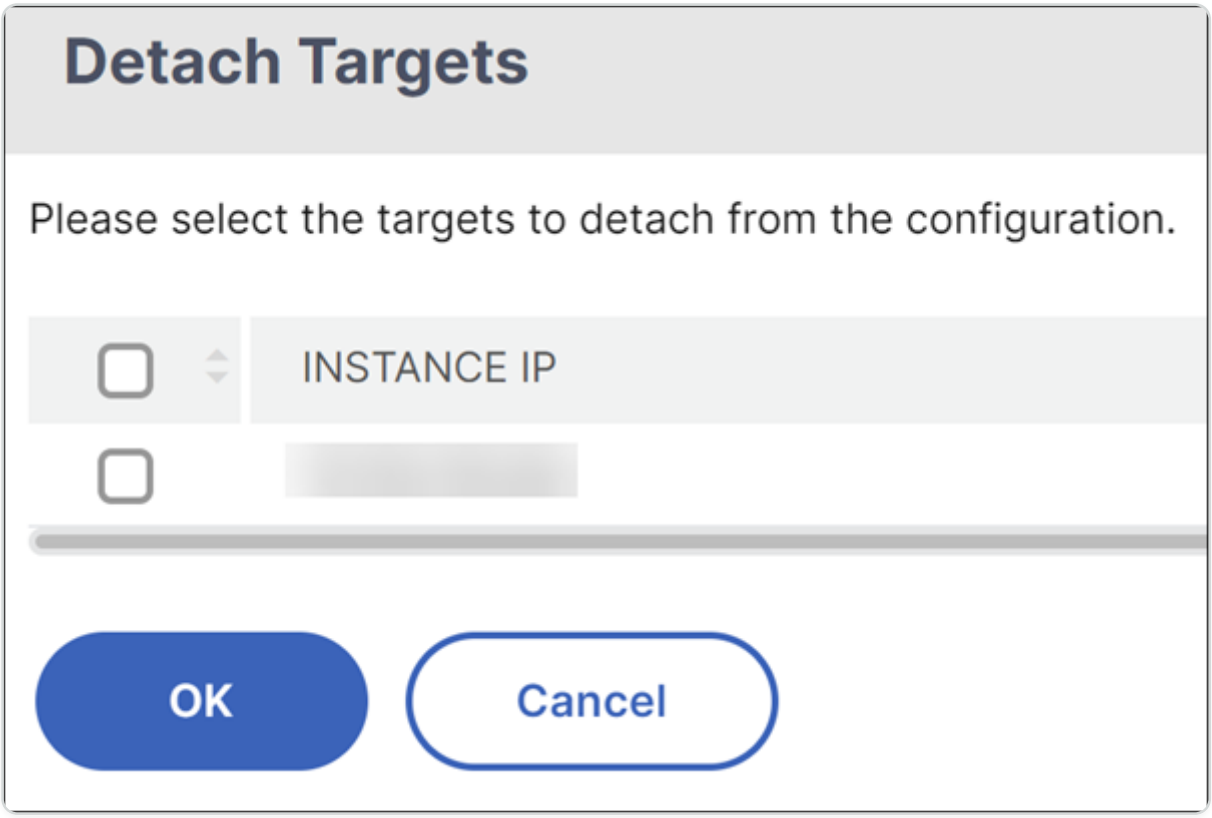
1. 导航到“**应用程序 > 配置 > 配置包**”。
2. 在“**配置页面**”上，选择一个 StyleBook，然后单击“**删除**”。
3. 在“**执行模式**”列表中，选择“**稍后**”。
4. 选择所需的计划时间和日期，然后单击“**提交**”。

从配置包中分离目标实例

要从配置包中分离目标实例，请执行以下操作：

1. 导航到“**应用程序 > 配置 > 配置包**”。
2. 选择包含要删除的目标实例的配置包。
3. 在“**选择操作**”中，选择“**分离目标**”。
4. 在“**分离目标**”窗格中，选择要从配置包中删除的目标实例。

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



5. 点击 **OK**。

显示一条消息，确认已创建重复的配置包，并已移除目标实例。

构建您的 StyleBook

example-lb StyleBook 的完整内容提供给您参考，如下所示：

```
name: example-lb

namespace: examples.stylebooks

version: "1.0"

display-name: Basic Load Balancer App

description: This is an example StyleBook that creates a load balancer
application

schema-version: "1.0"

import-stylebooks:

  -
```

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

```
    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

parameters-default-sources:

  - stlb::lb

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters
```

example-lb-mon StyleBook 的完整内容提供给您参考，如下所示：

```
name: example-lb-mon

namespace: examples.stylebooks

version: "1.0"

description: This is an example StyleBook that creates a load balancer
application with monitors

display-name: Basic Load Balancer App with Monitors

schema-version: "1.0"

import-stylebooks:
```

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

```
  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb

    version: "1.0"

  -

    namespace: com.citrix.adc.commontypes

    prefix: cmtypes

    version: "1.0"

parameters-default-sources:

  - stlb::lb

parameters:

  -

    name: monitors

    label: "List of Monitors"

    description: "List of Monitors to monitor Application Servers"

    type: cmtypes::monitor[]

substitutions:

  mon-name(appname, monname): $appname + "-mon-" + $monname
```

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

```
components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters

  -

    name: monitors-comp

    type: cmtypes::monitor

    condition: $parameters.monitors

    repeat: $parameters.monitors

    repeat-item: mon

    repeat-index: ndx

    description: Builds a list of NetScaler monitor objects and binds them
to the servicegroup of this LB config

    properties-default-sources:

      - $mon

    properties:

        monitorname: $substitutions.mon-name($parameters.lb-appname,
$mon.monitorname)

    components:
```

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

```
      -

        name: monitor-svcg-binding-comp

        condition:  $parameters.svc-servers

        type: ns::servicegroup_lbmonitor_binding

        properties:

          servicegroupname: $components.lb-
comp.outputs.servicegroup.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

创建 StyleBook 以将文件上传到 NetScaler Console

NetScaler Application Delivery Management (NetScaler Console) StyleBook 允许您创建 NetScaler 配置，其中可能包括通过使用 NetScaler Console GUI 或 API 将任何类型的文件从本地文件系统上传到 NetScaler 实例。这些文件可以是示例证书文件或地理位置文件。您还可以指定上传这些文件的目录。

StyleBook 配置

以下是一个 StyleBook 示例，描述了如何将地理位置文件上传到 NetScaler 实例。地理文件通常用于 GSLB 配置中，以根据地理位置定义静态邻近性：

构建您的 StyleBook -1

```
name: upload-geolocations

namespace: com.citrix.adc.stylebooks.samples

version: "1.0"

display-name: GeoLocation File Upload

description: This StyleBook is used to upload a geolocation file to
NetScaler

schema-version: "1.0"
```

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

```
import-stylebooks:

-

 namespace: netscaler.nitro.config

 version: "11.1"

 prefix: ns



parameters:

-

 name: locationfile

 label: Location File

 description: The system file path of the geolocation file on NetScaler
Console

 type: file

 required: true



components:

-

 name: upload-file-comp

 type: ns::systemfile

 properties:

    filename: $parameters.locationfile.filename

    filelocation: "/var/netscaler/inbuilt_db/"
```

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

```
    filecontent: base64.encode($parameters.locationfile.contents)
```

注意

此示例中使用的参数类型为文件。您可以将此 StyleBook 导入 NetScaler Console 并使用它来上传地理位置文件。

此 StyleBook 要求文件已存在于 NetScaler Console 中（例如，您已经使用 scp 等实用程序将其复制到 NetScaler Console）。 如果您想通过 NetScaler Console 将文件上传到 NetScaler，而无需先将其复制到 NetScaler Console 文件系统，您可以构建一个包含两个“字符串”参数的 StyleBook，一个用于指定要在 NetScaler 上使用的文件名，另一个用于指定文件内容，并在 upload-file-comp 组件中使用这两个参数。以下是上传地理位置文件的另一种 StyleBook：

构建您的 StyleBook - 2

```
name: upload-geolocations-alt

namespace: com.citrix.adc.stylebooks.samples

version: "1.0"

display-name: GeoLocation File Upload

description: This StyleBook is used to upload a geolocation file to
NetScaler

schema-version: "1.0"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  version: "11.1"

  prefix: ns
```

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

```
parameters:
 -
  name: filename
  label: Location Filename
  description: The name of the location file on the NetScaler
  type: string
  required: true
 -
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true


components:
 -
  name: upload-file-comp
  type: ns::systemfile
  properties:
   filename: $parameters.filename
   filelocation: "/var/NetScaler/inbuilt_db/"
```

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

```
filecontent: base64.encode($parameters.filecontents)
```

创建用于上传文件的配置

以下过程在选定的 NetScaler 实例上创建配置，该配置将使用上述第一个 StyleBook 上传地理位置文件。

创建用于上传文件的配置：

1. 在 NetScaler Console 中，导航到 **应用程序** > **配置**，然后单击 **新建**。“选择 StyleBook”页面显示 NetScaler Console 中所有可用的 StyleBook。向下滚动并选择您导入的 StyleBook。

   StyleBook 参数显示为一个用户界面页面，允许您输入此 StyleBook 中定义的所有参数的值。
2. 在基本负载均衡器设置部分中输入负载均衡器的名称和虚拟 IP 地址。
3. 在 **位置文件** 部分，输入文件的名称或位置。

   > **注意**
   >
   > 确保在 NetScaler Console 中，文件仅位于当前租户的文件夹下。使用任何文件传输协议将文件复制到 NetScaler Console 文件系统。
4. 在访问目标实例之前，系统可能会要求您提供用户凭据。
5. 选择需要创建配置的目标 NetScaler 实例，然后单击 **创建**。

> **注意**
>
> 我们建议您选择 **试运行** 以检查在实例上执行实际配置之前在目标实例上创建的配置对象。

当配置包创建成功后，文件将保存在 NetScaler 实例文件系统的以下位置：/var/netscaler/inbuilt_db/

> **注意**
>
> 您还可以单击刷新图标，将 NetScaler Console 中最近发现的 NetScaler 实例添加到此窗口中可用的实例列表中。

使用 NetScaler Console API 创建配置包

您还可以使用 NetScaler Console API 创建一个配置包，将文件上传到选定的 NetScaler 实例。有关如何使用 API 的更多信息，请参阅 如何使用 API 创建配置以上传任何文件类型。

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

创建 StyleBook 以将 SSL 证书和证书密钥文件上传到 NetScaler Console

创建使用 SSL 协议的 StyleBook 配置时，必须根据 StyleBook 参数的要求上传 SSL 证书文件和证书密钥文件。StyleBook 允许您使用 NetScaler Console GUI 直接从本地系统上传 SSL 文件和密钥文件。您还可以使用 NetScaler Console API 上传已由 NetScaler Console 管理的证书文件和密钥文件。

StyleBook 配置

本文档帮助您创建自己的 StyleBook - **负载平衡虚拟服务器 (SSL)** 包含用于上传 SSL 证书和密钥文件的组件。此处提供的 StyleBook 示例在选定的 NetScaler 实例上创建了一个基本的负载平衡虚拟服务器配置。该配置使用 SSL 协议。要使用此 StyleBook 创建配置，您必须提供虚拟服务器的名称和 IP 地址，选择负载平衡方法参数，并为虚拟服务器上传证书文件和证书密钥文件，或者使用 NetScaler Console 中已有的证书文件和证书密钥文件。这些在“parameters”部分中指定，如下所示：

```
parameters:

 -

  name: name

  type: string

  required: true

 -

  name: ip

  type: ipaddress

  required: true

 -

  name: lb-alg

  type: string

  allowed-values:
```

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

```
    - ROUNDROBIN

    - LEASTCONNECTION

  default: ROUNDROBIN

 -

  name: certificate

  label: "SSL Certificate File"

  description: "The file name of the SSL certificate file"

  type: certfile

 -

  name: key

  label: "SSL Certificate Key File"

  description: "The file name of the server certificate's private key
file"

  type: keyfile
```

然后，在 StyleBook 的 components 部分创建两个组件，如下所示。“my-lbvserver-comp”组件的类型为 ns::lbvserver，其中：

- “ns”是前缀，指代您在 import-stylebooks 部分中指定的内置命名空间 netscaler.nitro.config 和版本 10.5。
- “lbvserver”是此命名空间中的内置 StyleBook。它对应于同名的 NetScaler NITRO 负载平衡虚拟服务器资源。

第二个组件“lbvserver-certificate-comp”的类型为 stlb::vserver-certs-binds。前缀“stlb”指代 StyleBook 的 import-stylebooks 部分中指定的命名空间“com.citrix.adc.stylebooks”和版本 1.0。如果将“com.citrix.adc.stylebooks”命名空间视为一个文件夹，那么“vserver-certs-binds”就是该文件夹中的另一个 StyleBook（或文件）。位于命名空间“com.citrix.adc.stylebooks”中的 StyleBook 作为 NetScaler Console 的一部分提供。

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

用户定义的 StyleBook 使用的“vserver-certs-binds”StyleBook 允许您通过将证书和密钥文件上传到目标 NetScaler 实例，以及配置证书和密钥文件与相应虚拟服务器的绑定来轻松配置证书。此组件的属性是 - lb 虚拟服务器的名称以及您在创建配置包时提供的 SSL 证书的名称。

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

  properties:

   name: $parameters.name

   servicetype: SSL

   ipv46: $parameters.ip

   port: 443

   lbmethod: $parameters.lb-alg

 -

  name: lbvserver-certificate-comp

  type: stlb::vserver-certs-binds

  description: Binds lbvserver with server certificate

  properties:

   vserver-name: $components.my-lbvserver-comp.properties.name

   certificates:

    -

     cert-name: $parameters.name + "-lb-cert"

     cert-file: $parameters.certificate
```

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

```
    ssl-inform: PEM

    key-name: $parameters.name + "-key"

    key-file: $parameters.key
```

当您使用 API 从此类 StyleBook 创建配置时，只需使用文件名（而不是完整文件路径）。这些文件应已在 NetScaler Console 上的证书和密钥文件文件夹中可用。上传的 SSL 证书文件存储在 NetScaler Console 的 /var/mps/tenants/.../ns_ssl_certs 目录中，SSL 证书密钥文件存储在 NetScaler Console 的 /var/mps/tenants/.../ns_ssl_keys 目录中。

创建用于上传 SSL 文件的配置

以下过程使用上述 StyleBook 中的 SSL 协议，在选定的 NetScaler 实例上创建基本的负载平衡虚拟服务器配置。您可以使用此过程在 NetScaler Console 中上传 SSL 证书文件和证书密钥文件。

创建用于上传文件的配置

1. 在 NetScaler Console 中，导航到 **Applications** > **Configuration > StyleBooks**。“**StyleBooks**”页面显示 NetScaler Console 中所有可用的 StyleBook。
2. 向下滚动并选择 **Load Balancing Virtual Server (SSL)**，或在搜索字段中键入 **Load Balancing Virtual Server (SSL)**，然后按 **Enter** 键。
3. 在 StyleBook 面板中单击**创建配置**链接。

   StyleBook 参数显示为一个用户界面页面，您可以在其中输入此 StyleBook 中定义的所有参数的值。
4. 在基本负载均衡器设置部分中输入负载均衡器名称和虚拟 IP 地址。
5. 在**SSL 证书设置**部分中，从本地存储文件夹中选择相应文件。或者，您可以选择 NetScaler Console 本身中存在的文件。
6. 选择需要在其上创建配置的目标 NetScaler 实例，然后单击**创建**。

注意：

您还可以单击刷新图标，将 NetScaler Console 中最近发现的 NetScaler 实例添加到此窗口中可用的实例列表。

在 NetScaler Console 中，以下作为 NetScaler Console 的一部分提供的默认 StyleBook，通过上传 SSL 证书和密钥，使您能够创建 SSL 支持。

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

- HTTP/SSL 负载均衡 StyleBook (lb)
- HTTP/SSL 负载均衡（带监视器）StyleBook (lb-mon)
- 带监视器的 HTTP/SSL 内容切换应用程序 (cs-lb-mon)
- 使用 CS、LB 和 SSL 功能的示例应用程序 StyleBook (sample-cs-app)

您还可以创建自己的 StyleBook，以与上述 StyleBook 中描述的相同方式利用 SSL 证书

构建您的 StyleBook

文件 lb-vserver-ssl.yaml 的完整内容如下所示：

```
name: lb-vserver-ssl

description: "This stylebook defines a load balancing virtual server
configuration."

display-name: "Load Balancing Virtual Server (SSL)"

namespace: com.example.ssl.stylebooks

schema-version: "1.0"

version: "0.1"



import-stylebooks:

 -

  namespace: netscaler.nitro.config

  prefix: ns

  version: "10.5"

 -

  namespace: com.citrix.adc.stylebooks

  prefix: stlb
```

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

```
  version: "1.0"


parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: certificate
  label: "SSL Certificate File"
  description: "The file name of the SSL certificate file"
```

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

```
  type: certfile

 -

  name: key

  label: "SSL Certificate Key File"

  description: "The file name of the server certificate's private key
file"

  type: keyfile



components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

  properties:

    name: $parameters.name

    servicetype: SSL

    ipv46: $parameters.ip

    port: 443

    lbmethod: $parameters.lb-alg

 -

  name: lbvserver-certificate-comp

  type: stlb::vserver-certs-binds

  description: Binds lbvserver with server certificate
```

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

```
properties:
 vserver-name: $ components.my-lbvserver-comp.properties.name
 certificates:
  -
   cert-name: $parameters.name + "-lb-cert"
   cert-file: $parameters.certificate
   ssl-inform: PEM
   key-name: $parameters.name + "-key"
   key-file: $parameters.key
```

使用 NetScaler Console API 创建配置包

您还可以使用 NetScaler Console API 创建配置包，用于将证书和密钥文件上传到所选 NetScaler 实例。有关如何使用 API 的更多信息，请参阅如何使用 API 创建配置以上传证书和密钥文件。

查看在 NetScaler 实例上定义的对象

在 NetScaler Console 上创建 StyleBook 配置包后，单击 **查看已创建对象** 以显示在目标 NetScaler 实例上创建的所有 NetScaler 对象

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

Objects

Objects Added on Instance : 10.102.29.200

Type : lbvserver

ipv46 : 10.10.10.1
lbmethod : ROUNDROBIN
name : vserver-1
port : 80
servicetype : SSL

Type : systemfile

filecontent :
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMzakNDQWtlZ0F3SUJBZ0lCQURBTkJna3Foa2lHOXcwQkFRc0ZBREEvTVFzd0NRWURWUVFHRXdKVlV6RUwKTUFrR0ExVUVDQk1DWTJFeEV6QVJCZ05WQkFjVENuTmhiblJoWTJ4aGNtRXhEakFNQmdOVkJBb1RCV0Z3Y0d4bApNQjRYRFRFMU1ERXhOekEyTURZMU5Gb1hEVEUyTURFeE56QTJNRFkxTkZvd1B6RUxNQWtHQTFVRUJoTUNWVk14CkN6QUpCZ05WQkFnVEFtTmhNUk13RVFZRFZRUUhFd3B6WVc1MFlXTnNZWEpoTVE0d0RBWURWUVFLRXdWaGNIQnMKWlRDQm56QU5CZ2txaGtpRzI3MEJBUUVGQUFPQmpRQXdnWWtDZ1lFQXZFa2FoNjJFRnViTmVGUkNaQk9nN0pEZAo0dVQ1ZDBlM3UycUtaMTQrdzRjVkd5U053L1RxT2RhK1F3T0xiaU9OdDBhLzhKRDVyc096Q3NCWHRldUsyZzRPCnhuNi8wc28zZFJKZTVKeFErNmNsT2VsVjdPbUpFTWVXZDd5WlJGbVFqZHgrZEROMjUxT25aa0pmeXN3NXdSVTUKSnpUQnRza3hRcjBQbnJ2S0tBa0NBd0VBQWFPQjZUQ0I1akFkQmdOVkhRNEVGZ1FVam5XYVJsalF5N0pqNFozcwp0LzFIWmYvWUprZ3dad1lEVlIwakJHQXdYb0FVam5XYVJsalF5N0pqNFozc3QvMUhaZi9ZSmtpaFE2UkJNRDh4CkN6QUpCZ05WQkFZVEFsVlRNUXN3Q1FZRFZRUUlFd0pqWVRFVE1CRUdBMVVFQnhNS2MyRnVkR0ZqYkdGeVlURU8KTUF3R0ExVUVDaE1GWVhCd2JHV0NBUUF3REFZRFZSMFRCQVV3QXdFQi96QUxCZ05WSFE4RUJBTUNBUVl3RVFZSgpZSVpJQVliNFFnRUJCQVFEQWdFR01DNEdDV0NHU0FHRytFSUJEUVFoRmg5T1pYUlRZMkZzWlhJZ1IyVnVaWEpoCmRHVmtjRU5sY25ScFptbGpZWFJsTUEwR0NTcUdTSWIzRFFFQkN3VUFBNEdCQUs0RWY3aUFSRlRQUlo0b2pJWm0KTHlTeFhGaTE0SGxjK0VpMUNJejV3R09Db3pibWNXemZOZXVSSTdRQVlSSXQ3WkhhYWt0VGg0NXIvUHdPZXFLcgpSc2xNTzBnQ1hES3BtU2tXQ3VHdFhBbVhXU2xrTEt3bTFHL0pKdTBhSEFkdVhtRVkwNW52M016RWhTWW8xelhjCnFsYXJNcG9QUE14Qks0RmlBNWxsQnAwTwotLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg==
fileencoding : BASE64
filelocation : /nsconfig/ssl
filename : test_cert.pem

Type : systemfile

filecontent :
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlDWEFJQkFBS0JnUUM4U1JxSHJZUVc1czE0VkVKa0U2RHNrTjNpNVBsM1I3ZTdhb3BuWGo3RGdoVWJKSTNECjlPbzUxcjVEQTR0dUk0MjNSci93a1BtdXc3TUt3RmUxNjRyYURnN0dmci9TeWpkMUVsN2tuRkQ3cHlVNTZWWHMKNllrUXg1WjN2SmxFV1pDTjNINTBNM2JuVTZkbVFsL0t6RG5CRlRrbk5NRzJ5VEZDdlErZXU4b29DUUlEQVFBQgpBb0dBUUlENjZjaDBIRFJ0NSs5VjMxc3FJbUZ1NHJCM0Zub25ZN21ZT05sOHZ4WHRqU0wwdmxGRmZSTW9rMlMvCmU3Z0tjT040Rmo1VWk1N1gwN01aV1dXY1o0aEhrMm5jMjlmOENLSW5oelhnYjFLQjRaMGp1TnUvNE1paVIyaHIKNkFROXluV0VMRlBDTjZWMHFQZWxGYXpVbnZJaHZpMFZGZCsyRUNBY0drVHg0Z0VDUVFEMklVODhGaUkzVFJOYwpMcVJEMHh2ZVFWMkF6ZVBEYmFnTVFFRlNWZVZ3Yk11V3RJM2J0SkdwWXMxUkpIeitOdGw0dVprRGVQbnNJZE5ZCjNJWjNsNUp4QWtFQXc5WDdKTDJaNVpyaEVpM0YzdjYwU1U5RWM4Z01FdVhFZlhUendCc2puanJsckRIMUI0enYKR0hSU1ImUEdYeHh5cjRKVmc4Q25kczZVOHExN0N0SUxHUUpBS1FtT3UzYjVSMzByWURCS3BTQmF3aWpsM1NiMgo5Y3VmdkVNdVlQci9ZVXBTZTVNcEg5dXdlYXlHalNQblR6OTM3UUFNK2g0K2xWZGlkS3Q0SkJKNmtRSkJBTHVSClRaUHBEV2UrcWVleGM1MmJzcTJzZ0ZHc3Z2T3lvam5QTkU5Qkx5STBJeHFFVnlyK25KcDlmeEpXWEI5b3JlZXcKRzV1dmdEWG9zdnlrYi83eklyRUNRRDMzV1lHeUw2MjJaRzZveHlxR1o1d1pCTFVtV1VyVE1zSngzOWZ5NUJoZgpkajNWcE10Y3plOFVKVmlPaGtydWNmb29tRlNPaUN4ZXhPQXM2MmVEZXNnPQotLS0tLUVORCBSU0EgUFJJVkFURSBLRVktLS0tLQo=
fileencoding : BASE64
filelocation : /nsconfig/ssl
filename : test_cert_key.pem

Type : sslcertkey

cert : test_cert.pem
certkey : vserver-1-lb-cert
inform : PEM
key : test_cert_key.pem

Type : sslvserver_sslcertkey_binding

certkeyname : vserver-1-lb-cert
vservername : vserver-1

使用 StyleBooks 从证书存储管理 SSL 证书

NetScaler Console 证书存储可帮助您在一个位置存储和管理 SSL 证书。因此，您可以将 SSL 证书存储在 NetScaler Console 中，并在 NetScaler 配置期间重复使用它们。

本文介绍如何创建 StyleBook 定义，该定义允许您从 NetScaler Console 证书存储上传和重复使用 SSL 证书。

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

参数

StyleBook 定义支持 `certkey` 作为新的内置参数类型。使用此参数类型可从 NetScaler Console 证书存储中重复使用 SSL 证书。

```
parameters:

-

    name: certificate

    label: Certificate

    description: "Certificate to be bound to this virtual load balanced application"

    type: certkey

    required: true
```

在此示例中，证书参数指代 NetScaler Console 证书存储中的 SSL 证书或证书链。

在 **StyleBook** 定义中，您可以引用 `certkey` 参数的以下属性：

- `certkeyname` – 您要在实例上配置的 SSL 证书密钥的名称。
- `cert_filename` – SSL 证书的文件名。
- `password` – （如果需要）访问 SSL 证书所需的密码。
- `key_filename` – SSL 证书密钥的文件名。
- `keyfile_contents` – SSL 证书的内容。
- `subject` – SSL 证书中提及的主题。
- `issuer` – 颁发 SSL 证书的颁发机构。
- `certchain_certkeyname` – 证书链的名称。

注意：

有时，许多分层证书颁发机构 (CA) 会签署服务器证书，这意味着这些证书形成一个链。当证书存储区包含证书链时，请使用此属性。它有助于您引用和绑定证书。创建配置包时，证书链会显示为列表。

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

这些属性可帮助您在 **StyleBook** 定义中创建所需的组件。

组件

当 StyleBook 具有 `type: certkey` 参数时，您可以从 NetScaler Console 证书存储区为此参数提供证书。在此工作流程中，除了从 NetScaler Console 证书存储区查看和选择证书外，您还可以执行以下操作：

- 上传新证书。
- 更新现有证书。例如，已过期证书。
- 删除证书。

注意：

- 您还可以使用 NetScaler Console SSL 控制板管理 NetScaler Console 证书存储区中的证书。
- 在 NetScaler Console 证书存储区中更新 SSL 证书后，您必须更新与 SSL 证书关联的配置包。要了解有关更新配置包的更多信息，请参阅 使用 API 更新现有配置包 或 创建和编辑配置包。

构建您的 StyleBook

以下 StyleBook 定义使用 NetScaler Console 证书存储区中的 SSL 证书。此 StyleBook 包含将主证书和密钥文件上传到 NetScaler 实例的组件。如果这些文件已存在于 NetScaler 实例上，NetScaler Console 将跳过上传步骤，并且这些组件将不起作用。

```
name: lb-with-cert-from-certstore

namespace: com.example.stylebooks

version: "1.0"

display-name: Application using a CertStore certificate

description: This StyleBook defines a simple SSL Vserver.

schema-version: "1.0"
```

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

```
import-stylebooks:
 -
    namespace: netscaler.nitro.config
    version: "13.0"
    prefix: ns


parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: certificate
  label: Application Certificate
```

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

```
  description: Certificate chain and key to be bound to this application

  type: certkey

  required: true




components:

 -

    name: pem-cert-files-comp

    type: ns::systemfile

    description: This component uploads the PEM certificate file onto the
NetScaler

    condition: $parameters.certificate

    properties:

      filename: $parameters.certificate.cert_filename

      filelocation: /nsconfig/ssl

      filecontent: base64($parameters.certificate.certfile_contents)

      fileencoding: BASE64

 -

    name: pem-KEY-files-comp

    type: ns::systemfile

    description: This component uploads the PEM key file onto the
NetScaler.

    condition: $parameters.certificate
```

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

```
    properties:

      filename: $parameters.certificate.key_filename

      filelocation: /nsconfig/ssl

      filecontent: base64($parameters.certificate.keyfile_contents)

      fileencoding: BASE64

 -

    name: cert-files-comp

    type: ns::sslcertkey

    description: This component creates the certkey on the NetScaler using
the uploaded files.

    condition: $parameters.certificate

    properties:

      certkey:  $parameters.certificate.certkeyname

      cert: $parameters.certificate.cert_filename

      key: $parameters.certificate.key_filename

 -

  name: lbvserver-comp

  type: ns::lbvserver

  description: This component creates the lbvserver of the application.

  properties:

   name: $parameters.name + "-lbvserver"

   servicetype: SSL
```

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

```
  ipv46: $parameters.ip

  port: 443

  lbmethod: ROUNDROBIN

 components:

     -

       name: sslvserver-comp

       type: ns::sslvserver

       description: This component configures SSL settings on the vserver

       properties:

         vservername: $parent.properties.name

         ssl3?: ENABLED

         tls1?: ENABLED

         tls11?: ENABLED

     -

      name: cert-bindings-adv-comp

      type: ns::sslvserver_sslcertkey_binding

      description: This component binds the certkey to the vserver

      condition: $parameters.certificate

      properties:

        vservername: $parent.properties.name

        certkeyname: $parameters.certificate.certkeyname
```

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

在 StyleBook 中定义的虚拟服务器上启用分析并配置警报

您可以使用操作构造来配置 NetScaler Console 分析，以收集由属于 StyleBook 的任何虚拟服务器组件处理的所有或部分流量事务上的 appflow 记录。您还可以使用此构造来配置警报，以深入了解虚拟服务器管理的流量。

以下示例显示了 StyleBook 的操作部分：

```
operations:

  analytics:

   -

    name: lbvserver-ops

    properties:

    target: $components.basic-lb-comp.outputs.lbvserver

    filter: HTTP.REQ.URL.CONTAINS("catalog")

   -

    alarms:

     -

      name: lbvserver-alarm

      properties:

      target: $outputs.lbvserver

      email-profile: $parameters.emailprofile

      sms-profile: "NetScalerSMS"



    rules:

     -
```

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

```
      metric: "total_requests"

      operator: "greaterthan"

      value: 25

      period-unit: $parameters.period

     -

       metric: "total_bytes"

       operator: "lessthan"

       value: 60

       period-unit: "day"
```

分析部分中的属性用于指示 NetScaler Console 分析功能在由目标属性标识的虚拟服务器组件上收集 appflow 记录。您还可以选择指定一个过滤器属性，该属性接受 NetScaler 策略表达式，以过滤在虚拟服务器上收集 appflow 记录的请求。

当从该 StyleBook 创建配置包时，NetScaler Console 分析功能被配置为在创建配置包过程中指定的虚拟服务器上收集 appflow 记录。

警报部分中的属性用于设置阈值，以在由目标属性标识的虚拟服务器上生成警报并发送通知。在上述示例中，email-profile 和 sms-profile 属性用于指定通知应发送到何处。规则部分定义了阈值。例如，如果虚拟服务器处理的总请求数大于 25 并在用户定义的时间段内，则会设置警报并发送通知。“period-unit”指定警报触发的频率。它可以取值“天”、“小时”或“周”。

在比较指标值与阈值时，您可以使用以下运算符：

- “greaterthan”表示“>”
- “lessthan”表示“<”
- "大于等于" 表示 ">="
- "小于等于" 表示 "<="

请注意，StyleBooks 使用 API 名称作为指标，而不是 NetScaler Console 分析 GUI 上显示的名称。

要了解如何查看和分析作为配置包一部分创建的虚拟服务器上收集的数据，请参阅 NetScaler Console 分析文档。

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

实例角色

在 NetScaler Console 中，可能存在这样一种情况：您需要为单个应用程序配置多个 NetScaler 实例，但每个 NetScaler 实例又需要部署不同的配置。此类情况的一个示例是默认的 Microsoft Skype for Business StyleBook。

StyleBooks 目前支持创建配置包并在多个 NetScaler 实例上应用相同配置的功能。在这种所有 NetScaler 实例上的配置都相同的情况下，可以称之为对称配置。

现在，借助 StyleBooks 的“实例角色”功能，您可以创建非对称配置，即一个配置包可以应用于多个 NetScaler 实例，但在不同的 NetScaler 实例上具有不同的配置。

当使用具有实例角色功能的 StyleBook 创建配置包时，配置包中的每个 NetScaler 实例都可以分配不同的角色。此角色决定了 NetScaler 实例将接收的配置包的配置对象。

注意要点：

- StyleBook 中的实例角色集是在创建 StyleBook 时定义的。
- 在创建或更新配置包时，角色会分配给特定的 NetScaler 实例。

目标角色部分

StyleBook 中引入了一个名为“target-roles”的新部分，其中声明了 StyleBook 支持的所有角色。

此部分通常放置在 StyleBook 的“import-StyleBooks”部分之后，以及参数部分之前。

在以下 StyleBook 示例中，在“target-roles”部分中定义了两个角色 - A 和 B。

```
target-roles:



  -

   name: A

   name: B

     min-targets: 2

     max-targets: 5
```

您可以看到角色 B 还定义了两个可选子属性：min-targets 和 max-targets。

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

尽管这两个子属性是可选的，但 min-targets 指定了从该 StyleBook 创建配置包时应分配此角色的最小强制 NetScaler 实例数，而 max-targets 指定了从该 StyleBook 创建配置包时可分配此角色的最大 NetScaler 实例数。

如果未指定这些子属性，则对可为该角色配置的 NetScaler 实例数量没有限制。如果 min-targets = 0，则与该角色关联的配置是可选的；如果 min-targets = 1，则该配置是强制性的，并且至少需要为该角色配置一个 NetScaler 实例。

角色“默认”

除了显式定义的角色之外，所有 StyleBook 都具有一个隐式角色，该角色称为默认角色。此角色可以像 StyleBook 中的任何其他角色一样使用。创建配置包时，如果 NetScaler 实例未分配特定角色，则该实例将隐式分配给“默认”角色。该实例现在将接收由具有“默认”角色的组件生成的任何配置对象。

具有角色的组件

定义了 StyleBook 可以支持的角色（包括“默认”角色）后，这些角色可以在 StyleBook 的组件部分中使用。如果您希望组件仅部署在扮演特定角色的 NetScaler 实例上，那么您可以将角色属性指定为组件的一部分，如下面的组件示例所示：

```
-

  name: C1

  type: ns::lbvserver

  roles:

    - A

  properties:

    name: lb1

    servicetype: HTTP

    ipv46: 1.1.1.1

    port: 80
```

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

在上面的示例中，组件生成一个“lbvserver”，该“lbvserver”将部署在扮演角色 A 的实例上。请注意，组件的角色属性是一个列表，并且一个组件可以分配多个角色。这些角色本应在 StyleBook 的“target-roles”部分中声明。

注意：如果 StyleBook 中的组件未指定角色属性，则由该组件生成的配置对象将在所有 NetScaler 实例上创建，无论其角色如何。您可以有效地使用此功能来创建可应用于配置包所有实例的配置对象。

假设有一个 StyleBook 定义了两个角色 - A 和 B，并且包含四个组件。

- 组件 C1 具有角色 A 和 B
- 组件 C2 具有角色 B
- 组件 C3 未定义任何角色
- 组件 C4 具有“默认”角色

此 StyleBook 的组件部分如下所示：

```
components:

  -

    name: C1

    type: ns::lbvserver

    roles:

      - A

      - B

    properties:

      name: lb1

      servicetype: HTTP

      ipv46: 1.1.1.1

      port: 80

  -
```

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

```
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
```

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

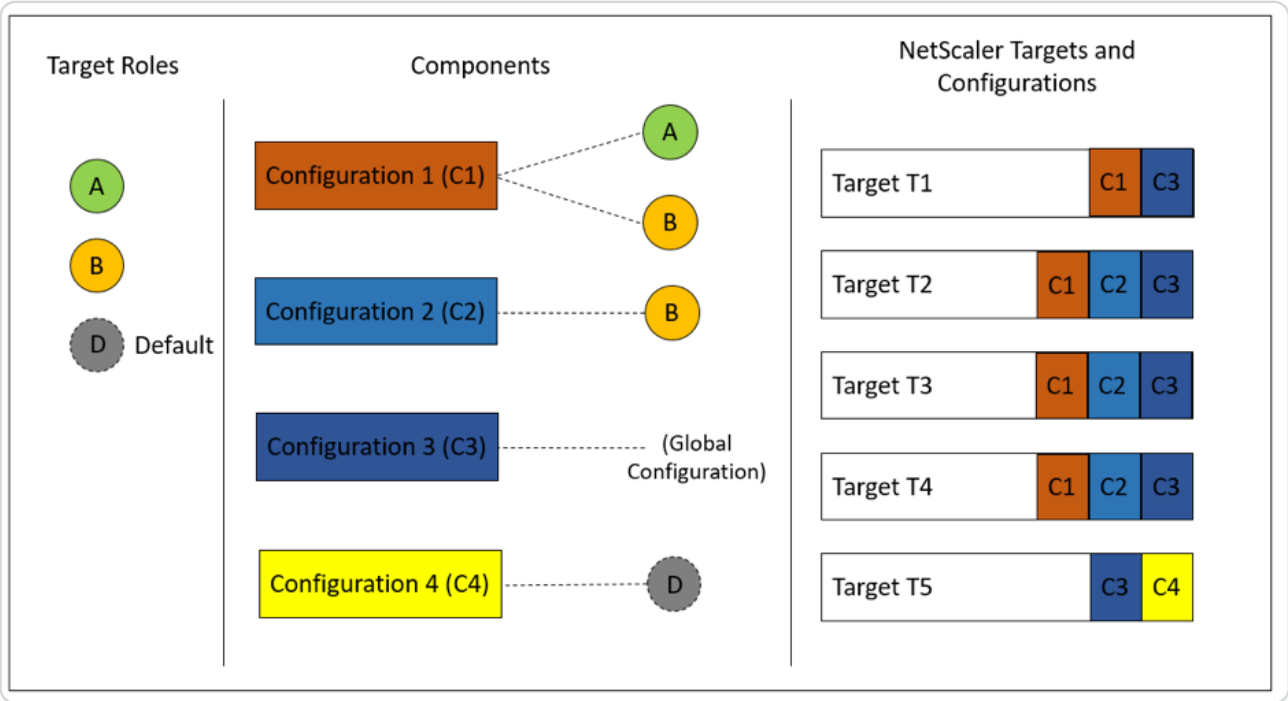
```
    properties:

      name: lb4

      servicetype: HTTP

      ipv46: 14.14.14.14

      port: 80
```

请注意，组件 C3 未定义角色，这意味着该组件将部署在所有实例上，无论其角色如何。另一方面，组件 C4 具有“默认”角色，这意味着它将应用于未分配显式角色的任何实例。

现在，假设您想使用此 StyleBook 创建一个配置包，并将其部署在五个 NetScaler 实例上。在此阶段，您可以按以下方式将角色分配给实例：

- 角色 A 分配给实例 T1、T2、T3 和 T4
- 角色 B 分配给实例 T2、T3 和 T4
- 实例 T5 未分配任何角色

下图总结了角色分配，并显示了每个 NetScaler 实例将接收的最终配置：



请注意，组件 C3 部署在所有实例上，无论角色如何，因为此组件没有角色属性。

在创建配置包时，您还可以使用“试运行”功能来查看和验证角色的正确分配以及将在每个 NetScaler 实例上创建的配置对象。

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

构建您的 StyleBook

StyleBook “demo-target-roles” 的完整内容如下：

```
---

name: demo-target-roles

namespace: com.example.stylebooks

version: "1.2"

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"

parameters:

  -

    name: appname

    type: string

    required: true

    key: true

target-roles:

  -

    name: A

  -
```

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

```
    name: B
    min-targets: 2
    max-targets: 5
  components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
```

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

```
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
```

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

下图显示了为示例配置包创建的对象：

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

Objects created (9)

Instance : 10.102.102.136 | Roles : B | Count : 3

Type : lbvserver
ipv46 : 1.1.1.1
name : lb1
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 12.12.12.12
name : lb2
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 13.13.13.13
name : lb3
port : 80
servicetype : HTTP

Instance : 10.102.102.135 | Roles : B | Count : 3

Type : lbvserver
ipv46 : 1.1.1.1
name : lb1
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 12.12.12.12
name : lb2
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 13.13.13.13
name : lb3
port : 80
servicetype : HTTP

Instance : 10.102.102.62 | Roles : A, default | Count : 3

Type : lbvserver
ipv46 : 1.1.1.1
name : lb1
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 13.13.13.13
name : lb3
port : 80
servicetype : HTTP

Type : lbvserver
ipv46 : 14.14.14.14
name : lb4
port : 80
servicetype : HTTP

使用 API

使用 REST API 时，您可以在创建或更新配置包时为每个 NetScaler 实例指定角色，如下所示。在“targets”块中，指定要部署各个组件的特定 NetScaler 实例的 UUID。

```
"targets": [

            {

             "id": "<ADC-UUID>",

             "roles": ["A"]

            },

           ]
```

提供了完整的 REST API 示例供您参考。

POST /`<Console-IP`>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"

    },

     "targets": [

        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",

        "roles": ["A"]

        },

        {
```

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

```
          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",
          "roles": ["A", "B"]
        },
        {
          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
          "roles": ["A", "B"]
        },
        {
          "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
          "roles": ["A", "B"]
        },
        {
          "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
          "roles": ["default"]
        }
      ]
    }
}
```


创建 StyleBook 以执行非 CRUD 操作

StyleBook 通过计算 NetScaler 实例上必要的配置对象来管理 NetScaler 配置。每次创建或更新 ConfigPack 时，这些对象都会从实例中添加、更新或删除。这就是您指定“期望状态”的时候。

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

然而，某些 NetScaler 配置对象支持除创建、更新或删除（CRUD 操作）之外的一些操作。例如，负载均衡器对象 (lbvserver) 或 NetScaler 功能对象 (nsfeature) 可以支持“启用”或“禁用”操作。同样，NetScaler 证书密钥支持“链接”和“取消链接”操作，以将证书链接或取消链接到另一个证书。NetScaler 对象上的这些操作称为非 CRUD 操作。本节介绍如何使用 StyleBook 对支持非 CRUD 操作的配置对象执行非 CRUD 操作。

注意

配置对象之间的绑定（例如，将证书密钥绑定到 lbvserver）不被视为非 CRUD 操作。这是因为 Nitro 绑定本身就是配置对象。这些对象像任何其他 NetScaler 配置对象一样被创建和删除。

支持非 CRUD 操作

在组件中添加了一个名为“meta-properties”的新构造，它与“properties”构造处于同一级别。此构造目前唯一支持的属性名为“action”。此属性可以采用该配置对象支持的值，例如“enable”或“disable”。

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

  meta-properties

   action: enable

  properties:

    name: $parameters.name

    servicetype: HTTP

    ipv46: $parameters.ip

    port: 80

    lbmethod: $parameters.lb-alg
```

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

在上面的示例中，“my-lbvserver-comp”组件的类型为“ns::lbvserver”。“ns”是前缀，它引用您在 import-stylebooks 部分中指定的命名空间 netscaler.nitro.config 和版本 10.5。“lbvserver”是此命名空间中的 NITRO 资源。作为隐式操作，lbvserver 首先由 StyleBook 创建；然后对其执行“enable”操作。

meta-properties 中指定的操作仅在创建 ConfigPack 期间对配置对象执行。对 ConfigPack 的更新不执行非 CRUD 操作。

注意

action 属性的值不能是动态评估的 StyleBook 表达式。

将 StyleBook 的配置包迁移到另一个 StyleBook

在 NetScaler Console 中，配置包始终绑定到创建它们的 StyleBook。对配置包的任何更新只能通过配置包所绑定的 StyleBook 进行。NetScaler Console 现在允许您将现有配置包迁移到新的 StyleBook。新的 StyleBook 可以是当前绑定到配置包的 StyleBook 的更原始版本。或者，您也可以将配置包迁移到完全不同的 StyleBook。

例如，您创建了一个名为 **example-lb** 的 StyleBook。此 StyleBook 用于在 NetScaler 实例上部署基本的负载均衡器配置。您从该 StyleBook 在 NetScaler 实例上创建了一个配置包 CP1。后来，您意识到您的 StyleBook 不包含监控配置。因此，您现在创建了一个名为 **example-lb-mon** 的 StyleBook。此 StyleBook 具有与 example-lb StyleBook 相同的负载均衡器配置，但增加了配置监视器的功能。

现在您想更新在配置包 CP1 中创建的现有配置以添加一些监视器。以前，您必须删除配置包 CP1 并从新的 StyleBook 创建配置包 CP2，才能将监视器添加到您的配置中。删除 CP1 会导致删除一个或多个 NetScaler 实例上在配置包 CP1 中创建的所有配置。以前，您必须通过新的 StyleBook 重新创建新的配置包，并为所有参数键入值。

相反，您现在可以将现有配置包 CP1 迁移到新的 example-lb-mon StyleBook。您的新 StyleBook 可以配置监视器详细信息。只有那些与监视器相关的配置对象才会添加到部署了配置包的 NetScaler 实例中。您现在只需提供监视器详细信息。NetScaler 实例上已部署但未更改的现有配置不受影响。

迁移配置包

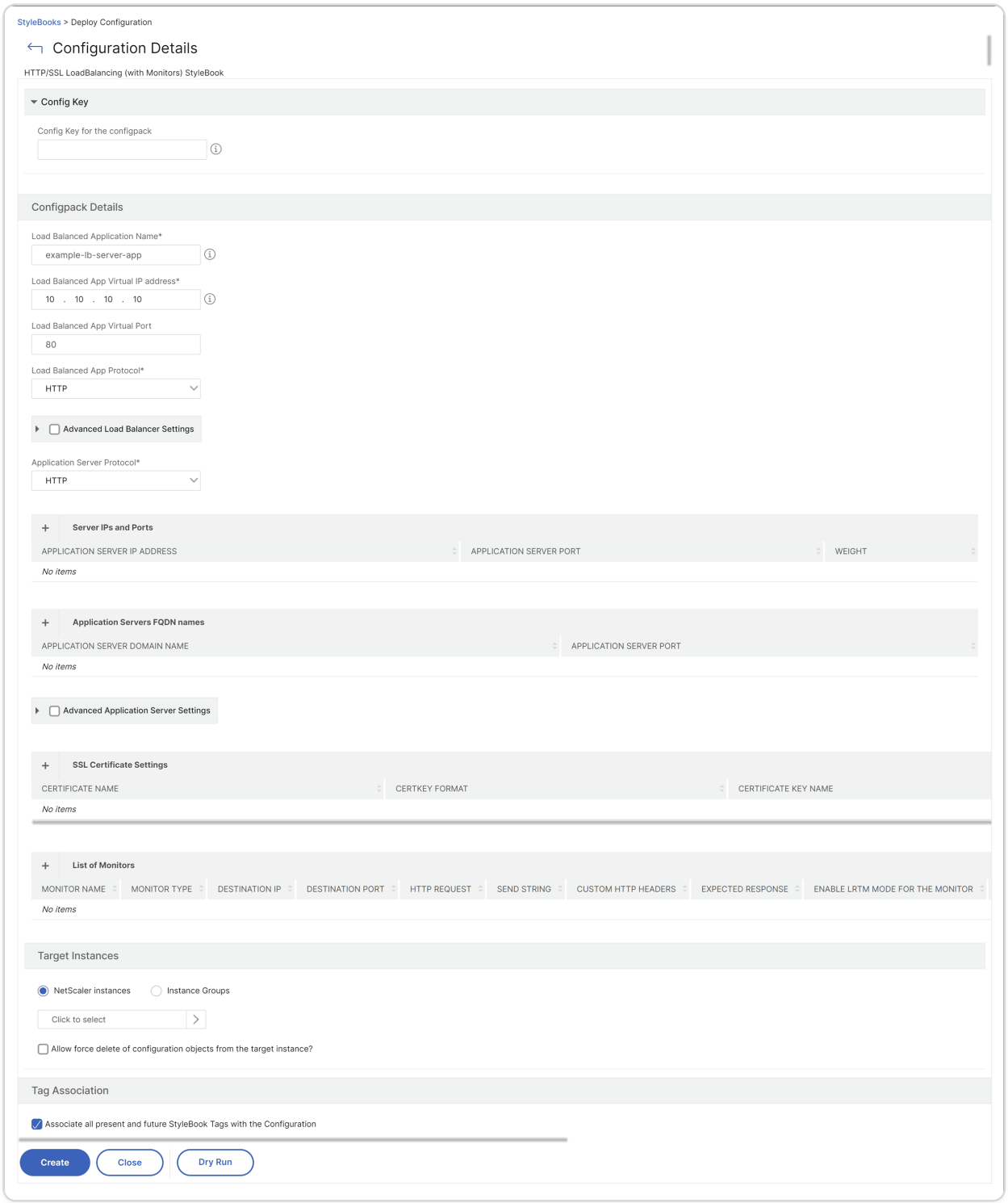
将使用 example-lb StyleBook 创建的配置包迁移到 example-lb-mon StyleBook

1. 在 NetScaler Console 中，导航到 **应用程序** \> **配置**。“**配置**”页面显示系统中存在的所有配置包。
2. 向下滚动以找到您之前创建的 **example-lb** 配置包，然后单击“**Migrate Configpack**”。

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

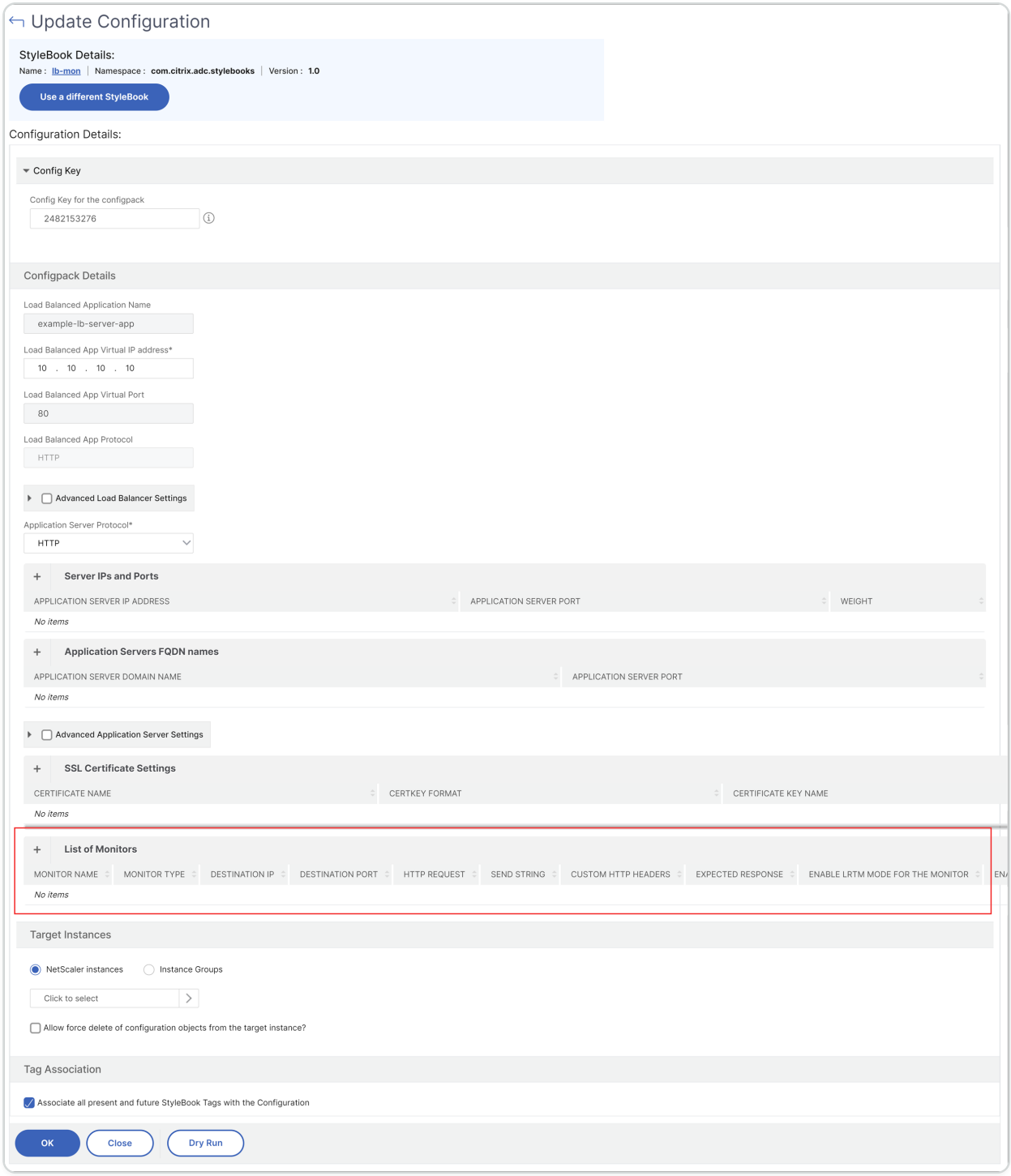
3. “**Choose target StyleBook for migration**”页面打开，其中列出了 NetScaler Console 中所有可用的 StyleBook。向下滚动以找到 **example-lb-mon** StyleBook，然后单击“**Select StyleBook**”。您也可以通过键入 example-lb-mon 来搜索 StyleBook。

   如果您从一个 StyleBook 迁移到另一个 StyleBook，两个 StyleBook 中的所有参数可能不具有相同的结构。如果参数结构相似，则以前的值会自动保留在参数字段中。新 StyleBook 中的少数参数可能是新的，或者它们的结构可能发生了变化。在这种情况下，您必须手动填写 StyleBook 参数的值。例如，下图显示了 example-lb StyleBook 的参数。



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

下图显示了将配置包迁移到 example-lb-mon StyleBook 后的参数。



在这种情况下，您可以看到 StyleBook 保留了基本负载均衡器配置的旧值。但是，您必须手动键入监视器参数的值。

4. 输入用于在该实例上创建监视器的新参数的值。
5. 在 **目标实例** 下，单击并选择要运行配置的 NetScaler 实例的 IP 地址。请注意，您可以通过指定所需数量的目标实例，将配置部署到多个 NetScaler 上。
6. 单击 **试运行**。**对象** 页面显示将从 NetScaler 实例中新建、修改或删除的对象。

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

7. 单击 **创建** 以创建或更新所选实例的配置。如果目标实例是新的，则会创建配置包。否则，将更新部署在实例上的现有配置。

> **注意：**
>
> 您还可以单击刷新图标以添加最近发现的 NetScaler 实例。因此，这些实例会立即在此窗口的实例列表中可用。刷新图标目前仅在 NetScaler Console 上可用。

您还可以将配置包从 StyleBook 的一个版本迁移到下一个版本。在此，您可能还需要输入新版本中存在的任何新必需参数的值。您还可以将配置包迁移到 StyleBook 的旧版本。在这种情况下，旧 StyleBook 中不存在的额外参数将被删除。**对象** 页面显示从配置中删除的任何对象。

成功迁移后，ConfigPack 将绑定到新的 StyleBook。

您可以看到配置包的名称和配置包 ID 与之前相同。但 NetScaler Console 会将 StyleBook 名称从 example-lb 更新为 example-lb-mon。

构建您的 StyleBook

example-lb StyleBook 的完整内容如下所示，供您参考：

```
name: example-lb

namespace: examples.stylebooks

version: "1.0"

display-name: Basic Load Balancer App

description: This is an example StyleBook that creates a load balancer
application

schema-version: "1.0"

import-stylebooks:

  -

    namespace: com.citrix.adc.stylebooks

    prefix: stlb
```

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

```
    version: "1.0"

parameters-default-sources:

  - stlb::lb

components:

  -

    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters
```

example-lb-mon StyleBook 的完整内容如下所示，供您参考：

```
name: example-lb-mon

namespace: examples.stylebooks

version: "1.0"

description: This is an example StyleBook that creates a load balancer
application with monitors

display-name: Basic Load Balancer App with Monitors

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config
```

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

```
    prefix: ns
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: "1.0"
parameters-default-sources:
  - stlb::lb
parameters:
  -
    name: monitors
    label: "List of Monitors"
    description: "List of Monitors to monitor Application Servers"
    type: cmtypes::monitor[]
substitutions:
  mon-name(appname, monname): $appname + "-mon-" + $monname
components:
  -
```

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

```
    name: lb-comp

    type: stlb::lb

    description: Uses the default lb StyleBook to build the typical lb
configuration objects

    properties-default-sources:

      - $parameters

  -

    name: monitors-comp

    type: cmtypes::monitor

    condition: $parameters.monitors

    repeat: $parameters.monitors

    repeat-item: mon

    repeat-index: ndx

    description: Builds a list of NetScaler monitor objects and binds them
to the servicegroup of this LB config

    properties-default-sources:

      - $mon

    properties:

        monitorname: $substitutions.mon-name($parameters.lb-appname,
$mon.monitorname)

    components:

      -

        name: monitor-svcg-binding-comp
```

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

```
        condition:  $parameters.svc-servers

        type: ns::servicegroup_lbmonitor_binding

        properties:

          servicegroupname: $components.lb-
comp.outputs.servicegroup.properties.servicegroupname

          monitor_name: $parent.properties.monitorname
```

管理数据源

在 NetScaler Console 中定义数据源有助于您在创建或更新 StyleBook 配置时，将外部源的数据用作输入。否则，您必须显式提供 StyleBook 所需的每个输入。在 NetScaler Console 中，您可以将任何托管的 NetScaler 实例用作 StyleBook 配置输入的源。您还可以定义自定义数据源，这些数据源可在创建或更新配置时用作输入。

集合：就像数据库可以有多个表一样，数据源可以包含多个集合。每个集合都有一个名称，并包含一个相似元组的列表，其中每个元组都是一组键值对。例如，一个集合可以由元组组成，其中每个元组都包含 (`<name>: <value>, <virtualip>:<value>`)。

数据源类型：数据源类型区分了检索数据的源类型。NetScaler Console 支持两种数据源类型。

- **managed-adc** - 它是一个内置数据源。它用于从 NetScaler Console 管理的任何现有 NetScaler 中检索数据。有关更多信息，请参阅 使用 NetScaler 实例作为数据源。

  您还可以使用目标 NetScaler 实例作为数据源。有关更多信息，请参阅 使用目标 NetScaler 实例作为数据源。

- **自定义数据源类型** - 您可以定义自定义数据源类型，其中数据在 NetScaler® Console 上本地填充。

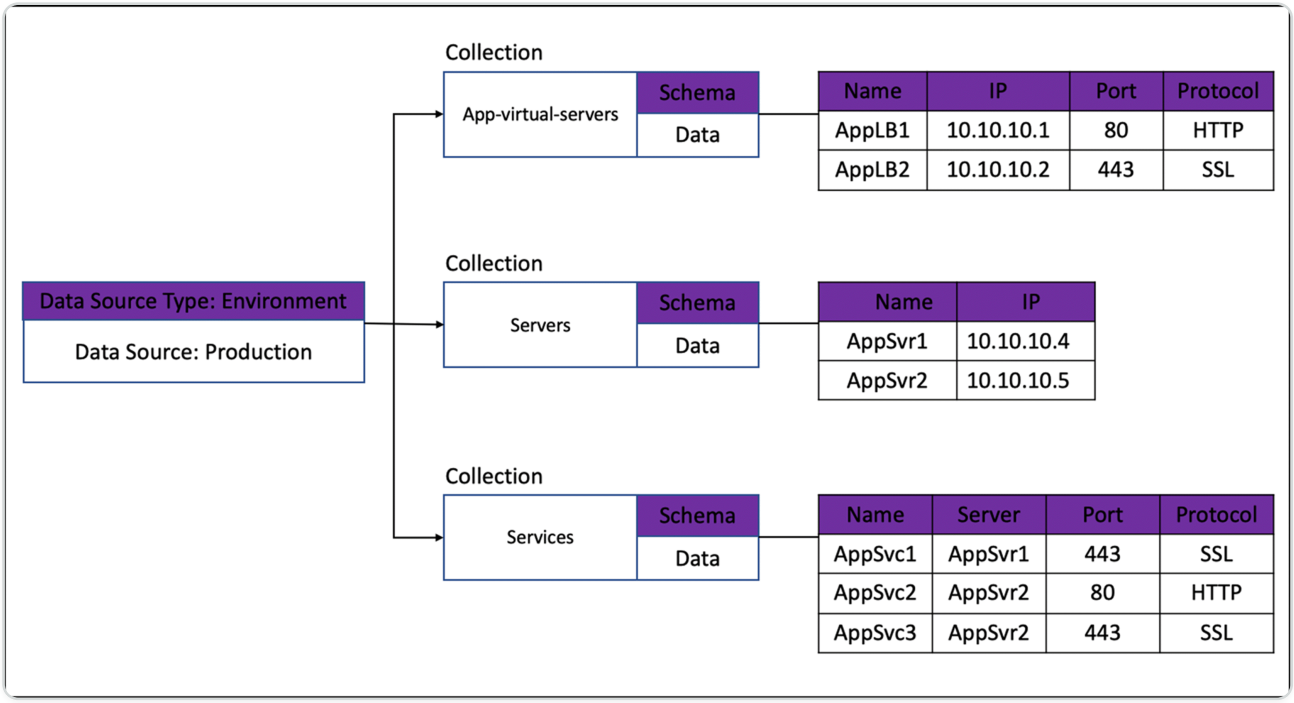
  考虑数据源类型 `Environment`。此数据源类型有两个数据源 `Production` 和 `Staging`。在创建 StyleBook 配置时，StyleBook 用户可以选择类型为 `Environment` 的任何数据源。根据选择，来自 `Production` 或 `Staging` 的数据值将用作 StyleBook 的输入。

  有关更多信息，请参阅 使用自定义数据源

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

集合架构：它描述了可以存储在集合元组中的数据类型。集合架构描述了元组中每个键的名称及其预期类型。在数据库类比中，集合架构类似于表的数据库架构，其中每个列都有明确定义的名称和支持类型。

下图是数据源的各个组件及其相互关系的通用表示：



将 NetScaler 实例用作数据源

您可以将托管的 NetScaler 实例用作数据源。`managed-adc` 是一种内置数据源类型，可直接用作 NetScaler Console 中的数据源。NetScaler Console 中的每个托管 NetScaler 实例默认都是一个数据源。如果您在创建配置包时需要来自 NetScaler Console 托管的现有 NetScaler 的数据，则可以在 StyleBook 中开始使用这些数据源。

在 StyleBook 定义中，指定 `datum` 内置类型参数。您可以在 StyleBook 中使用数据源类型。StyleBook 用户可以选择一个数据源，用于从该源检索数据。

不带集合使用内置数据源

```
parameters:

  - name: selected-adc

    label: Select an existing NetScaler

    type: datum
```

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

```
    required: true

    data-source:

      type: managed-adc
```

在此示例中，`datum` 参数用于选择 NetScaler Console 托管的任何 NetScaler 实例。`managed-adc` 内置数据源允许您从 NetScaler Console 托管的任何 NetScaler 实例中检索数据。

在您的 StyleBook 中，您可以访问所选 NetScaler 实例中的任何配置。并且，您可以在同一 NetScaler 或不同的 NetScaler 实例上创建或更新配置时使用该配置；这取决于所选的目标 NetScaler 实例。

从数据源访问集合：

在所选的 NetScaler 实例中，要访问集合，请使用以下表达式：

```
$parameters.selected-adc.collections.<collection-name>
```

示例：

```
$parameters.selected-adc.collections.lbvserver
```

此表达式返回所选 NetScaler 实例上的 `lbvserver` 实体列表。例如，您可以遍历此列表以选择满足特定条件的 `lbvserver`。

不带集合的 StyleBook 示例

```
name: add-vservers-from-managed-adc-instances

namespace: com.citrix.adc.stylebooks

version: "1.0"

schema-version: "1.0"



import-stylebooks:

  -
```

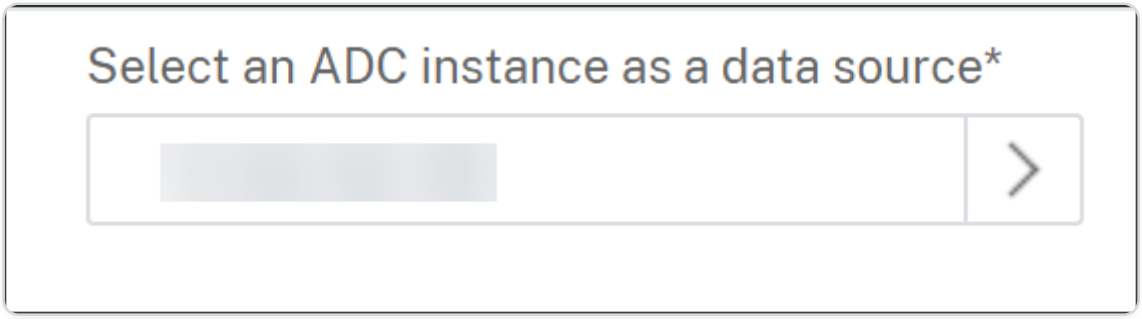
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"


parameters:
    -
      name: selected-adc
      label: Select a NetScaler instance
      type: datum
      required: true
      data-source:
        type: "managed-adc"


components:
  -
    name: sslvserver-comp
    type: ns::sslvserver
    repeat: $parameters.selected-adc.collections.lbvserver
    repeat-item: lbvs
    repeat-condition: $lbvs.attributes.servicetype == "SSL"
    properties:
      name: $lbvs.attributes.name
```

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

```
      ssl2: DISABLED

      ssl3: DISABLED

      tls1: DISABLED

      tls11: ENABLED

      tls12: ENABLED
```

配置包 GUI 显示 NetScaler Console 托管的 NetScaler 实例，StyleBook 用户在创建或更新配置包时可以选择任何 NetScaler。



此 StyleBook 使用所选的 NetScaler 并遍历所有 `lbvserver` 实体。它选择 SSL 虚拟服务器并设置每个虚拟服务器上允许的 SSL 协议版本。

以下表达式允许您遍历 NetScaler 实例中的 `lbvserver` 实体列表。

```
repeat: $parameters.selected-adc.collections.lbvserver
```

- `collections`：指的是 NetScaler 实例上的所有实体类型。例如 `csvserver`、`lbmonitor`、`servicegroup` 等。
- `lbvserver`：指的是 NetScaler 实例中负载均衡虚拟服务器实体的列表。

使用带集合的内置数据源

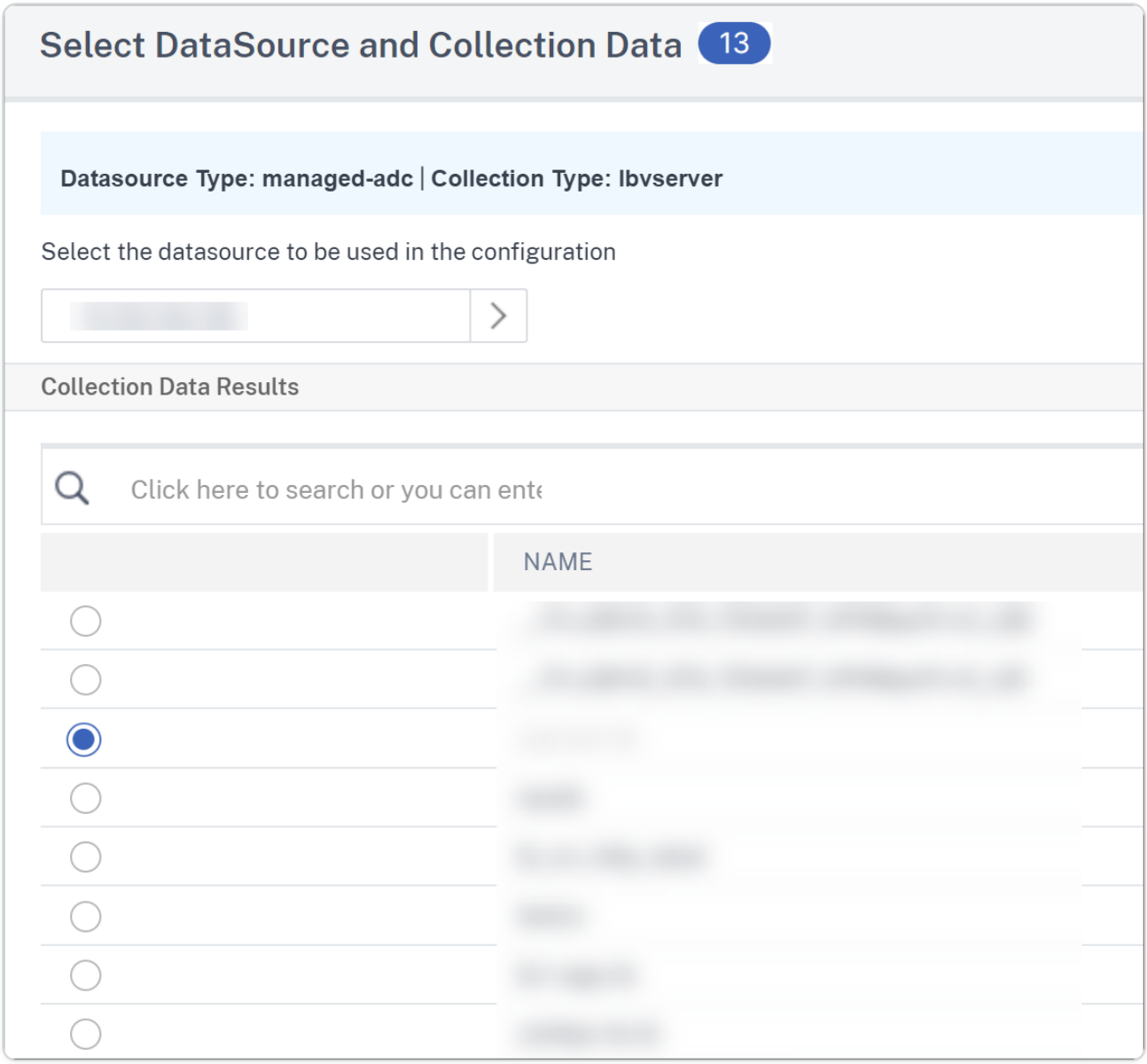
```
parameters:

  - name: selected-lbvserver

    label: Select an existing lbvserver

    type: datum
```

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

```
    required: true

    data-source:

      type: managed-adc

      collection: lbvserver
```

在此示例中，使用 `datum` 参数允许用户从 `managed-adc` 数据源类型中选择 NetScaler 实例和特定的 `lbvserver`。

当您在 `parameters` 部分定义集合类型时，StyleBook 用户可以从该实例上的集合中选择 NetScaler 实例和特定实体。



访问所选项目的属性：

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

当 StyleBook 用户选择虚拟服务器时，StyleBook 中的以下表达式可以访问所选项目的任何属性。

```
$parameters.selected-lbvserver.attributes.<attribute-name>
```

在此示例中，所选的 `datum` 是 `lbvserver`。因此，您可以访问 NetScaler 实体 `lbvserver` 的任何属性，例如 `name`、`servicetype`、`ipv46` 等。

示例：

```
$parameters.selected-lbvserver.attributes.ipv46
```

此表达式检索所选负载均衡虚拟服务器的 IP。有关 NetScaler 实体（集合）及其属性的更多信息，请参阅 NetScaler NITRO API 参考。

从集合中选择多个项目：

以下参数部分允许 StyleBook 用户选择集合中的多个项目。

```
parameters:

  - name: selected-lbvservers

    label: Select existing lbvservers

    type: datum[]

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver
```

在此示例中，datum 参数用于定义数据源数组。用户可以从单个 NetScaler® 实例或跨多个 NetScaler 实例选择一个或多个 lbvserver。

以下代码片段描述了访问所选项目及其属性的方法。

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

```
components:

  - name: sslvserver-comp

    type: ns::sslvserver

    repeat:

      repeat-list: $parameters.selected-lbvservers

      repeat-item: vserverObj

    properties:

      name: $vserverObj.attributes.name

      ssl2: DISABLED

      ssl3: DISABLED

      tls1: DISABLED

      tls11: ENABLED

      tls12: ENABLED
```

通过所选项目的引用访问集合：

除了允许 StyleBook 用户在托管的 NetScaler 实例上选择特定实体外，您还可以访问所选 NetScaler 实例上相同或不同集合中的任何实体。要访问该 NetScaler 实例上的另一个集合，请在 `components` 部分中使用以下表达式：

```
$parameters.selected-lbvserver.datasource.collections.<collection-name>
```

示例：

```
$parameters.selected-lbvserver.datasource.collections.csvserver
```

此表达式返回所选 NetScaler 实例中的内容切换虚拟服务器列表。

并且，以下表达式返回 `lbvservers` 和 `servicegroups` 之间的所有绑定列表：

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

```
$parameters.selected-
lbvserver.datasource.collections.lbvserver_servicegroup_binding
```

带集合的 StyleBook 示例

以下是一个 StyleBook 示例，演示如何将托管的 NetScaler 实例用作数据源：

```
name: bind-lb-to-servicegroup-using-ADC-as-datasource

namespace: com.citrix.adc.stylebooks

version: "1.1"

display-name: "HTTP/SSL LoadBalancing StyleBook with Service Binding"

description: "This stylebook defines a typical Load Balanced Application
configuration where we allow the user to select an existing lbvserver on
the NetScaler using datum type parameter. Then a servicegroup for the
selected lb is created if it does not exist on the NetScaler. Finally, the
selected lbvserver is bound to the service "

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



parameters:

  -

    name: selected-vserver

    label: "Select an Existing VServer"
```

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

```
    description: "Load Balancing Application Vservers to be bound to
service on the ADC"

    type: datum

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver



components:

  -

    name: servicegroup-discovery-comp

    type: object

    repeat: $parameters.selected-
vserver.datasource.collections.servicegroup

    repeat-item: svcgrp

    repeat-condition: $svcgrp.attributes.servicegroupname ==
 $parameters.selected-vserver.attributes.name + "-svcgrp"

    properties:

      servicegroupname: $svcgrp.attributes.servicegroupname

  -

    name: servicegroup-creation-if-not-exists-comp

    type: ns::servicegroup

    condition: not exists($components.servicegroup-discovery-comp)
```

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

```
    properties:

      servicegroupname: $parameters.selected-vserver.attributes.name + "-
svcgrp"

      servicetype: $parameters.selected-vserver.attributes.servicetype

    components:

      -

        name: lbvserver-servicegroup-binding

        type: ns::lbvserver_servicegroup_binding

        properties:

          name: $parameters.selected-vserver.attributes.name

          servicegroupname: $parent.properties.servicegroupname
```

在此 StyleBook 中，`components` 部分检查与所选负载均衡虚拟服务器名称连接 `svcgrp` 匹配的服务组名称。

如果所选负载均衡虚拟服务器的名称是 `lbv1`，此 StyleBook 将检查名称为 `lbv1-svcgrp` 的服务组。如果未找到，它将创建服务组 `lbv1-svcgrp` 并与 `lbv1` 虚拟服务器绑定。

以下表达式获取 NetScaler 实例中的服务组列表。

```
repeat: $parameters.selected-vserver.datasource.collections.servicegroup
```

在此表达式中：

- `datasource`：指代由 NetScaler Console 管理的所选 NetScaler 实例。
- `collections`：指代 NetScaler 实例中的所有实体。
- `servicegroup`：指代 NetScaler 实例中的服务组。

筛选集合数据：

以下参数部分解释了如何在 StyleBook 定义中为内置数据源集合指定筛选器。它允许 StyleBook 用户从筛选后的集合中选择特定项。

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

```
parameters:

  - name: selected-lbvserver

    label: Select an existing lbvserver

    type: datum

    required: true

    data-source:

      type: managed-adc

      collection: lbvserver

      collection-filters:

        protocol: SSL
```

在此示例中，datum 参数用于允许用户从 managed-adc 数据源类型中选择 NetScaler 实例和具有 SSL 协议的特定 lbvserver。

StyleBook 用户选择虚拟服务器后，可以按照上一节中说明的相同方式访问所选项目的任何属性。

将目标 NetScaler 实例用作数据源

您还可以将配置的目标 NetScaler 本身用作配置的数据源输入。在这种情况下，您可能希望参考目标 NetScaler 上的现有配置来在该 NetScaler 上创建新配置。

要将目标实例用作数据源，您不必使用 `datum` 内置类型参数，因为 StyleBook 用户无需选择任何 NetScaler 实例。您可以直接在 StyleBook 的 `components` 部分中编写表达式，以从目标 NetScaler 实例检索数据。

使用以下表达式从目标 NetScaler 实例中检索以下内容：

- 集合：

  ```
  $current-target-as-datasource.collections.<collection-name>
  ```

  示例：

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

```
$current-target-as-datasource.collections.lbvserver
```

- 属性：

```
$current-target-as-datasource.collections.attributes.<attribute>
```

将目标 NetScaler 实例用作数据源的示例 StyleBook

以下是一个示例 StyleBook，演示如何将目标 NetScaler 实例用作数据源：

```
---

name: lb-add-service-with-target-adc

namespace: com.citrix.adc.stylebooks

version: "1.1"

display-name: "HTTP/SSL LoadBalancing StyleBook with Service Binding"

description: "This stylebook defines a typical Load Balanced Application
configuration."

schema-version: "1.0"

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    prefix: ns

    version: "10.5"



components:

  -

    name: servicegroup-comp
```

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

```
    type: ns::servicegroup
    properties:
      servicegroupname: "lb-demo-svcgrp"
      servicetype: "HTTP"


    components:
      -
        name: lbvserver-svg-binding
        type: ns::lbvserver_servicegroup_binding
        repeat: $current-target-as-datasource.collections.lbvserver
        repeat-item: lbvsrvr
        repeat-condition: $lbvsrvr.attributes.name == "lb-demo-lb"
        properties:
          name: $lbvsrvr.attributes.name
          servicegroupname: $parent.properties.servicegroupname
```

在此示例中，配置包检查目标 NetScaler 实例中的负载平衡虚拟服务器。如果给定的负载平衡虚拟服务器 IP 地址匹配，它将检索名称和服务组名称。

将目标 NetScaler 实例用作数据源(/en-us/netscaler-application-delivery-management-software/media/target-instance-as-datasource.png)

使用自定义数据源

除了 将托管的 NetScaler 实例作为数据源 之外，如果输入数据重复用于创建多个配置，您还可以定义和使用自定义数据源。您可以将输入数据作为数据源保存在 NetScaler Console 中。而且，您可以修改 StyleBook 以使用此数据，而无需 StyleBook 用户重复提供输入。

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

在 StyleBook 定义中使用自定义数据源之前，请执行以下操作来定义自定义数据源：

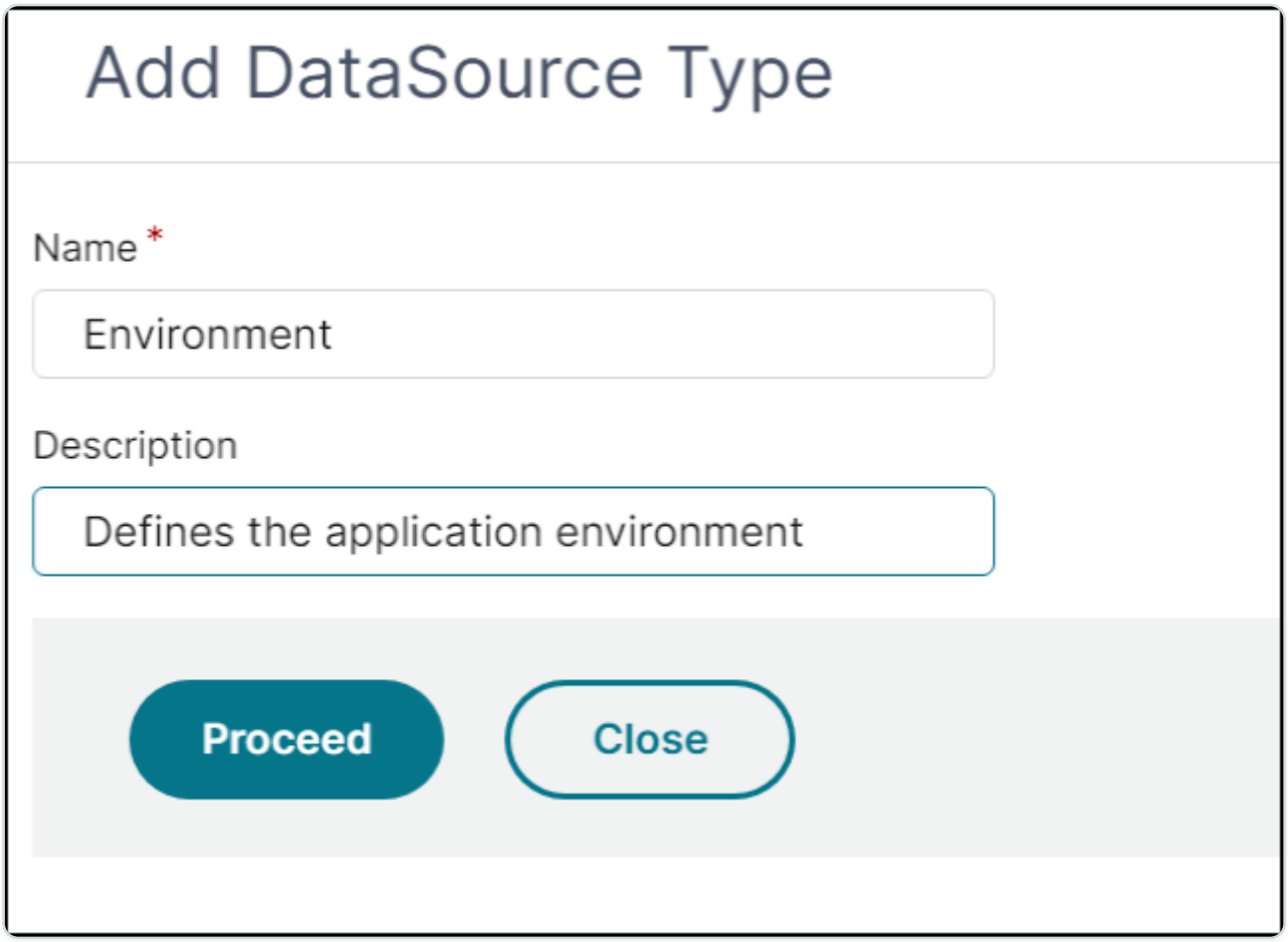
1. 添加数据源类型。
2. 在数据源类型下添加集合架构。
3. 添加数据源。
4. 添加集合数据。

添加数据源后，您可以在 StyleBook 定义中使用此数据源。有关详细信息，请参阅 在 StyleBook 定义中使用自定义数据源。

添加数据源类型

指定数据源类型以区分检索数据的来源。

1. 在 **应用程序 > 配置 > 数据源** 中。
2. 选择 **数据源类型**，然后单击 **添加**。
3. 指定数据源类型的 **名称** 和 **描述**。
4. 单击 **继续** 以保存 **数据源类型**。单击 **关闭** 以退出工作流而不保存任何更改。



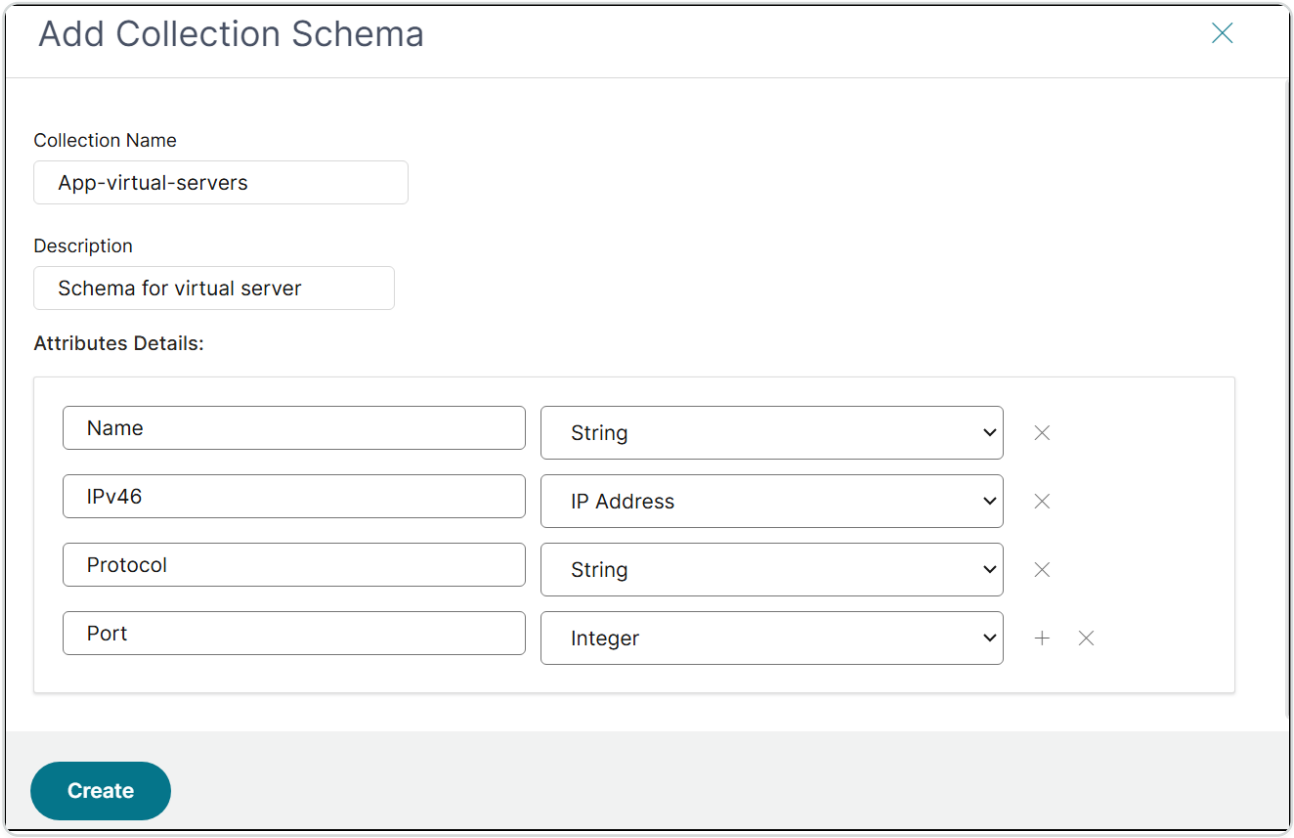
在此示例中，数据源类型设置为 **Environment**。此类型可用于将应用程序环境定义为数据源。

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

在数据源类型下添加集合架构

添加 **Data Source Type** 后，将显示一个用于为 ""Data Source Type** 添加 **Collection Schemas** 的屏幕。

1. 单击 **Add**。
2. 为集合架构指定 **Collection Name**。
3. 输入 **Description**。
4. 根据需要，在 **Attribute Details** 下添加属性（名称及其类型）。
5. 单击 **Create**。



在此示例中，**App-virtual-servers** 集合架构有四个属性。因此，您要存储的集合必须具有这些已设置数据类型的属性。

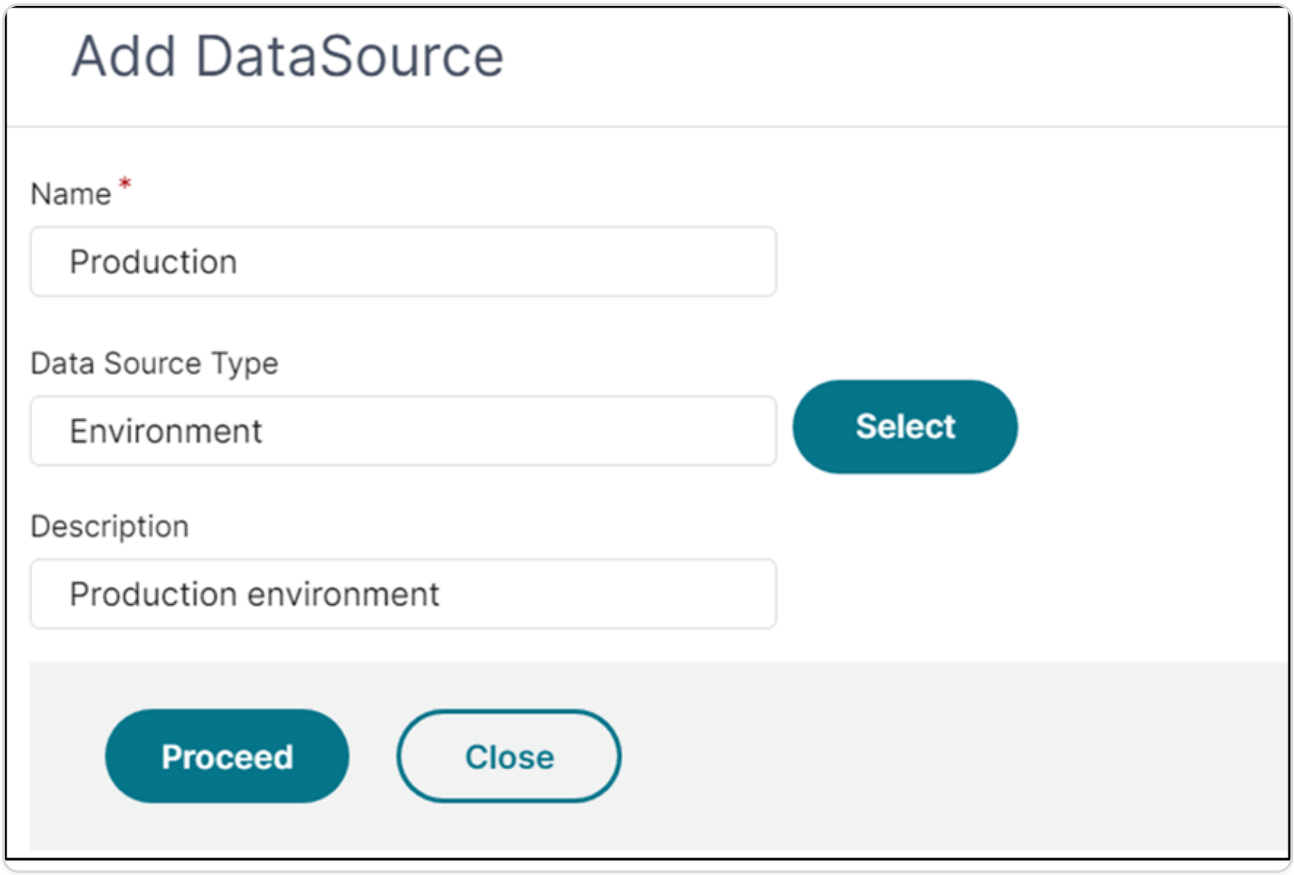
添加数据源

为特定数据源类型定义数据源。

1. 转到 **应用程序 > 配置 > 数据源**。
2. 选择 **Data Sources** 选项卡，然后单击 **Add**。
3. 指定 **Name**。
4. 选择**数据源类型**，然后输入**描述**。

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

5. 单击**继续**以保存**数据源**。单击**关闭**以退出工作流而不保存任何更改。



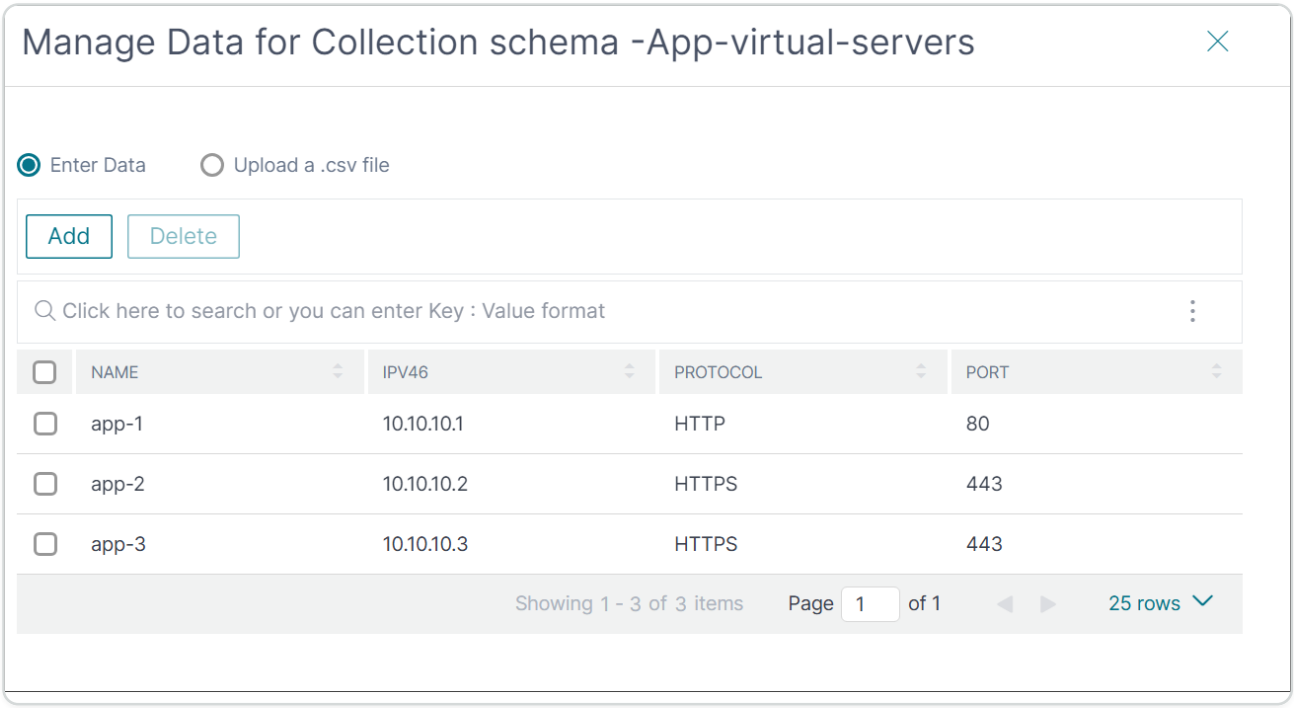
在此示例中，**生产环境**被添加为数据源。

添加集合数据

添加**数据源**后，将显示一个用于输入**数据源**数据的屏幕。您可以看到**集合架构**的列表。

1. 选择要向其中添加集合数据的**集合架构**。
2. 单击**管理集合数据**。
3. 将数据添加到集合。您可以逐个添加数据或上传 CSV 文件。上传 CSV 文件时，请确保列名与集合架构的属性名匹配。
4. 单击**确定**。

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



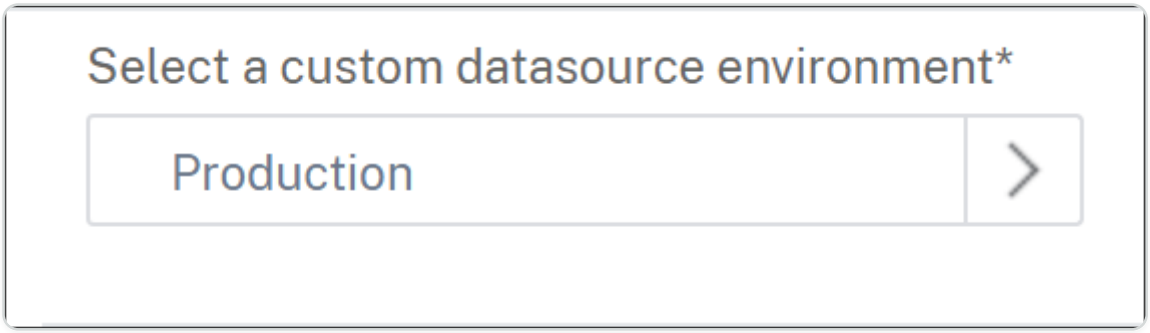
使用不带集合的自定义数据源

以下 `parameters` 部分解释了如何在 StyleBook 定义中定义不带集合的自定义数据源。

```
parameters:

    - name: selected-environment

      label: Select a custom datasource environment

      type: datum

      required: true

      data-source:

        type: "Environment"
```

配置包 GUI 显示适用的数据源，StyleBook 用户可以选择其中任何一个来创建配置包。

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



在此示例中，它使用 `Production` 数据源来检索数据。

在 `Environment` 数据源类型中，要访问 `App-virtual-servers` 集合类型，请使用以下表达式：

```
$parameters.selected-environment.collections.App-virtual-servers
```

示例代码片段：

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    repeat: $parameters.selected-environment.collections.App-virtual-
servers

    repeat-item: app

    properties:

      name: $app.attributes.Name + "-lb"

      ipv46: ip($app.attributes.IPv46 )

      port: $app.attributes.Port

      servicetype: $app.attributes.Protocol

    components:
```

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

```
    -

      name: servicegroup-comp

      type: ns::servicegroup

      properties:

        servicegroupname: $parent.properties.name + "-svcgrp"

        servicetype: $parent.properties.servicetype



      components:

        -

          name: lbvserver-svg-binding

          type: ns::lbvserver_servicegroup_binding

          properties:

            name: $parent.parent.properties.name

            servicegroupname: $parent.properties.servicegroupname
```

将自定义数据源与集合一起使用

以下 `parameters` 部分说明了如何在 StyleBook 定义中定义自定义数据源。它允许 StyleBook 用户选择集合中的特定项。

```
parameters:

  - name: selected-app-vserver

    label: Select a collection from the datasource

    type: datum

    required: true
```

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

```
    data-source:

      type: Environment

      collection: App-virtual-servers
```

在此示例中，`datum` 参数用于定义自定义数据源。它使用 `Production` 数据源从 `App-virtual-servers` 集合架构中检索数据。

在 `Environment` 数据源类型中，要从 `App-virtual-servers` 集合访问协议，请使用以下表达式：

```
$parameters.selected-app-vserver.attributes.Protocol
```

示例代码片段：

```
components:

  - name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: $parameters.selected-app-vserver.attributes.Name

      ipv46: $parameters.selected-app-vserver.attributes.IPv46

      port: $parameters.selected-app-vserver.attributes.Port

      servicetype: $parameters.selected-app-vserver.attributes.Protocol
```

当您在 `parameters` 部分中定义集合类型时，StyleBook 用户可以选择数据源和集合。

从集合中选择多个项目：

以下参数部分允许 StyleBook 用户选择集合中的多个项目。

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

```
parameters:

  - name: selected-app-vservers

    label: Select app-vservers from the collection

    type: datum[]

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers
```

在此示例中，datum 参数用于定义自定义数据源数组。用户可以从单个数据源或跨多个数据源的“App-virtual-servers”集合中选择一个或多个项目。

下面的代码片段描述了访问所选项目及其属性的方法。

```
components:

  -

   name: lbvserver-comp

   type: ns::lbvserver

   repeat:

   repeat-list: $parameters.selected-app-vservers

   repeat-item: vserverObj

    properties:

      name: $vserverObj.attributes.Name

      ipv46: $vserverObj.attributes.IPv46

      port: $vserverObj.attributes.Port
```

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

```
      servicetype: $vserverObj.attributes.Protocol
```

筛选集合数据：

以下参数部分说明了如何在 StyleBook 定义中指定自定义数据源集合的筛选器。它允许 StyleBook 用户从筛选后的集合中选择特定项目。

```
parameters:

  - name: selected-app-vserver

    label: Select a collection from the datasource

    type: datum

    required: true

    data-source:

      type: Environment

      collection: App-virtual-servers

      collection-filters:

        Protocol: SSL
```

在此示例中，datum 参数用于定义自定义数据源。它使用类型为 Environment 的数据源来检索 App-virtual-servers 集合架构中的过滤数据。

StyleBook 用户选择虚拟服务器后，可以按照上一节中说明的相同方式访问所选项目的任何属性。

使用 API 从 StyleBook 创建配置

构建 StyleBook 后，您必须使用 NetScaler Console GUI 或 NetScaler Console API 导入它。导入时，NetScaler Console 会验证您的 StyleBook。如果验证成功，您的 StyleBook 将出现在 NetScaler Console 的 StyleBook 目录中，可用于创建配置。

您现在可以使用 StyleBook API 基于此 StyleBook 创建配置。您可以使用任何工具，例如 cURL 命令行工具或 Postman Chrome 浏览器扩展程序，向 NetScaler Console 发送 HTTP 请求。

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

示例 1

考虑您在 StyleBook to Create a Load Balancing Virtual Server 中创建的 lb-vserver StyleBook。使用 REST API 从此 StyleBook 创建配置包，如下所示：

HTTP 方法：POST **URL**：`https://<IP>/stylebook/nitro/v2/config/configpacks`

请求头：

内容类型: application/json

接受: application/json

请求正文负载：

```
{
  "configpack":
  {
    "parameters": {
      "name": "lb1",
      "vip-ipaddress": "10.102.117.31"
    },
    "targets":
    [
      {
        "instance_id": "deecee30-f478-4446-9741-a85041903410"
      }
    ],
    "stylebook": {
```

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

```
            "name": "lb-vserver",

            "namespace": "com.example.stylebooks",

            "version": "1.0"

        }

    }

}
```

在此 HTTP 请求中，IP 地址为 10.102.117.31 的负载均衡虚拟服务器 `lb1` 在实例 ID 为“deecee30-f478-4446-9741-a85041903410”的 NetScaler 实例上创建。NetScaler 实例的实例 ID 是从 NetScaler Console 中检索的。

要获取由 NetScaler Console 管理的实例的 ID，您可以使用 NetScaler Console API。例如，要检索 IP 地址为 192.168.153.160 的 NetScaler 实例的实例 ID，您可以使用以下 API：

HTTP 方法：GET

URL：`https://<IP>/nitro/v2/config/ns?filter=ip_address:192.168.153.160`

请求头：

接受: application/json

响应在 JSON 有效负载中包含 ID：

预期响应头（成功时）：

200 OK

内容类型: application/json

预期响应正文（成功时）：

```
{

  "errorcode": 0,

  "message": "Done",
```

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

```
  "operation": "get",

  "resourceType": "ns",

  "username": "nsroot",

  "tenant_name": "Owner",

  "resourceName": "",

  "ns":

  [

    {

    "is_grace": "false",

    "hostname": "",

    "std_bw_config": "0",

    "gateway_deployment": "false",

    "id": "deecee30-f478-4446-9741-a85041903410",

   }

 ]

}
```


如果配置（配置包）成功创建，您将收到以下 HTTP 响应：

预期响应头（成功时）：

202 OK

内容类型: application/json

预期响应正文（成功时）：

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

```
{
  "job":
  {
    "job_id": "1460806080"
  }
}
```

您已创建您的第一个作业，该作业通过 ID 1460806080 唯一标识。您可以使用此 ID 查询、更新或删除配置。

您可以使用以下 URL 查询作业状态：

`https://<IP>/stylebook/nitro/v2/config/jobs/<jobid>`。

示例 2

您可以使用相同的 StyleBook 创建另一个配置包，并在相同或不同的 NetScaler 实例上运行它。在此示例中，创建另一个配置并为虚拟服务器提供不同的名称和 IP 地址。将 LEASTCONNECTION 指定为负载均衡方法。将此配置部署到两个 NetScaler 实例上。

HTTP 请求如下所示：

HTTP 方法：POST

URL：`https://<IP>/stylebook/nitro/v2/config/configpacks`

请求头：

内容类型: application/json

接受: application/json

请求正文负载：

```
{
  "configpack":
```

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

```
{
  "parameters": {
    "name": "lb1",
    "vip-ipaddress": "10.102.117.31",
    "lb-alg": "LEASTCONNECTION"
  },
  "targets":
  [
    {
      "instance_id": "deecee30-f478-4446-9741-a85041903410"
    },
    {
      "instance_id": "abcdee30-f478-4446-9741-a85041903410"
    }
  ],
  "stylebook": {
          "name": "lb-vserver",
          "namespace": "com.example.stylebooks",
          "version": "1.0"
      }
}
```

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

```
}
```

在此 HTTP 请求中，IP 地址为 10.102.117.31 的负载均衡虚拟服务器 lb1 在两个 NetScaler 实例上创建，其实例 ID 分别为“deecee30-f478-4446-9741-a85041903410”和“abcdee30-f478-4446-9741-a85041903410”。

成功创建配置包后，将收到以下 HTTP 响应：

预期响应头（成功时）：

202 OK

内容类型: application/json

预期响应正文（成功时）：

```
{
    "job": {
        "job_id": "165769629"
    }
}
```

此新配置包具有不同的 ID，即 1657696292。您可以使用此 ID 更新或删除此配置。

示例 3

考虑您在创建基本负载均衡配置的样式簿中创建的“basic-lb-config”样式簿。使用 REST API 从此样式簿创建配置包，如下所示：

HTTP 方法：POST

URL：`https://<IP>/stylebook/nitro/v2/config/configpacks`

请求头：

内容类型: application/json

接受: application/json

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

请求正文负载：

```
Content-Type: application/json

Accept: application/json

{

  "configpack":

  {

    "parameters":

    {

      "name": "myapp",

      "ip": "10.70.122.25",

      "svc-servers": ["192.168.100.11","192.168.100.12"],

       "svc-port": 8080

    },

    "targets":

    [

     {

      "instance_id": "deecee30-f478-4446-9741-a85041903410"

     },

     {

      "instance_id": "abcdefgi-d589-4557-8632-a74032802412"

     }

    ],
```

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

```
    "stylebook": {
            "name": "basic-lb-config",
            "namespace": "com.example.stylebooks",
            "version": "0.1"
        }
  }
}
```

预期响应头（成功时）：

202 OK

内容类型: application/json

预期响应正文（成功时）：

```
{
    "job": {
        "job_id": "3628681382"
    }
}
```

在此 HTTP 请求中，负载均衡配置在两个 NetScaler 实例上运行。您可以登录这些 NetScaler 实例，以验证是否已创建虚拟服务器以及绑定了两个服务的服务组。

示例 4

考虑您在创建复合样式簿中创建的复合样式簿 **composite-example**。使用 REST API 从此样式簿创建配置包，如下所示：

HTTP 方法：POST

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

URL： `https://<IP>/stylebook/nitro/v2/config/configpacks`

请求头：

内容类型: application/json

接受: application/json

请求正文负载：

```
{
  "configpack":
  {
    "parameters": {
      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53"]
    },
    "targets":
    [
     {
      "id": "deecee30-f478-4446-9741-a85041903410"
     },
     {
      "id": "abcdefgg-d589-4557-8632-a74032802412"
     }
    ],
```

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

```
    "stylebook": {
            "name": "composite-example",
            "namespace": "com.example.stylebooks",
            "version": "0.1"
        }
  }
```

在此 HTTP 请求中，配置在两个 NetScaler 实例上创建，这些实例由其 ID 表示。如果您登录到 NetScaler 实例，则可以查看由导入到“composite-example”StyleBook 中的“basic-lb-config”StyleBook 创建的配置对象。您还可以看到一个名为 myapp-mon 的新 HTTP 监视器，它是“composite-example”StyleBook 的一部分。

成功创建配置包后，将收到以下 HTTP 响应：

预期响应头（成功时）：

202 OK

内容类型: application/json

预期响应正文（成功时）：

```
{
    "job": {
        "job_id": "3628681382"
    }
}
```

更新配置

假设您要使用 IP 地址为 10.102.29.54 的新后端服务器更新配置。要将服务器添加到负载平衡虚拟服务器 myapp，请使用以下 API：

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

HTTP 方法：PUT

URL： `https://<IP>/stylebook/nitro/v2/config/configpacks/<configpackid>`

请求头：

内容类型: application/json

接受: application/json

请求正文负载：

```
{
  "configpack": {
    "parameters": {
      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
  },
  "targets":
   [
     {
      "instance_id": "deecee30-f478-4446-9741-a85041903410"
     },
     {
      "instance_id": "abdcedff-d589-4557-8632-a74032802412"
     }
   ]
```

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

```
  }

}
```

成功更新配置包后，将收到以下 HTTP 响应：

预期响应头（成功时）：

202 OK

内容类型: application/json

预期响应正文（成功时）：

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

删除配置

要删除此配置（从所有 NetScaler 实例中），您可以使用删除配置包的 API，如下所示：

成功删除配置包后，将收到以下 HTTP 响应：

HTTP 方法：DELETE

URL：`https://<DNS-or-IP>//stylebook/nitro/v2/config/configpacks/<configpackid>`

请求头:

接受: application/json

预期响应头 (成功时):

202 OK

内容类型: application/json

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

预期响应负载 (成功时):

```
{

    "job": {

        "job_id": "3628681382"

    }

}
```

登录到 NetScaler 实例并验证属于此配置包的所有配置对象已被移除。

要从特定的 NetScaler 实例中移除配置，而不是从所有实例中移除，请使用 (#updating-a-configuration) 中的操作。更改 JSON 负载中的 targets 属性以移除特定的 NetScaler 实例 ID。

使用 API 创建配置以上传证书和密钥文件

使用 StyleBook API 基于此 StyleBook 创建配置。您可以使用任何工具，例如 curl 命令行工具或 Postman Chrome 浏览器扩展程序，向 NetScaler Console 发送 HTTP 请求。

请参考您在 如何创建 StyleBook 以上传 SSL 证书和证书密钥文件到 NetScaler Console 中创建的用于上传证书和密钥文件的 StyleBook 示例。使用 REST API 从此 StyleBook 创建配置包，如下所示：

```
POST



https://<MAS_IP_Address>/stylebook/nitro/v2/config/configpacks?mode=async
```

```
Content-Type: application/jsonAccept: application/json



{

    "configpack": {
```

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

```
        "stylebook": {
            "name": "lb-mon_test",
            "namespace": "com.citrix.adc.stylebooks",
            "version": "2.0"
        },
        "parameters": {
            "lb-service-type": "SSL",
            "ip-address-type": "IP Address",
            "lb-appname": "testvip",
            "lb-virtual-port": 80,
            "svc-service-type": "SSL",
            "lb-virtual-ip": "10.10.20.11",
            "certificates": [
                {
                    "ssl-inform": "PEM",
                    "certkey-param": {
                        "id": "d0982579-42a9-417a-b24e-1f9ae5592f1d",
                        "name": "testcertkey"
                    }
                }
            ]
        },
```


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

```
        "targets": [
            {
                "instance_id": "f383b454-b777-454a-8c17-c477f0bad21e"
            }
        ]
    }
}
```

此配置包通过 ID f383b454-b777-454a-8c17-c477f0bad21e 唯一标识。您可以使用此 ID 查询、更新或删除配置。配置包成功更新后，证书和密钥文件将上传到 NetScaler Console 文件系统。

使用 API 创建配置以上传任何文件类型

您还可以使用 NetScaler Console API 创建配置包，将文件上传到所选的 NetScaler 实例。 有关上传任何文件类型的示例，请参阅 如何创建 StyleBook 以将文件上传到 NetScaler MA 服务。 如示例中所述，创建一个配置包，并将“locationfile”参数的值设置为 NetScaler Console 上位置文件的文件路径。 使用 REST API 从此 StyleBook 创建配置包，如下所示：

```
POST



https://<mas_ip>/stylebook/nitro/v2/config/configpacks?mode=sync
```

```
Content-Type: application/json

Accept: application/json

{

    "configpack": {

        "stylebook": {
```

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

```
            "name": "upload-geolocations",
            "namespace": "com.citrix.adc.stylebooks.samples",
            "version": "1.0"
        },
        "parameters": {
            "locationfile": {
                "name": "servercert1.key",
                "contents": "<base64-contents>",
                "encoding_type": "base64"
            }
        },
        "targets": [
            {
                "instance_id": "d9dca475-abde-47ef-bf99-8434fe6ad886"
            }
        ]
    }
}
```

使用 API 导入自定义 StyleBook

您现在可以使用 StyleBook API 将自定义 StyleBook 导入到 NetScaler Console 中。您可以使用 REST API 在任何工具（例如 curl 命令行工具或 Postman Chrome 浏览器扩展程序）中按照以下方

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

式从该 StyleBook 创建配置包。例如，您可以导入名为 example-lb 的 StyleBook，该 StyleBook 可用于在 NetScaler 实例上创建负载均衡器配置。

```
HTTP Method: POST

URL: http://<mas-ip>/stylebook/nitro/v2/config/stylebooks/actions/import?
mode=sync

Headers:

Content-Type: application/json

Accept: application/json

RequestBody:

{

    "import": {

        "file_name": "example-lb.yaml",

        "source": "<base64-contents>",

        "encoding": "base64"

    }

}
```

其中，“source”属性的值是您的 StyleBook 文件内容的 base64 编码。您可以将 StyleBook 文件的 YAML 内容粘贴到在线工具中， 例如， `<https://www.browserling.com/tools/file-to-base64>` 以获取 base64 字符串，然后将其用作上述“source”属性的值。

使用此 API 调用，您还可以在一个 API 操作中上传包含多个 StyleBook 文件的压缩 tarball 文件（.tgz 文件）。为此，只需将 file_name 属性更改为 .tgz 文件名，并将 source 属性的值更改为 .tgz 文件内容的 base64 编码。

在工具中成功运行 API 后，您将收到以下响应，表明 StyleBook 已导入到 NetScaler Console 中。

```
200 OK
```

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

响应正文：

```
{

    "import": {

        "name": "example-lb",

        "namespace": "com.citrix.adc.stylebooks",

        "version": "2.0"

    }

}
```

使用 API 下载自定义 StyleBook

您可以通过提供以下 StyleBooks REST API 来下载自定义 StyleBook：

```
POST

http://<MAS_IP>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/
<VERSION>/<NAME>/actions/actions/download?dependencies=true



payload



dependencies=true
```

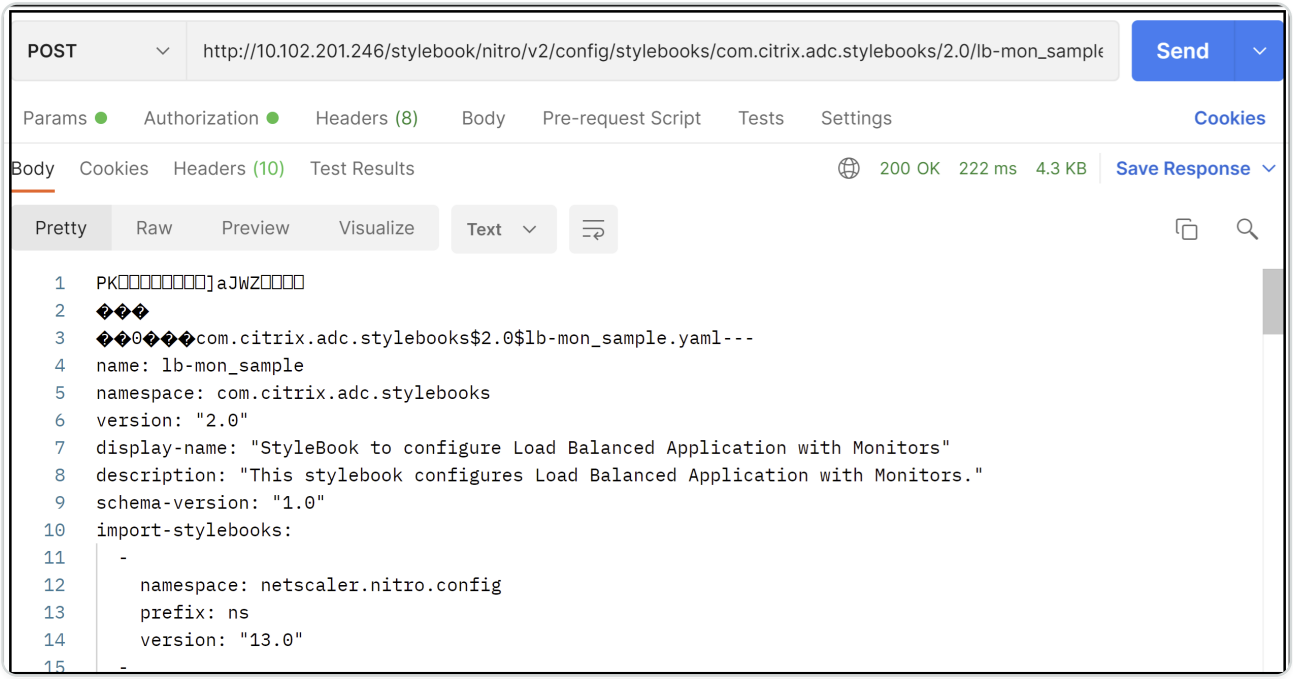
在修改 IP 地址、名称、版本和命名空间字段后，您可以在任何工具（例如 curl 命令行工具或 Postman Chrome 浏览器扩展程序）中运行此 API。

```
POST
```

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

```
http://10.102.201.246/stylebook/nitro/v2/config/stylebooks/
com.samples.adc.stylebooks/1.2/lb-mon/actions/download?dependencies=true



payload

dependencies=true
```

将下载 .yaml 格式的 StyleBook。



使用 API 删除自定义 StyleBook

您可以通过提供以下 StyleBooks REST API 来删除自定义 StyleBook：

```
DELETE



http://<MAS_IP>/stylebook/nitro/v2/config/stylebooks/<NAMESPACE>/
<VERSION>/<NAME>?dependencies=true
```

如果 URL 中未提供依赖项查询参数或其值设置为 false，则不会删除 StyleBook 依赖项（仅删除 StyleBook 本身）。

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

当您收到 HTTP 响应状态码 200 时，表示自定义 StyleBook 及其依赖项已成功从 NetScaler Console 中删除。

注意：

您不能删除在 MA Service 中有其他 StyleBook 依赖的自定义 StyleBook。

例如，假设您在 NetScaler Console 中创建了一个名为“lb-virtual-ssl-extended”的 StyleBook。您后来决定删除该 StyleBook。

在修改 IP 地址、名称、版本和命名空间字段后，您可以在任何工具中运行该 API，例如 curl 命令行工具或 Postman Chrome 浏览器扩展。

DELETE `<http://10.102.201.246/stylebook/nitro/v2/config/stylebooks/com.citrix.adc.stylebooks/2.0/lb-mon_delete?dependencies=false>`

StyleBook 将从 NetScaler Console 中删除。

StyleBooks 语法

您可以设计自己的 StyleBooks，将其导入 NetScaler Console，然后使用 NetScaler Console GUI 或 API 创建配置。要创建自己的 StyleBooks，您必须首先了解可使用的不同构造和属性的语法和句法。

本文档介绍了在创建 StyleBooks 时可以使用的不同构造和引用。

单击下表中的部分、构造或引用名称以查看详细信息。

标头	导入 StyleBooks
参数	参数默认源构造
替换	组件
可选属性	辅助组件
属性默认源	嵌套组件
条件构造	重复构造
重复条件构造	输出

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

嵌套重复	父引用
参数引用	替换引用
组件引用	操作
变量引用	警报
分析	内置函数
表达式	依赖项检测
就地插值	

注意

在定义 repeat-item、repeat-index 或替换函数的参数时，请勿使用以下保留字来命名用户定义的变量，$`<var-name>`

- 样式簿, 参数, 替换, 组件, 属性, 输出, 父级, 自身, 操作, 分析, 警报
- 重复项, 重复项-0, 重复项-1, 重复项-2
- 重复索引, 重复索引-0, 重复索引-1, 重复索引-2
- 默认值
- 角色, 角色, 目标, 目标
- 上下文, 父上下文, 父上下文

有关如何设计自己的 StyleBook 的信息和示例，请参阅如何创建自己的 StyleBook。

标头

StyleBook 的前六行构成标头部分。此部分允许您定义 StyleBook 的身份并描述其功能。这是必填部分。

下表描述了标头部分的属性：

属性	描述
名称	用于标识 StyleBook 的名称。此属性为必填项。

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

属性	描述
显示名称	StyleBook 的描述性名称。此名称显示在 NetScaler Console GUI 上。这是可选属性。
描述	描述文本定义了此 StyleBook 的功能。此描述显示在 NetScaler Console GUI 上。这是可选属性。**注意：**这是一个 HTML 片段，您可以使用 HTML 标签自定义标题或使用带有 URL 或嵌入图像的 `<img>` 标签插入图像。
作者	创建 StyleBook 的作者个人或组织。这是可选属性。
命名空间	命名空间是 StyleBook 唯一标识符的一部分，用于避免名称冲突。命名空间可以是任何字符串，但最佳实践是将其用于命名创建或拥有一组 StyleBook 的公司、部门或单位。例如，您可以使用以下格式：`<company>.<department>.<unit>.stylebooks`。这是必填属性。
版本	StyleBook 的版本号。更新 StyleBook 时可以更改版本号。不同版本的 StyleBook 可以共存。这是一个强制属性。
架构版本	StyleBooks 架构的版本。在当前版本的 NetScaler Console 中，其值为“1.0”。这是一个强制属性。
私有	如果此属性设置为 true，则 StyleBook 不会显示在 NetScaler Console GUI 上。这对于作为其他 StyleBook 构建块且不打算由用户直接使用的 StyleBook 来说是一个有用的设置。这是一个可选属性。其默认值为 false。

示例:

```
    name: lb
```

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

```
    description: "This stylebook defines a sample load balancing
configuration."

    display-name: "Load Balancing StyleBook (HTTP)"

    author: Mike Smith (ACME Infra team)

    namespace: com.example.stylebooks

    schema-version: "1.0"

    version: "0.1"
```

名称、命名空间和版本的组合在系统中唯一标识一个 StyleBook。在 NetScaler Console 中，不能有两个 StyleBook 具有相同的名称、命名空间和版本组合。但是，您可以有两个 StyleBook 具有相同的名称和版本但命名空间不同，或者具有相同的命名空间和版本但名称不同。

导入 StyleBooks

这是您的 StyleBook 的第二部分，允许您声明希望从当前 StyleBook 引用哪些其他 StyleBook。这使您能够导入并重用其他 StyleBooks，而不是在您自己的 StyleBook 中重新构建相同的配置。这是一个强制性部分。

您必须声明您希望在当前 StyleBook 中引用的 StyleBook 的**命名空间**和**版本**号。如果任何 StyleBook 直接使用 NITRO 配置对象，则必须引用 netscaler.nitro.config 命名空间。此命名空间包含所有 NetScaler NITRO 类型，例如 lbvserver 服务或监视器。支持 NetScaler 10.5 及更高版本的 StyleBooks，这意味着您可以使用您的 StyleBook 在运行 10.5 或更高版本的任何 NetScaler 实例上创建和运行配置。

import-stylebooks 部分中使用的**前缀**属性是引用命名空间和版本组合的简写。例如，“ns”前缀可用于引用版本为 10.5 的命名空间 netscaler.nitro.config。在 StyleBook 的后续部分中，您无需每次引用具有此命名空间和版本的 StyleBook 时都使用命名空间和版本，只需使用所选的前缀字符串以及 StyleBook 的名称即可唯一标识它。

示例：

```
     import-stylebooks:

      -
```

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

```
      namespace: netscaler.nitro.config

      version: "10.5"

      prefix: ns

    -

     namespace: com.acme.stylebooks

      version: "0.1"

      prefix: stlb
```

在上述示例中，定义的第一个前缀称为 ns，它引用命名空间 netscaler.nitro.config 和版本 10.5。定义的第二个前缀称为 stlb，它引用命名空间 com.acme.stylebooks 和版本 0.1。

定义前缀后，每当您想引用属于特定命名空间和版本的类型或 StyleBook 时，您可以使用符号 **\<namespace-shorthand\>::\<type-name\>**。例如，**ns::lbvserver** 引用在命名空间 netscaler.nitro.config 版本 10.5 中定义的类型 lbvserver。

同样，如果您想引用 com.acme.stylebooks 命名空间中版本为“0.1”的 StyleBook，您可以使用符号 **stlb::\<stylebook-name\>**。

注意

按照惯例，前缀“ns”用于引用 NetScaler 的 NITRO 命名空间。

参数

本节允许您定义在 StyleBook 中创建配置所需的所有参数。它描述了 StyleBook 接受的输入。尽管此部分是可选的，但大多数 StyleBook 可能都需要它。您可以将参数部分视为定义字段，供使用 StyleBook 在 NetScaler 实例上创建配置的用户使用。

当您将 StyleBook 导入 NetScaler Console 并使用它创建配置时，GUI 会使用 StyleBook 的此部分来显示一个表单。此表单接受定义的参数值的输入。

以下部分描述了您需要在此部分中为每个参数指定的属性：

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

'名称'

您要定义的参数的名称。您可以指定一个字母数字名称。

名称必须以字母开头，并且可以包含更多字母、数字、连字符 (-) 或下划线 (_)。

编写 StyleBook 时，您可以使用此“name”属性，通过 $parameters.\<name> 符号在其他部分引用该参数。

必填？是

'标签'

在 NetScaler Console GUI 中显示为此参数名称的字符串。

必填？否

'描述'

描述参数用途的帮助字符串。当用户单击此参数的帮助图标时，NetScaler Console GUI 会显示此文本。

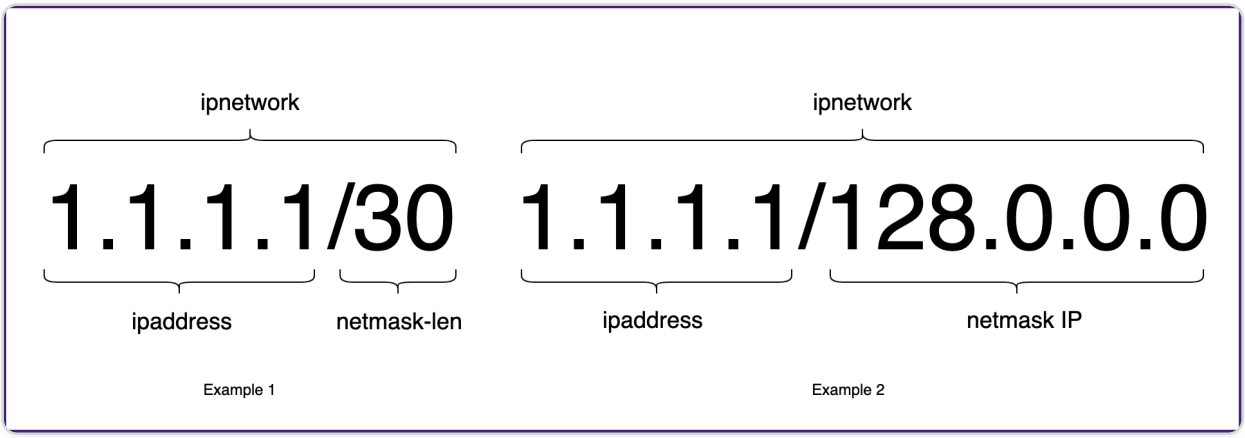
必填？否

'类型'

这些参数可以接受的值的类型。参数可以是以下任何 内置类型：

- string: 字符数组。如果未指定长度，则字符串值可以接受任意数量的字符。但是，您可以使用 min-length 和 max-length 属性来限制字符串类型的长度。
- `number`: 一个整数。您可以使用 min-value 和 max-value 属性来指定此类型可以接受的最小值和最大值。
- `boolean`: 可以是 true 或 false。YAML 将所有字面量视为布尔值（例如，Yes 或 No）。
- `ipaddress`: 表示有效 IPv4 或 IPv6 地址的字符串。
- `ipnetwork`: 它由两部分组成。第一部分是 IP 地址，第二部分是子网掩码。

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



子网掩码由子网掩码长度 (`netmask-len`) 或子网掩码 IP 地址 (`netmask_ip`) 组成。对于 IPv6 地址，子网掩码长度是 0-32 和 0-128 之间的整数。它用于确定网络中的 IP 地址数量。

从 NetScaler Console GUI 创建或更新配置包时，您可以执行以下操作之一：

- 启用子网掩码长度并输入 IP 地址和子网掩码长度
- 禁用子网掩码长度并输入 IP 地址和子网掩码 IP 地址

在 API 中，子网掩码长度和子网掩码 IP 地址作为单个值提供，如以下示例所示：

示例：

```
Content-Type: application/json

Accept: application/json

{

“configpack”:

{

      “stylebook”: {

      “namespace”: “com.example.stylebook”,

      “version”:“1.0”,

      “name”: “ipnetwork-example”,

      ..

      },
```

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

```
        “parameters”: {

           “name: “test-app”,

            “virtual-ip”: “212.100.30.0/255.255.255.0”,

        },

        “targets”:

        [

        ]

  }

  }
```

- `tcp-port`: 一个介于 0 到 65535 之间的数字，表示 TCP 或 UDP 端口。
- `password`：表示不透明/秘密字符串值。当 NetScaler Console GUI 显示此参数的值时，它会显示为星号 (*****).
- `certfile`：表示证书文件。使用 NetScaler Console GUI 创建 StyleBook 配置时，此值允许您直接从本地系统上传文件。上传的证书文件存储在 NetScaler Console 的 `/var/mps/tenants/\<tenant_path>/ns_ssl_certs` 目录中。

  证书文件将添加到 NetScaler Console 管理的证书列表中。
- `keyfile`：表示证书密钥文件。使用 NetScaler Console GUI 创建 StyleBook 配置时，此值允许您直接从本地系统上传文件。上传的证书文件存储在 NetScaler Console 的 `/var/mps/tenants/\<tenant_path>/ns_ssl_keys` 目录中。

  证书密钥文件将添加到 NetScaler Console 管理的证书密钥列表中。
- `file`：表示文件。
- `object`：当您想将多个相关参数分组到一个父元素下时，使用此类型。将父参数的类型指定为“object”。“object”类型的参数可以包含嵌套的“parameters”部分来描述其包含的参数。
- `another StyleBook`：当您使用此类型的参数时，此参数期望其值采用 StyleBook 中定义的参数形式，以表示其类型。

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

参数还可以具有 `type`，它是类型列表。为此，请在类型末尾添加 `[]`。例如，如果 `type` 属性是 `string[]`，则此参数接受字符串列表作为输入。从此 StyleBook 创建配置时，您可以为此参数提供一个、两个或多个字符串。

强制？是

'网络'

对于 `type: ipaddress`，您可以指定 `network` 属性，以从 NetScaler Console IPAM 网络自动分配 IP 地址。

当您创建 StyleBook 配置时，NetScaler Console 会从 `network` 属性自动分配 IP 地址。

示例：

```
name: virtual-ip

label: "Load Balancer IP Address"

type: ipaddress

network: "network-1"

required: true
```

在此示例中，`virtual-ip` 字段从 `network-1` 自动分配 IP 地址。当配置被删除时，IP 地址会释放回网络。

'动态分配'

在 `type:ipaddress` 的参数定义中添加了 `dynamic-allocation` 属性。使用此属性动态列出 NetScaler Console IPAM 网络。此属性可以接受 `true` 或 `false` 作为输入。对于 `type: ipaddress`，指定 `dynamic-allocation: true` 属性以动态列出 NetScaler Console 中的 NetScaler Console IPAM 网络。在配置包创建表单中，您可以执行以下操作：

1. 从列表中选择所需的 IPAM 网络。
2. 指定要从选定的 IPAM 网络分配的 IP 地址。

   如果未指定 IP 地址，NetScaler Console 会从选定的 IPAM 网络自动分配一个 IP 地址。

示例：

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

```
-

  name: virtual-ip

  label: "Load Balancer IP Address"

  type: ipaddress

  dynamic-allocation: true

  required: true
```

在此示例中，`virtual-ip` 字段列出了 NetScaler Console 中的 NetScaler Console IPAM 网络。从列表中选择一个网络以从该网络自动分配一个 IP 地址。当配置被删除时，IP 地址将释放回网络。

'键'

指定 true 或 false 以指示此参数是否为 StyleBook 的关键参数。

一个 StyleBook 只能有一个参数被定义为“key”参数。

当您从同一个 StyleBook（在相同或 不同的 NetScaler 实例上）创建不同的配置时，每个配置的此参数的值都不同/唯一。

默认值为 false。

强制？否

'必需'

指定 true 或 false 以指示参数是强制性的还是可选的。如果 设置为 true，则该参数是强制性的，用户在创建配置时必须为此参数提供一个 值。

NetScaler Console GUI 强制用户为此参数提供有效值。

默认值为 false。

强制？否

'允许值'

当类型设置为“string”时，使用此属性为参数定义有效值列表。

从 NetScaler Console GUI 创建配置时，系统会提示用户从此列表中选择参数值。

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

注意

如果要将列表值显示为单选选项，请设置 `layout` 属性。

示例 1：

```
-

      name: ipaddress

      type: string

      allowed-values:

            -  SOURCEIP

            -  DEST IP

            -  NONE
```

示例 2：

```
-

      name: TCP Port

      type: tcp-port

      allowed-values:

            -  80

            -  81

            -  8080
```

示例 3：

`tcp-ports` 列表，其中列表的每个元素只能具有 `allowed-values` 中指定的值。

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

```
-

      name: tcpports

      type: tcp-port[]

      allowed-values:

            -  80

            -  81

            -  8080

            -  8081
```

强制？否

'默认值'

使用此属性为可选参数分配默认值。当用户创建配置时未指定值，则使用默认值。

如果满足以下条件，则参数不带任何值：

- 参数没有默认值。
- 用户未提供参数值。

示例 1：

```
-

      name: timeout

      type: number

      default: 20
```

示例 2：

要列出参数的默认值：

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

```
-
      name: protocols
      type: string[]
      default:
            -  TCP
            -  UDP
            -  IP
```

示例 3：

```
-
      name: timeout
      type: number
      default: 20
```

示例 4：

```
-
      name: tcpport
      type: tcp-port
      default: 20
```

强制？否

'模式'

使用此属性定义一个模式（正则表达式），用于此 参数的有效值，当参数类型为“string”时。

示例：

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

```
-

      name: appname

      type: string

      pattern: "[a-z]+"
```

强制？否

'最小值'

使用此属性定义 `number` 或 `tcp-port` 类型参数的最小值。

示例：

```
-

      name: audio-port

      type: tcp-port

      min-value: 5000
```

数字的 `min-value` 可以是负数。但是，`tcp-port` 的 `min-value` 必须是正数。

强制性？否

'最大值'

使用此属性定义 `number` 或 `tcp-port` 类型参数的最大值。

确保最大值大于最小值（如果已定义）。

示例：

```
-

      name: audio-port

      type: tcp-port

      min-value: 5000
```

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

```
      max-value: 15000
```

强制性？否

'最小长度'

使用此属性定义参数可接受值的最小长度，该参数的 类型为“string”。

确保定义为值的字符的最小长度大于或等于零。

示例：

```
-

      name: appname

      type: string

      min-length: 3
```

强制性？否

'最大长度'

使用此属性定义参数可接受值的最大长度，该参数的 类型为“string”。

确保值的最大长度大于或等于 `min-length` 中定义的字符长度。

示例：

```
-

      name: appname

      type: string

      max-length: 64
```

必填？否

“最小项数”

使用此属性定义作为列表的参数中的最小项目数。

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

确保最小项目数大于或等于零。

示例：

```
-

      name: server-ips

      type: ipaddress[]

      min-items: 2
```

必填？否

“最大项数”

使用此属性定义参数中的最大项数，该参数是一个 列表。

如果已定义，请确保最大项目数大于最小项目数。

示例：

```
-

      name: server-ips

      type: ipaddress[]

      min-items: 2

      max-items: 250
```

必填？否

“GUI”

使用此属性自定义 NetScaler Console GUI 中参数的布局。

强制性？否

“列”

此属性是 `gui` 属性的子属性。使用此属性定义在 NetScaler Console GUI 中显示 `type: object[]` 参数的列数。

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

强制性？否

“可更新”

此属性是 `gui` 属性的子属性。使用此属性指定在创建配置后是否可以更新参数。仅在简单参数类型（例如字符串、布尔值或数字）上设置此属性。

如果值设置为 `false`，则在更新配置时，参数字段将灰显。

强制性？否

'collapse_pane'

此属性是 `gui` 属性的子属性。使用此属性指定定义此对象参数布局的窗格是否可折叠。

如果值设置为 true，用户可以展开或折叠此父参数下的子参数。

示例：

```
gui:


 collapse_pane: true


 columns: 2
```

完整参数部分的示例：

```


parameters:


   -


      name: name
```

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

```
      label: Name

      description: Name of the application

      type: string

      required: true

  -

      name: ip

      label: IP Address

      description: The virtual IP address used for this application

      type: ipaddress

      required: true

  -
```

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

```
      name: svc-servers

      label: Servers

      type: object\[\]

      required: true

      parameters:

        -

              name: svc-ip

              label: Server IP

              description: The IP address of the server

              type: ipaddress

              required: true
```

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

```
        -

            name: svc-port

            label: Server Port

            description: The TCP port of the server

            type: tcp-port

            default: 80

        -

            name: lb-alg

            label: LoadBalancing Algorithm

            type: string

            allowed-values:
```

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

```
                - ROUNDROBIN

                - LEASTCONNECTION

            default: ROUNDROBIN

        -

            name: enable-healthcheck

            label: Enable HealthCheck?

            type: boolean

            default: true
```

以下示例定义了列表的所有属性以及前面部分中解释的值：

```
        -
            name: features-list

            type: string[]
```

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

```
            min-length: 1

            max-length: 3

            min-items: 1

            max-items: 3

            pattern: "\[A-Z\]+"

            allowed-values:

              - SP

              - LB

              - CS

            default:
```

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

```
                - LB
```

“布局”

此属性是 `gui` 属性的子属性。使用此属性将列表值显示为单选按钮。在 StyleBook 定义的参数部分中，将 `layout` 属性设置为 `radio`。它适用于具有 `allowed-values` 属性的参数。创建配置包时，NetScaler Console GUI 会将 `allowed-values` 列表中的值显示为单选按钮。

示例：

```
-

    gui:

        layout: radio

    allowed-values:

        - One

        - Two

        - Three
```

值“One”、“Two”和“Three”在 NetScaler Console GUI 中显示为单选按钮。

'依赖参数'

此属性是 `gui` 属性的子属性。它根据在另一个参数中指定的值，动态控制 StyleBook 配置表单中参数的显示或其初始值。

在控制表单上参数行为的源参数上指定此属性。您可以包含控制其他参数的多个条件。例如，源参数 `protocol` 可以具有一个依赖参数 `certificate`，该参数仅在 `protocol` 参数值为 `SSL` 时显示。

每个条件可以具有以下属性：

- **target-parameter**：指定此条件适用的目标参数。
- **matching-values**：指定触发操作的源参数值列表。
- **action**：对目标参数指定以下操作之一：

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

  - `read-only`：该参数变为只读。
  - `show`：如果参数被隐藏，则它会显示在表单中。
  - `hide`：该参数从表单中移除。
  - `set-value`：参数值设置为 value 属性中指定的值。
- **value**：如果操作为 `set-value`，则为目标参数的值。

当用户输入与源参数上指定的值匹配时，目标参数的外观或值会根据指定的动作而改变。

示例：

```
-

  name: lb-virtual-port

  label: "Load Balanced App Virtual Port"

  description: "TCP port representing the Load Balanced application"

  type: tcp-port

  gui:

    updatable: false

    dependent-parameters:

          -

            matching-values:

              - 80

            target-parameter: $parameters.lb-service-type

            action: set-value

            allowed-values:

            - HTTP

            - TCP
```

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

```
            - UDP


    default: 80
```

在此示例中，依赖参数在 `lb-virtual-port` 参数（源参数）下指定。

当源参数值设置为 `80` 时， `lb-service-type` 参数会触发 `set-value` 动作。因此，用户可以选择以下选项之一：

- HTTP
- TCP
- UDP

参数-默认源构造

您可以使用此构造重用来自其他 StyleBook 的参数定义。

设想一个场景，其中一个参数或一组参数在多个 StyleBook 中重复使用。为了避免每次创建新 StyleBook 时都重新定义这些参数，您可以一次性定义它们，然后使用 **parameters-default-sources** 构造将其定义导入到需要这些参数的 StyleBook 中。

例如，如果您的许多 StyleBook 需要配置虚拟 IP，您可能需要在创建的每个新 StyleBook 中定义与虚拟 IP 相关的相同参数。相反，您可以创建一个单独的 StyleBook，例如名为“vip-params”，并在其中定义所有相关参数，如下例所示：

```
    -

    name: vip-params

    namespace: com.acme.commontypes

    version: "1.0"

    description: This StyleBook defines a typical virtual IP config.

    private: true

    schema-version: "1.0"
```

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

```
     parameters:

       -

           name: lb-appname

           label: Load Balanced Application Name

          description: Name of the Load Balanced application

           type: string

           required: true

       -

           name: lb-virtual-ip

           label: Load Balanced App Virtual IP address

           description: Virtual IP address representing the Load Balanced
application

           type: ipaddress

           required: true

       -

           name: lb-virtual-port

           label: Load Balanced App Virtual Port

           description: TCP port representing the Load Balanced
application

           type: tcp-port

           default: 80

       -

           name: lb-service-type
```

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

```
            label: Load Balanced App Protocol

            description: Protocol used for the Load Balanced application.

            type: string

            default: HTTP

            required: true

            allowed-values:

                 - HTTP

                 - SSL

                 - TCP
```

然后，您可以创建使用这些参数的其他 StyleBook。下面是此类 StyleBook 的一个示例。

```
     -

     name: acme-biz-app

     namespace: com.acme.stylebooks

     version: "1.0"

     description: This stylebook defines the NetScaler configuration for
Biz App

     schema-version: "1.0"

     import-stylebooks:

       -

          namespace: com.acme.commontypes

          prefix: cmtypes

          version: "1.0"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    parameters-default-sources:
          - cmtypes::vip-params
    parameters:
        -
          name: monitorname
          label: Monitor Name
          description: Name of the monitor
          type: string
          required: true
        -
          name: type
          label: Monitor Type
          description: Type of the monitor
          type: string
          required: true
          allowed-values:
            - PING
            - TCP
            - HTTP
            - HTTP-ECV
            - TCP-ECV
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            - HTTP-INLINE
```

在 StyleBook acme-biz-app 中，首先使用“import-stylebooks”部分导入 vip-params StyleBook 的命名空间和版本。然后添加 **parameters-default-sources** 构造，并指定 StyleBook 名称，即 vip-params。这与直接在此 StyleBook 中定义 vip-params StyleBook 的参数具有相同的效果。

您可以包含来自多个 StyleBook 的参数，因为 parameters-default-sources 是一个列表，并且列表中的每个项都应是一个 StyleBook。

除了包含来自其他 StyleBook 的参数外，您还可以使用 parameters 部分定义自己的参数。StyleBook 的完整参数列表是来自其他 StyleBook 的参数和在此 StyleBook 中定义的参数的组合。因此，表达式 **$parameters** 指的是这种参数组合。

请注意，如果参数在导入的 StyleBook 和当前 StyleBook 中都已定义，则当前 StyleBook 中的定义将覆盖从其他 StyleBook 导入的定义。如果需要，您可以通过自定义一些导入的参数来有效利用此功能，同时按原样使用其余导入的参数。

parameters-default-sources 构造也可以用于嵌套参数，如下所示：

```
parameters:

    -

      name: vip-details

      label: Virtual IP details

      description: Details of the Virtual IP

      type: object

      required: true

      parameters-default-sources:

              - cmtypes::vip-params
```

这类似于将 StyleBook vip-params 的参数直接添加为本 StyleBook 中 vip-details 参数的子参数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数源构造

使用 `parameters-source` 构造，您可以控制在创建配置包时导入的参数在 GUI 上如何显示。以下是一个示例 StyleBook，用于描述此构造：

```
parameters:

  -

    name: appname

    label: "LBVserver Name"

    description: "Name of the Load Balancer"

    type: string

    required: true

  -

   parameters-source: stlb::lb

  -

    name: vip-ipaddress

    label: "Load Balancer IP Address"

    description: "IP Address of the Load Balancer VIP"

    type: ipaddress

    required: true
```

在此示例中，`parameters-source` 构造被添加到 `parameters` 部分。`parameters-source` 包含一个值，该值等同于 `parameters-default-sources` 部分中的列表项。借助 `parameters-source`，您可以将不同 StyleBook 中的参数导入到所需位置并在 GUI 上呈现它们。而 `parameters-default-sources` 部分导入属性，并且只在 GUI 的开头呈现。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数条件

参数条件用于修改 StyleBook 定义中某些参数的行为。StyleBook 定义中的参数是用于创建配置包的输入。使用 `parameters-conditions` 在定义中定义参数条件。

参数在 StyleBook 定义中可以有许多约束。当用户更改参数行为时，参数条件用于解决冲突。例如，当用户选择 SSL 协议时，需要证书详细信息才能创建配置包。但是，证书详细信息最初可能未设置为必填字段。

参数条件具有以下属性：

- `target`：指定要对其应用操作的目标参数。您可以指定多个目标参数。
- `action`：指定要对目标参数执行的操作。参数条件支持以下操作：
  - 扩充允许值
  - 显示或隐藏参数
  - 设置默认值
  - 设置为必填字段
  - 设置允许值
  - 设置参数标签
  - 设置参数描述
  - 折叠或展开参数窗格
  - 设置参数模式
- `condition`：可选，指定一个条件以对指定的目标参数应用操作。如果不指定条件，则操作将直接应用于目标参数。
- `value`：根据操作设置目标参数属性的值。

注意：

目前，参数条件无法应用于列表对象中的参数。

'增加允许值'

当操作为 `augment-allowed-values` 时，目标参数在 GUI 中显示为下拉菜单。下拉菜单的值由 StyleBook 定义的 `value` 属性中定义的值设置。

示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
parameters-conditions:

  -

   target: $parameters.rewritepolicy.action

   action: augment-allowed-values

   value:  $parameters.rewriteaction
```

'显示' 或 '隐藏'

当操作为 `show` 且指定条件返回 `True` 时，目标参数将显示在 GUI 上。

当操作为 `hide` 且指定条件返回 `True` 时，目标参数将从 GUI 上消失。

示例：

```
parameters-conditions:

  -

   target: $parameters.security-settings.cert-details

   action: show

   condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

最初，证书详细信息对 `security-settings` 参数是隐藏的。当用户选择 SSL 或 SSL-Bridge 协议时，证书详细信息将显示。

'设置默认值'

当操作为 `set-default` 且指定条件返回 `True` 时，目标参数的值将设置为默认值。

示例 1：

```
parameters-conditions:

  -

   target: $parameters.port
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    action: set-default

    condition: $parameters.protocol == "SSL"

    value: 443

   -

    target: $parameters.port

    action: set-default

    condition: $parameters.protocol != "SSL"

    value: 80
```

示例 2:

```
parameters-conditions:

  -

    target: $parameters.port

    action: set-default

    value: if-then-else($parameters.protocol == "SSL", 443, 80)
```

当用户选择 **SSL** 协议时，默认端口值设置为 `443`。对于其他协议，默认端口值设置为 `80`。示例 1 和 2 会得到相同的结果。

'设置必需'

当操作为 `set-required` 并且指定条件返回 `True` 时，目标参数成为创建配置包的必填字段。

```
parameters-conditions:

  -

    target: $parameters.security-settings.cert-details
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    action: set-required

    condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

最初，`security-settings` 参数可能不需要证书详细信息。当用户选择 **SSL** 或 **SSL-Bridge** 协议时，证书详细信息成为创建配置包的必填字段。

'设置允许值'

当操作为 `set-allowed-values` 并且指定条件返回 `True` 时，目标参数允许您仅选择指定值。

示例:

```
parameters-conditions:

  -

    target: $parameters.app-name

    action: set-allowed-values

    value:

     - "SSL"

    condition: $parameters.lb-virtual-port ==  443
```

当用户将 `443` 指定为负载均衡器虚拟端口时，应用程序名称仅允许 **SSL** 选项。

'设置标签'

当操作为 `set-label` 并且指定条件返回 `True` 时，目标参数的标签将更改为指定的文本。

示例:

```
parameters-conditions:

  -

    target: $parameters.app-name

    action: set-label
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   value: if-then-else($parameters.lb-service-type == "TCP",
"TCPApp","UDPApp")
```

当用户选择负载均衡器协议为 **TCP** 时，应用程序的标签将更改为 **TCPApp**。如果用户选择不同的选项，应用程序的标签将更改为 **UDPApp**。

'设置描述'

当操作为 `set-description` 并且指定条件返回 `True` 时，目标参数的描述将更改为指定的文本。此描述将显示在目标参数的工具提示中。

示例:

```
parameters-conditions:

  -

   target: $parameters.app-name

   action: set-description

   value: if-then-else($parameters.lb-service-type == "TCP", "Select a TCP
application name","Select a UDP application name")
```

当用户选择负载均衡器协议为 **TCP** 时，应用程序的工具提示会显示文本：`Select a TCP application name`。如果用户选择其他选项，应用程序的描述会显示 `Select a UDP application name`。

'折叠窗格' 或 '展开窗格'

当操作为 `collapse-pane` 且指定条件返回 `True` 时，目标参数的窗格会在 GUI 中折叠。

当操作为 `expand-pane` 且指定条件返回 `True` 时，目标参数的窗格会在 GUI 中展开。

示例:

```
parameters-conditions:

  -

    target: $parameters.security-settings.cert-details
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    action: expand-pane

    condition: $parameters.protocol in ["SSL", "SSL-BRIDGE"]
```

最初，`security-settings` 参数的证书详细信息窗格可能未展开。当用户选择 **SSL** 或 **SSL-Bridge** 协议时，证书详细信息窗格会在 GUI 上展开。

'设置模式'

当操作为 `set-pattern` 且指定条件返回 `True` 时，目标参数字段会设置为指定的模式。

示例:

```
parameters-conditions:

  -

    target: $parameters.app-name

    action: set-pattern

    value: "[a-z]+"
```

在此示例中，应用程序名称只允许小写字母字符。

嵌套参数条件

在 StyleBook 定义中，您可以在参数条件中指定另一个参数条件。这些条件称为嵌套参数条件，并使用重复构造来定义这些条件。当您希望从另一个参数为某个参数应用操作时，嵌套参数条件会很有用。

示例:

```
parameters-conditions:

  -

    repeat: $parameters.lbvservers

    repeat-item: lbvserver

    parameters-conditions:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    -

      target: $lbvserver.port

      action: set-allowed-values

      condition: $lbvserver.protocol == "HTTPS"

      value: $parameters.ssl-ports
```

在此示例中，当用户为负载均衡虚拟服务器选择 HTTPS 协议时，端口值会动态填充。并且，它适用于列表中的每个负载均衡虚拟服务器。

替换

替换用于定义简写名称，这些名称可以替换 StyleBook 中的复杂表达式，从而使 StyleBook 更具可读性。

当 StyleBook 中重复使用相同的表达式或值（例如常量值）时，替换也很有用。为参数使用替换名称允许您只更新替换值，而不是更新 StyleBook 中参数的所有出现位置，这可能会导致错误。

替换也用于定义值之间的映射。

列表中的每个替换都由一个键和一个值组成。该值可以是一个简单值、一个表达式、一个函数或一个映射。

在以下示例中，定义了两个替换。第一个是 `http-port`，可以用作 8181 的简写。通过使用替换，您可以在 StyleBook 的其余部分中将其引用为 **$substitutions.http-port**，而不是 8181。

替换:

`http-port: 8181`

您可以为端口号指定一个助记名称，并在 StyleBook 中的一个位置定义此端口号，无论它被使用了多少次。如果您想将端口号修改为 8080，您可以在替换部分修改它，并且更改将在使用助记名称 `http-port` 的任何地方生效。

以下示例展示了如何在组件中使用替换。

```
 components:

  -
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: my-lbvserver-comp

    type: ns::lbvserver

    properties:

        name: $parameters.name + "-lb"

        servicetype: HTTP

        ipv46: $parameters.ip

        port: **$substitutions.http-port**

        lbmethod: $parameters.lb-alg
```

替换也可以是一个复杂表达式。以下示例展示了两个替换如何使用表达式。

```
substitutions:

  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS

  app-name: str("acme-") + $parameters.name + str("-app")
```

替换表达式也可以使用现有的替换表达式，如以下示例所示。

```
substitutions:

  http-port: 8181

  app-name: str("acme-") + $parameters.name + str($substitutions.http-
port) + str("-app")
```

替换的另一个有用功能是映射，您可以在其中将键映射到值。以下是映射替换的一个示例。

```
substitutions:

    secure-port:

        true: int("443")
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        false: int("80")

    secure-protocol:

        true: SSL

        false: HTTP
```

以下示例展示了如何使用 secure-port 和 secure-protocol 映射。

```
components:

 -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

          name: $parameters.name + "-lb"

          servicetype: $substitutions.secure-protocol[$parameters.is-
secure]

          ipv46: $parameters.ip

          port: $substitutions.secure-port[$parameters.is-secure]

          lbmethod: $parameters.lb-alg
```

这意味着，如果 StyleBook 用户为参数 is-secure 指定布尔值“true”，或在 NetScaler Console GUI 中选择与此参数对应的复选框，则此组件的 `servicetype` 属性被赋值为 **SSL**，并且 `port` 属性被赋值为 **443**。但是，如果用户为此参数指定“false”或清除 NetScaler Console GUI 中对应的复选框，则 `servicetype` 被赋值为 **HTTP**，并且端口被赋值为 **80**。

以下示例展示了如何将替换用作函数。替换函数可以接受一个或多个参数。参数可以是简单类型，例如字符串、数字、IP 地址、布尔值和其他类型。

替换：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

生成负载均衡器名称(名称): $name + "-lb"

在此示例中，定义了一个名为“form-lb-name”的替换函数，它接受一个名为“name”的字符串参数****，并使用该参数创建一个字符串，将“-lb”后缀添加到 name 参数中的字符串。使用此替换函数的表达式如下所示：

`$substitutions.form-lb-name("my")`

它返回 `my-lb`。

考虑另一个示例：

替换：

```
内容交换策略优先级(优先级): 10100 - 100 &ast; $priority
```

替换 `cspol-priority` 是一个函数，它接受一个名为“priority”的参数并使用它来计算值。在 StyleBook 的其余部分中，此替换显示为：

```
components:

  -

    name: cspolicy-binding-comp

    type: ns::csvserver_cspolicy_binding

    condition: not $parameters.is-default

    properties:

         name: $parameters.csvserver-name

         policyname: $components.cspolicy-comp.properties.policyname

         priority: $substitutions.cspol-
priority($parameters.pool.priority)
```

替换也可以由键和值组成。该值可以是简单值、表达式、函数、映射、列表或字典。

以下是名为 `slist` 的替换示例，其值为列表：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
substitutions:

  slist:

    - a

    - b

    - c
```

替换的值也可以是键值对的字典，如下面名为 `sdict` 的替换示例所示：

```
substitutions:

  sdict:

    a: 1

    b: 2

    c: 3
```

您可以通过组合列表和字典来创建更复杂的属性。例如，名为 `slistofdict` 的替换返回键值对列表。

```
  slistofdict:

    -

      a: $parameters.cs1.lb1.port

      b: $parameters.cs1.lb2.port

    -

      a: $parameters.cs2.lb1.port

      b: $parameters.cs2.lb2.port
```

但是，在以下示例中，替换 `sdictoflist` 返回一个键值对，其中值本身是另一个列表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
sdictoflist:
  a:
    - 1
    - 2
  b:
    - 3
    - 4
```

在组件中，这些替换可以在 condition、properties、repeat 和 repeat-condition 构造中使用。

以下组件示例展示了如何使用替换来指定属性：

```
  properties:
    a: $substitutions.slist
    b: $substitutions.sdict
    c: $substitutions.slistofdict
    d: $substitutions.sdictoflist
```

定义一个值为列表或字典的替换的用例是，当您配置内容交换虚拟服务器和多个负载均衡虚拟服务器时。由于所有绑定到相同内容交换虚拟服务器的负载均衡虚拟服务器可能具有相同的配置，因此请使用替换列表和字典来构建配置，以避免为每个负载均衡虚拟服务器重复相同的配置。

以下示例展示了 `cs-lb-mon` StyleBooks 中的替换和组件，用于创建内容交换虚拟服务器配置。在构建 `cs-lb-mon` StyleBooks 的属性时，复杂的替换“lb-properties”指定了与内容交换虚拟服务器关联的负载均衡虚拟服务器的属性。“lb-properties”替换是一个函数，它将名称、服务类型、虚拟 IP 地址、端口和服务器作为参数，并生成一个键值对作为其值。在 `cs-pools` 组件中，您可以将此替换的值分配给每个池的 `lb-pool` 参数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
substitutions:

  cs-port[]:

    true: int("80")

    false: int("443")

  lb-properties(name, servicetype, vip, port, servers):

    lb-appname: $name

    lb-service-type: $servicetype

    lb-virtual-ip: $vip

    lb-virtual-port: $port

    svc-servers: $servers

    svc-service-type: $servicetype

    monitors:

      -

        monitorname: $name

        type: PING

        interval: $parameters.monitor-interval

        interval_units: SEC

        retries: 3

components:

  -

    name: cs-pools

    type: stlb::cs-lb-mon
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    description: | Updates the cs-lb-mon configuration with the different
pools provided. Each pool with rule result in a dummy LB vserver, cs
action, cs policy, and csvserver_cspolicy_binding configuration.

    condition: $parameters.server-pools

    repeat: $parameters.server-pools

    repeat-item: pool

    repeat-condition: $pool.rule

    repeat-index: ndx

    properties:

      appname: $parameters.appname + "-cs"

      cs-virtual-ip: $parameters.vip

      cs-virtual-port: $substitutions.cs-port($parameters.protocol ==
"HTTP")

      cs-service-type: $parameters.protocol

      pools:

        -

          lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP",
"0.0.0.0", 0, $pool.servers)

          rule: $pool.rule

          priority: $ndx + 1
```

替换映射

您可以创建将键映射到值的替换。例如，考虑一个场景，您希望为每个协议（键）定义要使用的默认端口（值）。为此，请按如下方式编写替换映射。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
substitutions:

     port:

          HTTP: 80

          DNS: 53

          SSL: 443
```

在此示例中，HTTP 映射到 80，DNS 映射到 53，SSL 映射到 443。要检索作为参数给定的特定协议的端口，请使用表达式

$substitutions.port\[$parameters.protocol\]

该表达式根据用户指定的协议返回值。

- 如果键是 HTTP，表达式返回 80
- 如果键是 DNS，表达式返回 53
- 如果键是 SSL，表达式返回 443
- 如果映射中不存在该键，表达式不返回任何值

遍历替换列表

在以下示例中，StyleBook 遍历名为 `apps` 的替换列表，以创建一组 `lbvserver` 组件及其相应的服务组和绑定服务器。

```
substitutions:

  apps:

    -

      name: lb1

      vip: 1.2.3.4

      vport: 80

      protocol: HTTP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      servers:
        -
          ip: 10.8.11.11
          port: 8080
        -
          ip: 10.8.11.12
          port: 8080
    -
      name: lb2
      vip: 1.2.3.5
      vport: 81
      protocol: HTTP
      servers:
        -
          ip: 10.9.11.28
          port: 8080
        -
          ip: 10.9.11.29
          port: 8181
components:
  -
    name: lbvserver-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::lbvserver
    repeat: $substitutions.apps
    repeat-item: app
    properties:
      name: $app["name"]
      ipv46: $app["vip"]
      port: $app["vport"]
      servicetype: $app["protocol"]
    components:
      -
        name: servicegroup-comp
        type: ns::servicegroup
        properties:
          servicegroupname: $parent.properties.name + "-svg"
          servicetype: HTTP
        components:
          -
            name: servers-comp
            type: ns::server
            repeat: $app["servers"]
            repeat-item: server
            properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
              name: $server["ip"]

              ipaddress: $server["ip"]

            components:

              -

                name: servicegroup-servicegroupmember-binding-comp

                type: ns::servicegroup_servicegroupmember_binding

                properties:

                  servicegroupname:
$parent.parent.properties.servicegroupname

                  servername: $parent.properties.name

                  port: $server["port"]
```

组件

StyleBook 中的 Components 构造被认为是 StyleBook 中最重要的部分。在此部分中，您定义要创建的配置对象。使用此构造，您可以构建一个或多个相同类型的配置对象。

components 构造可以使用参数部分中提供的输入来调整 StyleBook 生成的配置。这是一个可选部分，尽管大多数 StyleBook 都有 components 部分。

下表描述了组件的主要属性。

属性	描述
名称	组件的名称。您可以指定一个字母数字名称。名称必须以字母开头，并且可以包含其他字母、数字、连字符 (-) 或下划线 (_)。
描述	此组件在 StyleBook 中的作用描述。
类型	类型决定了此组件提供哪些属性。组件有两种类型：**内置类型**：此类型由系统提供，您无需定义它，例如 NITRO 实体类

© 1997–2026 Citrix Systems, Inc. All rights reserved.

属性	描述
	型“lbvserver”或“servicegroup”。当组件具有内置类型属性时，它会在 NetScaler 上创建该类型的配置对象。例如，如果组件引用内置类型“lbvserver”，则此组件会在作为配置目标的 NetScaler 实例上创建负载平衡虚拟服务器。**复合类型**：此类型引用您已创建并导入到 NetScaler Console 中的现有 StyleBook。当组件具有复合类型属性时，它会在作为配置目标的 NetScaler 实例上创建引用 StyleBook 中指定的所有配置对象。这使您能够组合多个 StyleBook，其中每个 StyleBook 创建最终配置的一部分。有关复合 StyleBook 的更多信息，请参阅 创建复合 StyleBook。
属性	可用于组件类型属性的子属性。组件的有效属性由其类型决定。对于内置类型，这些是相应 Nitro 对象的属性。对于类型为另一个 StyleBook（即复合类型）的组件，这些属性对应于该 StyleBook 中定义的参数。

示例：

```
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
        name: $parameters.name
        servicetype: HTTP
        ipv46: $parameters.ip
        port: 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        lbmethod: $parameters.lb-alg
```

在此示例中，您定义了一个名为 my-lbvserver-comp 的组件。此组件的类型为 ns::lbvserver（一种内置类型），其中“ns”是引用您在 import-stylebooks 部分中指定的命名空间 netscaler.nitro.config 和版本 10.5 的前缀，而“lbvserver”是此命名空间中的一个 NITRO 资源。

本节中的属性包括“lbvserver”资源的四个强制属性和一个可选属性 (lbmethod)，并允许您为这些属性指定值。在此示例中，您为 servicetype 和 port 指定了静态值，而 name、ipv46 和 lbmethod 属性的值则来自输入参数。您可以使用 $parameters.\<name\> 符号引用 parameters 部分中定义的参数名称，例如 $parameters.ip。

注意

您必须对 NITRO 资源类型（其组件属性）的属性名称使用小写。否则，StyleBook 的导入将失败。

辅助组件

StyleBook 中组件部分的主要用途是通过 Nitro 内置类型或创建实际配置对象的另一个 StyleBook 来生成配置对象。辅助组件本身不构建配置对象。辅助组件从其他部分（如参数对象、其他组件的属性或其他组件的输出）获取输入，并将其转换为其他形式。这可以稍后由其他组件用于生成实际的配置对象。辅助组件可以是两种类型：对象类型或不包含组件部分的另一个 StyleBook。

以下示例显示了 StyleBook 的一个片段，该片段用于在 NetScaler 实例上创建带监视器 (lb-mon-comp) 的负载均衡服务器。

```
parameters:
  -
    name: appname
    type: string
  -
    name: ips
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ipaddress[]
  -
    name: vip
    type: ipaddress


components:
  -
    name: help-comp
    type: cmtypes::server-ip-port-params
    repeat:
      repeat-list: $parameters.ips
      repeat-item: server-ip
    properties:
      ip: $server-ip
      port: 80
 -
    name: lb-mon-comp
    type: stlb::lb-mon
    properties:
      lb-appname: $parameters.appname
      lb-virtual-ip: $parameters.vip
      lb-virtual-port: 80
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    lb-service-type: HTTP

    svc-service-type: HTTP

    svc-servers: $components.help-comp.properties
```

参数部分允许您输入应用程序名称和负载均衡服务器的 IP 地址。在 lb-mon-comp 组件部分中，lb-mon StyleBook 的 svc-servers 参数需要一个对象列表，其中每个项都有两个子参数：ip 和 port。

但是，此 StyleBook 的参数部分仅通过 $parameters.ips 接受服务器 IP。StyleBook 假定所有服务器都在端口 80 上运行。要使用 lb-mon StyleBook 创建负载均衡配置，您必须将 $parameters.ips 转换为对象列表。这可以通过使用上述示例中的辅助组件 help-comp 来实现。help-comp 组件的类型是 server-ip-port-params StyleBook。此 StyleBook 没有组件。因此，它不创建任何配置对象。help-comp 在 $parameters.ips 上创建一个重复列表，并为 $parameters.ips 的每个项构造一个包含 ip 和 port（设置为静态 80）的对象。因此，help-comp 将 IP 地址列表转换为对象列表，该列表稍后可在 lb-mon-comp 中用于分配 svc-servers 属性。help-comp 的结果被分配给 lb-mon-comp 的 svc-servers 属性。

可选属性

在某些情况下，组件的属性从表达式获取其值，该表达式可以是简单的表达式（例如参数引用），也可以是更复杂的表达式。在组件中设置此属性值是可选的。您可以选择仅当表达式返回实际值时才设置属性值，否则可以选择不设置此属性。

例如，假设您要设置的属性之一是类型为 ns::lbvserver 的组件的 lbmethod（负载平衡算法）。属性 lbmethod 的值取自用户提供的参数值，如下所示：

```
components

  -

    name: lbvserver_comp

    type: ns::lbvserver

    properties:

      name: $parameters.lb-appname + "-lb"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        servicetype: $parameters.lb-service-type

        ipv46: $parameters.lb-virtual-ip

        port: 80

        lbmethod: $parameters.lb-advanced.algorithm
```

现在，假设参数 **lb-advanced.algorithm** 是一个可选参数。而且，如果用户没有为该参数提供值（因为它可选），则表达式 **$parameters.lb-advanced.algorithm** 将评估为空值。因此，将为 lbmethod 属性传递一个无效值。为了避免这种情况，您可以通过在其名称后附加“?”来将属性标记为可选，如下所示：

```
components

   -

     name: lbvserver_comp

     type: ns::lbvserver

     properties:

       name: $parameters.lb-appname + "-lb"

       servicetype: $parameters.lb-service-type

       ipv46: $parameters.lb-virtual-ip

       port: 80

       lbmethod?: $parameters.lb-advanced.algorithm
```

如果右侧的表达式评估为空，则使用“?”会省略该属性，在这种情况下，这等同于按如下方式定义的组件：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components
  -
    name: lbvserver_comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb-appname + "-lb"
      servicetype: $parameters.lb-service-type
      ipv46: $parameters.lb-virtual-ip
      port: 80
```

由于 **lbmethod** 是可选的，省略它仍然会使此组件有效。请注意，如果 lbmethod 的类型“ns::lbvserver”中定义了默认值，则 lbmethod 可能会采用其默认值。

属性默认源 构造体

properties-default-sources 构造类似于 parameters-default-sources 构造。parameters-default-sources 构造允许在 StyleBook 中重用现有参数（来自其他 StyleBook），而 properties-default-sources 构造允许用户根据现有源指定组件的属性。

组件的属性可能分布在 StyleBook 的各个部分。例如，这些属性可能来自对象参数、返回对象的替换项、其他组件的属性或来自其他组件的输出。在这种情况下，您需要在组件的定义中重新定义 StyleBook 其他部分中出现的属性。显然，这是冗余的，并且可能导致错误。为了解决这个问题，可以使用 properties-default-sources 构造。properties-default-sources 构造是一个列表，其中每个项都标识了组件某些属性的源。

例如，考虑一个创建 lbvserver 配置的组件。此组件应按如下方式定义 lbvserver 的属性。

```
parameters:
  -
    name: lb
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb.name
      ipv46: $parameters.lb.ipv46
      port: $parameters.lb.port
      servicetype: $parameters.lb.servicetype
      lbmethod: $parameters.lb.lbmethod
```

在上面的示例中，请注意组件部分中定义的所有属性的值都取自 $parameters.lb 对象。尽管它们来自单个源，但这些属性在 StyleBook 中再次定义。此外，如果添加了与 lbvserver 配置相关的新子参数到 $parameters.lb 对象，则需要更新 lb-comp 组件以添加与新子参数对应的新属性。

为了避免重新定义属性并在不明确列出它们的情况下获取组件的所有相关属性，可以使用 properties-default-sources 构造。上面的示例可以按如下方式编写。

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::lbvserver

    properties-default-sources:

      - $parameters.lb
```

在上面的示例中，使用 properties-default-sources 构造可以减小组件定义的大小，从而允许您简洁地定义组件。此外，每当组件属性的源发生更改时，更改都会自动反映。例如，当 $parameters.lb 对象中添加了一个新属性（例如“persistencetype”）时，此属性会默认添加到 lb-comp 的配置中，因为 persistencetype 是 lbvserver 的一个属性。因此，properties-default-sources 构造提供了一个动态接口来定义组件，而无需担心组件属性源发生的变化。

组件属性的计算

本节讨论如果在组件中使用 properties-default-sources 构造，如何获取属性。首先，StyleBooks 编译器根据组件的类型（在上述示例中为 lbvserver）识别组件的属性列表。接下来，编译器按照它们定义的顺序（在组件的 properties-default-sources 部分中）从多个源获取这些属性。如果一个属性存在于多个源中，则最后一个源中出现的属性优先于其他源。最后，通过使用 properties-default-sources 构造获取的属性可以在组件的 properties 部分中被覆盖。重要的是要注意，组件部分的定义应至少包含 properties-default-sources 部分或 properties 部分。它可以同时包含两者。

嵌套组件

将一个组件嵌套在另一个组件中，允许嵌套组件通过引用父组件创建的配置对象或上下文来创建其配置对象。嵌套组件可以为父组件中创建的每个对象创建一个或多个对象。将一个组件嵌套在另一个组件中并不表示所创建的配置对象之间存在任何关系。嵌套是一种方便组件在父组件的现有上下文中构建配置对象的方式。

示例：

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

   properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      name: $parameters.name + "-lb"

      servicetype: HTTP

      ipv46: $parameters.ip

      port: 80

      lbmethod: $parameters.lb-alg

      components:

        -

         name: my-svcg-comp

         type: ns::servicegroup

         properties:

            name: $parameters.name + "-svcgrp"

            servicetype: HTTP

         components:

            -

              name: lbvserver-svg-binding-comp

              type: ns::lbvserver_servicegroup_binding

              properties:

                name: $parent.parent.properties.name

                servicegroupname: $parent.properties.name

                  -

                    name: members-svcg-comp

                    type: ns::servicegroup_servicegroupmember_binding
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    repeat:
                      repeat-list: $parameters.svc-servers
                      repeat-item: srv
                    properties:
                      ip: $srv
                      port: str($parameters.svc-port)
                      servicegroupname: $parent.properties.name
```

在此示例中，使用了多级嵌套。组件 my-lbvserver-comp 包含一个名为 my-svcg-comp 的子组件。并且，my-svcg-comp 组件内部包含两个子组件。my-svcg-comp 组件用于通过为内置 NITRO 资源类型“servicegroup”的属性提供值，在 NetScaler 实例上创建服务组配置对象。my-svcg 组件的第一个子组件 lbvserver-svg-binding-comp 用于将其父组件创建的服务组绑定到父组件的父组件创建的负载均衡虚拟服务器 (lbvserver)。$parent 符号（也称为父引用）用于引用父组件中的实体。第二个子组件 members-svcg-comp 用于将服务列表绑定到父组件创建的服务组。通过使用 StyleBook 的重复构造来迭代为参数 svc-servers 指定的服务列表，从而实现绑定。有关重复构造的信息，请参阅重复构造。

您也可以在不使用组件嵌套的情况下创建相同的配置对象。有关更多信息和示例，请参阅 使用 StyleBook 创建基本负载均衡配置。

条件构造

您可以使用条件构造使组件具有条件性。条件构造的值是一个布尔表达式，其计算结果为 true 或 false。如果条件为 true，则使用该组件构建其配置对象。如果条件为 false，则跳过该组件，并且不会通过它创建任何配置对象。布尔表达式通常基于参数值。

示例：

```
components:
      -
        name: servicegroup-comp
        type: ns::servicegroup
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        condition: $parameters.svc-server-ips

        properties:

              name: $parameters.name + "-svcgrp"

              servicetype: HTTP
```

在此示例中，如果用户为可选参数 svc-server-ips 指定了一个值，则 StyleBook 引擎会处理组件 servicegroup-comp。如果条件为 false，即如果用户未为此参数提供值，则会为此参数分配一个空值并计算结果为 false，那么 StyleBook 引擎将忽略此组件的存在，并且不会创建任何服务组。

请注意，布尔表达式可以基于 StyleBooks 中支持的任何有效表达式（例如，是否存在另一个组件，或者参数是否具有特定值）。

如果条件评估为 true，以下示例将构建 NITRO 类型 ns::systemfile 的配置对象。

示例：

```
     components

          -

            name: pem_key_files

            type: ns::systemfile

            condition: "$components.der-certificate-files-comp or
$components.pem-certificate-files-comp"

            properties:

                  filecontent: $certificate.keyfile.contents

                  fileencoding: "BASE64"

                  filelocation: "/nsconfig/ssl"

                  filename: $certificate.keyfile.filename
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在此示例中，条件是一个复杂的“OR”表达式，您希望仅当 StyleBook 中的另外两个组件已处理（未跳过）时，才由 StyleBook 创建此配置对象，从而在组件之间创建依赖关系。

重复构造

您可以使用组件的 **repeat** 构造来构建多个相同类型的配置对象。

在以下示例中，**members-svcg-comp** 组件用于将服务列表绑定到由父组件创建的服务组。为了创建将每个服务器绑定到服务组的配置对象，请使用 **repeat** 构造来迭代为参数 **svc-servers** 指定的服务列表。在迭代期间，组件会为服务组中的每个服务（在 **repeat-item** 构造中称为 **srv**）创建一个类型为 **servicegroup_servicegroupmember_binding** 的 NITRO 对象，并将每个 NITRO 对象中的 **ip** 属性设置为相应服务的 IP 地址。

示例：

```
components:

  -

      name: my-lbvserver-comp

      type: ns::lbvserver

      properties:

           name: $parameters.name + "-lb"

           servicetype: HTTP

           ipv46: $parameters.ip

           port: 80

           lbmethod: $parameters.lb-alg

          components:

               -

                  name: my-svcg-comp

                  type: ns::servicegroup
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    properties:
                         name: $parameters.name + "-svcgrp"
                         servicetype: HTTP
                   components:
                          -
                          name: lbvserver-svg-binding-comp
                          type: ns::lbvserver\servicegroup\binding
                          properties:
                                name: $parent.parent.properties.name
                                servicegroupname: $parent.properties.name
                          -
                          name: members-svcg-comp
                          type: ns::servicegroup\servicegroupmember\binding
                          repeat:
                            repeat-list: $parameters.svc-servers
                            repeat-item: srv
                          properties:
                                 ip: $srv
                                 port: $parameters.svc-port
                                 servicegroupname: $parent.properties.name
```

repeat 本身是一个对象，而 **repeat-list** 和 **repeat-item** 是 repeat 对象的属性。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- repeat-list 是一个强制属性，用于标识组件迭代的列表。
- repeat-item 是可选的，用于为迭代中的当前项提供一个友好的名称。

如果未指定，可以使用表达式 **$repeat-item** 访问当前项。上面示例中的最后一个组件也可以按如下方式编写：

```
-

name: members-svcg-comp

type: ns::servicegroup_servicegroupmember_binding

repeat:

  repeat-list: $parameters.svc-servers

properties:

       ip: $repeat-item

       port: $parameters.svc-port

       servicegroupname: $parent.properties.name
```

除了在迭代列表时能够引用当前项之外，还可以使用 **repeat-index** 引用列表中项的当前索引。在以下示例中，**repeat-index** 用于根据当前索引计算端口号：

```
   name: services

   type: ns::service

   repeat:

      repeat-list: $parameters.app-services

      repeat-item: srv

   properties:

       ip: $parameters.app-ip

       port: $parameters.base-port + repeat-index
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                servicegroupname: $parent.properties.name
```

与 **repeat-item** 构造类似，您可以分配不同的变量名来引用迭代的当前索引。上一个示例等同于以下示例：

```
    -

            name: services

            type: ns::service

            repeat:

               repeat-list: $parameters.app-services

               repeat-item: srv

               repeat-index: idx

            properties:

                ip: $parameters.app-ip

                port: $parameters.base-port + $idx

                servicegroupname: $parent.properties.name
```

重复条件构造

重复条件构造在重复构造的每次迭代中进行评估，其结果决定是否在该次迭代中构建配置对象，或者移至下一次迭代。以下示例展示了重复条件构造的用法：

示例：

```
components

   -

      name: der-key-files-comp

      type: ns::systemfile
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      repeat:

      repeat-list: $parameters.certificates

      repeat-item: certificate

        repeat-condition: $certificate.ssl-inform == DER

        properties:

         filecontent: base64($certificate.keyfile.contents)

         fileencoding: BASE64

         filelocation: /nsconfig/ssl

         filename: $certificate.keyfile.file
```

在此示例中，der-key-files-comp 组件迭代用户提供的所有证书，但它只构建与 DER 编码证书对应的配置对象。在每次迭代中，重复条件表达式进行评估，以测试证书编码是否为 DER 类型。如果不是 DER 类型，则在当前迭代中不构建任何配置对象，并且迭代移至列表中的下一个证书。

嵌套重复

使用嵌套重复构造，您可以在每个组件中拥有多个重复构造，具体取决于组件的定义。考虑一个两级嵌套重复。对于外部列表（第一个重复列表）中的每个元素，您可以为内部列表（第二个重复列表）的所有元素创建一个重复列表。StyleBook 编译器支持最多三级嵌套重复。每个重复级别都关联有 repeat-item 和 repeat-index 属性。repeat-item 和 repeat-index 属性都是可选的。此外，每个重复还可以指定一个重复条件。

示例:

```
parameters:

  -

      name: vips

      type: ipaddress[]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -

      name: vip-ports

      type: tcp-port[]

components:

  -

      name: lbvservers-comp

      type: ns::lbvserver

      repeat:

         repeat-list: $parameters.vips

         repeat-item: ip

         repeat:

              repeat-list: $parameters.vip-ports

              repeat-item: port

      properties:

         name: str("lb-") + str($ip) + '-' + str($port)

         servicetype: HTTP

         ipv46: $ip

         port: $port
```

在上述示例中，对于 $parameters.vips 中的每个项，我们遍历 $parameters.vip-ports 的所有项。因此，对于 $parameters.vips 中指定的每个 IP 地址，我们为 $parameters.vip-ports 中指定的所有端口创建 lbvserver 配置对象。properties 部分定义了对象的名称，其中“lb”作为 IP 地址和端口组合的前缀。因此，对于每次迭代，$ip + $port 定义了 IP 地址和端口号的唯一组合。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

如果未提供 repeat-item 属性，编译器会为其生成一个默认值。repeat-item 的默认值分别为：$repeat-item、$repeat-item-1、$repeat-item-2，对应每个重复级别。同样，如果未提供 repeat-index 属性，编译器会为其生成一个默认值。repeat-index 的默认值分别为：$repeat-index、$repeat-index-1 和 $repeat-index-2，对应每个重复级别。

以下示例描述了在嵌套重复对象中缺少 repeat-item 和 repeat-index 属性时的命名约定。

示例:

```
components:
-
    name: lbvservers-comp
    type: ns::lbvserver
    repeat:
        repeat-list: $parameters.vips
        repeat:
           repeat-list: $parameters.vip-ports
    properties:
       name: str("lb-") + str($repeat-item) + '-' + str($repeat-item-1)
       servicetype: HTTP
       ipv46: $repeat-item
       port: $repeat-item-1
```

输出

在输出部分，您可以指定 StyleBook 在成功创建所有配置对象后向其用户公开的内容。StyleBook 的输出部分是可选的。StyleBook 不需要返回输出。但是，通过将一些内部组件作为输出返回，它允许任何导入它的 StyleBook 具有更大的灵活性，这在创建复合 StyleBook 时可以看到。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

下表描述了输出部分中使用的属性。

属性	说明	强制
名称	与您要公开的配置对象对应的输出名称。	是
描述	描述输出的文本字符串。	否
值	此属性指定如何提取 StyleBook 返回的值。	是

示例：

```
outputs:
 -
   name: lbvserver
   description: LBVServer component
   value: $components.my-lbvserver-comp
 -
   name: svc-grp
     description: ServiceGroup name
     value: $components.my-svcg.properties.name
```

在此示例中，您公开了由 StyleBook 创建的 **lbvserver** 组件以及服务组的**名称**。名为 **lbvserver** 的输出的值是组件 **my-lbvserver-comp**。同样，名为 **svc-grp** 的输出的值是由组件 **my-svcg** 创建的服务组的名称。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数参考

在 components 构造中，您可以通过使用 `$parameters.<parametername>` 符号来引用 parameters 部分中定义的参数。如果 `<parametername>` 本身包含参数（当类型为对象时），则必须使用 `$parameters.<parametername>.<sub-parametername>` 符号，依此类推。

示例：

```
parameters:

  -

    name: name

    label: Name

    type: string

    required: true

     -

      name: vip

      label: Virtual IP and Port

      type: object

      required: true

      parameters:

        -

          name: ip

          label: Virtual IP

          description: The Virtual IP Address

          type: ipaddress

          required: true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            -

              name: port

              label: The Virtual Port

              description: The TCP port for the Virtual IP

              type: tcp-port

              default: 80

components:

  -

    name: my-lbvserver-comp

    type: ns::lbvserver

    properties:

       name: $parameters.name

       servicetype: HTTP

       ipv46: $parameters.vip.ip

       port: $parameters.vip.port
```

父级引用

如果您正在使用嵌套组件，您可以使用 $parent 表示法引用父组件。如果父组件使用重复构造构建多个配置对象，并且在每次迭代中，子组件构建其他配置对象，那么 $parent 表示法始终引用父组件的当前迭代。例如，$parent.properties.name 引用父组件在当前迭代中构建的配置对象的 name 属性。

示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
components:
 -
   name: my-lbvserver-comp
   type: ns::lbvserver
   properties:
     name: $parameters.name + "-lb"
     servicetype: HTTP
     ipv46: $parameters.ip
     port: 80
     lbmethod: $parameters.lb-alg
     components:
       -
         name: my-svcg-comp
         type: ns::servicegroup
         properties:
           name: $parameters.name + "-svcgrp"
           servicetype: HTTP
           components:
            -
              name: lbvserver-svg-binding-comp
              type: ns::lbvserver_servicegroup_binding
              properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                  name: $parent.parent.properties.name

                  servicegroupname: $parent.properties.name

                    -

                      name: members-svcg-comp

                      type: ns::servicegroup_servicegroupmember_binding

                      repeat: $parameters.svc-servers

                      repeat-item: srv

                      properties:

                        ip: $srv

                        port: str($parameters.svc-port)

                        servicegroupname: $parent.properties.name
```

您还可以通过访问父组件的父组件的属性，一直向上导航到顶级组件，从而遍历组件层次结构。例如，组件 **lbvserver-svg-binding-comp** 的属性名称通过使用 **$parent.parent** 表示法，从其父组件的父组件（即 **my-lbvserver-comp** 组件）的属性名称中获取其值。

组件参考

在组件构造中，您可以使用 **$components.\<componentname\>** 符号引用 StyleBook 中的顶级组件。如果顶级组件中存在嵌套组件，则使用 **$components.\<componentname\>.components.\<component-name\>** 符号引用它们，依此类推。

示例：

```
components:

 -

    name: my-lbvserver-comp

     type: ns::lbvserver
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    properties:
          name: $parameters.name + "-lb"
          servicetype: HTTP
          ipv46: $parameters.ip
          port: 80
          lbmethod: $parameters.lb-alg
 -
    name: my-svcg-comp
    type: ns::servicegroup
    properties:
         name: $parameters.name + "-svcgrp"
         servicetype: HTTP
-
    name: members-svcg-comp
    type: ns::servicegroup_servicegroupmember_binding
    repeat: $parameters.svc-servers
    repeat-item: srv
    properties:
       ip: $srv
         port: str($parameters.svc-port)
         servicegroupname: $components.my-svcg-comp.properties.name
-
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: lbvserver-svg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    properties:

          name: $components.my-lbvserver-comp.properties.name

          servicegroupname: $components.my-svcg-comp.properties.name
```

在此示例中，组件 **my-svcg-comp** 和 **my-lbvserver-comp** 必须在构建最后一个组件 **lbvserver-svg-binding-comp** 之前构建，因为最后一个组件中引用了这些组件。这些引用是通过使用 **$components.\<componentname\>** 表示的组件引用提供的。

替换引用

在组件部分或操作部分中，您可以使用 `$substitutions.<substitution-name>` 表示法引用在替换部分中定义的替换。例如，**$substitutions.http-port**。

如果替换是一个映射，您可以将映射中的元素引用为 `$substitutions.<substitutions-name>[<map-key>]`。例如，`$substitutions.protocol-map[$parameters.port]`。

变量引用

当您在组件中使用 repeat 和 repeat-item 构造来构建多个配置对象时，可以将变量名分配给 repeat-item 构造。然后，可以通过使用 `$\<varname\>` 符号在该组件的属性或子组件中引用此变量。请注意，当在组件中不使用 repeat-item 构造而使用 repeat 构造时，可以使用名为 $repeat-item 的默认变量来访问迭代项。

示例：

```
components:

  -

    name: server-members-comp

    type: ns::server

    condition: $parameters.svc-server-domain-names
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    repeat: $parameters.svc-server-domain-names

    repeat-item: server-name

    properties:

      name: $server-name + "-server"

      domain: $server-name

    components:

      -

         name: service-members-comp

         type: ns::service

         properties:

           name: $server-name + "-service"

           servername: $parent.properties.name

           servicetype: $parameters.svc-service-type

           port: $parameters.svc-server-port
```

在上面的示例中，变量名 server-name 被分配给 repeat-item 构造。此变量名在同一组件的属性以及子组件 `$\<varname\>` 中被引用。

操作

操作是 StyleBook 中的一个可选部分。在此部分中，您可以配置 NetScaler Console 分析以收集所有或部分流量事务的 AppFlow 记录。通过 StyleBook 在 NetScaler 实例上创建的虚拟服务器处理这些流量事务。在此部分中，您还可以配置 NetScaler Console，以便在虚拟服务器上满足特定流量条件时触发警报。

您可以通过 StyleBook 配置 NetScaler Console，以从以下列出的各种 NetScaler Console Insights 收集流量统计信息：

- Web 洞察

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- WAF 安全违规
- HDX™ 洞察
- NetScaler Gateway 洞察。

支持的虚拟服务器包括负载平衡、内容切换和 VPN 虚拟服务器。

对于负载平衡或内容切换虚拟服务器上的分析，请启用 Web Insight 和 WAF 安全违规两者，或其中之一。但是，对于 VPN 虚拟服务器，您必须同时启用 HDX Insight 和 NetScaler Gateway Insight，或其中之一。

通过 StyleBook 在 NetScaler 实例上启用的任何 NetScaler Console Insight 都使用 IPFIX 协议 (AppFlow) 将数据从实例发送到 NetScaler。

此外，当您启用 Web Insight 时，客户端测量会在负载平衡和内容切换虚拟服务器上启用。启用客户端测量后，NetScaler Console 通过 HTML 注入捕获 HTML 页面的加载时间和渲染时间指标。管理员可以使用这些指标来识别 L7 延迟问题。

示例 1：

以下示例展示了如何在 StyleBook 中编写操作部分，以在 VPN 虚拟服务器上同时启用 HDX Insight 和 NetScaler Gateway Insight：

```
name: simple-vpn-ops

namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"

description: Test StyleBook to enable hdxinsight and gatewayinsight on a
VPN vserver

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    version: "10.5"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    prefix: ns
components:
    -
        name: vpnvserver-comp
        type: ns::vpnvserver
        properties:
            name: str("vpn-") + str($current-target.ip)
            servicetype: SSL
            ipv46: 1.1.21.37
            port: 443
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.vpnvserver-comp
                filter: "true"
                insights:
                  -
                 type: hdxinsight**
                  -
                    type: gatewayinsight
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
outputs:

  -

    name: myvpns

    value: $components.vpnvserver-comp
```

示例 2：

以下示例展示了如何在 StyleBook 中编写操作部分，以在负载平衡虚拟服务器上同时启用 Web Insight 和 WAF 安全违规：

```


name: simple-lb-ops

namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"

description: Test StyleBook to enable webinsight and securityinsight on LB
vserver

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    version: "10.5"

    prefix: ns

components:

    -

        name: lbvserver-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        type: ns::lbvserver

        properties:

            name: str("lb-") + str($current-target.ip)

            servicetype: HTTP

            ipv46: 1.1.21.37

            port: 80

operations:

    analytics:

        -

            name: comp-ops

            properties:

                target: $components.lbvserver-comp

                filter: "true"

                 insights:

                 -

                  type: webinsight

                   -

                  type: securityinsight

outputs:

  -

    name: mylbs
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    value: $components.lbvserver-comp
```

分析

分析部分中的每个元素都用于为 StyleBooks 中创建的一个或多个虚拟服务器配置 NetScaler Console 分析功能。

分析部分中的元素具有以下属性：

属性	描述	必填
名称	分析元素的名称。	是
描述	描述此元素是什么的文本字符串。	否
条件	一个布尔表达式。当此条件评估为 false 时，整个分析元素将被跳过。	否
重复	遍历列表。	否
重复条件	一个布尔表达式。如果表达式评估为 false，则跳过当前迭代。	否
重复项	当前迭代中项的名称。	否
重复索引	当前迭代中索引值的名称。	否
属性	分析操作属性列表。	是
目标	列表中的一个属性。目标表达式是 NetScaler 上配置的虚拟服务器的名称，用于收集分析数据。	是
筛选器	列表中的一个属性。此属性的值是一个 NetScaler 高级策略表达式，用于筛选收集分析数据的虚拟服务器上的请求。默	否

© 1997–2026 Citrix Systems, Inc. All rights reserved.

属性	描述	必填
	认情况下，分析数据会收集通过虚拟服务器的所有流量。	
洞察	列表中的一个属性。此属性的值是要从目标虚拟服务器收集的洞察数据类型。默认情况下，所有允许的洞察都根据虚拟服务器类型配置在目标虚拟服务器上，如 目标虚拟服务器和洞察类型 中所述。	否
传输模式	列表中的一个属性。此属性的值为 `logstream` 或 `ipfix`。`logstream` 是默认值。	否
客户端测量	列表中的一个属性。此属性的值为 ENABLED 或 DISABLED。DISABLED 是默认值。	否
http-x-forwarded-for	列表中的一个属性。此属性的值为 ENABLED 或 DISBALED。此属性启用或禁用 X-Forwarded-For 标头插入，以将客户端 IP 信息传递到后端服务器。DISABLED 是默认值。	否
启用 HDXInsight 功能	列表中的一个属性。此属性的值为 ICA 或 TCP。此属性为特定流量数据启用 `hdxinsight`。ICA 是默认值。	否

示例 1：为单个虚拟服务器配置分析

```
operations:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  analytics:

    -

    name: lbvserver-ops-comp

    properties:

        target: $components-basic-lb-comp.outputs.lbvserver-name

        filter: HTTP.REQ.URL.CONTAINS("catalog")

        transport-mode: logstream

        client-side-measurements: ENABLED

        insights:

          -

            type: webinsight

          -

            type: securityinsight
```

示例 2：为 VPN 虚拟服务器列表配置分析

```
operations:



    analytics:

    -

      name: vpnvserver-ops-comp

      repeat: $outputs.staging-vpnvservers

      repeat-item: vpnvsvr
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      properties:

        target: $vpnvsvr.outputs.vpnvserver

        filter: HTTP.REQ.URL.CONTAINS("catalog")

         http-x-forwarded-for: ENABLED

        insights:

          -

            type: hdxinsight

            enable-hdxinsight-for: TCP
```

分析部分中的每个属性都配置 NetScaler 实例，以在由目标属性标识的虚拟服务器上收集 AppFlow 记录。

目标虚拟服务器和洞察类型

目标虚拟服务器和相应的允许洞察类型如下所示：

目标虚拟服务器	洞察类型
负载均衡虚拟服务器	WebInsight、SecurityInsight、BotInsight
CSV服务器	网络洞察、安全洞察、机器人洞察
VPN服务器	HDX洞察、网关洞察

注意：

IPFIX 是在 StyleBooks 中为虚拟服务器配置分析时使用的默认传输模式。

告警

操作部分中的告警子部分具有与分析子部分类似的结构和相同的属性。唯一的区别在于 properties 属性。有关所有属性（properties 属性除外）的列表，请参阅 分析。

告警子部分中提供以下属性：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

属性	描述	必需
目标	一个表达式，其计算结果为 NetScaler 上配置的虚拟服务器的名称，并为其配置了告警。	是
电子邮件配置文件	在 NetScaler Console Analytics 功能中定义的电子邮件配置文件的名称，其中包含当告警触发时您希望通知的电子邮件地址列表。	否（必须定义 email-profile 或 sms-profile 之一）
短信配置文件	在 NetScaler Console Analytics 功能中定义的短信配置文件的名称，其中包含当告警触发时您希望通知的电话号码列表。	否（必须定义 email-profile 或 sms-profile 之一）
规则	一个规则列表，用于定义触发由目标属性定义的虚拟服务器警报的条件。	是
度量	规则的一个属性。您希望跟踪的与NetScaler虚拟服务器相关的度量名称。	是
运算符	规则的一个属性。用于将度量与值进行比较的运算符。有效运算符为“大于”和“小于”。	是
值	规则的一个属性。使用运算符将度量与之进行比较的阈值。如果度量值超过此阈值，则会触发相关警报。	是
周期单位	规则的一个属性。如果满足警报规则，向用户发出警报的频率。这可以包含“天”、“小时”或“周”值。这意味着如果满足规则，将每隔一个周期单位发送一次警报（例如，每天一次）。	是

© 1997–2026 Citrix Systems, Inc. All rights reserved.

下表提供了与 NetScaler 虚拟服务器相关的跟踪指标列表。

计数器|描述|详细描述|NetScaler Console 计算

对于 VPN 虚拟服务器：			
app_count	VPN 应用程序启动计数	用户指定时间间隔内在此 VPN 虚拟服务器上启动的唯一 VPN 应用程序总数。	每次新应用程序启动时单调递增的计数器
app_launch_duration	VPN 应用程序启动持续时间	启动应用程序的平均时间（以毫秒为单位）	在此 VPN 虚拟服务器上启动的所有 VPN 应用程序的启动时间持续时间计算出的平均值
其他虚拟服务器（CS、LB、Auth、GSLB）			
total_requests	请求数	自上次设备重启或自虚拟服务器创建以来，此虚拟服务器上的客户端请求数，以较新的时间为准。	单调递增计数器，在此虚拟服务器的每个新请求上递增。
total_bytes	字节	在指定时间间隔内从虚拟服务器传输到 NetScaler Console 的总字节数。	单调递增计数器，用于计算此虚拟服务器提供的总字节数。
application_response_time	响应时间	虚拟服务器的平均响应时间。	此虚拟服务器自设备上次重启（或自虚拟服务器创建）以来收到的所有请求的平均响应时间值，以较晚者为准。

StyleBook 中警报部分的示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
operations:

alarms:

 -

  name:lbvserver_alarm

  properties:

  target: $outputs.lbvserver

  email-profile: $parameters.emailprofile

  sms-profile: "NetScalerSMS"

     rules:

      -

        metric: "total_requests"

        operator: "greaterthan"

        value: 25

        period-unit: weekly

        -

          metric: "total_bytes"

          operator: "lessthan"

          value: 1024

          period-unit: day
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

表达式

表达式是 StyleBook 最强大的功能之一。您可以在各种场景中使用 StyleBook 表达式来计算动态值。以下示例是一个将参数值与文字字符串连接起来的表达式。

示例：

```
$parameters.appname + "-mon"
```

此表达式检索名为 `appname` 的参数，并将其与字符串 `-mon` 连接起来。

支持以下类型的表达式：

算术表达式

- 加法 (+)
- 减法 (-)
- 乘法 (*)
- 除法 (/)
- 取模 (%)

示例：

- 两个数相加：$parameters.a + $parameters.b
- 两个数相乘：$parameters.a * 10
- 求一个数除以另一个数后的余数：

`15%10` 结果为 `5`

字符串表达式

- 连接两个字符串 (+)

示例:

连接两个字符串: str("app-") + $parameters.appname

列表表达式

合并两个列表 (+)

示例:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 连接两个列表: $parameters.external-servers + $parameters.internal-servers
- 如果 `$parameters.ports-1` 为 且 `$parameters.port-2` 为 ，则 `$parameters.ports-1 + $parameters.ports-2` 将显示为列表 。

关系表达式

- **==** : 测试两个操作数是否相等，如果相等则返回 true，否则返回 false。
- **!=** : 测试两个操作数是否不同，如果不同则返回 true，否则返回 false。
- **\>** : 如果第一个操作数大于第二个操作数则返回 true，否则返回 false。
- **\>=** : 如果第一个操作数大于或等于第二个操作数则返回 true，否则返回 false。
- **\<** : 如果第一个操作数小于第二个操作数，则返回 true，否则返回 false。
- **\<=** : 如果第一个操作数小于或等于第二个操作数，则返回 true，否则返回 false。

示例：

- 相等运算符的使用：`$parameters.name = = "abcd"`
- 不等运算符的使用：`$parameters.name != "default"`
- 其他关系运算符的示例
  - 10 > 9
  - 10 >= 10
  - 0 < 9
  - 10 <= 9
  - 10 == 10
  - 10 != 1

逻辑表达式 - 布尔型

- **and**：逻辑“与”运算符。如果两个操作数都为 true，则结果为 true，否则为 false。
- **or**：逻辑“或”运算符。如果其中一个操作数为 true，则结果为 true，否则为 false。
- **非**：一元运算符。如果操作数为真，则结果为假，反之亦然。
- **in**：测试第一个参数是否是第二个参数的子字符串
- **in**：测试某个项是否是列表的一部分

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

您可以对表达式进行类型转换，其中字符串可以转换为数字，数字可以转换为字符串。同样，您可以将 `tcp-port` 转换为数字，并且可以将 IP 地址转换为字符串。

在任何运算符之前和之后使用分隔符。您可以使用以下分隔符：

- 在运算符之前：`space`、`tab`、`comma`、`(`、`)`、`[`、`]`
- 在运算符之后：`space`、`tab`、`(`、`[`

例如：

- `abc + def`
- `100 % 10`
- `10 > 9`

逐字字符串表达式

当字符串中的特殊字符必须采用其字面形式时，可以使用逐字字符串。这些字符串可以包含转义字符、反斜杠、引号、括号、空格、方括号等。在逐字字符串中，特殊字符的常规解释会被跳过。字符串中的所有字符都以其字面形式保留。

在 StyleBooks 中，您可以使用逐字字符串以字面形式包含 NetScaler 策略表达式。策略表达式通常包含特殊字符。如果没有逐字字符串，您必须通过将字符串分解为子字符串来转义特殊字符。

要创建原义字符串，请按如下方式将字符串封装在特殊字符之间：

```
~{string}~
```

您可以在 StyleBook 中的任何位置使用原义字符串。

注意

请勿在输入字符串中使用字符序列 `}~`，因为此序列表示原义字符串的结束。

示例：

```
~{HTTP.REQ.COOKIE.VALUE("jsessionid") ALT
HTTP.REQ.URL.BEFORE_STR("=").AFTER_STR(";jsessionid=") ALT
HTTP.REQ.URL.AFTER_STR(";jsessionid=")}~
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

目标表达式

在 StyleBook 定义中，您可以使用 `$current-target` 表达式来引用当前目标 NetScaler 实例。要专门引用目标 NetScaler 实例的 IP 地址，请按如下方式使用此表达式：

```
$current-target.ip
```

示例：

```
components:

 -

  name: lb-comp

  type: ns::lbvserver

  properties:

    name: $current-target.ip + "-lbvserver"
```

在此示例中，`lbvserver` 的名称是使用目标 NetScaler 实例的 IP 地址构建的。

表达式类型验证

StyleBook 引擎允许在编译时进行更严格的类型检查，也就是说，在编写 StyleBook 时使用的表达式在导入 StyleBook 本身时进行验证，而不是在创建配置包时进行验证。

对参数、替换、组件、组件属性、组件输出、用户定义变量（重复项、重复索引、替换函数的参数）等的所有引用都将验证其存在性和类型。

类型检查示例：

在以下示例中，`lbvserver` StyleBook 的端口属性的预期类型为 `tcp-port`。在 NetScaler Console 中，类型验证在编译时（导入时）进行。编译器发现字符串和 `tcp-port` 不是兼容类型，因此 StyleBook 编译器会显示错误并无法导入或迁移 StyleBook。

```
components:

  -

    name: lbvserver-comp
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str("80")
      servicetype: HTTP
```

要成功编译此 StyleBook，请在编译器中将以下内容声明为数字：

`port: 80`

标记无效表达式的示例：

在早期版本中，当无效表达式被分配给属性名称时，编译器未检测到无效表达式，并允许将 StyleBook 导入到 NetScaler Console 中。现在，如果此 StyleBook 导入到 NetScaler Console 中，编译器会识别并标记此类无效表达式。因此，StyleBook 无法导入到 NetScaler Console 中。

在此示例中，分配给 `lb-sg-binding-comp` 组件中名称属性的表达式为：`$components.lbvserver-comp.properties.lbvservername`。但是，在 `lbvserver-comp` 组件中没有名为 `lbvservername` 的属性。在早期 NetScaler Console 版本中，编译器会允许此表达式并成功导入它。实际的故障会在用户希望使用此 StyleBook 创建配置包时发生。然而现在，此类错误在导入期间被识别，并且 StyleBook 未导入到 NetScaler Console 中。手动更正此类错误并导入 StyleBook。

```
Components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.lbvservername
      servicegroupname: $components.sg-comp.properties.servicegroupname
```

列表索引

现在可以通过直接对列表中的项进行索引来访问它们：

表达式	描述
`$components.test-lbs[0]`	指 test-lbs 组件中的第一个项
`$components.test-lbs[0].properties.p1`	指 test-lbs 组件中第一个项的属性 p1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname`	指 `servicegroups` 组件中第二个项的属性 `servicegroupname`，它是来自 `lbcomps` 组件的第一个项的输出

就地插值

现在可以使用 StyleBook 表达式替换字符串的一部分或多部分。当 StyleBook 编译器评估这些字符串表达式时，字符串中使用 StyleBook 表达式的部分将被表达式的值替换。要在字符串中包含 StyleBook 表达式，我们使用以下表示法：

```
"...%{...}%..."
```

其中，介于“%{”和“}%”之间的字符构成一个 StyleBook 表达式。这些表达式称为“就地插值”。

例如，字符串“lb-%{$parameters.appname}%-svc”是一个带有 StyleBook 表达式就地插值的字符串表达式。字符串表达式的值取决于插值表达式的值。假设 **$parameters.appname** 被赋值为“app1”。那么，该字符串表达式将评估为 **lb-app1-svc**。这使得值不必在字符串表达式中硬编码，而是可以根据用户定义的值进行评估。

就地插值的一个实际用例是在 StyleBook 中参数化策略表达式。考虑这样一种情况：您想编写一个策略表达式，检查 HTTP URL 是否包含特定单词，例如“jpeg”。

为此，您可以按如下方式编写策略表达式：“HTTP.REQ.URL.CONTAINS(\\"jpeg\\")”。

现在，如果您想参数化 HTTP URL 中的对象，可以在 StyleBook 中添加一个字符串参数，例如 $parameters.url-object。策略表达式应基于此参数编写。为此，您可以使用字符串连接来实现结果。表达式将如下所示：

```
str("HTTP.REQ.URL.CONTAINS(\\"" + $parameters.url-object + "\\")")
```

如果 $parameter.url-object 被赋值为“csv”，则上述表达式将评估为“HTTP.REQ.URL.CONTAINS(\\"csv\\")”。但是，此表达式不易阅读。为了使此参数化易于阅读和理解，您可以使用就地插值。

带有就地插值的表达式现在是：

```
str("HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)")
```

在上述表达式中，您使用了在 $parameters.url-object 的值周围添加内部引号的插值表达式。此表达式的结果与上述相同，但它看起来更直观，更接近实际结果。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

插值中允许的类型

您可以在插值中使用生成以下类型值的表达式：布尔值、数字、TCP 端口、IP 地址和字符串。当插值被结果替换时，生成的值会自动转换为字符串。

字符串表达式可以有 0 个、1 个或多个插值。在顺序插值中，字符串表达式的不同部分可以被不同的 StyleBook 表达式替换。例如，如果 $parameters.appname 是 "app1" 且 $parameters.vip 是 "1.1.1.1"，则字符串 lb-%{$parameters.appname}%-%{$parameters.vip}% 返回 "lb-app1-1.1.1.1"。

字符串表达式还支持嵌套插值。也就是说，一个插值表达式可以嵌套在另一个插值表达式中，以便一个表达式的值可以作为第二个表达式的输入。

例如，考虑字符串 "%{lb-%{$parameters.port + 1}%}%"

如果 $parameters.port 为 80，则内部字符串 "**%{$parameters.port + 1}%**" 返回 "lb-81"。这里，此表达式嵌套在另一个插值表达式中。

下表描述了不同类型的插值及其示例和相应结果。示例中使用的参数值为：

- $parameters.appname: "lb1"
- $parameters.vip: "1.1.1.1"
- $parameters.n1: 1
- $parameters.n2: 3

简单插值

表达式	结果
负载均衡器-%{$parameters.appname}%-默认	负载均衡器-lb1-默认

自动类型转换

表达式	结果
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
负载均衡器-%{true}%	负载均衡器-True

© 1997–2026 Citrix Systems, Inc. All rights reserved.

顺序插值

表达式	结果
%{$parameters.appname}%-%{str($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

嵌套插值

表达式	结果
%{abc-%{$parameters.n1 + 1}%}%	abc-2
字符串("%{abc-%{$parameters.n1}%}%-%{$parameters.n2}%")	bc-1-3

带引号包装的插值

表达式	结果
字符串("%{引用包装(示例文本)}%") 字符串("%{引用包装(`https://)}%` `+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")`	"示例文本 "<`https://"+HTTP.REQ.HOST` `NAME+HTTP.REQ.URL`

插值中的转义字符

如果字符 "%{" 或 "}%" 是字符串的一部分，您必须提供 "`\`" 作为转义字符，以便 StyleBook 编译器不会将它们评估为插值标签。

示例：

str("%{\%\{ + str($parameters.vip) + \}\%}%") 如果 $parameters.vip 为 1.1.1.1，则返回 "%{1.1.1.1}%"

下表描述了更多表达式及其结果：

类别	表达式	结果
转义插值	str("%{str($parameters.n1) + }\%}%")	1}%

© 1997–2026 Citrix Systems, Inc. All rights reserved.

类别	表达式	结果
	负载均衡器-%{str($参数.n1) + }\%}%	lb-1}%
	"%{str($parameters.n1) + \"\}\%\"}%"	1}%

内置函数

StyleBook 中的表达式使用内置函数。

例如，您可以使用内置函数 `str()` 将数字转换为字符串。

`str($parameters.order)`

或者，您可以使用内置函数 `int()` 将字符串转换为整数。

`int($parameters.priority)`

以下是 StyleBook 表达式中支持的内置函数列表及其使用示例：

字符串()

`str()` 函数将输入参数转换为字符串值。

允许的参数类型：

- `string`
- `number`
- `TCP-port`
- `boolean`
- `IP address`

示例:

- `"set-" + str(10)` 函数返回 `"set-10"`。
- `str(10)` 函数返回 `10`。
- `str(1.1.1.1)` 函数返回 `1.1.1.1`。
- `str(T rue)` 函数返回 `"T rue"`。
- `str(ADM)` 函数返回 `"mas"`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

整数()

`int()` 函数将字符串、数字、IP 地址或 `tcpport` 作为参数，并返回一个整数。

示例:

- `int("10")` 函数返回 `10`。
- `int(10)` 函数返回 `10`。
- `int(ip('0.0.4.1'))` 函数返回 `1025`。

布尔()

`bool()` 函数接受任何类型作为参数。如果参数值为 `false`、空或缺失，此函数返回 `false`。

否则，它返回 `true`。

示例：

- `bool(true)` 函数返回 `true`。
- `bool(false)` 函数返回 `false`。
- 如果 `$parameters.a` 为 `false`、空或缺失，则 `bool($parameters.a)` 函数返回 `false`。

len() 函数

`len()` 函数接受字符串或列表作为参数，并返回字符串中的字符数或列表中的项目数。

示例 1：

如果您按如下方式定义替换：

`items: ["123", "abc", "xyz"]`

`len($substitutions.items)` 函数返回 `3`

示例 2：

`len("NetScaler Console")` 函数返回 `10`。

示例 3：

如果 `$parameters.vips` 具有值 `['1.1.1.1', '1.1.1.2', '1.1.1.3']`，则 `len($parameters.vips)` 函数返回 `3`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

min() 函数

函数 `min()` 接受列表、一系列数字或 `tcp-ports` 作为参数，并返回最小项。

一系列数字/TCP 端口的示例：

- 函数 `min(80, 100, 1000)` 返回 `80`。
- 函数 `min(-20, 100, 400)` 返回 `-20`。
- 函数 `min(-80, -20, -10)` 返回 `-80`。
- 函数 `min(0, 100, -400)` 返回 `-400`。

数字/TCP 端口列表的示例：

- 支持 `$parameters.ports` 是 `tcp-ports` 的列表，其值为：`[80, 81, 8080]`。

  函数 `min($parameters.ports)` 返回 `80`。

max() (最大值)

函数 `max()` 接受列表、一系列数字或 `tcp-ports` 作为参数，并返回最大项。

一系列数字/TCP 端口的示例：

- 函数 `max(80, 100, 1000)` 返回 `1000`。
- 函数 `max(-20, 100, 400)` 返回 `400`。
- 函数 `max(-80, -20, -10)` 返回 `-10`。
- 函数 `max(0, 100, -400)` 返回 `100`。

数字/TCP 端口列表示例：

- 支持 `$parameters.ports` 是 `tcp-ports` 的列表，其值为：`[80, 81, 8080]`。

  函数 `max($parameters.ports)` 返回 `8080`。

二进制()

函数 `bin()` 接受一个数字作为参数，并返回一个以二进制格式表示该数字的字符串。

表达式示例：

函数 `bin(100)` 返回 `0b1100100`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

八进制()

函数 `oct()` 接受一个数字作为参数，并返回一个以八进制格式表示该数字的字符串。

表达式示例：

函数 `oct(100)` 返回 `0144`。

十六进制()

函数 `hex()` 接受一个数字作为参数，并返回一个以十六进制格式表示该数字的小写字符串。

表达式示例：

`hex(100)` 函数返回 `0x64`。

小写()

`lower()` 函数将字符串作为参数，并返回小写形式的相同字符串。

示例：

`lower("ADM")` 函数返回 `adm`。

大写()

`upper()` 函数将字符串作为参数，并返回大写形式的相同字符串。

示例：

`upper("NetScaler Console")` 函数返回 `NetScaler Console`。

求和()

`sum()` 函数将数字列表或 `tcpports` 作为参数，并返回列表中数字的总和。

示例 1：

如果按如下方式定义替换： substitutions:

`list-of-numbers = [11, 22, 55]`

`sum($substitutions.list-of-numbers)` 函数返回 `88`。

示例 2:

如果 `$parameters.ports` 是 `[80, 81, 82]`，则 `sum($parameters.ports)` 函数返回 `243`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

pow() (幂函数)

`pow()` 函数接受两个数字作为参数，并返回一个数字，该数字表示第一个参数的第二个参数次幂。

示例:

`pow(3,2)` 函数返回 `9`。

ip()

`ip()` 函数接受整数、字符串或 IP 地址作为参数，并根据输入值返回 IP 地址。

示例:

- 在 `ip` 函数中指定 IP 地址：

  `ip(3.1.1.1)` 函数返回 `3.1.1.1`。
- 在 `ip` 函数中指定字符串：

  `ip('2.1.1.1')` 函数返回 `2.1.1.1`
- 在 `ip` 函数中指定整数：
  - `ip(12)` 函数返回 `0.0.0.12`。
  - 当您在 `ip` 函数中将整数指定为字符串时，它会返回输入的等效 IP 地址。

    `ip('1025')` 函数返回 `0.0.4.1`。

  此函数还支持整数加法和减法运算，并返回一个结果 IP 地址。

  - 加法：`ip(1025) + ip(12)` 函数返回 `0.0.4.13`。
  - 减法：`ip('1025') - ip(12)` 函数返回 `0.0.3.245`。
  - 组合加法和减法：`ip('1.1.1.1') + ip('1.1.1.1') – ip(2)` 返回 `2.2.2.0`。

base64.encode()

`base64.encode()` 函数接受一个字符串参数并返回 base64 编码的字符串。

示例：

`base64.encode("abcd")` 函数返回 `YWJjZA==`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

base64.decode()

`base64.decode` 函数接受一个 base64 编码的字符串作为参数并返回解码后的字符串。

示例：

`base64.decode("YWJjZA==")` 函数返回 `abcd`。

存在()

函数 `exists()` 接受任意类型的参数并返回一个布尔值。如果输入有任何值，则返回值为 `True`。如果输入参数没有值（即，无值），则返回值为 `False`。

假设 `$parameters.monitor` 是一个可选参数。如果在创建配置包时为此参数提供值，则 `($parameters.monitor)` 函数返回 `True`。

否则，它返回 `False`。

过滤()

`filter()` 函数接受两个参数。

参数 1：一个替换函数，它接受一个参数并返回一个布尔值。

参数 2：一个列表。

该函数返回原始列表的一个子集，其中每个元素在传递给第一个 参数中的替换函数时，其计算结果为 `True`。

示例：

考虑一个替换函数，如下所示：

替换：

`x(a): $a != 81`

如果输入值不等于 `81`，则此函数返回 True。否则，它返回 `False`。

假设 `$parameters.ports` 是 `[81, 80, 81, 89]`。

`filter($substitutions.x, $parameters.ports)` 通过从列表中删除 `81` 的所有出现项来返回 `[80, 89]`。

如果-那么-否则()

函数 `if-then-else()` 接受三个参数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数 1: 布尔表达式

参数 2: 任意表达式

参数 3: 任意表达式 (可选)

如果参数 1 中的表达式评估为 `True`，则函数返回作为参数 2 提供的表达式的值。

否则，如果提供了参数 3，函数返回参数 3 中表达式的值。

如果未提供参数 3，函数返回 `no`。

示例 1:

`if-then-else($parameters.servicetype == HTTP, 80, 443)` 函数在 `$parameters.servicetype` 的值为 `HTTP` 时返回 `80`。否则，函数返回 `443`。

示例 2:

`if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` 函数在 `$parameters.servicetype` 的值为 `HTTP` 时返回 `$parameters.hport` 的值。

否则，函数返回 `$parameters.sport` 的值。

示例 3:

`if-then-else($parameters.servicetype == HTTP, 80)` 在 `$parameters.servicetype` 的值为 `HTTP` 时返回 `80`。

否则，该函数不返回任何值。

连接()

`join()` 函数接受两个参数：

参数 1：数字、`tcp-ports`、字符串或 IP 地址列表

参数 2：分隔符字符串（可选）

此函数将作为参数 1 提供的列表元素连接成一个字符串，其中每个元素由作为参数 2 提供的分隔符字符串分隔。如果未提供参数 2，则列表中的元素将连接成一个字符串。

示例：

- `$parameters.ports` 是 `[81, 82, 83]`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 带分隔符参数：

  `join($parameters.ports, '-')` 函数返回 `81-82-83`。

- 不带分隔符参数：

  `join($parameters.ports)` 函数返回 `818283`。

分割()

`split()` 函数根据指定的分隔符将输入字符串拆分为多个列表。如果未指定分隔符或指定为空白 (`''`)，则此函数将空格视作分隔符并将字符串拆分为列表。

示例：

- `split('Example_string_split', 's')` 函数返回 `['Example_','tring_','plit']`。
- `split('Example string split')` 函数返回 `['Example','string','split']`。
- `split('Example string split', '')` 函数返回 `['Example','string','split']`。
- `split('Example string')` 函数返回 `['Example','string']`。

  此函数将连续空格视为一个空格。

映射()

`map()` 函数接受两个参数；

参数 1：任何函数

参数 2：元素列表。

此函数返回一个列表，其中列表中的每个元素都是将 `map()` 函数（参数 1）应用于参数 2 中相应元素的结果。

参数 1 中允许的函数：

- 接受一个参数的内置函数：

  `base64.encode, base64.decode, bin, bool, exists, hex, int, ip, len, lower, upper, oct, quotewrap, str, trim, upper, url.encode, url.decode`

- 接受至少一个参数的替换函数。

示例：

假设 $parameters.nums 是 `[81, 82, 83]`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 使用内置函数 str 进行映射

  `map(str, $parameters.nums)` 函数返回 `["81", "82", "83"]`

  映射函数的结果是字符串列表，其中每个字符串元素都是通过对输入列表 ($parameters.nums) 中的相应元素应用 str 函数计算得出的。

- 使用替换函数进行映射

  - 替换：

    `add-10(port): $port + 10`

  - 表达式：

    `map($substitutions.add-10, $parameters.nums)` 函数返回一个数字列表：`[ 91, 92, 93 ]`

此映射函数的结果是一个数字列表。每个元素都是通过对输入列表 `($parameters.nums)` 中的相应元素应用替换函数 `$substitutions.add-10` 计算得出的。

引用包装()

`quotewrap()` 函数接受一个字符串作为参数，并在输入值前后添加双引号字符后返回一个字符串。

示例：

`quotewrap("ADM")` 函数返回 `"mas"`

替换()

函数 `replace()` 接受三个参数：

参数 1：以下内置类型之一的 `string` 或列表：

- `string`
- `number`
- `ipaddress`
- `tcp-port`
- `boolean`

参数 2：单个值或值列表，其类型与参数 1 中指定的类型匹配

参数 3：与参数 1 中指定的类型相同的单个值（可选）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`replace()` 函数将参数 1 中参数 2 的所有出现替换为参数 3。

如果未提供参数 3，则参数 1 中参数 2 的所有出现都将被移除。

示例：

- `replace('abcdef', 'def', 'xyz')` 函数返回 `abcxyz`。

  `def` 的所有出现都替换为 `xyz`。
- `replace('abcdefabc', 'def')` 返回 `abcabc`。

  由于没有参数 3，`def` 将从结果字符串中移除。
- `replace('An#example@to%replace!characters', ['@', '#', '!', '%'], '_')` 函数返回 `An_example_to_replace_characters`。

  输出字符串使用下划线 (_) 代替 `['@', '#', '!', '%']` 中指定的字符。
- `replace([10.10.10.1, 10.10.10.2, 10.10.10.3, 10.10.10.4], [10.10.10.2, 10.10.10.4])` 函数返回 `[10.10.10.1, 10.10.10.3]`。

  由于没有参数 3，`10.10.10.2` 和 `10.10.10.4` 将从结果 IP 地址列表中移除。
- `replace([8080, 8081, 8082, 8083, 8084], 8083, 80)` 函数返回 `[8080, 8081, 8082, 80, 8084]`。

  `8083` 的所有出现都将替换为 `80`。

修剪()

`trim()` 函数返回一个字符串，其中输入字符串的前导和尾随空格已被去除。

示例：

`trim(' abc ')` 函数返回 `abc`。

截断()

`truncate()` 函数接受两个参数：

参数 1: 字符串

参数 2: 数字

该函数返回一个字符串，其中参数 1 中的输入字符串被截断为参数 2 指定的长度。

示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`truncate('NetScaler Console', 6)` 返回 `Citrix`。

去重()

`distinct()` 函数从列表输入中提取唯一项。

示例： 如果 `$parameters.input_list` 是 `['ADM', 'ADC', 'VPX', 'ADC', 'ADM', 'CPX']`，则 `distinct($parameters.input_list)` 函数返回 `['ADM', 'ADC', 'VPX', 'CPX']`。

url.encode()

`url.encode()` 函数返回一个字符串，其中字符根据 RFC 3986 使用 ASCII 字符集进行转换。

示例：

`url.encode("a/b/c")` 函数返回 `a%2Fb%2Fc`。

url.decode()

`url.decode()` 函数返回一个字符串，其中 URL 编码的参数根据 RFC 3986 解码为常规字符串。

示例：

`url.decode("a%2Fb%2Fc")` 函数返回 `a/b/c`。

是-IPv4()

`is-ipv4()` 函数将 IP 地址作为参数，如果 IP 地址是 IPv4 格式，则返回布尔值 `True`。

`is-ipv4(10.10.10.10)` 函数返回 `True`

是-ipv6()

`is-ipv6()` 函数将 IP 地址作为参数，如果 IP 地址是 IPv6 格式，则返回布尔值 `True`。

`is-ipv6(2001:DB8::)` 函数返回 `True`

以开头()

`startswith()` 函数确定字符串是否以给定前缀开头。此函数需要两个强制字符串参数。

`startswith(str, sub_str)`

当字符串 (`str`) 以子字符串 (`sub_str`) 开头时，此函数返回 `True`。

示例：

- `startswith('Citrix', 'Ci')` 函数返回 `True`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `startswith('Citrix', 'iC')` 函数返回 `False`
- `startswith('Citrix', 'Ab')` 函数返回 `False`

以结尾()

`endswith()` 函数确定字符串是否以给定后缀结尾。此函数需要两个强制字符串参数。

`endswith(str, sub_str)`

当字符串 (`str`) 以子字符串 (`sub_str`) 结尾时，此函数返回 `True`。

示例：

- 函数 `endswith('Citrix', 'ix')` 返回 `True`。
- 函数 `endswith('Citrix', 'Ix')` 返回 `False`。
- 函数 `endswith('Citrix', 'ab')` 返回 `False`。

包含()

函数 `contains()` 用于确定字符串是否包含给定子字符串。此函数需要两个强制字符串参数。

`contains(str, sub_str)`

当子字符串 (`sub_str`) 包含在字符串 (`str`) 中的任何位置时，此函数返回 `True`。

示例：

- 函数 `contains('Citrix', 'tri')` 返回 `True`。
- 函数 `contains('Citrix', 'Ci')` 返回 `True`。
- 函数 `contains('Citrix', 'ti')` 返回 `False`

子串()

使用 `substring()` 函数从字符串中提取子字符串。

`substring(str, start_index, end_index)`

此函数需要两个强制参数和一个可选的整数参数。

- `str` (强制)
- `start_index` (强制)
- `end_index` (可选)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

此函数返回字符串 (`str`) 中位于指定索引位置之间的子字符串。如果未指定结束索引位置，则函数将从起始索引提取子字符串直到字符串末尾。

注意

当您指定 `end_index` 时，子字符串不包括 `end_index` 位置的字符。

示例：

- `substring('Citrix', 2)` 函数返回 `trix`
- `substring('Citrix', 10)` 函数返回 (`''`)

  在此示例中，函数返回一个空字符串，因为它具有无效的 `start_index` 位置。
- `substring('Citrix', 2, 4)` 函数返回 `tr`

  在此示例中，函数提取索引位置 2 到 4 之间的字符。
- 函数 `substring('Citrix', -3)` 返回 `rix`

  如果要提取字符串末尾的字符，请为 `start_index` 参数指定一个负值。

  在此示例中，该函数提取包含字符串中最后三个字符的子字符串。

多重()

函数 `multiple()` 接受两个参数：

参数 1：一个 `number`、`string`、`boolean`、`ipaddress`、`tcp-port` 或 `password`

参数 2：一个 `number`

函数 `multiple(argument1, argument2)` 返回一个列表，其中包含参数 1 的多个副本。副本的数量等于传递给参数 2 的数字。

示例：

- 函数 `multiple(10.10.10.10, 3)` 返回 `[10.10.10.10, 10.10.10.10, 10.10.10.10]`。
- 函数 `multiple(8080, 4)` 返回 `[8080, 8080, 8080, 8080]`。

反转()

reverse() 函数接受一个项目列表作为参数，并返回一个包含相同项目但按相反顺序排列的列表。

参数可以是以下内置类型的列表：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `string`
- `number`
- `ipaddress`
- `ipnetwork`
- `tcp-port`
- `boolean`
- `password`
- `object`
- `file`
- `certfile`
- `keyfile`
- `certkey`

示例：

- reverse() 返回 。
- reverse() 返回 。
- reverse() 返回 。

依赖检测

StyleBook 中的组件可以引用同一 StyleBook 中其他组件的属性或部分。组件本身是完整的块，它们可能不会按照需要执行的顺序编写。StyleBook 编译器会检查组件的编写顺序，然后按逻辑顺序执行它们。

示例：

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.name
      servicegroupname: $components.sg-comp.properties.servicegroupname
  -
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
```

在上面的示例中，定义了三个组件：**lbvserver-comp**、**lb-sg-binding-comp** 和 **sg-comp**。当执行此 StyleBook 时，首先创建 lbvserver-comp。lb-sg-binding-comp 引用 lbvserver-comp 属性，但即使它是 StyleBook 中定义的第二个组件，它也不能紧接着创建。这是因为 lb-sg-binding-comp 还依赖于尚未创建的 sg-comp。因此，编译器会重新排序组件，以便在创建组件时解决其依赖关系，并执行此重新排序的组件列表。上述 StyleBook 的执行顺序是：lbvserver-comp、sg-comp 和 lb-sg-binding-comp。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

因此，StyleBook 的作者无需担心组件的正确顺序。组件可以以任何顺序出现。编译器会根据组件之间相互引用的方式计算组件的正确执行顺序。请注意，这种依赖检测和重新排序也适用于替换和输出部分。

循环依赖

由于一个组件可能引用另一个组件，因此在 StyleBook 的定义中可能会引入依赖循环。例如，如果组件 A 引用组件 B 中定义的属性，而组件 B 又引用组件 A 中定义的属性。这种依赖关系称为循环依赖。循环依赖无法自动解决。StyleBook 的作者应手动更正 StyleBook 定义以消除此类循环依赖。编译器将能够识别循环依赖（如果存在）并进行报告。

以下示例显示了组件的循环依赖：

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $components.lb-sg-binding-comp.properties.name
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    name: mylb

     servicegroupname: $components.sg-comp.properties.servicegroupname

  -

    name: sg-comp

    type: ns::servicegroup

    properties:

      servicegroupname: mysg

      servicetype: $components.lbvserver-comp.properties.servicetype
```

在上面的示例中，有三个组件：**lbvserver-comp**、**lb-sg-binding-comp** 和 **sg-comp**。lbvserver-comp 依赖于 lb-sg-binding-comp，lb-sg-binding-comp 依赖于 sg-comp，sg-comp 依赖于 lbvserver-comp。这里，这些组件之间形成了依赖循环，无法自动解决。因此，此 StyleBook 无法执行。StyleBook 编译器会检测到这一点，并阻止 StyleBook 导入到 NetScaler Console 中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全

NetScaler Console 安全分析可帮助您监控、检测和缓解对应用程序的威胁。以下主题可帮助您查看和处理安全洞察：

- 应用程序安全仪表板
- 安全违规
- API 安全

应用程序安全仪表板

应用程序安全仪表板为您提供已发现/已许可应用程序的安全指标概述。此仪表板显示已发现/已许可应用程序的安全攻击信息，例如同步攻击、小窗口攻击、DNS 洪水攻击等。

要在应用程序安全仪表板上查看安全指标，请执行以下操作：

1. 导航到 **安全** > **安全仪表板**。
2. 从实例列表中选择实例 IP 地址。

   报告包含每个应用程序的以下信息：

   - **威胁指数**。一个一位数评级系统，指示应用程序上攻击的严重性。应用程序上的攻击越严重，该应用程序的威胁指数就越高。值范围为 1 到 7。

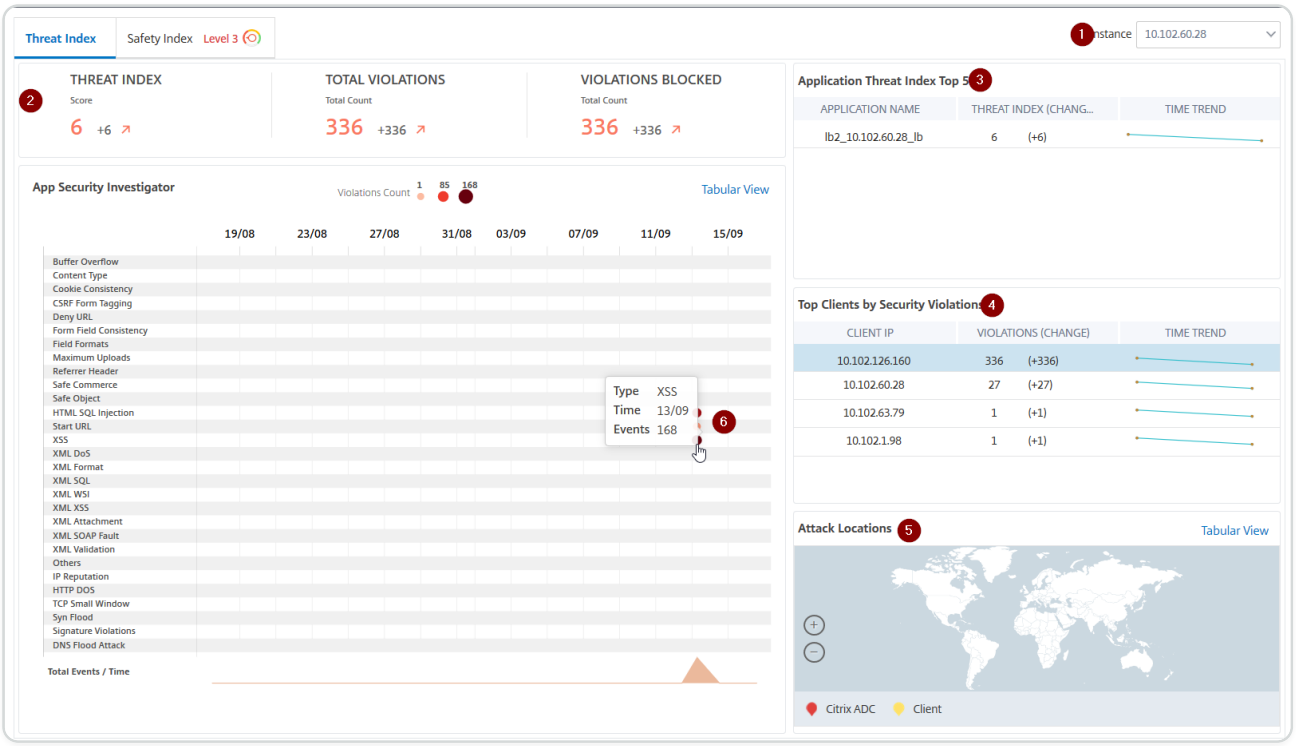
     威胁指数基于攻击信息。攻击相关信息，例如违规类型、攻击类别、位置和客户端详细信息，可深入了解应用程序上的攻击。违规信息仅在发生违规或攻击时发送到 NetScaler Console。大量的漏洞和弱点会导致较高的威胁指数值。
   - **安全指数**。一个一位数评级系统，指示您配置 NetScaler 实例以保护应用程序免受外部威胁和漏洞的安全性。应用程序的安全风险越低，安全指数就越高。值范围为 1 到 7。

     安全指数同时考虑应用程序防火墙配置和 NetScaler 系统安全配置。为了获得高安全指数值，这两种配置都必须强大。例如，如果已实施严格的应用程序防火墙检查，但未提供 NetScaler 系统安全措施（例如 `nsroot` 用户的强密码），则应用程序将被分配较低的安全指数值。

您可以在 **应用程序安全调查器** 上查看报告的差异。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

威胁指数详细信息



1 - 显示您可以查看其详细信息的 NetScaler 实例 IP 地址。

2 - 显示详细信息，例如威胁指数分数、发生的总违规次数和被阻止的总违规次数。

3 - 显示所选实例的虚拟服务器。

4 - 显示基于客户端的安全违规。每个客户端都会显示 App Security Investigator 图表。您可以单击每个客户端 IP 以查看结果。

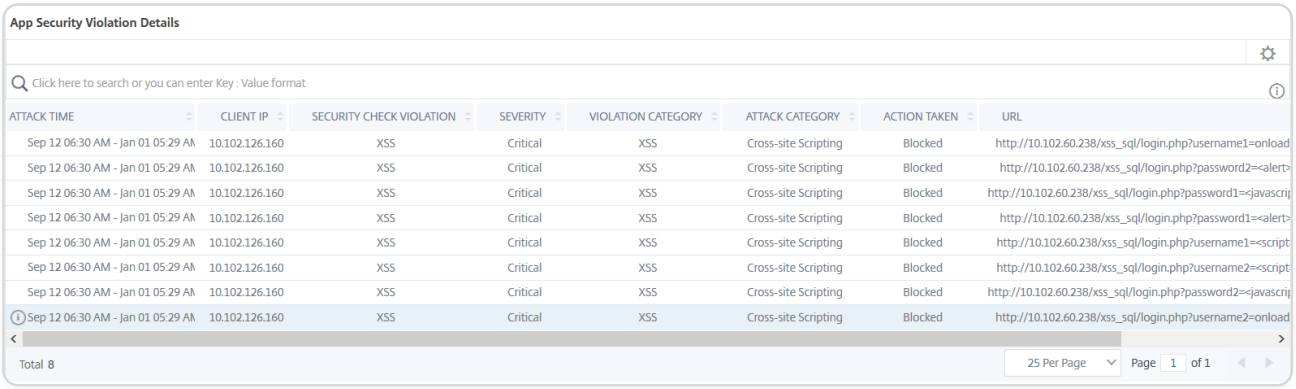
5 - 在地图视图和表格视图中显示违规。

6 - 显示违规详细信息。当您将鼠标指针悬停在图表上时，会显示违规类型、攻击时间、事件总数等详细信息。

当您单击气泡图时，详细信息将显示在“**App Security Violation Details**”页面中。例如，如果您想进一步查看跨站点脚本 (cross-site script) 违规的详细信息，请单击“**App Security Investigator**”中为“**XSS**”填充的图表。

“**App Security Violation Details**”显示违规详细信息，例如攻击时间、攻击类别、严重性、URL 等。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您还可以单击“**Settings**”选项以选择要显示的项目。

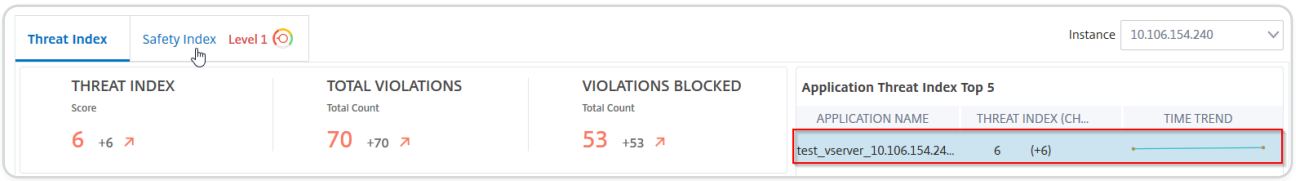
安全指数详情

在审查应用程序的威胁暴露后，您需要确定该应用程序已有哪些安全配置以及缺少哪些配置。您可以通过深入查看应用程序安全指数摘要来获取此信息。

安全指数摘要为您提供有关以下安全配置有效性的信息：

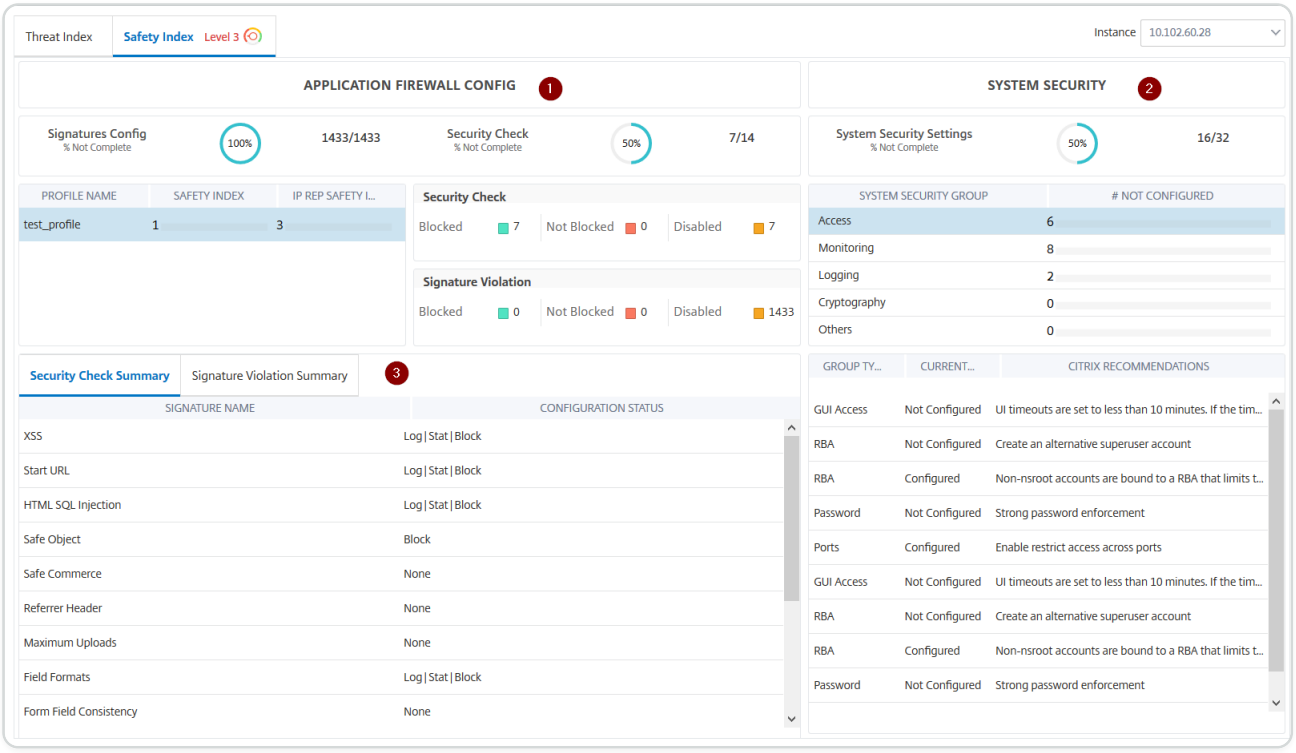
- **应用程序防火墙配置**。显示有多少签名和安全实体未配置。
- **NetScaler Console 系统安全**。显示有多少系统安全设置未配置。

要查看“**Safety Index**”详细信息，请选择一个虚拟服务器/应用程序，然后单击“**Safety Index**”选项卡。



显示详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1 - 显示应用程序防火墙配置的详细信息。

2 - 显示系统安全的详细信息。单击每个安全组可获取当前状态和 Citrix 建议的详细信息。

3 - 显示安全检查和签名违规的摘要。

您还可以通过为虚拟服务器启用 **WAF 安全违规**来查看威胁环境的摘要，然后导航到**安全** > **安全违规**。

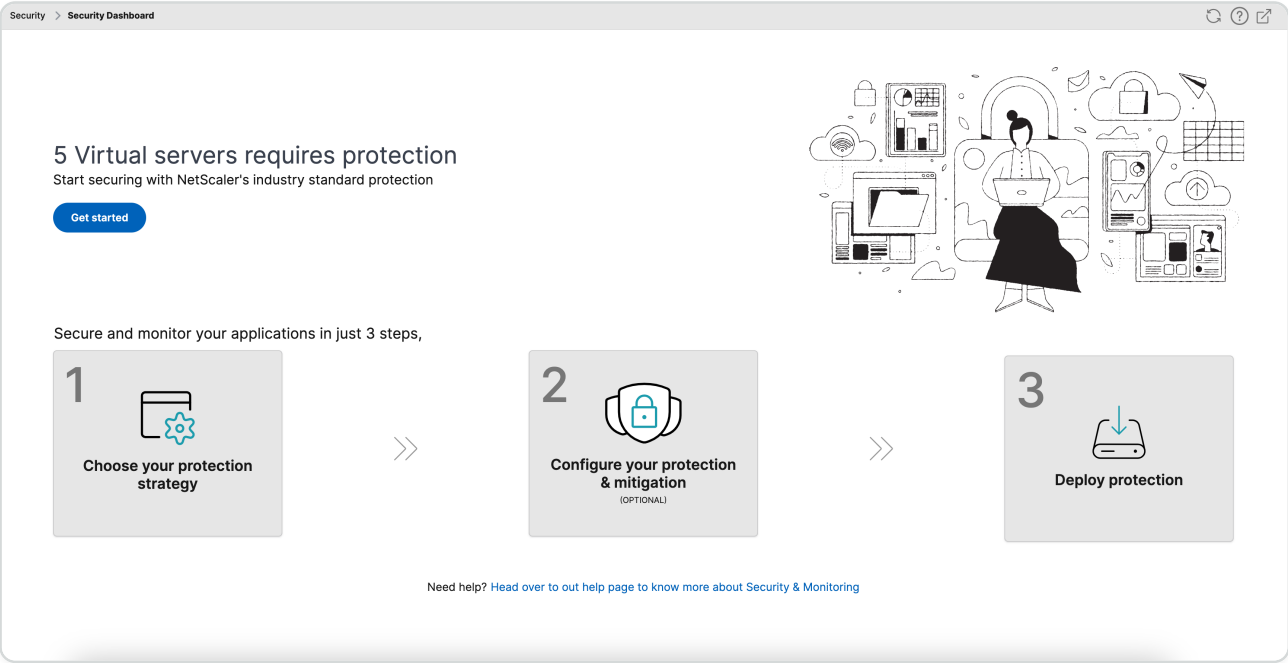
统一安全仪表板

“**统一安全**”仪表板是一个单窗格仪表板，您可以在其中配置保护、启用分析并将保护部署到您的应用程序。在此仪表板中，您可以从各种模板选项中进行选择，并在单个工作流中完成整个配置过程。要开始使用，请导航到 **Security > Security Dashboard**，然后单击 **Manage Application**。在 **Manage Application** 页面中，您可以查看已保护和未受保护应用程序的详细信息。

注意：

- 如果您是新用户，或者尚未通过 StyleBooks 或直接在 NetScaler® 实例上配置任何保护，则在单击 **Security > Security Dashboard** 后将显示以下页面。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

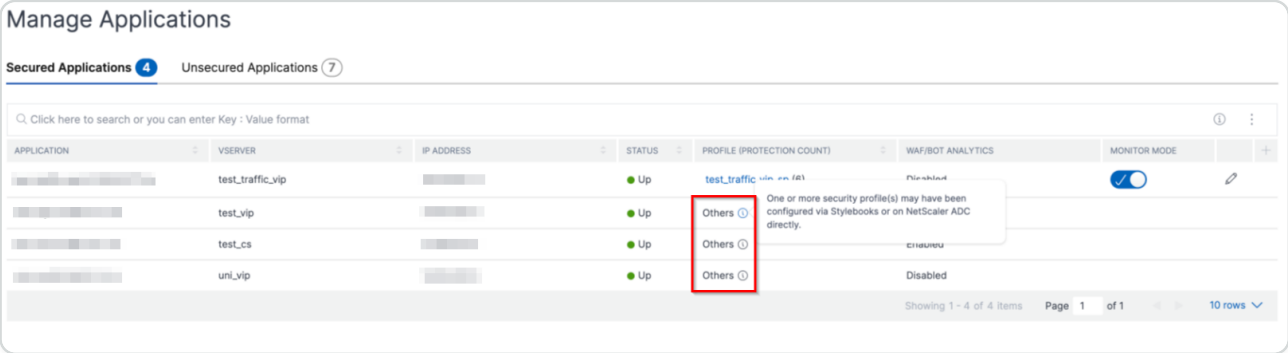


- 您可以查看需要保护的虚拟服务器总数。单击 **Get Started** 以在 **Unsecured Applications** 中查看详细信息。
- 可用于配置保护的合格虚拟服务器类型是负载平衡和内容切换。

已保护的应用程序

使用统一安全仪表板配置保护后，您可以查看详细信息。有关更多信息，请参阅配置未受保护应用程序的保护。

如果您已直接在 NetScaler 实例上或通过 StyleBooks 配置了保护，则可以在 **Secured Applications** 选项卡中查看在 **Profile** 下标记为 **Others** 的应用程序。



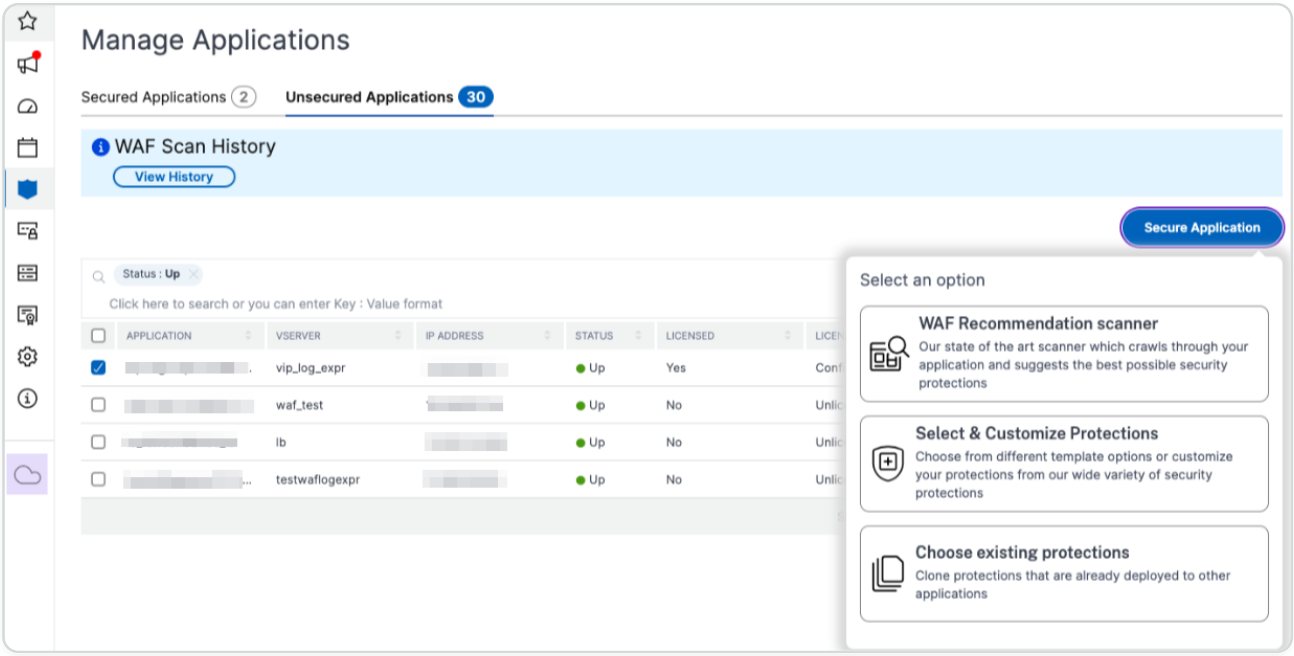
配置未受保护应用程序的保护

注意：

阻止列表中支持的最大配置实体（规则）为 32。

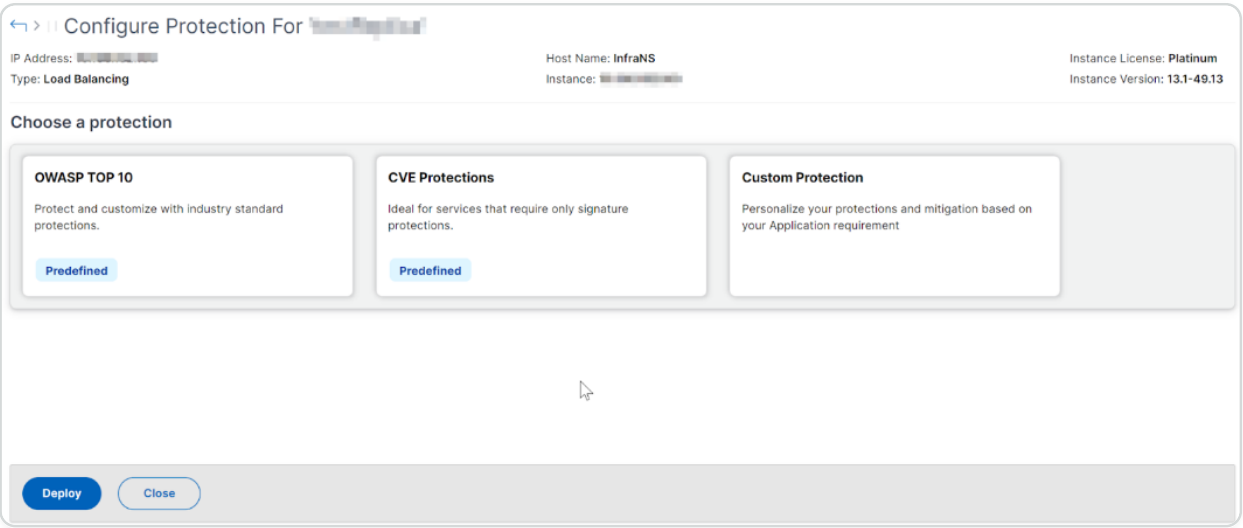
© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 **Unsecured Applications** 选项卡中，选择一个应用程序，然后单击 **Secure Application**。



您可以选择以下任一选项来保护您的应用程序：

- **WAF 推荐扫描器** - 此选项使您能够对应用程序运行扫描。根据扫描的某些参数，结果会为您建议应用程序的保护措施。您可以考虑应用这些建议。
- **选择和自定义保护** - 此选项使您能够从不同的模板选项中进行选择，或自定义您的保护并进行部署。



  - **OWASP Top 10** - 一个预定义模板，包含针对 OWASP 十大安全风险的行业标准保护措施。有关更多信息，请参阅 `https://owasp.org/www-project-top-ten/`。
  - **CVE 保护** - 您可以从已知漏洞类别下分类的预配置签名规则列表中创建签名集。当签名模式与传入流量匹配时，您可以选择签名来配置日志或阻止操作。日志消息包含漏洞详细信息。
  - **自定义保护** - 根据您的要求选择并部署保护措施。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **选择现有保护** - 此选项克隆已部署在现有应用程序中的保护。如果您想将相同的保护部署到另一个应用程序，您可以选择此选项并按原样部署到另一个应用程序。您还可以选择此选项作为模板，修改保护，然后进行部署。

WAF 推荐扫描器

注意：

- 您一次只能为一个应用程序运行一个扫描。要为同一应用程序或不同应用程序启动新扫描，您必须等到上一个扫描完成。
- 您可以单击 **查看历史记录** 以查看过去扫描的历史记录和状态。您还可以单击 **查看报告**，然后稍后应用建议。

先决条件：

- NetScaler 实例必须是 13.0 41.28 或更高版本（用于安全检查）以及 13.0 或更高版本（用于签名）。
- 必须拥有高级许可证。
- 必须是负载均衡虚拟服务器。

要开始 WAF 推荐扫描，您必须提供以下信息：

1. 在 **扫描参数** 下：
   - **域名** – 指定一个有效的可访问 IP 地址或与应用程序关联的公共可访问域名。例如：`www.example.com`。
   - **HTTP/HTTPS 协议** – 选择应用程序的协议。
   - **流量超时** – 扫描期间单个请求的等待时间（以秒为单位）。该值必须大于 0。
   - **开始扫描的 URL** – 用于启动扫描的应用程序主页。例如，`https://www.example.com/home`。该 URL 必须是有效的 IPv4 地址。如果 IP 地址是私有的，则必须确保可以从 NetScaler Console 本地管理 IP 访问该私有 IP 地址。
   - **登录 URL** – 用于发送登录数据进行身份验证的 URL。在 HTML 中，此 URL 通常称为操作 URL。
   - **身份验证方法** – 为您的应用程序选择支持的身份验证方法（基于表单或基于标头）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - 基于表单的身份验证需要将表单与登录凭据一起提交到登录 URL。这些凭据必须以表单字段及其值的形式存在。然后，应用程序会共享用于在扫描期间维护会话的会话 Cookie。
  - 基于标头的身份验证需要在标头部分提供身份验证标头及其值。身份验证标头必须具有有效值，并用于在扫描期间维护会话。基于标头的身份验证应将表单字段留空。

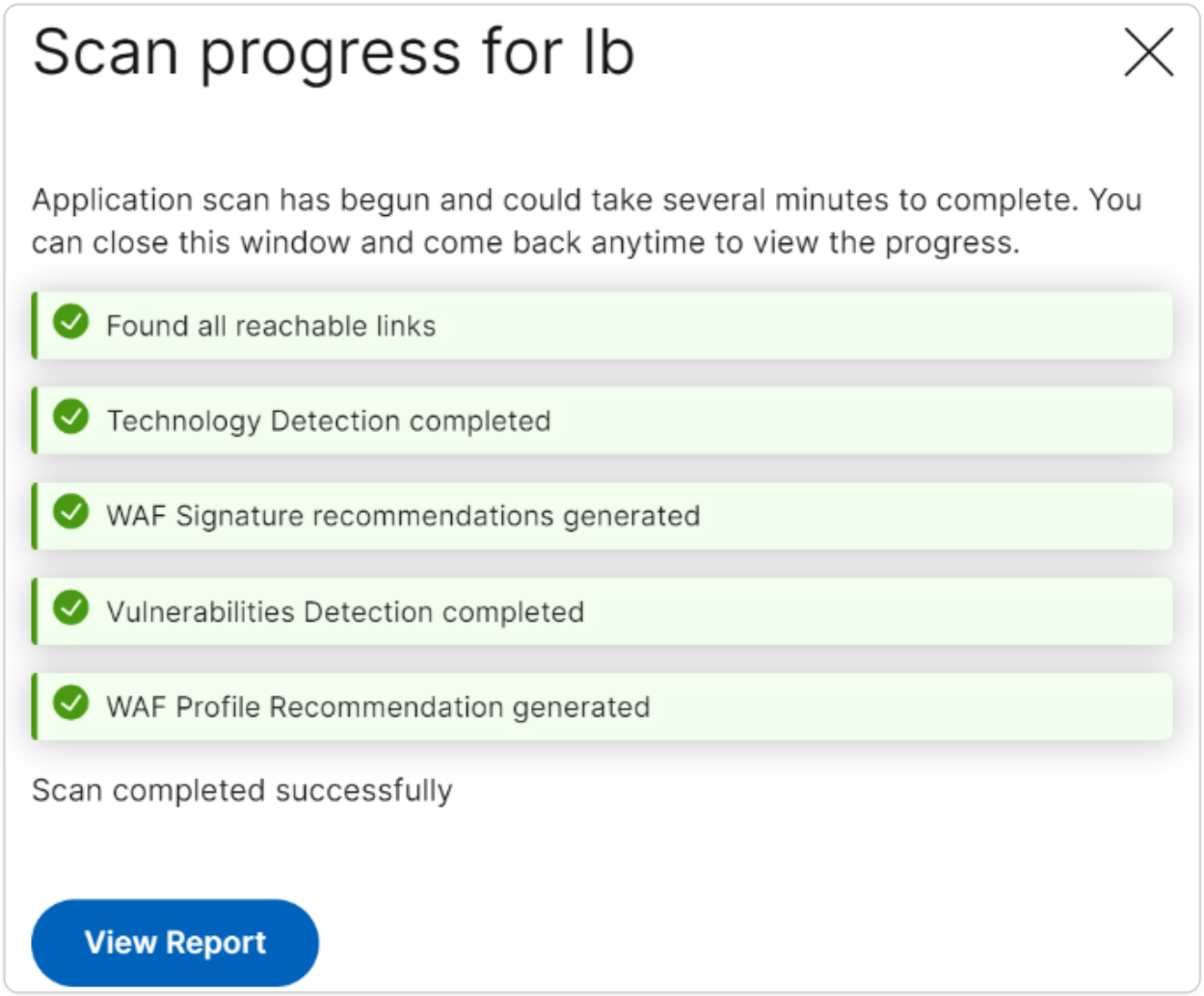
- **请求方法** – 选择向登录 URL 提交表单数据时使用的 HTTP 方法。允许的请求方法是 **POST**、**GET** 和 **PUT**。
- **表单字段** – 指定要提交到登录 URL 的表单数据。仅当您选择基于表单的身份验证时才需要表单字段。您必须以键值对的形式指定，其中 **字段名称** 是键，**字段值** 是值。确保正确添加了登录所需的所有表单字段，包括密码。这些值在存储到数据库之前会进行加密。您可以单击 **添加** 以添加多个表单字段。例如，**字段名称** – 用户名，**字段值** – admin。
- **注销 URL** – 指定访问后终止会话的 URL。例如：`https://www.example.com/customer/logout`。

2. 在**扫描配置**下：

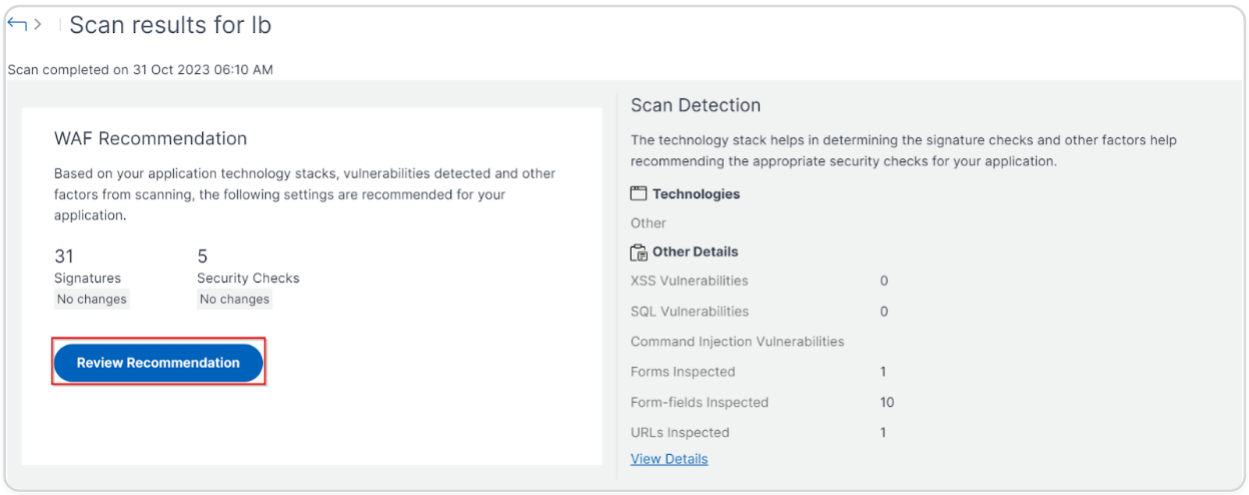
   - **要检查的漏洞** – 选择扫描程序要检测的漏洞。目前，这适用于 SQL 注入和跨站点脚本违规。默认情况下，所有违规都处于选中状态。选择漏洞后，它会在应用程序上模拟这些攻击，以报告潜在的漏洞。建议在非生产环境中启用此检测。所有其他漏洞也会被报告，而无需在应用程序上模拟这些攻击。
   - **响应大小限制** – 响应大小的最大限制。超出指定值的任何响应都不会被扫描。建议限制为 10 MB (1000000 字节)。
   - **请求并发** – 并行发送到 Web 应用程序的总请求数。

3. WAF 扫描设置配置已完成。您可以单击“**开始扫描**”以开始扫描过程并等待进度完成。扫描完成后，单击“**查看报告**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

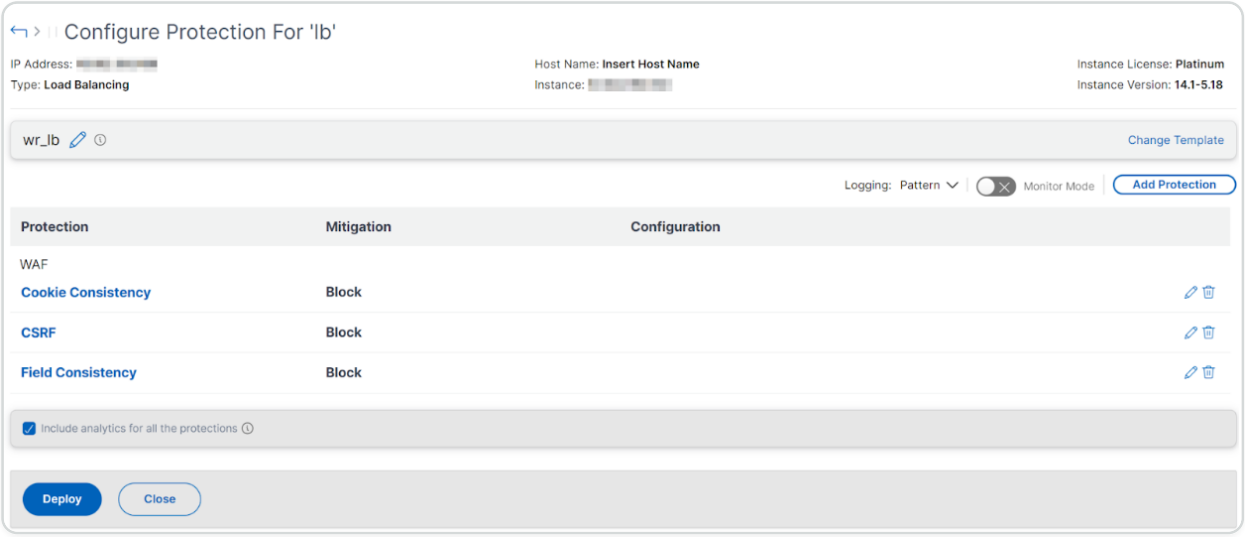


4. 在扫描结果页面中，单击“**查看建议**”。



5. 查看保护措施或编辑/添加任何其他保护措施，然后单击“**部署**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



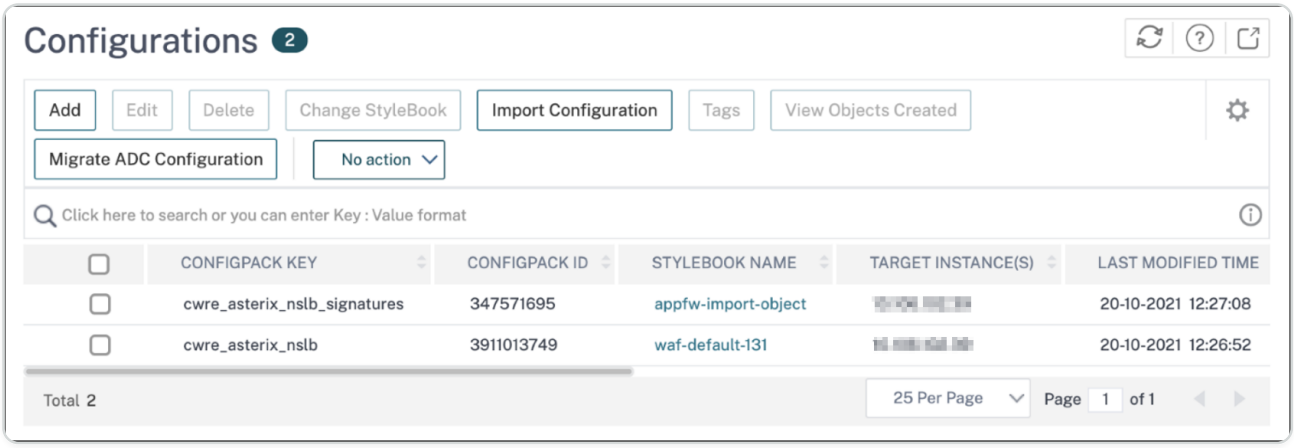
成功应用安全检查后：

- 配置通过 StyleBooks 应用于 NetScaler 实例，具体取决于版本。
  - 对于 NetScaler 13.0，使用 `unified-appsec-protection-130` StyleBook。
  - 对于 NetScaler 13.1，使用 `unified-appsec-protection-131` StyleBook。
  - 对于 NetScaler 14.1，使用 `unified-appsec-protection-141` StyleBook。
- 该 `Appfw` 配置文件在您的 NetScaler 上创建，并使用 `policylabel` 绑定到应用程序。
- 如果已应用推荐的签名，则签名将绑定到 appfw 配置文件。

注意

NetScaler 13.0 41.28 或更高版本支持安全检查。

您可以通过导航到 **应用程序 > 配置 > 配置包** 来验证 WAF 配置文件和签名是否已通过默认 StyleBooks 应用。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

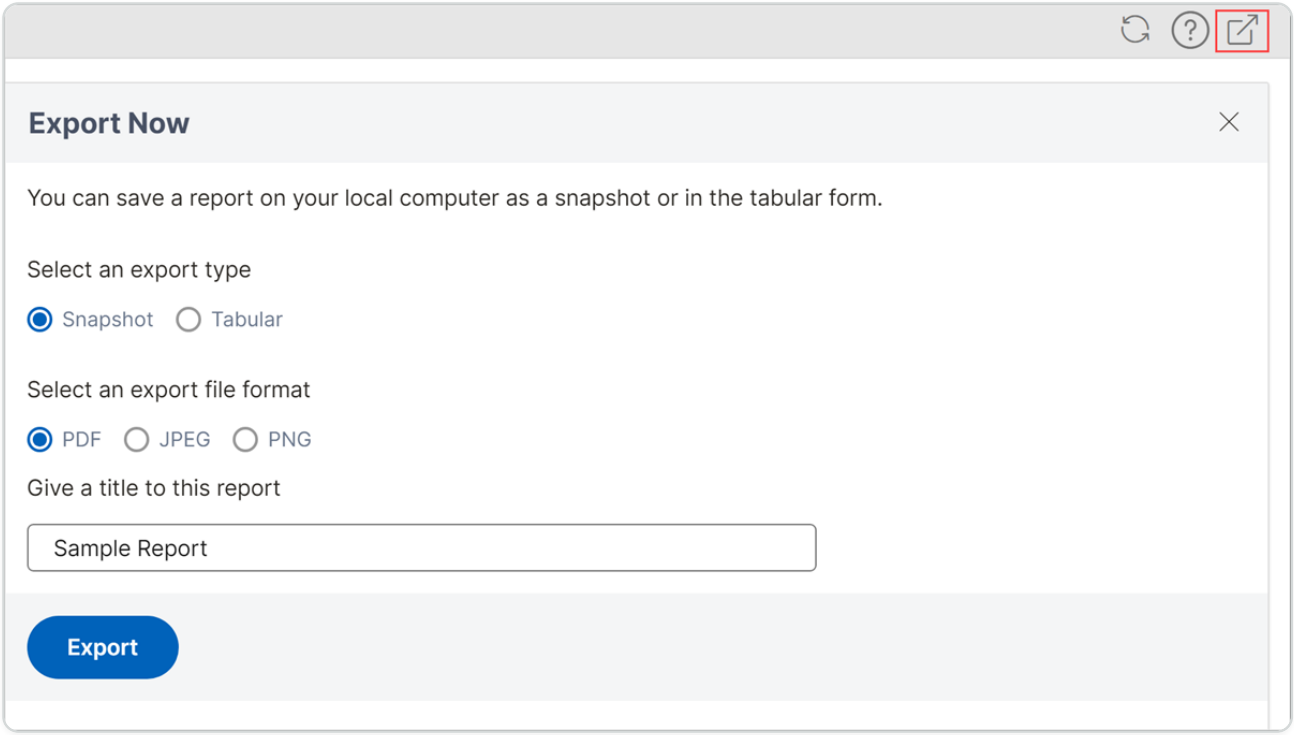
导出 WAF 扫描器报告

要导出 WAF 扫描器报告，请按照以下步骤操作：

1. 导航到 **安全 > 控制板 > 管理应用程序。**
2. 在 **未受保护的应用程序** 选项卡中，单击 **查看历史记录**。
3. 在 **扫描历史记录** 页面上，选择所需的扫描并单击 **查看报告**。
4. 在 **扫描结果** 页面上，单击 **导出** 图标。
5. 在 **立即导出** 页面上，选择导出类型。

对于 **快照** 导出类型：

1. 选择导出文件格式：PDF、JPG 或 PNG
2. 为报告输入标题。
3. 单击 **导出**。

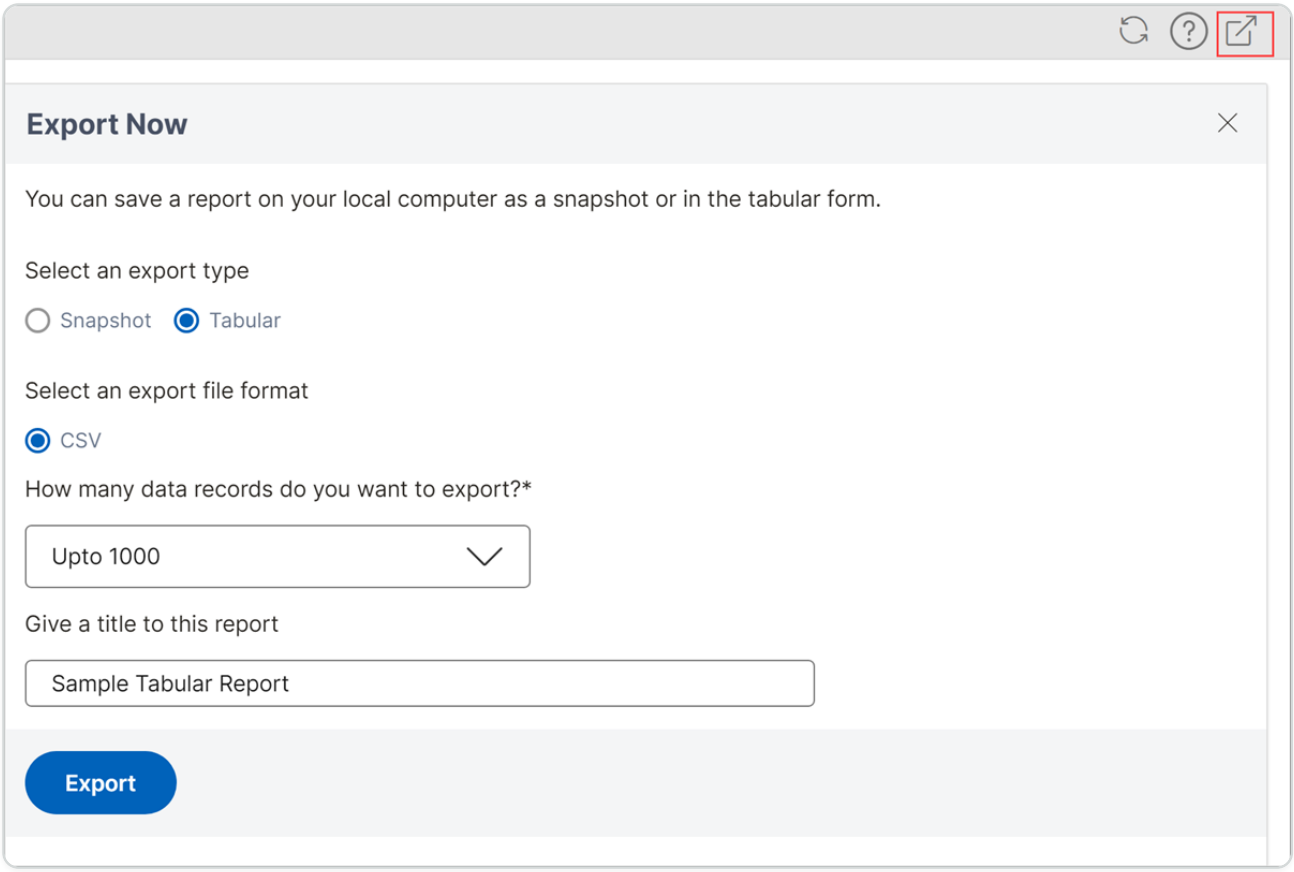


对于 **表格** 导出类型：

从版本 14.1 build 25.x 开始，您可以以表格格式导出 WAF 扫描器报告。

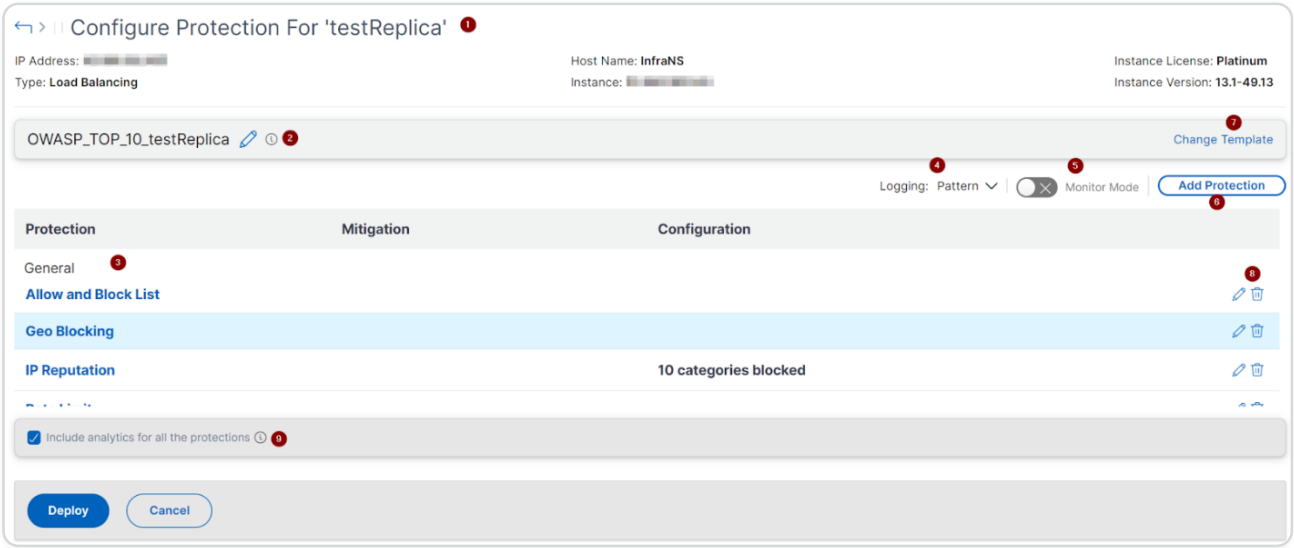
1. 选择 CSV 文件格式。
2. 从列表中选择要导出的数据记录数。
3. 为报告输入标题。
4. 单击 **导出**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



选择并自定义保护

OWASP 十大



1 - 提供有关应用程序的信息，例如 IP 地址、虚拟服务器类型、许可证类型、配置应用程序的实例等。

2 - 显示所选模板。您可以根据自己的选择重命名它。

3 - 显示防护。某些防护需要额外信息。

4 - 显示详细日志类型。您可以选择以下选项：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **模式**。仅记录违规模式。
- **模式有效负载**。记录违规模式和 150 字节的额外 JSON 有效负载。
- **模式、有效负载、标头**。记录违规模式、150 字节的额外 JSON 有效负载和 HTTP 标头信息。

5 - 允许您启用监视模式。如果启用监视模式，则仅记录流量，不激活缓解措施。

6 - 使您能够添加更多防护。单击“**添加防护**”并查看以添加。

7 - 允许您使用“更改模板”选项选择新模板。

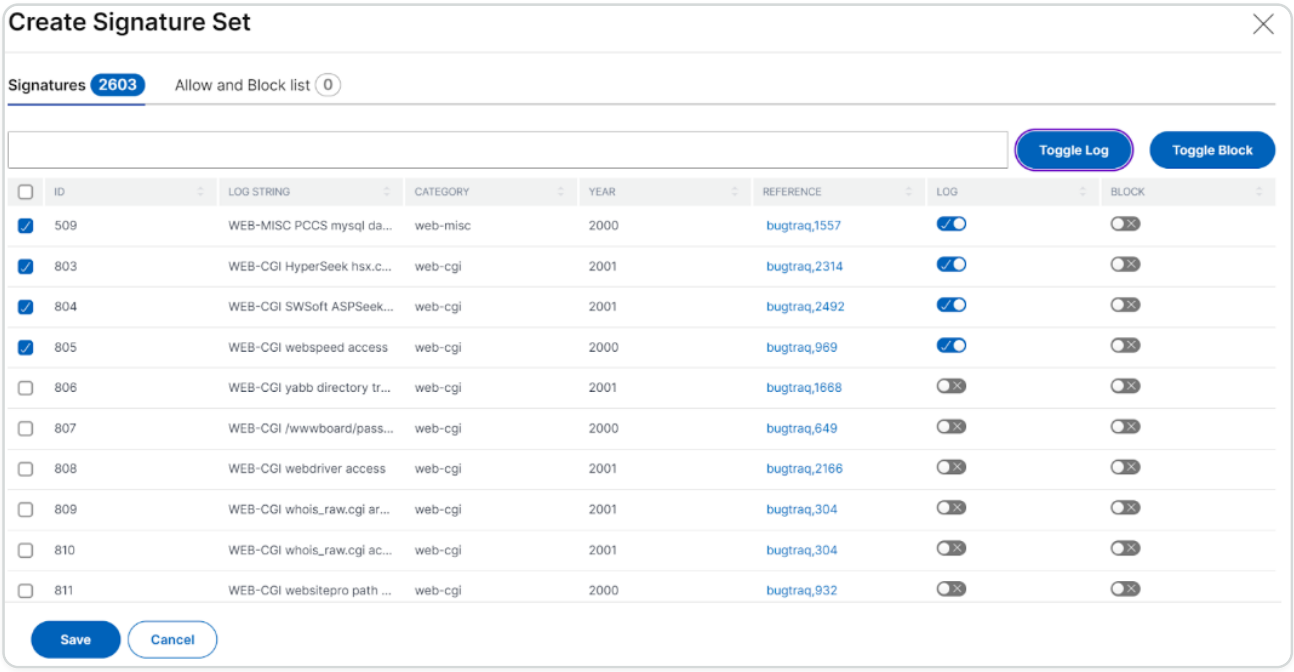
8 - 使您能够编辑或删除防护。

9 - 为您选择的防护启用分析。此选项默认处于选中状态。您可以在“**安全 > 安全违规**”处查看已配置防护的分析。

配置防护后，单击“**部署**”。

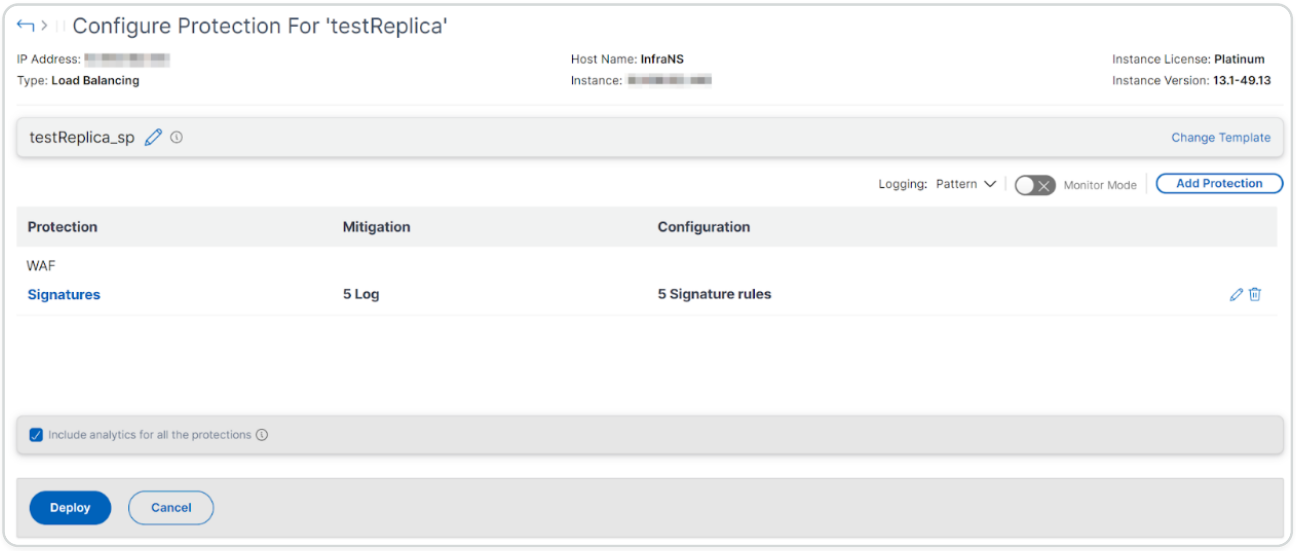
CVE 防护

要部署 CVE 防护，请单击“**创建 CVE 防护**”。在“**创建签名集**”页面中，从列表中选择签名以配置日志或阻止操作，然后单击“**保存**”。



单击“**保存**”后，您可以在配置页面中查看已添加的签名。

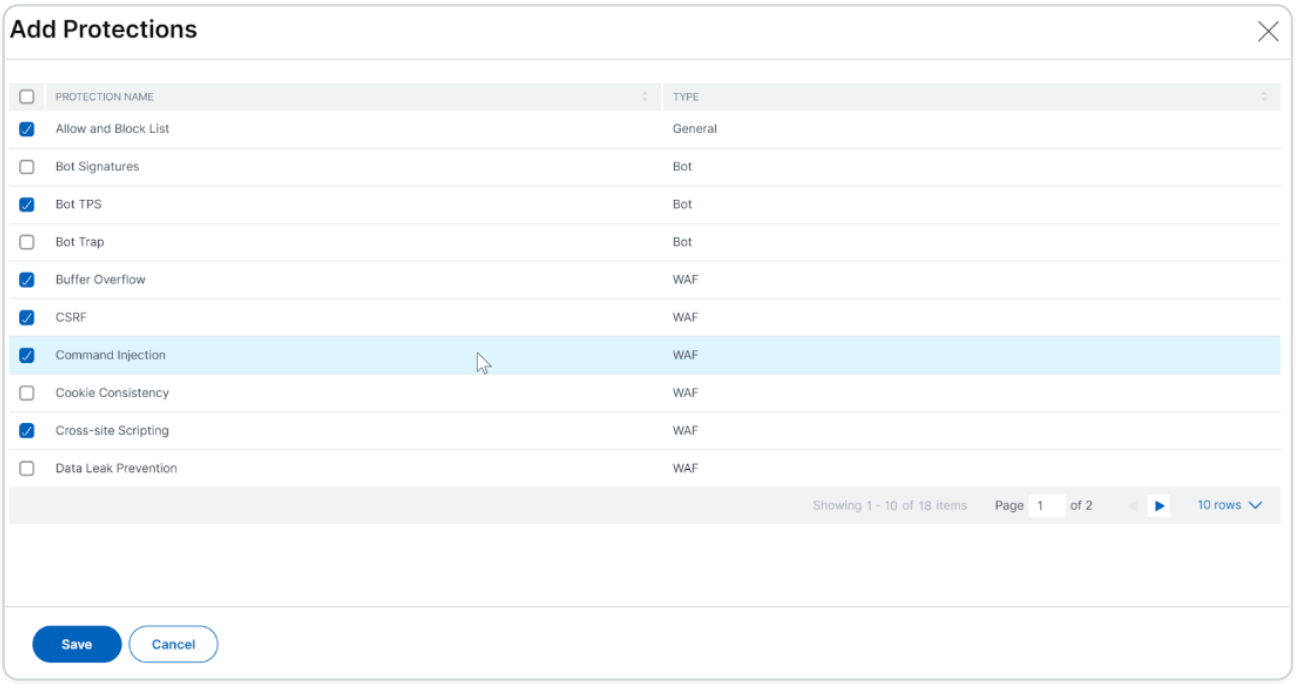
© 1997–2026 Citrix Systems, Inc. All rights reserved.



您还可以单击“**添加保护**”为应用程序添加更多保护。配置所有保护后，单击“**部署**”。

自定义保护

要根据您的要求部署保护，请单击“**创建新保护**”。在“**添加保护**”页面中，选择要部署的保护，然后单击“**保存**”。

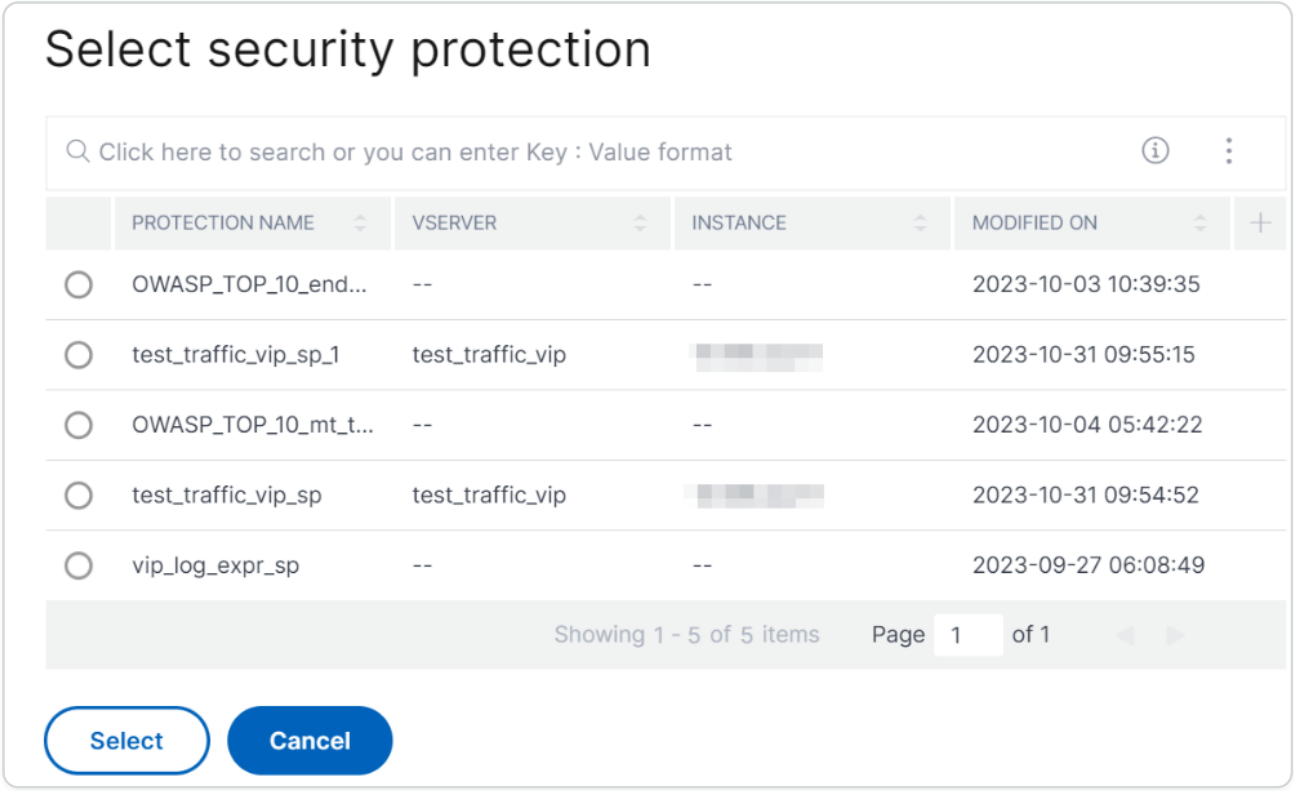


单击“**保存**”后，在配置页面中查看所选保护，然后单击“**部署**”。

选择现有保护

要将现有保护从一个应用程序部署到另一个应用程序，请从列表中选择一个现有保护。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



选择保护后，现有保护将被克隆并显示在配置页面中。您可以根据需要进行修改，然后单击“**部署**”。

查看应用程序安全违规详情

暴露在互联网上的Web应用程序已大幅度变得容易受到攻击。NetScaler Console 使您能够可视化可操作的违规详情，以保护应用程序免受攻击。导航到 **安全** > **安全违规**，以获取一个单一面板解决方案，用于：

- 可视化应用程序，全面了解WAF安全违规和Bot安全违规中相关的威胁详情
- 根据其类别（例如 **网络**、**Bot** 和 **WAF**）访问应用程序安全违规
- 采取纠正措施以保护应用程序

安全违规 页面包含以下选项：

- **应用程序概述** – 显示应用程序的概述，包括总违规数、WAF和Bot违规总数、按国家/地区划分的违规等。有关详细信息，请参阅应用程序概述。
- **所有违规** – 显示应用程序安全违规详情。有关详细信息，请参阅所有违规。

先决条件

确保已启用 **指标收集器**。有关详细信息，请参阅配置智能应用程序分析。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

API 安全

NetScaler Console API 安全提供对您的应用程序所服务的 API 流量的可见性，帮助您分析使用情况并发现暴露的 API 端点。以下主题可帮助您入门：

- 查看 API 分析
- 发现 API 端点

查看 API 分析

API 分析可让您深入了解 API 流量。此分析允许 IT 管理员监控 API 网关提供的 API 实例和端点。它提供对 API 请求的集成式定期监控。

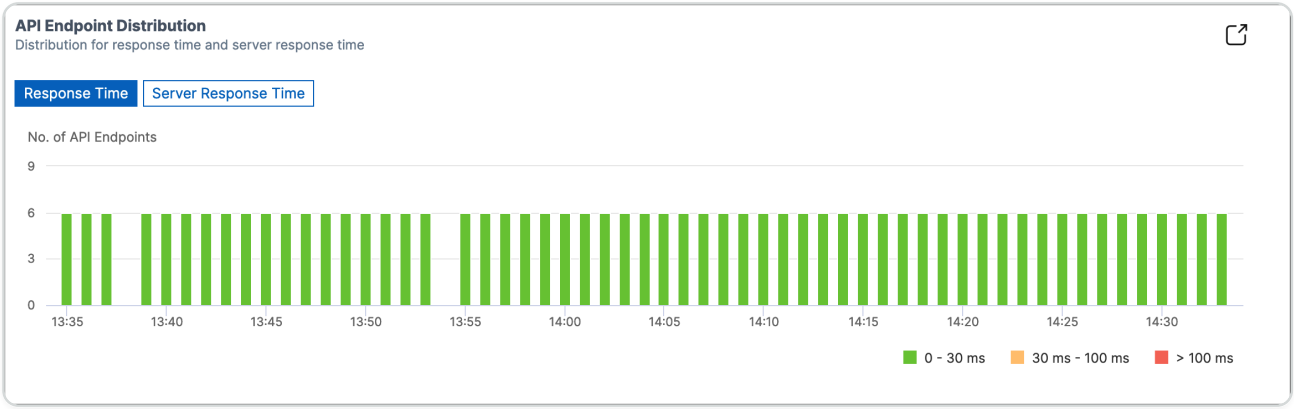
在监控 API 分析之前，请确保在 API 实例上启用 Web Insight。有关详细信息，请参阅在虚拟服务器上配置分析。

在**API 分析**中，您可以监控作为 API 定义一部分添加的 API 实例和端点的响应时间。它还显示 API 实例和端点消耗的带宽。

默认情况下，仪表板显示过去一小时的 API 分析。您可以选择一个持续时间来查看该时间间隔的 API 分析。单击每个磁贴上的**查看更多**以查看整个列表。在此视图中，您可以按 API 实例和端点的部分名称进行搜索，但**地理位置**磁贴除外。

API 端点分布

此图显示了 API 端点的应用程序和服务器响应时间分布。您可以识别响应时间过长的 API 端点并采取必要的措施。



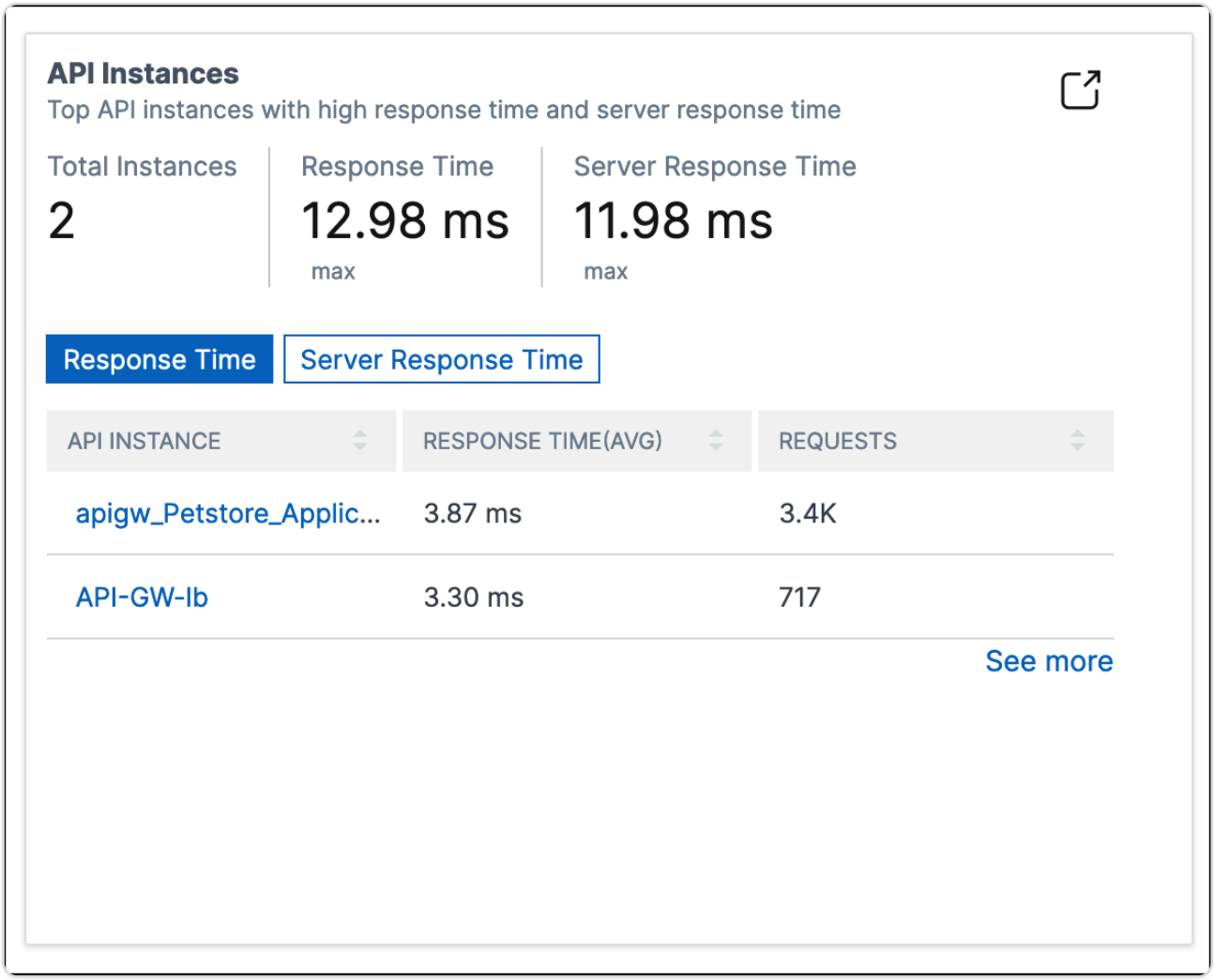
API 端点根据其响应时间限制显示为以下颜色之一：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **绿色** – 如果响应时间小于 30 毫秒。
- **橙色** – 如果响应时间介于 30–100 毫秒之间。
- **红色** – 如果响应时间超过 100 毫秒。

API 实例

API 实例磁贴显示应用程序和服务器响应时间较高的顶级 API 实例。



选择一个 API 实例以查看其性能、使用情况和安全详细信息。所选的 API 实例显示以下信息：

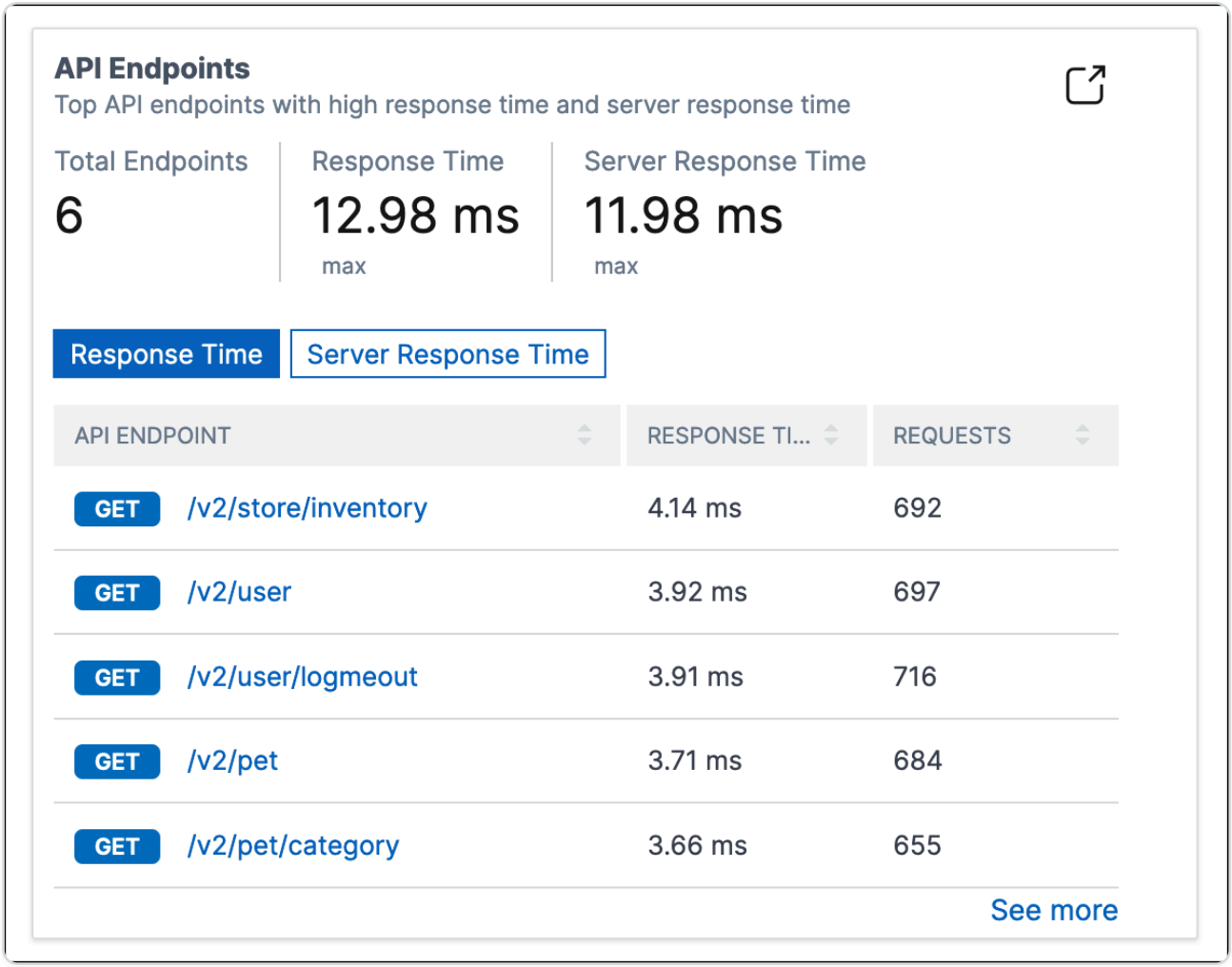
- API 端点计数
- 请求计数
- 应用程序和服务器响应时间
- 消耗的带宽
- 身份验证失败

© 1997–2026 Citrix Systems, Inc. All rights reserved.

API Endpoints	Requests	Response Time	Server Response Time	Bandwidth	Auth Failures
5	3.5K	3.88 ms	1.98 ms	3.04 MB	0

API 端点

API 端点磁贴显示应用程序和服务器响应时间较高的热门端点。

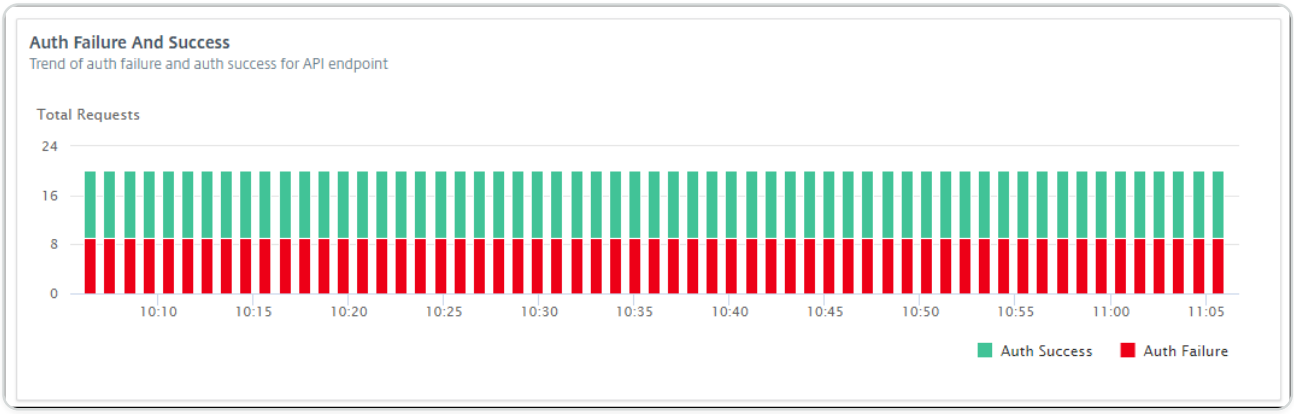


选择一个 API 端点以查看性能、使用情况和安全详细信息。

身份验证失败

身份验证失败磁贴显示身份验证失败次数较多的热门 API 端点。身份验证的失败或成功取决于添加到 API 定义的策略。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



如果您想查看 API 端点中的身份验证失败和成功率，请执行以下操作：

1. 从 **API 端点**中选择一个端点。
2. 选择**安全**选项卡。此选项卡显示所选端点中的身份验证失败和成功情况。

如果您想查看实例的 API 端点中的身份验证失败和成功率，请执行以下操作：

1. 从 **API 实例**中选择一个实例。
2. 选择**安全**选项卡。此选项卡显示所选实例的端点中的身份验证失败和成功情况。

查看不同的 API 洞察

浏览 API 分析以查看以下特定信息：

- 实例中的热门 API 端点
- 访问最多的 API
- 端点的地理位置
- HTTPS 响应状态

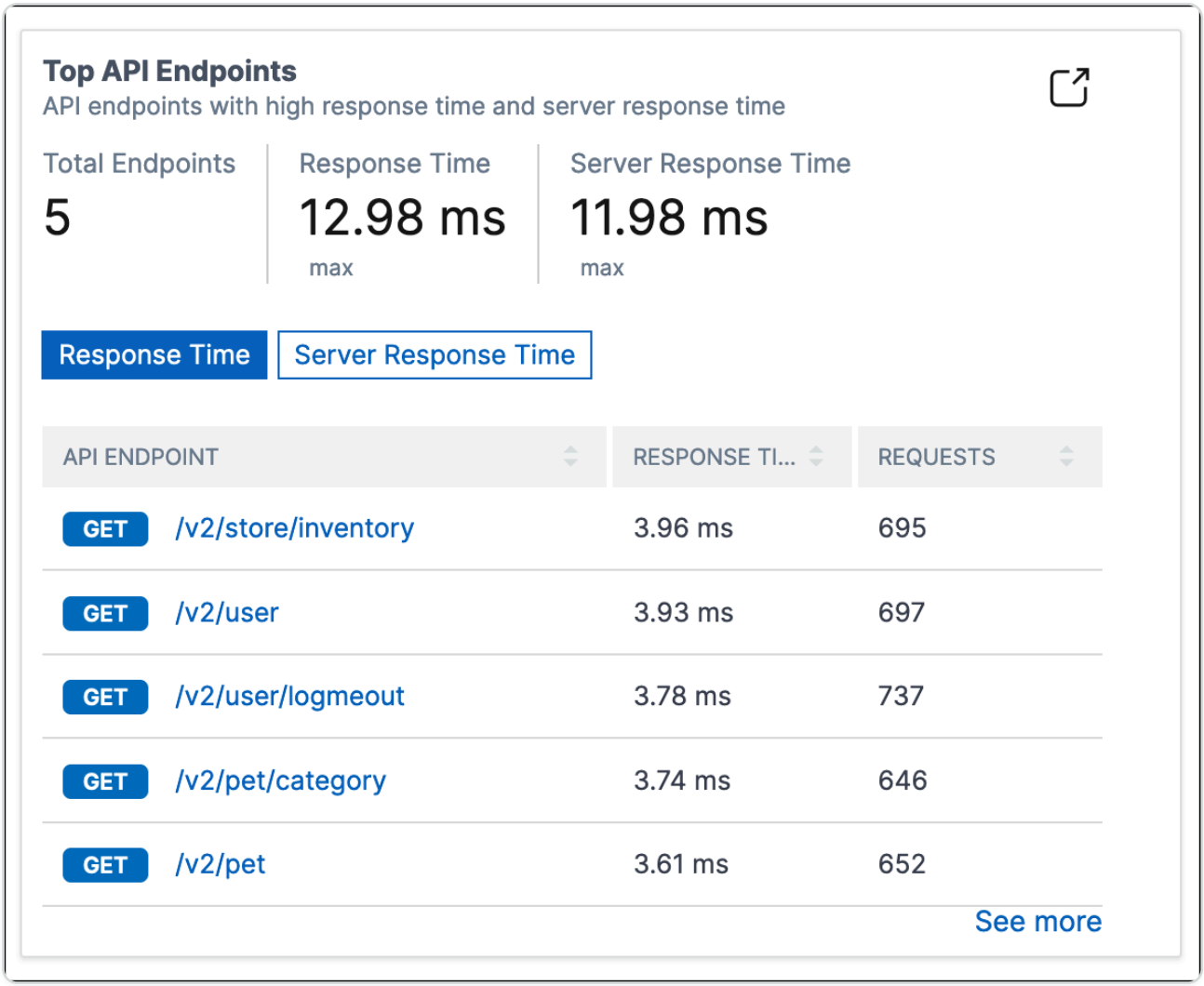
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- API 请求趋势
- 端点的带宽消耗
- SSL 错误和使用情况

查看实例中的热门 API 端点

API 分析页面显示响应时间较高的热门端点。如果要查看实例的类似端点，请从**API 实例**中选择一个实例。

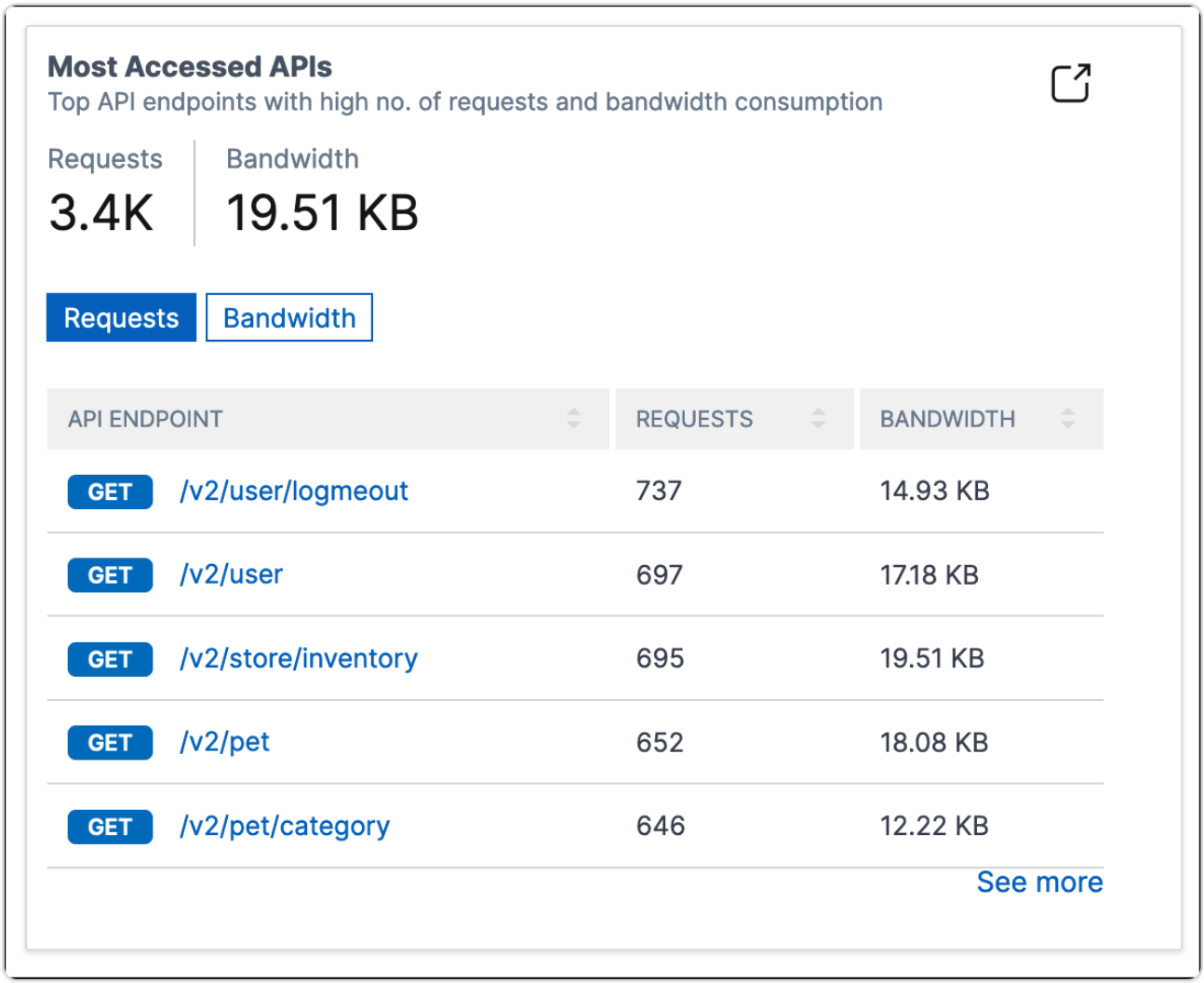
热门 API 端点磁贴显示应用程序和服务器响应时间较高的端点。



查看访问量最大的 API

在**API 分析**中，从 API 实例中选择一个 API 实例。**访问量最大的 API**磁贴显示请求和带宽较多的热门端点。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

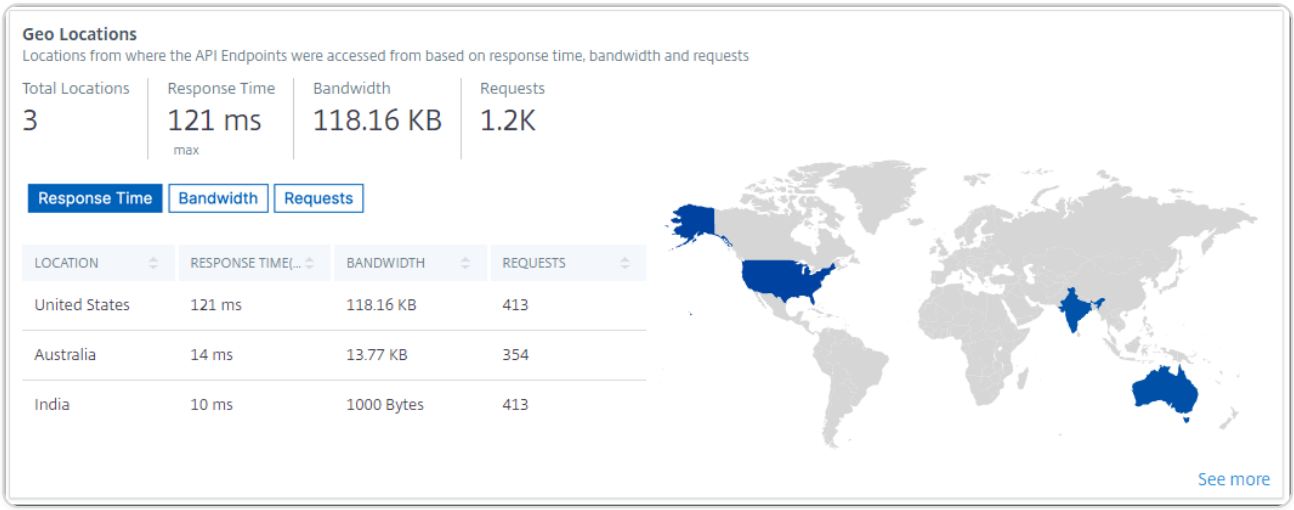


查看端点的地理位置

1. 在**API 分析**中，选择以下任意一项：
   - 从**API 实例**中选择一个实例，以查看所选实例的端点接收请求的位置。
   - 从**API 端点**中选择一个端点，以查看该端点接收请求的位置。
2. 在**性能和使用情况**中，将显示**地理位置**磁贴。

   您可以根据响应时间、带宽和请求对位置进行排序。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

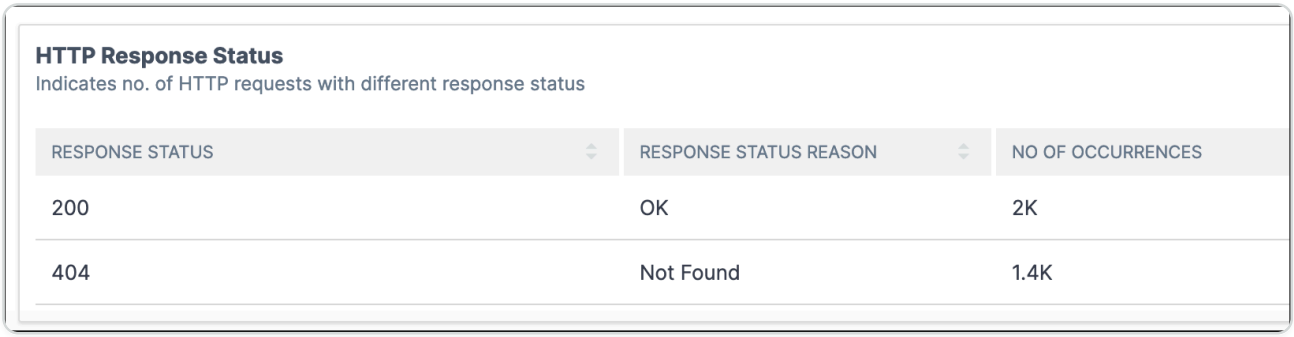


查看 HTTPS 响应状态

HTTPS 响应状态磁贴显示响应状态及其原因和发生次数。您可以通过以下方式之一查看 HTTPS 响应状态：

- 从 **API 实例**中选择一个实例。
- 从 **API 端点**中选择一个端点。

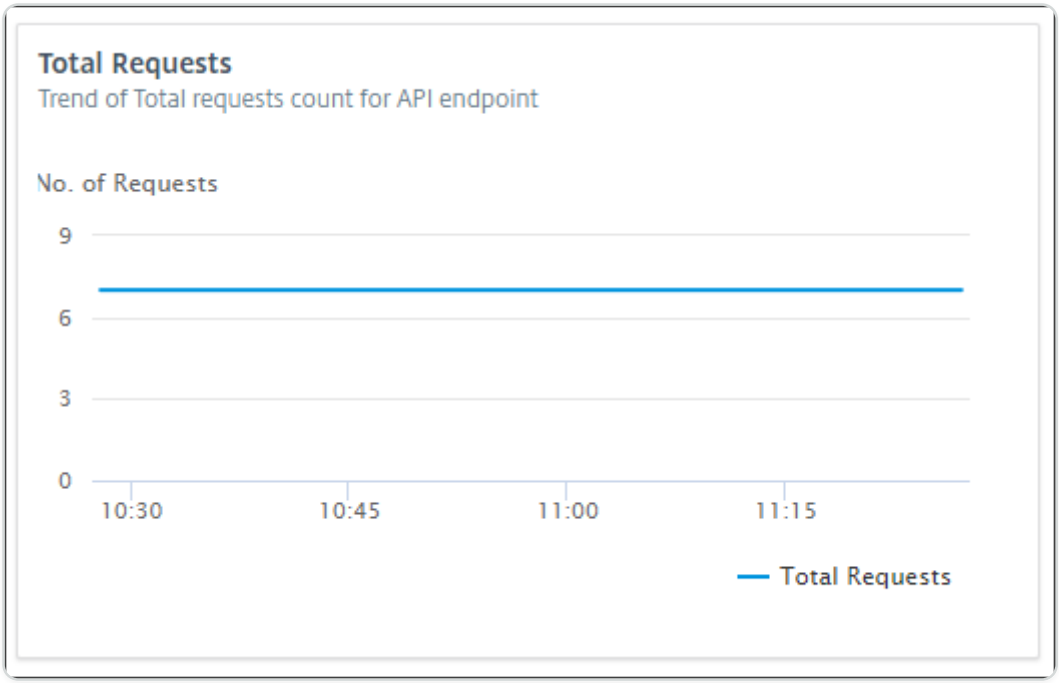
此磁贴显示在**性能和使用情况**选项卡中。



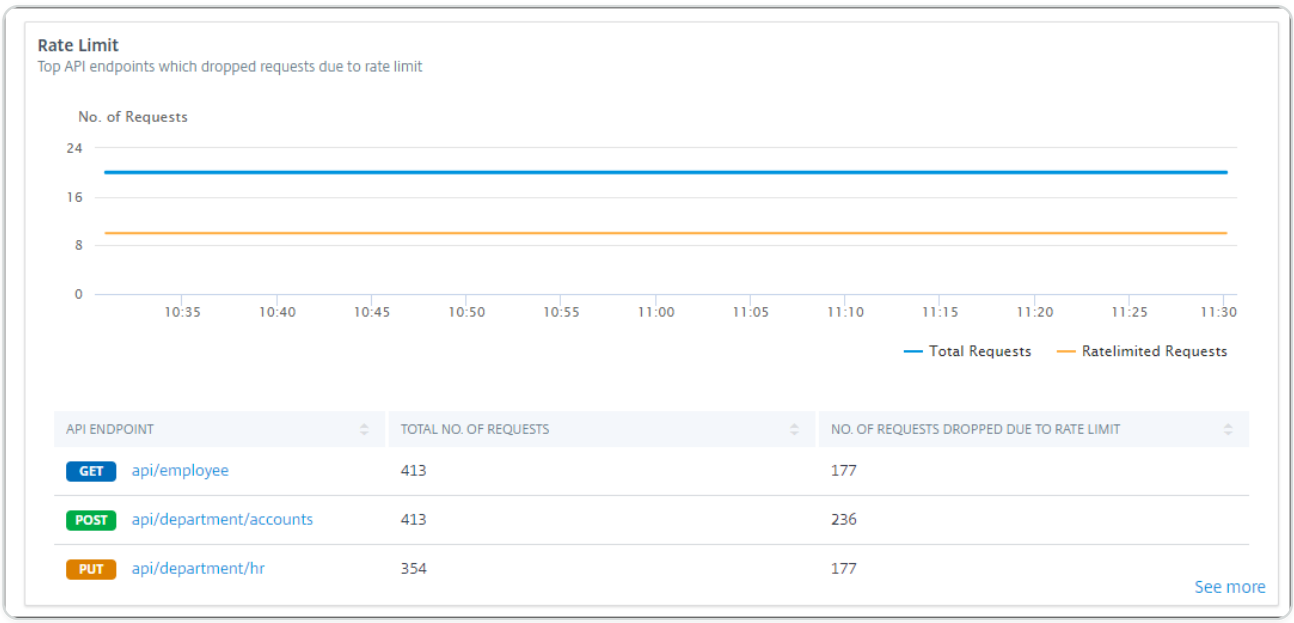
查看 API 请求趋势

从 **API 端点**中选择一个端点。在**性能和使用情况**中，**总请求数**磁贴显示端点收到的总请求数的趋势。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



如果要查看因速率限制而丢弃的请求趋势，请从 **API 实例**中选择一个实例。在**安全**中，**速率限制**磁贴显示丢弃请求的趋势。它还显示端点收到的总请求数的趋势。

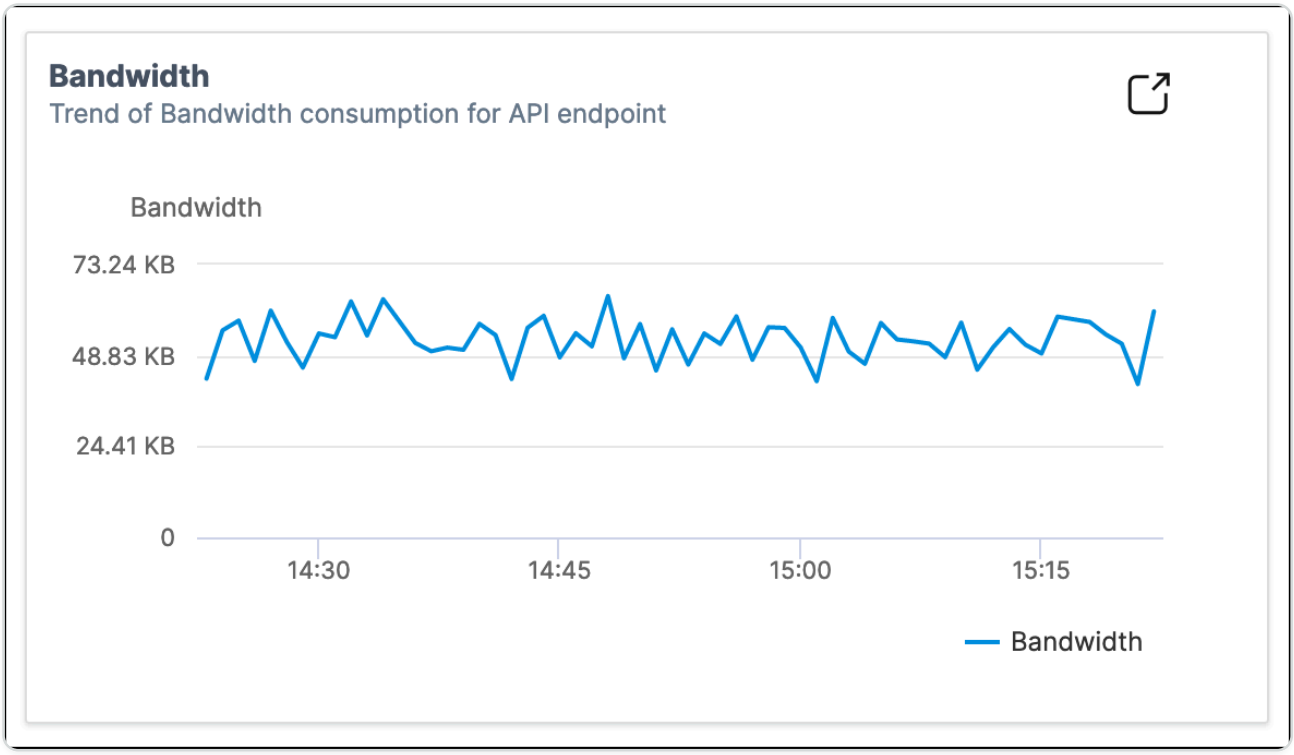


通过此比较，您可以确定在总请求中，有多少请求因速率限制而被丢弃。

查看端点的带宽消耗

要查看端点的带宽消耗趋势，请从 API 端点中选择一个端点。**带宽**磁贴显示带宽消耗图。

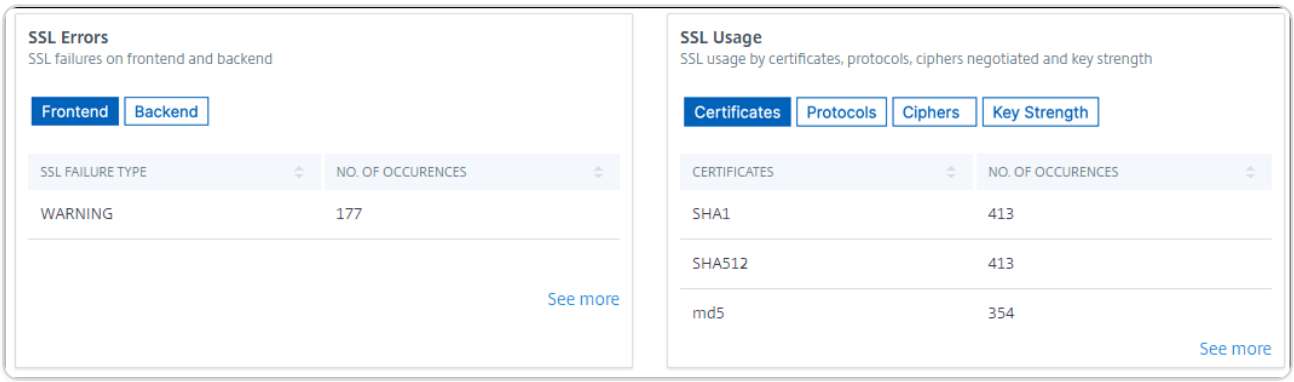
© 1997–2026 Citrix Systems, Inc. All rights reserved.



查看 SSL 错误和使用情况

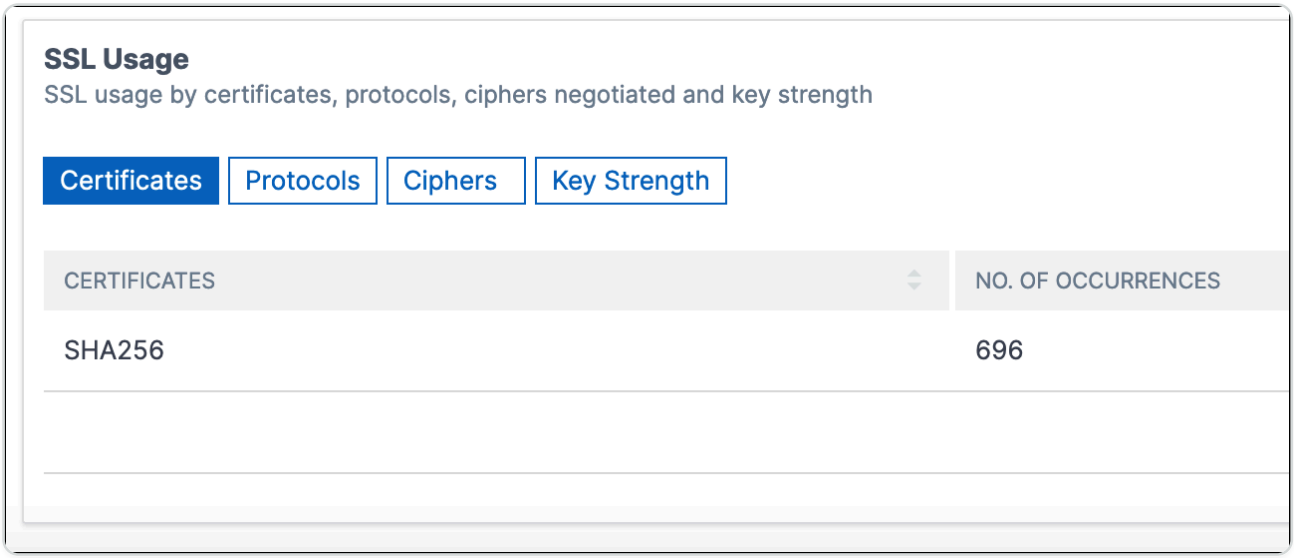
从 **API 实例**中选择一个实例。在**安全**中，显示以下磁贴：

- **SSL 错误** – 显示发生在客户端和应用程序服务器上的 SSL 故障。
- **SSL 使用情况** – 显示 SSL 证书、协议、密码和密钥强度及其出现次数。



要查看端点中的 SSL 使用情况，请从 API 端点中选择一个端点。**SSL 使用情况**磁贴显示在**安全**选项卡中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



发现 API 端点

使用 API 安全功能查看组织中发现的 API 端点。NetScaler Console 根据 NetScaler 实例上收到的 API 流量发现 API 端点。

在 NetScaler Console 中，**安全 > API 安全 > API 发现** 页面显示发现的 API 端点。

VServers 选项卡显示来自您的 NetScaler 实例的虚拟服务器。当虚拟服务器在指定期间内收到 API 请求时，它们会在此选项卡中显示。

注意：

确保配置分析并在虚拟服务器上启用 Web Insights。请参阅 在 API 实例上启用 Web Insight。

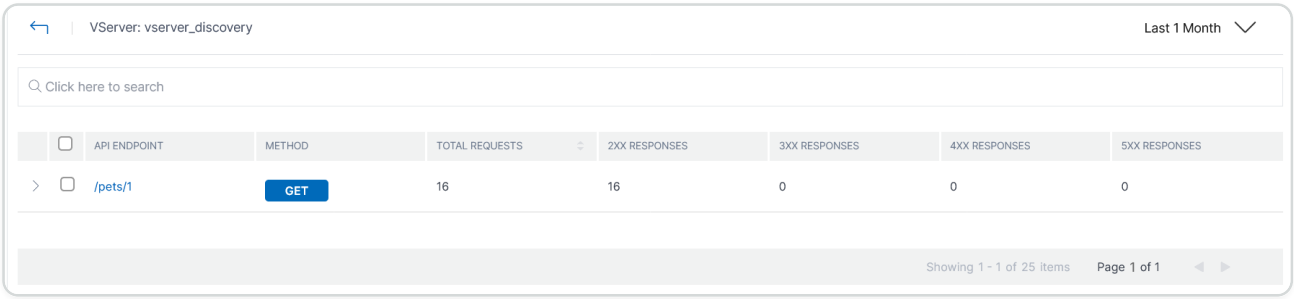
查看 API 端点

在 **API 发现** 中，当您选择一个虚拟服务器时，NetScaler Console GUI 会显示 API 端点及其详细信息，例如：

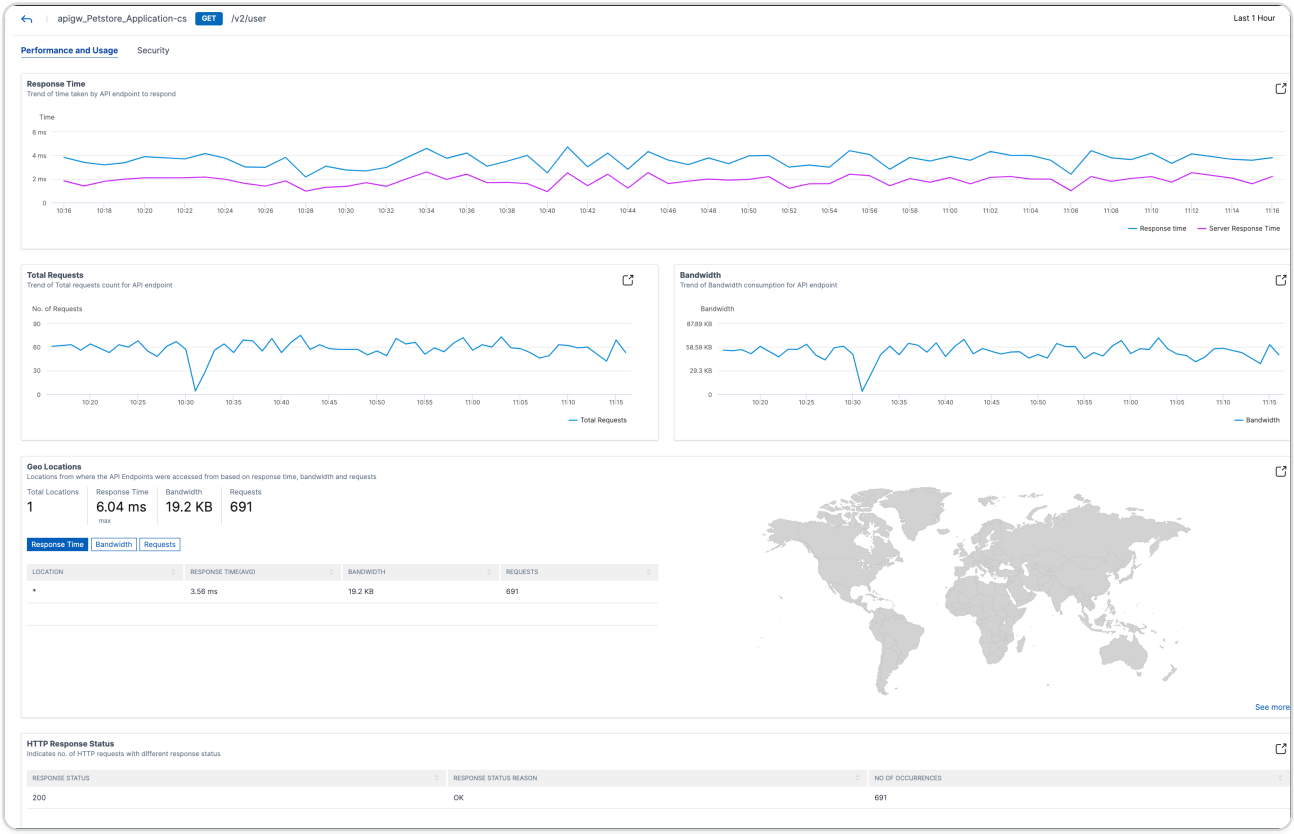
- **方法** - 它显示 API 端点中使用的方法。例如，`GET` 和 `POST` 方法。
- **总请求数** - 它显示 API 端点上的 API 请求计数。
- **响应状态** - 它显示每个响应状态的计数。例如，`2xx`、`3xx`、`4xx` 和 `5xx`。

虚拟服务器中的 API 端点可用情况如下：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您还可以选择所需的 API 端点以查看其详细分析报告。



有关每个部分的更多信息，请参阅查看 API 分析。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

网关

NetScaler Console 提供网关分析，让您了解通过 NetScaler Gateway 提供的流量的性能和用户体验。以下主题可帮助您监控和排查网关流量：

- 网关洞察
- HDX 洞察

网关洞察

在 NetScaler Gateway 部署中，用户访问详细信息的可见性对于排查访问失败问题至关重要。作为网络管理员，您希望了解用户何时无法登录 NetScaler Gateway，并希望了解用户活动和登录失败的原因。除非用户发送解决请求，否则此信息通常不可用。

Gateway Insight 提供所有用户在登录 NetScaler Gateway 时遇到的故障的可见性，无论访问模式如何。您可以随时查看所有可用用户列表、活动用户数、活动会话数以及所有用户使用的字节数和许可证。您可以查看用户的端点分析 (EPA)、身份验证、单点登录 (SSO) 和应用程序启动失败。您还可以查看用户的活动会话和已终止会话的详细信息。

Gateway Insight 还提供虚拟应用程序的应用程序启动失败原因的可见性。这增强了您排查任何类型的登录或应用程序启动失败问题的能力。您可以查看启动的应用程序数量、总会话数和活动会话数、总字节数以及应用程序消耗的带宽。您可以查看应用程序的用户、会话、带宽和启动错误的详细信息。

您可以随时查看与 NetScaler Gateway 设备关联的所有网关使用的网关数量、活动会话数、总字节数和带宽。您可以查看网关的 EPA、身份验证、单点登录和应用程序启动失败。您还可以查看与网关关联的所有用户的详细信息及其登录活动。

所有日志消息都存储在 NetScaler Console 数据库中，因此您可以查看任何时间段的错误详细信息。您还可以查看登录失败摘要，并确定登录过程的哪个阶段发生了故障。

注意事项

- Gateway Insight 支持以下部署：
  - 访问网关
  - 统一网关

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Console 版本和内部版本必须与 NetScaler Gateway 设备相同或更高。
- 具有高级许可证的 NetScaler 实例可以查看一小时的 Gateway Insight 报告。必须拥有高级许可证才能查看超过一小时的 Gateway Insight 报告。

限制

- 当身份验证方法配置为基于证书的身份验证时，NetScaler Gateway 不支持 Gateway Insight。
- 对于 Gateway Insight 报告，NetScaler 设备不提供地理位置信息。
- 成功的用户登录、延迟以及虚拟 ICA 应用程序和桌面的应用程序级别详细信息仅在 HDX™ Insight 用户仪表板上可见。
- 在双跳模式下，无法查看第二 DMZ 中 NetScaler Gateway 设备上的故障。
- 不报告远程桌面协议 (RDP) 桌面访问问题。
- Gateway Insight 支持以下身份验证类型。如果使用这些类型之外的其他身份验证类型，您可能会在 Gateway Insight 中看到一些差异。
  - 本地
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - 本机 OTP
  - OAuth-OpenID 连接

    对于 OAuth-OpenID Connect 身份验证，NetScaler 可以充当 OAuth-OpenID Connect 依赖方 (RP) 或 OAuth-OpenID Connect 身份提供商 (IdP)。身份验证成功后，用户名会在 Gateway Insight 报告的“用户”选项卡下报告。但是，您无法识别会话是在 IdP 还是 RP 上创建的。

    注意： OAuth-OpenID Connect 身份验证从 NetScaler Console 13.1 版本 4.xx 及更高版本开始支持。

启用 网关洞察

要为您的 NetScaler Gateway 设备启用 Gateway Insight，您必须首先将 NetScaler Gateway 设备添加到 NetScaler Console。然后，您必须为表示 VPN 应用程序的虚拟服务器启用 AppFlow。有关将设备添加到 NetScaler Console 的信息，请参阅“添加设备”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

要在 NetScaler Console 中查看端点分析 (EPA) 故障，您必须在 NetScaler Gateway 设备上启用 AppFlow 身份验证、授权和审计用户名 日志记录。

如果您的 NetScaler Console 版本为 **13.0 Build 36.27**，则以下启用网关洞察的步骤适用：

1. 导航到 **Infrastructure > Instances**，然后选择要为其启用 AppFlow 的实例。
2. 从 **Select Action** 列表中，选择 **Configure Analytics**。
3. 在 **Configure Insight** 页面中，在 **Configure Analytics** 下，选择 **NetScaler Gateway**。
4. 选择虚拟服务器，然后单击 **Enable AppFlow**。
5. 在 **Enable AppFlow** 屏幕上，在 **Select Expression** 列表中，单击 true。
6. 在 **Transport Mode** 旁边，选择 **Logstream** 复选框。

   注意

   您可以选择 **IPFIX** 或 **Logstream** 作为传输模式。

   有关 **IPFIX** 和 **Logstream** 的更多信息，请参阅 **Logstream 概述**。
7. 单击 **OK**。

对于 NetScaler Console 版本 13.0 Build 41.x 或更高版本

1. 导航到 **Infrastructure > Instances**，然后选择实例。
2. 从 **选择操作** 列表中，选择 **配置分析**。
3. 选择虚拟服务器，然后单击 **启用分析**。
4. 在 **高级选项** 下：
   a. 选择 **Logstream**
   b. 选择 **NetScaler Gateway**
5. 单击 **确定**。

使用 GUI 在 NetScaler Gateway 设备上启用 AppFlow 身份验证、授权和审计用户名日志记录

1. 导航到 **配置 > 系统 > AppFlow > 设置**，然后单击 **更改 AppFlow 设置**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 在 **Configure AppFlow Settings** 屏幕中，选择 **AAA Username**，然后单击 **确定**。

查看 Gateway Insight 报告

在 NetScaler Console 中，您可以查看与 NetScaler Gateway 设备关联的所有用户、应用程序和网关的报告，并且可以查看特定用户、应用程序或网关的详细信息。在 **概述** 部分，您可以查看 EPA、SSO、身份验证和应用程序启动失败。您还可以查看用户登录所使用的不同会话模式、客户端类型以及每小时登录用户数的摘要。

注意

创建组时，您可以为组分配角色，为组提供应用程序级访问权限，并将用户分配给组。NetScaler Console 分析现在支持基于虚拟 IP 地址的授权。您的用户现在可以查看所有 Insights 的报告，但仅限于他们被授权访问的应用程序（虚拟服务器）。有关组以及如何将用户分配给组的更多信息，请参阅 配置组。

查看 EPA、SSO、身份验证、授权和应用程序启动失败

1. 在 NetScaler Console 中，导航到 **Gateway > Gateway Insight**。
2. 选择您要查看用户详细信息的时间段。您可以使用时间滑块进一步自定义所选时间段。单击“**Go**”。
3. 单击 EPA（端点分析）、身份验证、授权、SSO（单点登录）或应用程序启动选项卡以显示故障详细信息。

   单击 EPA 查看故障详细信息(/en-us/netscaler-application-delivery-management-software/media/gateway-insight-reports-failure.png)

查看会话模式、客户端和用户数量的摘要

在 NetScaler Console 中，导航到“**Gateway > Gateway Insight**”，向下滚动以查看报告。

网关洞察页面(/en-us/netscaler-application-delivery-management-software/media/gateway-insight-reports-summary.png)

活动图(/en-us/netscaler-application-delivery-management-software/media/gateway-insight-reports-logon-activity.png)

查看用户的 Gateway Insight 报告

您可以查看以下报告：

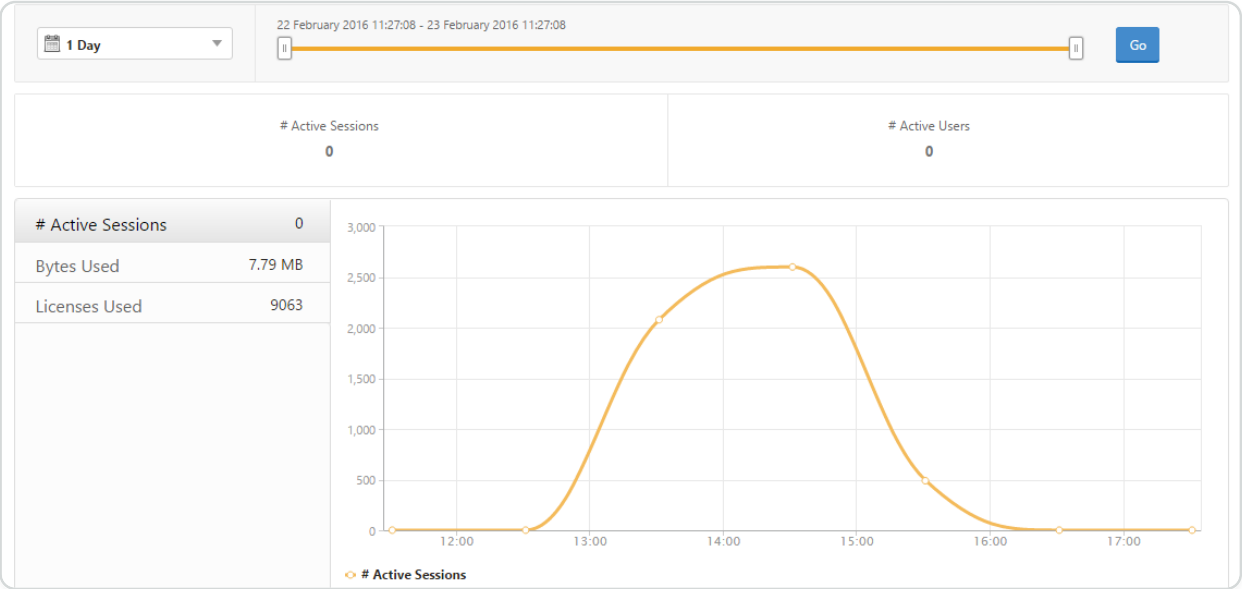
- 与 NetScaler Gateway 设备关联的所有用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

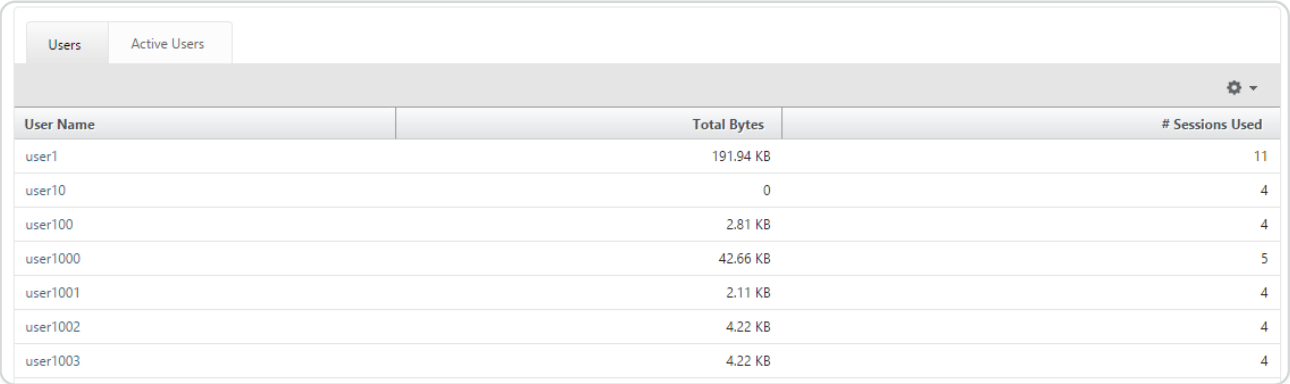
- 用户的 EPA、身份验证、SSO 和应用程序启动故障。
- 用户的活动会话和已终止会话的详细信息。
- 会话模式的类型，例如完全隧道、无客户端 VPN 和 ICA® 代理。

查看用户详细信息

1. 在 NetScaler Console 中，导航到 **网关 > Gateway Insight > 用户**。
2. 选择您要查看用户详细信息的时间段。您可以使用时间滑块进一步自定义所选时间段。单击 **Go**。
3. 您可以查看在此时间段内所有用户使用的活动用户数、活动会话数、字节数和许可证数。



向下滚动以查看可用用户和活动用户的列表。



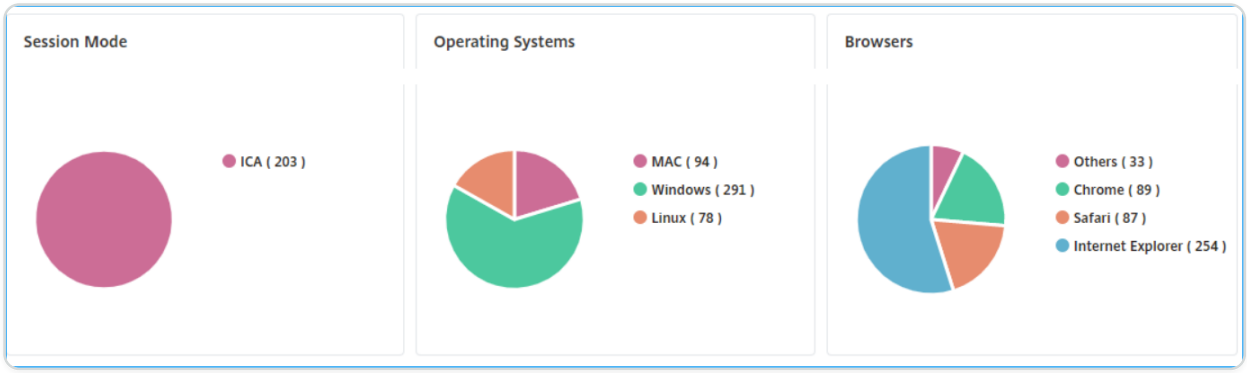
Users | Active Users

User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

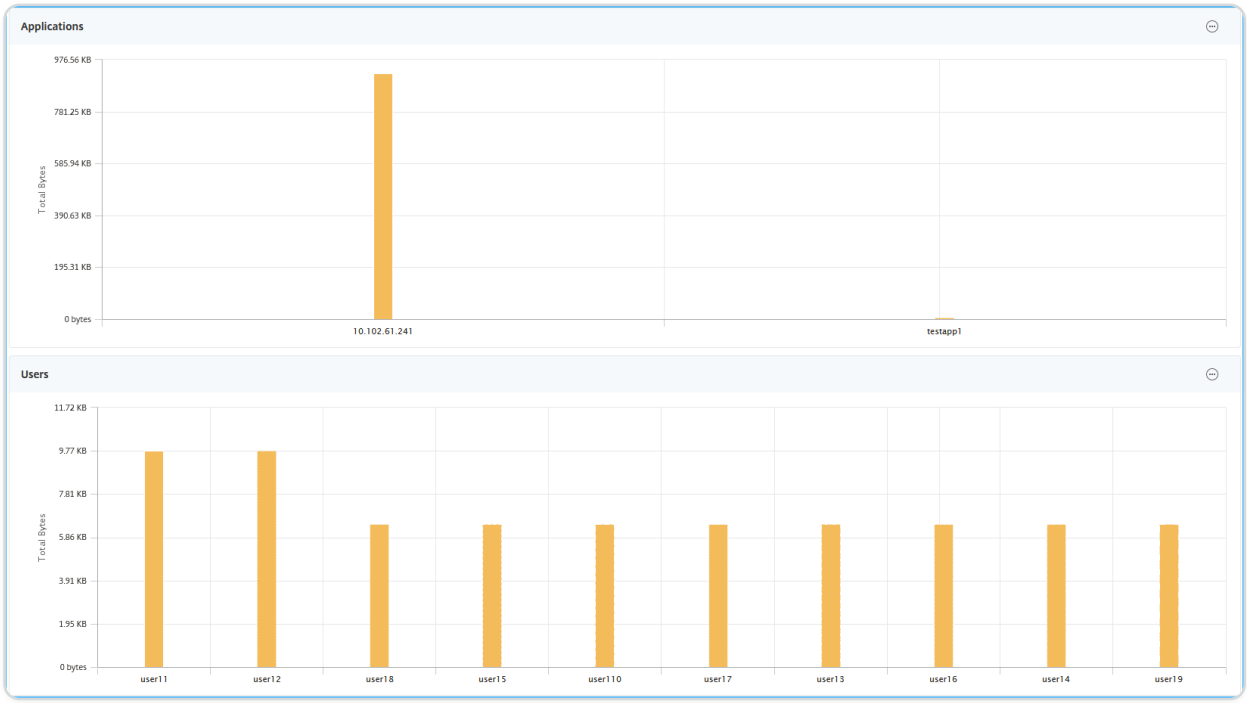
在 **Users** 或 **Active Users** 选项卡上，单击用户以查看以下用户详细信息：

- **用户详细信息** - 您可以查看与 NetScaler Gateway 设备关联的每个用户的洞察。导航到 **Gateway** > **Gateway Insight** > **Users**，然后单击用户以查看所选用户的洞察，例如会话模式、操作系统和浏览器。

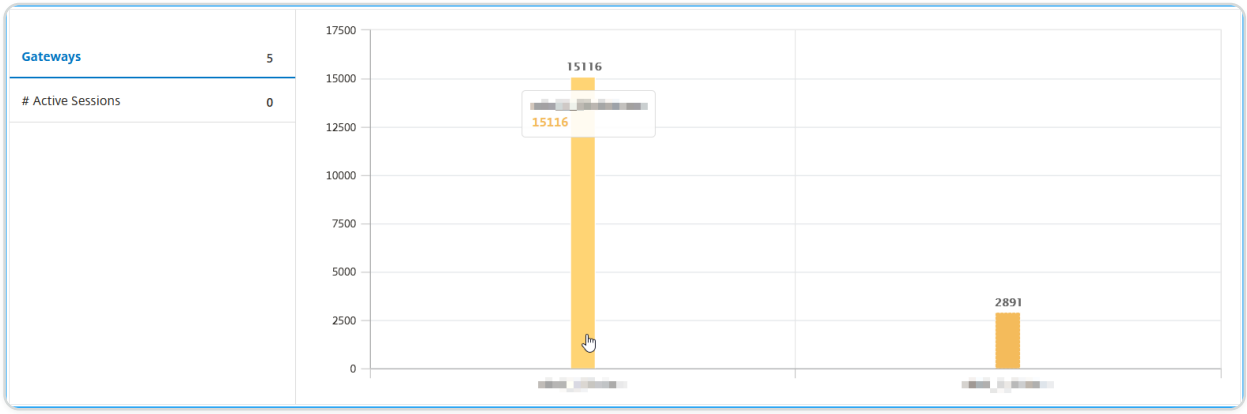
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **所选网关的用户和应用程序** - 导航到 **Gateway** > **Gateway Insight** > **Gateway**，然后单击网关域名以查看与所选网关关联的排名前 10 位的应用程序和排名前 10 位的用户。

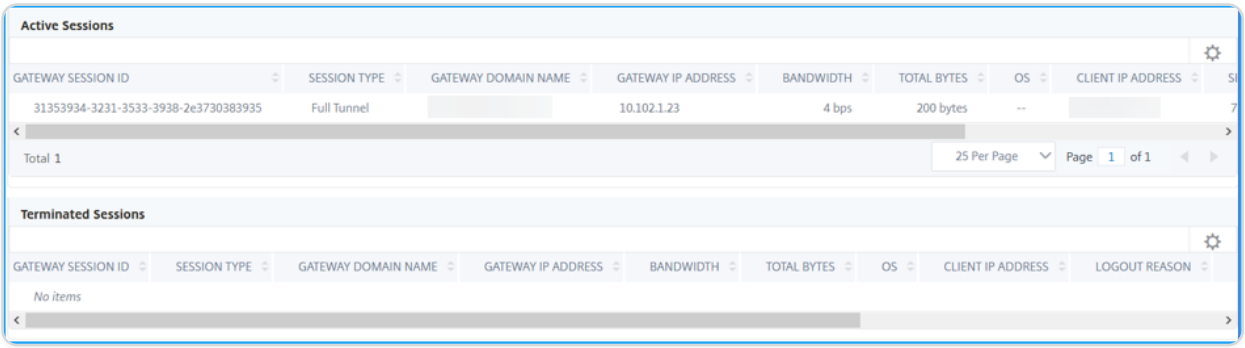


- **查看应用程序和用户的更多选项** – 对于超过 10 个应用程序和用户，您可以单击“应用程序和用户”中的“更多”图标，以查看与所选网关关联的所有用户和应用程序详细信息。
- **通过单击条形图查看详细信息** – 当您单击条形图时，可以查看相关详细信息。例如，导航到 **Gateway > Gateway Insight > Gateway**，然后单击网关条形图以查看网关详细信息。

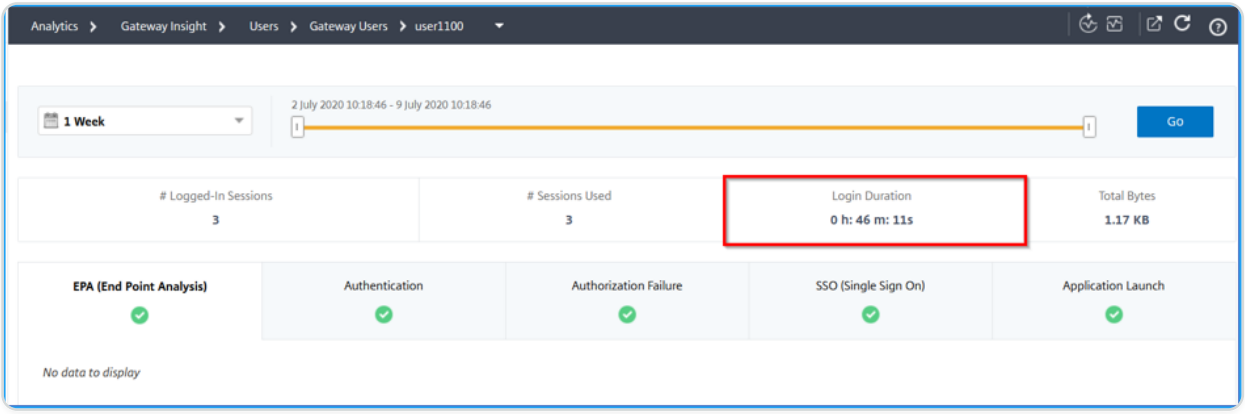


- 用户的 **活动会话** 和 **已终止会话**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 网关域名和网关 IP 地址在“**活动会话**”中。
- 用户登录持续时间。



- 用户注销会话的原因。注销原因可能包括：
  - 会话超时
  - 因内部错误而注销
  - 因非活动会话超时而注销
  - 用户已注销
  - 管理员已停止会话

查看应用程序的 Gateway Insight 报告

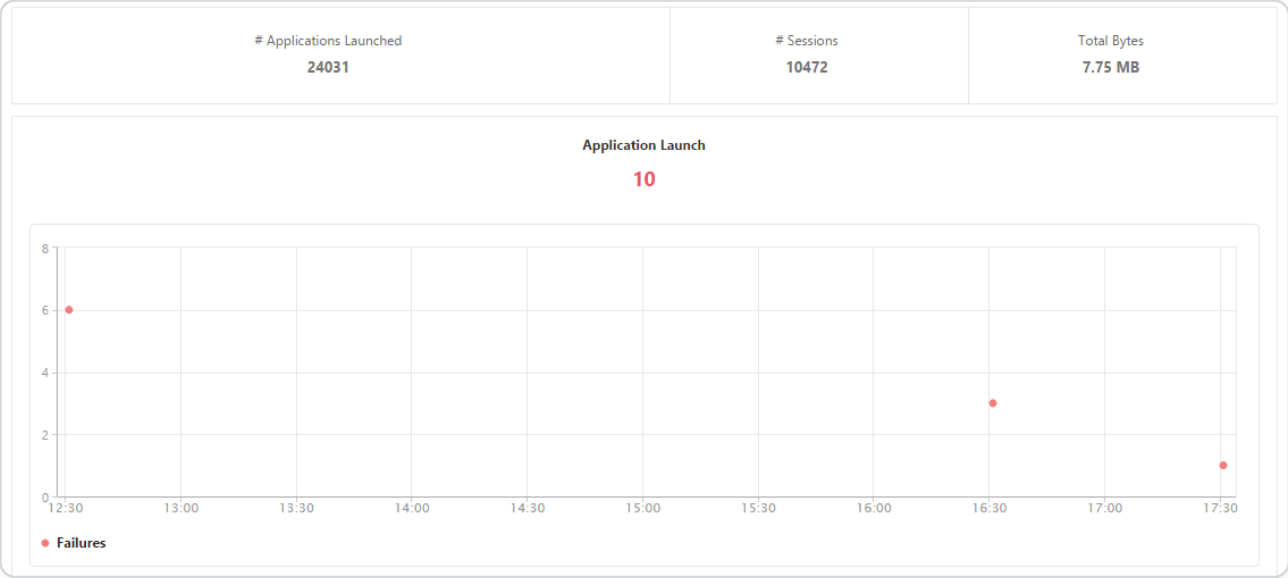
您可以查看启动的应用程序数量、总会话数和活动会话数，以及应用程序消耗的总字节数和带宽。您可以查看应用程序的用户、会话、带宽和启动错误的详细信息。

查看应用程序详细信息

1. 在 NetScaler Console 中，导航到“**网关 > Gateway Insight > 应用程序**”。
2. 选择要查看应用程序详细信息的时间段。您可以使用时间滑块进一步自定义所选时间段。单击“**Go**”。

您现在可以查看启动的应用程序数量、总会话数和活动会话数，以及应用程序消耗的总字节数和带宽。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



向下滚动以查看 ICA 和其他应用程序消耗的会话数、带宽和总字节数。

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	3972	52 bps	3.79 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB

在“**其他应用程序**”选项卡上，您可以单击“**名称**”列中的应用程序以显示该应用程序的详细信息。

查看网关的 Gateway Insight 报告

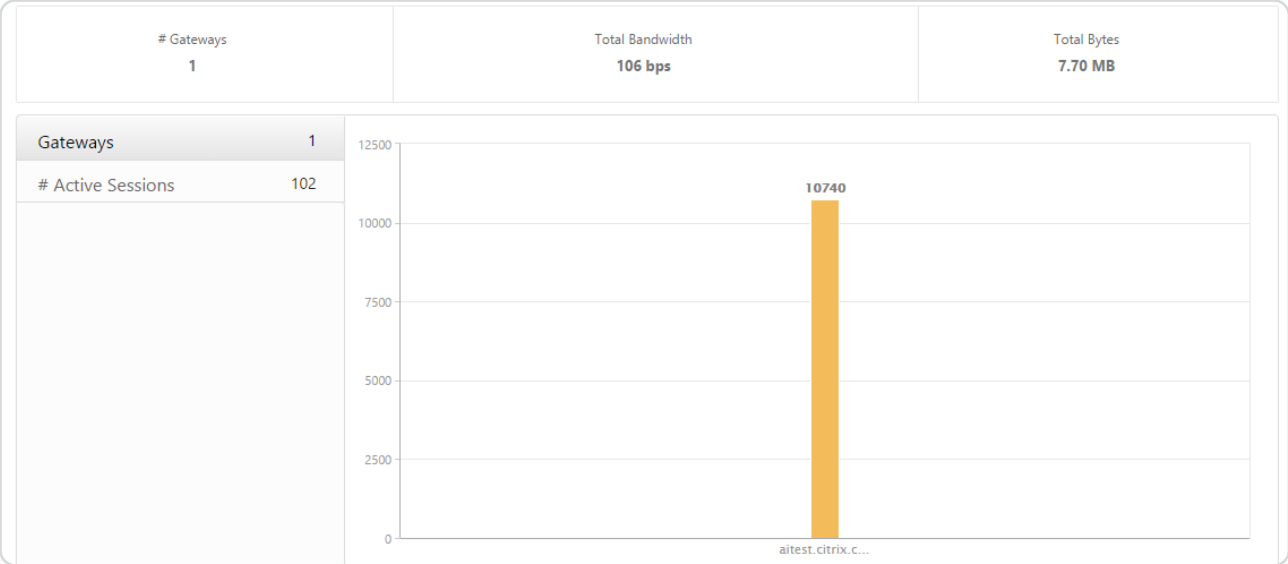
您可以随时查看与 NetScaler Gateway 设备关联的所有网关使用的网关数量、活动会话数量、总字节数和带宽。您可以查看网关的 EPA、身份验证、单点登录和应用程序启动失败。您还可以查看与网关关联的所有用户的详细信息及其登录活动。

要查看网关详细信息

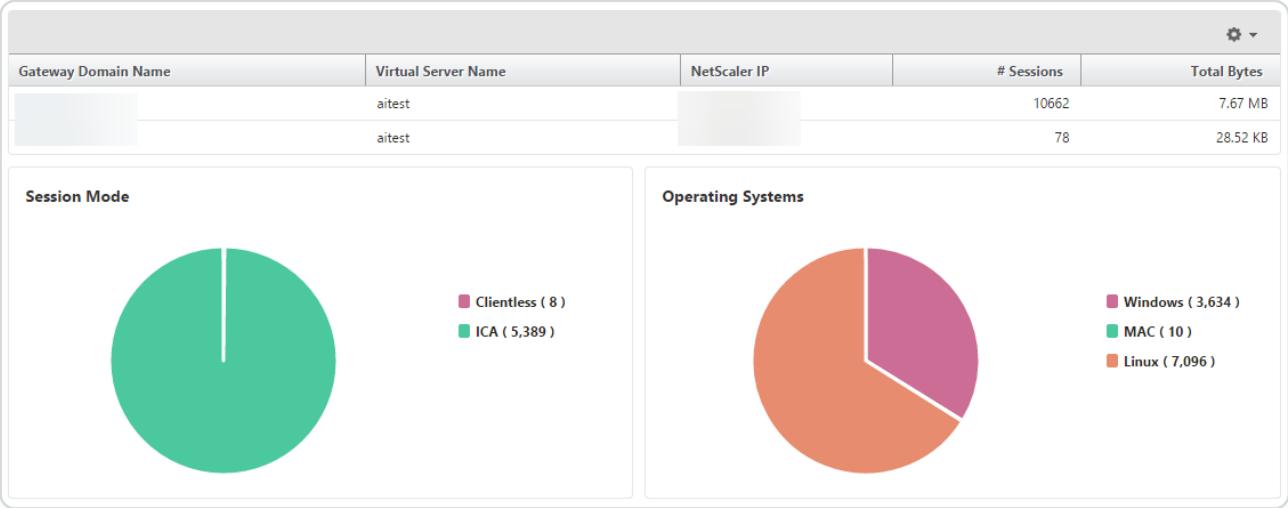
1. 在 **NetScaler Console** 中，导航到 **网关 > 网关洞察 > 网关**。
2. 选择要查看网关详细信息的时间段。您可以使用时间滑块进一步自定义所选时间段。单击“**Go**”。

您现在可以随时查看与 NetScaler Gateway 设备关联的所有网关使用的网关数量、活动会话数量、总字节数和带宽。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



向下滚动以查看网关详细信息，例如网关域名、虚拟服务器名称、NetScaler® IP 地址、会话模式和总字节数。



您可以单击“**网关域名**”列中的网关，以显示网关的 EPA、身份验证、单点登录和应用程序启动失败以及其他详细信息。

导出报告

您可以将 Gateway Insight 报告及其在 GUI 中显示的所有详细信息以 PDF、JPEG、PNG 或 CSV 格式保存到本地计算机。您还可以安排在不同时间间隔将报告导出到指定的电子邮件地址。

注意

- 只读访问权限的用户无法导出报告。
- 仅当 NetScaler Console 具有互联网连接时，才能导出地理地图报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

导出报告

1. 在**仪表板**选项卡上，在右侧窗格中，单击**导出**按钮。
2. 在**立即导出**下，选择所需格式，然后单击**导出**。

安排导出：

1. 在**仪表板**选项卡上，在右侧窗格中，单击**导出**按钮。
2. 在**安排导出**下，指定详细信息并单击**安排**。

添加电子邮件服务器或电子邮件分发列表：

1. 在**配置**选项卡上，导航到**设置 > 通知 > 电子邮件**。
2. 在右侧窗格中，选择**电子邮件服务器**以添加电子邮件服务器，或选择**电子邮件分发列表**以创建电子邮件分发列表。
3. 指定详细信息并单击**创建**。

导出整个 Gateway Insight 仪表板：

1. 在“**仪表板**”选项卡中，在右侧窗格中，单击“**导出**”按钮。
2. 在“**立即导出**”下，选择“**PDF**”格式，然后单击“**导出**”。

网关洞察用例

以下用例展示了如何使用 Gateway Insight 深入了解 NetScaler Gateway 设备上的用户访问详细信息、应用程序和网关。

用户无法登录到 NetScaler Gateway 设备或内部 Web 服务器

您是 NetScaler Gateway 管理员，通过 NetScaler Console 监控 NetScaler Gateway 设备，您想了解用户无法登录的原因，或者登录过程在哪个阶段发生了故障。

NetScaler Console 使您能够查看登录过程以下阶段的用户登录错误详细信息：

- 身份验证
- 端点分析 (EPA)
- 单点登录

在 NetScaler Console 中，您可以搜索特定用户，然后查看该用户的所有详细信息。

搜索用户：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 NetScaler Console 中，导航到“**网关 > Gateway Insight**”，然后在“**搜索用户**”文本框中，指定要搜索的用户。

身份验证失败

您可以查看身份验证错误，例如凭据不正确或身份验证服务器无响应。您还可以查看身份验证失败的因素。

查看身份验证失败详细信息：

1. 在 NetScaler Console 中，导航到 **Gateway > Gateway Insight**。
2. 在 **Overview**（概述）部分中，选择要查看身份验证错误的时间段。您可以使用时间滑块进一步自定义所选时间段。单击 **Go**（前往）。

   身份验证错误视图(/en-us/netscaler-application-delivery-management-software/media/use-cases-auth-failure-overview.png)
3. 单击 **Authentication**（身份验证）选项卡。您可以在 **Failures**（失败）图中查看任意给定时间的身份验证错误数量。

   身份验证失败图(/en-us/netscaler-application-delivery-management-software/media/use-cases-auth-failure-graph.png)

向下滚动以查看每个身份验证错误的详细信息，例如同一选项卡上的表中的 **用户名、客户端 IP 地址、错误时间、身份验证类型、身份验证服务器 IP 地址** 等。表中的 **错误描述** 列显示了登录失败的原因，**状态** 列显示了发生失败的第 n 个因素。

身份验证失败详细信息(/en-us/netscaler-application-delivery-management-software/media/use-cases-auth-failure-errors-13.png)

您可以单击 **Username**（用户名）列中的用户以显示该用户的身份验证错误和其他详细信息。您可以使用设置图标自定义表以添加或删除列。

重要提示：

如果 OAuth-OpenID Connect 身份验证失败，则在 Gateway Insight 报告中，某些失败（例如“令牌验证失败”）的用户名为 **NA**。在此类失败中，由于 OAuth-OpenID Connect 依赖方处的“令牌验证失败”，用户名称不适用于身份验证失败。

OAuth-OpenID 连接失败(/en-us/netscaler-application-delivery-management-software/media/oauth-openid-authentication-failure.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EPA 失败

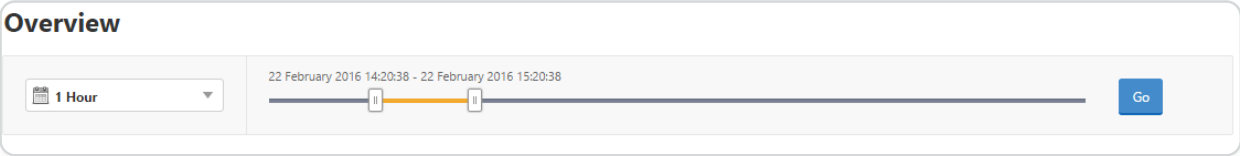
您可以在预身份验证或后身份验证阶段查看 EPA 失败。

重要提示：

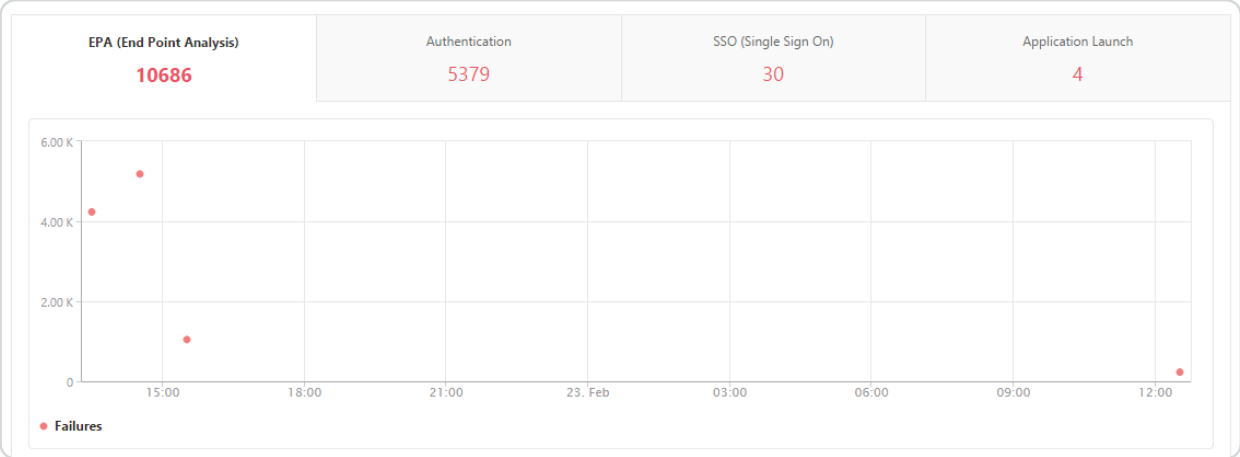
NetScaler Gateway 向 NetScaler Console 报告经典和高级表达式的 EPA 故障。对于高级表达式，策略名称不会显示在 Gateway Insight 控制板中。如果 EPA 配置为 nFactor 身份验证流中的一个因素，则会报告故障。

查看 EPA 故障详细信息：

1. 在 NetScaler Console 中，导航到 **Gateway > Gateway Insight**。
2. 在“概述”部分中，选择要查看 EPA 错误的时间段。您可以使用时间滑块进一步自定义选定的时间段。单击 **Go**。



3. 单击 **EPA (End Point Analysis)** 选项卡。您可以在“**故障**”图中查看任意给定时间的 EPA 错误数量。



向下滚动以查看每个 EPA 错误的详细信息，例如同一选项卡上的表格中的**用户名、NetScaler IP 地址、网关 IP 地址、VPN、错误时间、策略名称、网关域名**等。

表格中的“**错误描述**”列显示了 EPA 故障的原因。例如，当 EPA 检查因 nFactor EPA 故障而失败时，会出现错误消息“EPA 预身份验证检查失败”。

“**策略名称**”列显示导致故障的策略。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

您可以单击“**用户名**”列中的用户以显示该用户的 EPA 错误和其他详细信息。您可以使用向下箭头自定义表格以添加或删除列。如果 EPA 用作 nFactor 身份验证流中的一个因素，则在未分配用户名的条目上显示案例 ID。

注意

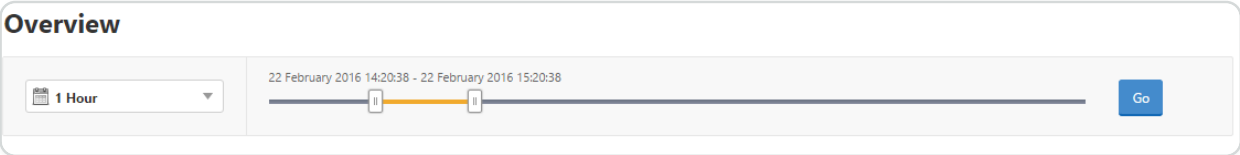
当“clientSecurity”表达式配置为 VPN 会话策略规则时，NetScaler Gateway 不会报告 EPA 故障。

SSO 故障

您可以查看用户通过 NetScaler Gateway 设备访问任何应用程序时，在任何阶段发生的所有 SSO 失败。

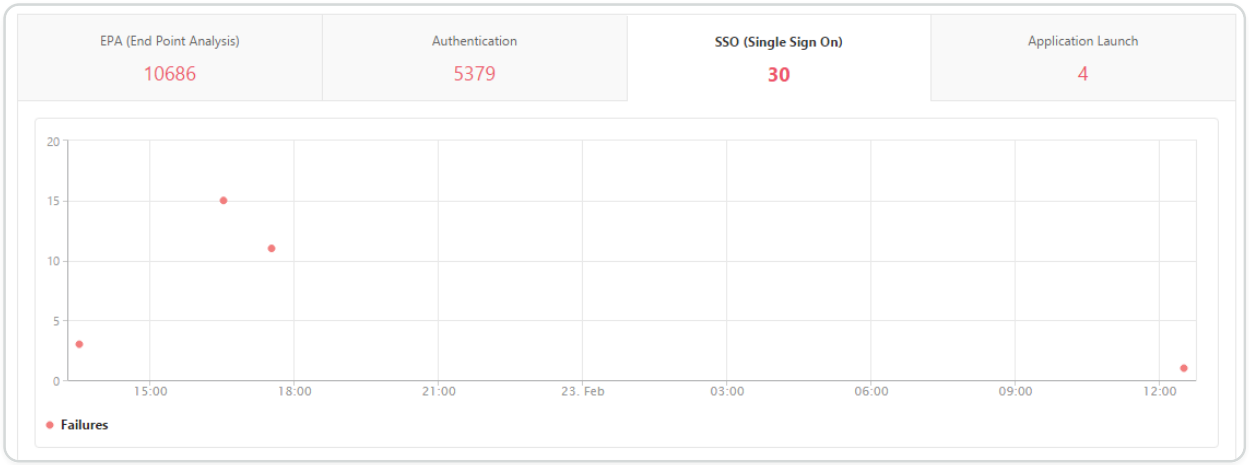
查看 SSO 失败详细信息：

1. 在 NetScaler Console 中，导航到 **Gateway > Gateway Insight**。
2. 在“概述”部分中，选择要查看 SSO 错误的时间段。您可以使用时间滑块进一步自定义所选时间段。单击 **Go**。

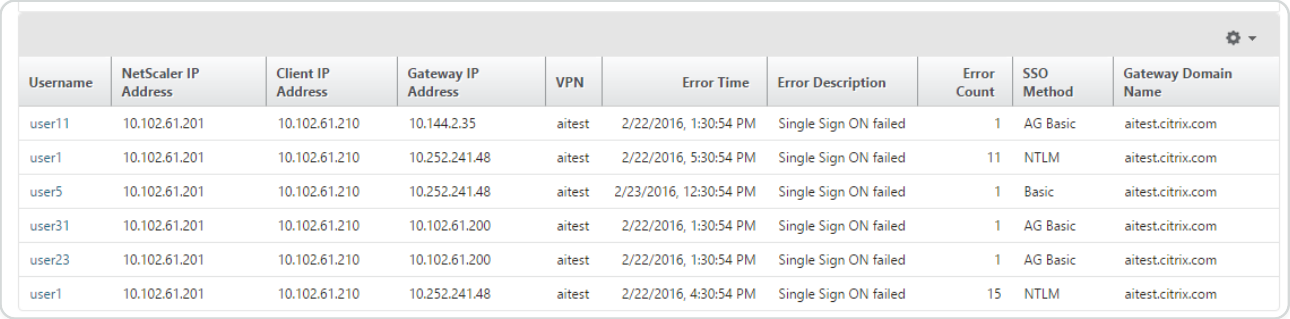


3. 单击 **SSO (Single Sign On)** 选项卡。您可以在“失败”图表中查看任意给定时间的 SSO 错误数量。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



向下滚动以查看同一选项卡上的表格中每个 SSO 错误的详细信息，例如**用户名**、**NetScaler IP 地址**、**错误时间**、**错误描述**、**资源名称**等。



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

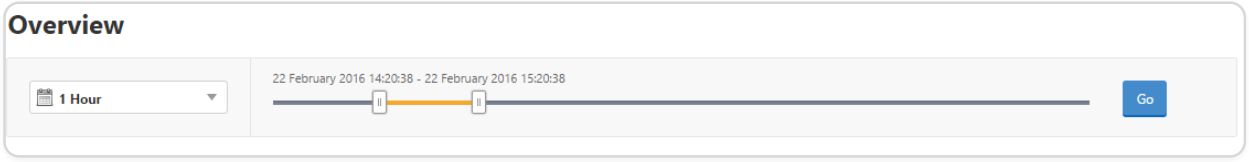
您可以单击“**用户名**”列中的用户以显示该用户的 SSO 错误和其他详细信息。您可以使用向下箭头自定义表格以添加或删除列。

用户成功登录 NetScaler Gateway 后无法启动任何虚拟应用程序

对于应用程序启动失败，您可以了解其原因，例如无法访问的安全票证颁发机构 (STA) 或 Citrix Virtual App 服务器，或无效的 STA 票证。您可以查看错误发生的时间、错误详细信息以及 STA 验证失败的资源。

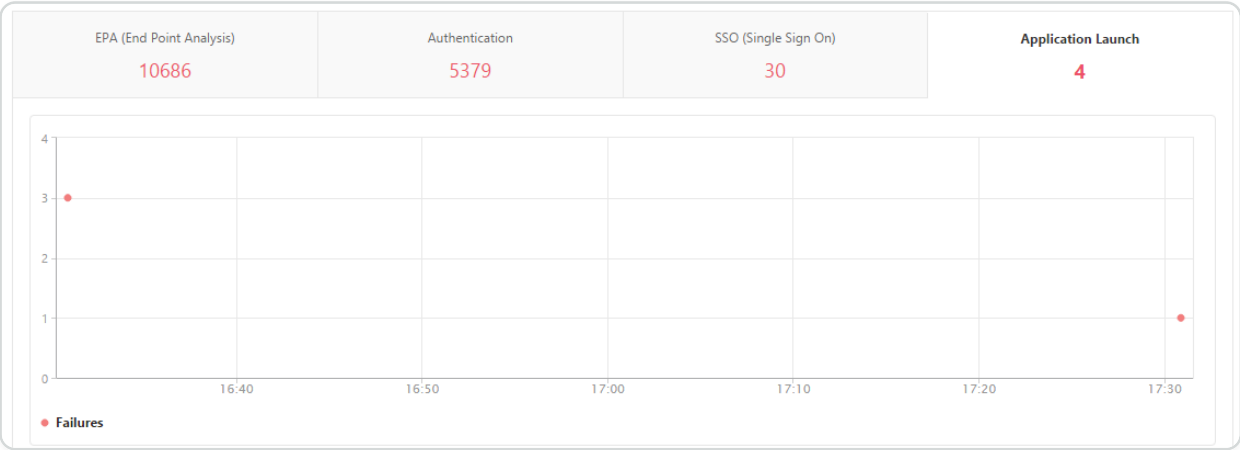
查看应用程序启动失败详细信息：

1. 在 NetScaler Console 中，导航到 **Gateway > Gateway Insight**。
2. 在“**概述**”部分中，选择要查看 SSO 错误的时间段。您可以使用时间滑块进一步自定义所选时间段。单击 **Go**。



3. 单击“**应用程序启动**”选项卡。您可以在“**失败**”图中查看任意给定时间应用程序启动失败的次数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



向下滚动以查看每个应用程序启动错误的详细信息，例如**NetScaler IP 地址、错误时间、错误描述、资源名称、网关域名**等，在同一选项卡上的表格中。表格中的**错误描述**列显示 STA 服务器的 IP 地址，**资源名称**列显示 STA 验证失败的资源的详细信息。

您可以单击“**用户名**”列中的用户，以显示该用户的应用程序启动错误和其他详细信息。您可以使用向下箭头自定义表格以添加或删除列。

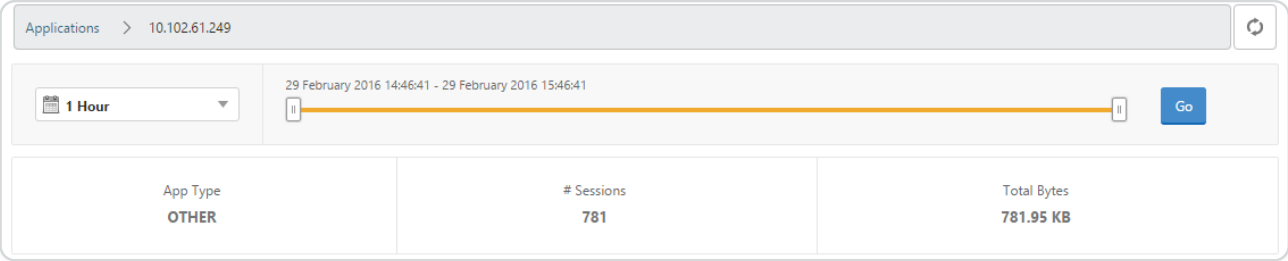
成功启动新应用程序后，用户想要查看该应用程序消耗的总字节数和带宽

成功启动新应用程序后，您可以在 NetScaler Console 中查看该应用程序消耗的总字节数和带宽。

要查看应用程序消耗的总字节数和带宽：

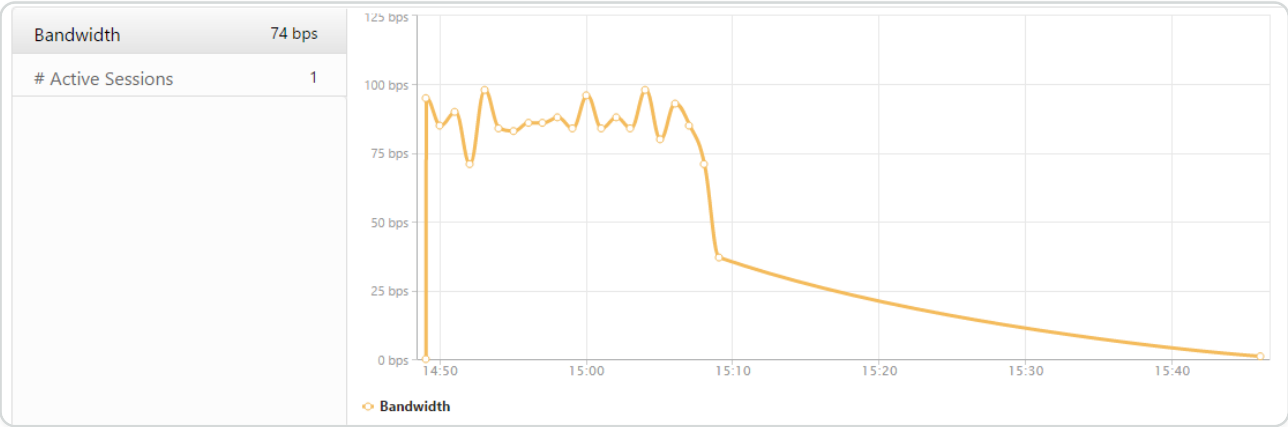
在 NetScaler Console 中，导航到“**网关 > 网关洞察 > 应用程序**”，向下滚动，然后在“**其他应用程序**”选项卡上，单击要查看其详细信息的应用程序。

您可以查看该应用程序消耗的会话数和总字节数。



您还可以查看该应用程序消耗的带宽。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

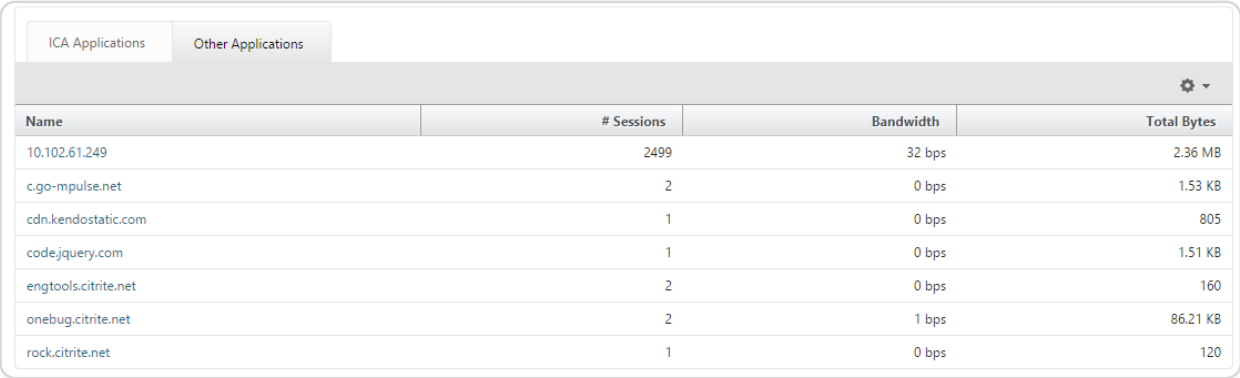


用户已成功登录 NetScaler Gateway，但无法访问内部网络中的某些网络资源

使用 Gateway Insight，您可以确定用户是否可以访问网络资源。您还可以查看导致失败的策略名称。

查看资源的用户访问权限：

1. 在 NetScaler Console 中，**导航到 网关 > 网关洞察 > 应用程序**。
2. 在出现的屏幕上，向下滚动，然后在**其他应用程序**选项卡上，选择用户无法登录的应用程序。



ICA Applications | Other Applications

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

3. 向下滚动，在**用户**表中，将显示所有有权访问该应用程序的用户。

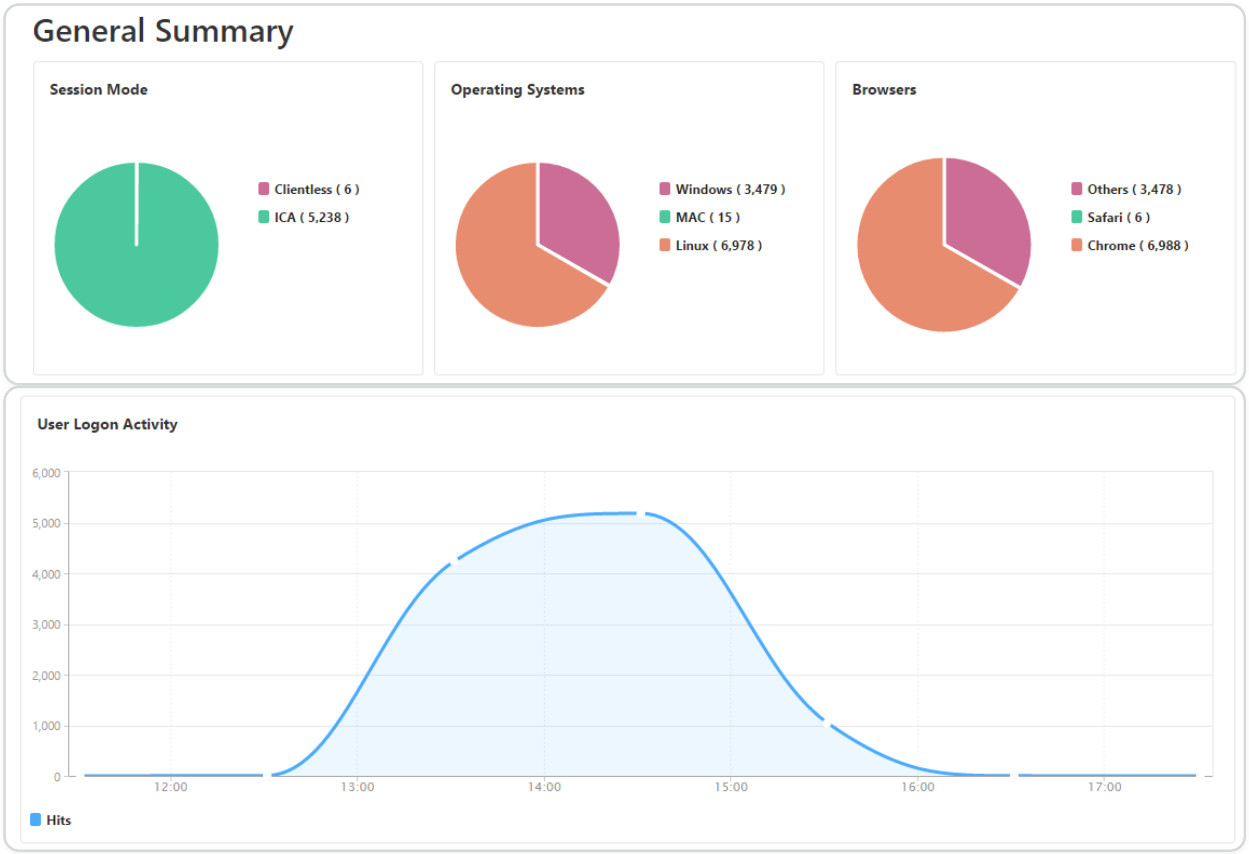
不同的用户可能使用不同的 NetScaler Gateway 部署，或者可能通过不同的访问模式登录到 NetScaler Gateway。管理员必须能够查看有关部署类型和访问模式的详细信息

借助 Gateway Insight，您可以查看用户用于登录的不同会话模式、客户端类型以及每小时登录用户数的摘要。您还可以确定用户的部署是统一网关还是经典 NetScaler Gateway 部署。对于统一网关部署，您可以查看内容交换虚拟服务器名称和 IP 地址以及 VPN 虚拟服务器名称。

查看会话模式、客户端类型和登录用户数的摘要：

1. 在 NetScaler Console 中，导航到 **Gateway > Gateway Insight**。
2. 在**概述**部分，向下滚动以查看**会话模式**、**操作系统**、**浏览器**和**用户登录活动**图表，这些图表显示了用户用于登录的不同会话模式、客户端类型以及每小时登录用户数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



排查 Gateway Insight 问题

如果 Gateway Insight 解决方案未按预期运行，问题可能出在以下某一方面。有关故障排除，请参阅相应部分中的清单。

- 网关洞察配置。
- NetScaler 与 NetScaler Console 之间的连接问题。
- NetScaler 中的记录生成。
- NetScaler Console 中的验证。

Gateway Insight 配置清单

- 确保在 NetScaler 设备中启用了 AppFlow 功能。有关详细信息，请参阅 启用 AppFlow。
- 检查 NetScaler 运行配置中的 Gateway Insight 配置。

  运行 `show running | grep -i <appflow_policy>` 命令以检查 Gateway Insight 配置。确保绑定类型为 REQUEST。例如；

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  绑定类型 OTHERTCP_REQUEST 对于 Gateway Insight 也是必需的。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind vpn vserver afsanity -policy afp -priority 100 -type
OTHERTCP_REQUEST
```

- 对于单跳、Access Gateway 或统一网关部署，请确保 Gateway Insight AppFlow 策略绑定到 VPN 流量流经的 VPN 虚拟服务器。有关详细信息，请参阅 启用 HDX Insight 数据收集。
- 对于双跳，必须在两个跳上配置 Gateway Insight。
- 检查 NetScaler Gateway/VPN 虚拟服务器中的 `appflowlog` 参数。有关详细信息，请参阅 为虚拟服务器启用 AppFlow。

NetScaler 与 NetScaler Console 之间的连接清单

- 检查 NetScaler 中的 AppFlow 收集器状态。有关详细信息，请参阅 如何检查 NetScaler 与 AppFlow 收集器之间的连接状态。
- 检查 Gateway Insight AppFlow® 策略命中数。

  运行命令 `show appflow policy <policy_name>` 以检查 AppFlow 策略命中数。

  您还可以导航到 GUI 中的 **设置 > AppFlow > 策略** 以检查 AppFlow 策略命中数。
- 验证是否有任何防火墙阻止 AppFlow 端口 4739 或 5557。

NetScaler 中的记录生成清单

- 运行 `nsconmsg -d stats -g ai_tot` 命令并检查 NetScaler 中的统计信息增量。
- 捕获 `nstrace logs` 并检查 CFLOW 数据包，以确认 NetScaler 导出 AppFlow 记录。

> **注意：**
>
> `nstrace logs` 仅适用于 IPFIX。对于 Logstream，nstrace 日志无法确认 NetScaler 设备是否导出了 AppFlow 记录。

NetScaler Console 中记录的验证

- 运行 `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` 命令检查日志，以确认 NetScaler Console 正在接收 AppFlow 记录。
- 确保 NetScaler 实例已添加到 NetScaler Console。
- 确保 NetScaler Gateway/VPN 虚拟服务器已在 NetScaler Console 中获得许可。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console 中 Logstream 日志的验证

可以使用以下方法验证 NetScaler Console 接收到的 Logstream 数据：

- **在 NetScaler Console 中启用数据记录日志**

  启用后，可以在 /var/mps/log/mps_afdecoder.log 中查看日志

- **启用 ULFD 库日志记录**

  运行命令 `/mps/decoder_enable_debug`

  日志捕获在 `/var/ulflog/libulfd.log` 中

  您可以使用命令 `/mps/decoder_disable_debug` 禁用日志记录

Gateway Insight 计数器

提供以下 Gateway Insight 计数器。

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled
- ai_tot_appflow_pol_eval_in_gwinsight
- ai_tot_app_launch_success

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler 日志中的 AppFlow 记录

从版本 13.0 build 71.x 开始，您可以检查 NetScaler 日志以确认 AppFlow 记录是否已导出。`syslogparams` 的默认日志级别会捕获所有错误和信息日志。如果您找不到有关错误的线索，请在 `syslogparams` 中启用所有日志级别（包括 DEBUG）以捕获 DEBUG 日志。

日志示例

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 147 0 : "GwInsight:
Sent auth record Func=ns_sslvpn_export_auth_data Username=<name>
Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid> Gwip=<ip>:443
StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<vpnfqdn> Authtype=3
EPAid=(null) AuthStage=1 AuthDuration=309 AuthAgent=<auth_server_ip>
Groupname= Policyname=<name> CurfactorPolname=<name> NextfactorPolname=
CSecExpr= Devicetype=16777219 Deviceid=0 email="

<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight:
Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is zero"

<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight:
Func=update_session_appflow_collector pcb or session is NULL"

<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 165 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record Username=<>
Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=1 Sessid=<sessid>
Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn>
SSOAuthMethod=0 SessState=2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/
Citrix/Store

Web BackendServername= SSOurl= email="

SSO logs:
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 463 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=1 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 582 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=3 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 513 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:80 SessSeq=2
Sessid=<sessid> Gwip=<ip>:443 StatusCode=150 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=2 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "GwInsight:
Sent session update record Func=ns_sslvpn_send_update_record
Username=<name> Clientip=<ip>:<port> Destip=<ip>:443 SessSeq=c
Sessid=<sessid> Gwip=<ip>:443 StatusCode=155 CSappid=0 CSAppname=(null)
VPNfqdn=<fqdn> SSOAuthMethod=6 SessState=4 SessMode=3 IIP=0 AppByteCount=0
ReqURL= BackendServername=<> SSOurl= email="
```

联系 Citrix 技术支持

为了快速解决问题，请在联系 Citrix 技术支持之前确保您拥有以下信息：

- 部署和网络拓扑的详细信息。
- NetScaler 和 NetScaler Console 版本。
- NetScaler 和 NetScaler Console 的技术支持包。
- 问题发生期间的 `nstrace` 捕获。

已知问题

有关 Gateway Insight 的已知问题，请参阅 NetScaler 发行说明。

HDX™ 洞察

HDX 洞察为通过 NetScaler 的 Citrix Virtual Apps and Desktop 的 HDX 流量提供端到端可见性。它还使管理员能够查看实时客户端和网络延迟指标、历史报告、端到端性能数据，并排除性能问题。实时和历史可见性数据的可用性使 NetScaler Console 能够支持各种用例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要显示任何数据，您需要在 NetScaler Gateway 虚拟服务器上启用 AppFlow。AppFlow 可以通过 IPFIX 协议或 LogStream 方法提供。

注意

要允许记录 ICA® 往返时间计算，请启用以下策略设置：

- ICA 往返计算
- ICA 往返计算间隔
- 针对空闲连接的 ICA 往返计算

如果您点击单个用户，您可以看到该用户在选定时间范围内进行的每个 HDX 会话（活动的或已终止的）。其他信息包括多个延迟统计信息和会话期间消耗的带宽。您还可以从各个虚拟通道（例如音频、打印机映射和客户端驱动器映射）获取带宽信息。

注意

创建组时，您可以为组分配角色，为组提供应用程序级访问权限，并将用户分配给该组。NetScaler Console 分析现在支持基于虚拟 IP 地址的授权。您的用户现在可以查看所有洞察的报告，但仅限于他们被授权访问的应用程序（虚拟服务器）。有关组以及将用户分配给组的更多信息，请参阅 配置组。

您还可以导航到 **Gateway > HDX Insight > 应用程序**，然后点击 **启动持续时间** 以查看应用程序启动所需的时间。您还可以通过导航到 **Gateway > HDX Insight > 用户** 来查看所有已连接用户的用户代理。

注意

HDX 洞察支持在运行软件版本 12.0 的 NetScaler 实例中配置的管理员分区。

以下瘦客户端支持 HDX 洞察：

- WYSE 基于 Windows 的瘦客户端
- WYSE 基于 Linux 的瘦客户端
- WYSE 基于 ThinOS 的瘦客户端
- 10ZiG 基于 Ubuntu 的瘦客户端

© 1997–2026 Citrix Systems, Inc. All rights reserved.

识别性能缓慢问题的根本原因

场景 1

用户在访问 Citrix Virtual Apps and Desktops 时遇到延迟。

延迟可能是由于服务器网络延迟、服务器网络导致的 ICA 流量延迟或客户端网络延迟造成的。

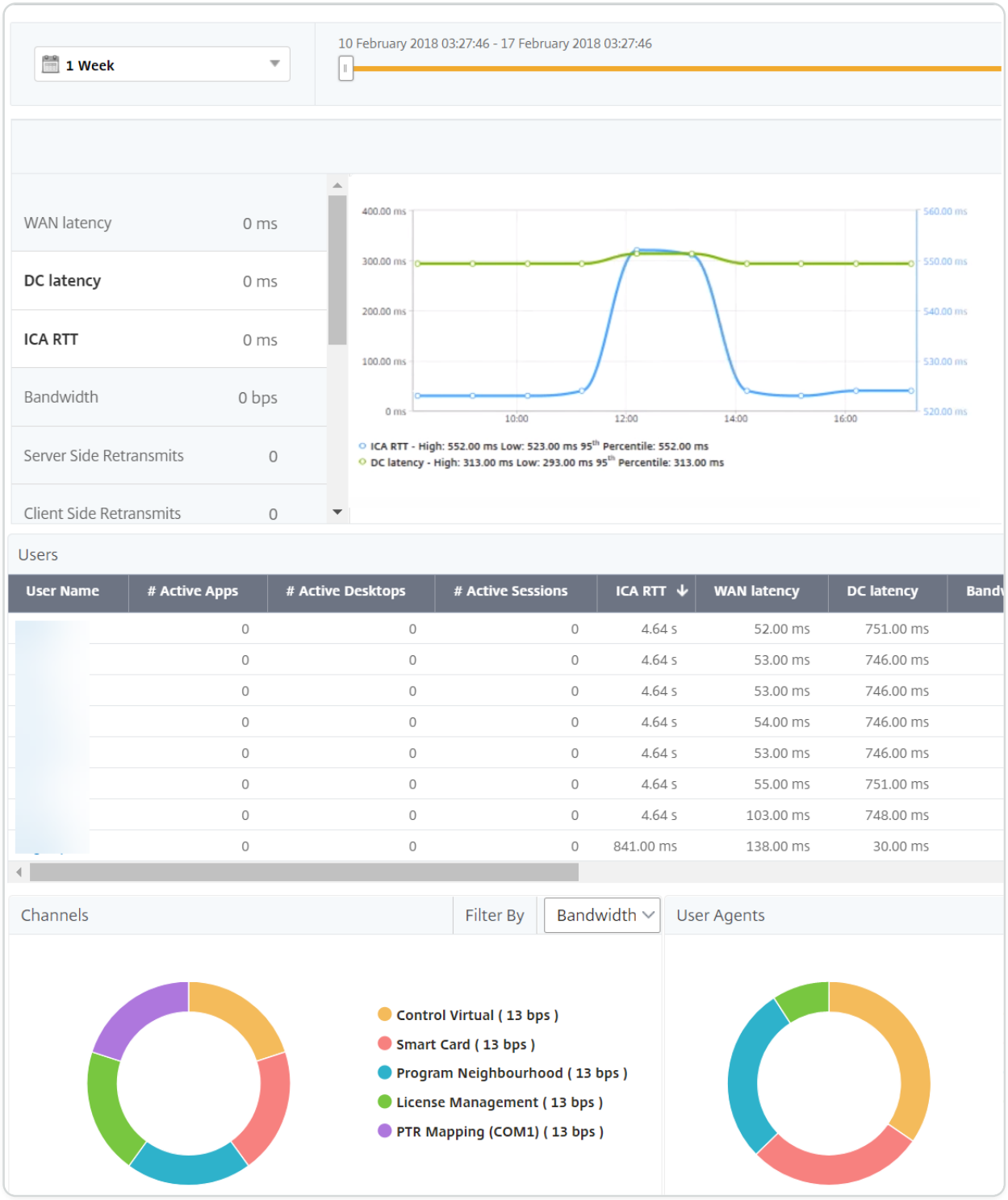
要识别问题的根本原因，请分析以下指标：

- WAN 延迟
- DC 延迟
- 主机延迟

查看客户端指标：

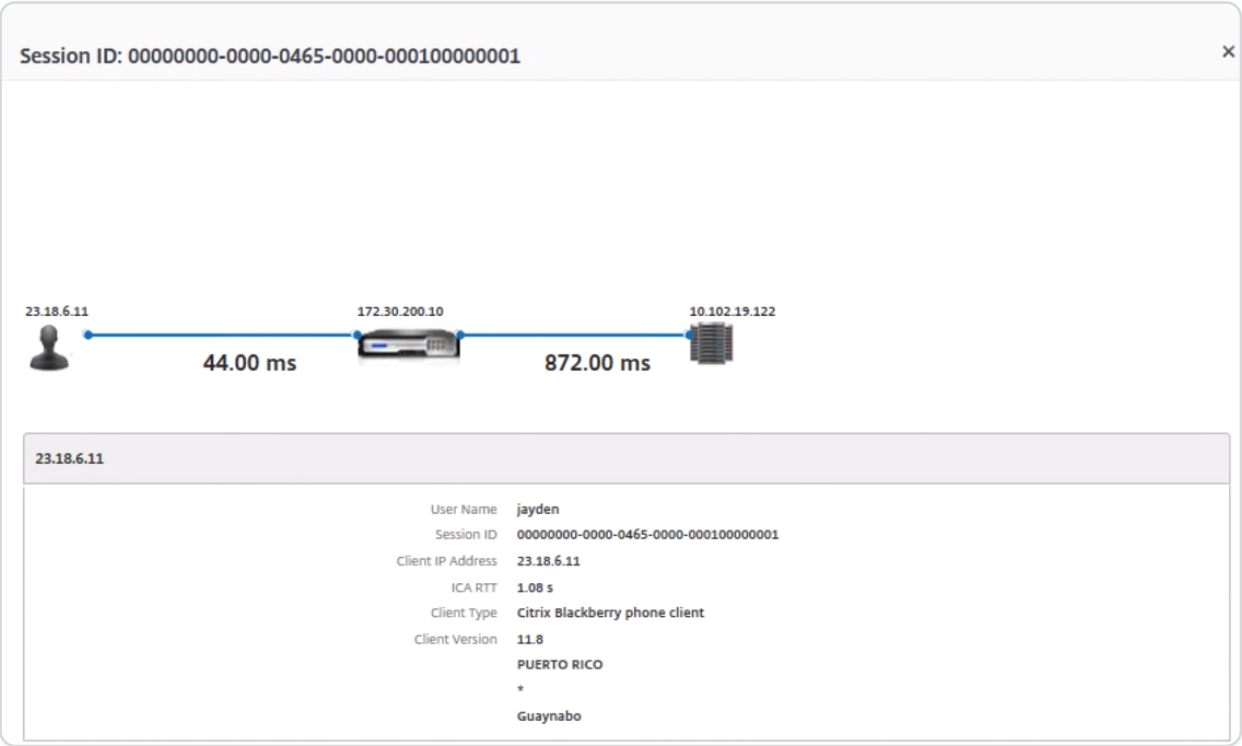
1. 导航到 **网关 > HDX Insight > 用户**。
2. 向下滚动并从列表中选择用户名和时间段。时间段可以是一天、一周、一个月，您甚至可以自定义要查看数据的时间段。
3. 图表以图形形式显示用户在指定时间段内的 ICA RTT 和 DC 延迟值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 在 **当前会话** 表中，将鼠标悬停在 **RTT** 值上，并记下主机延迟、DC 延迟和 WAN 延迟值。
5. 在 **当前会话** 表中，单击跳图符号以显示客户端和服务器之间连接的信息，包括延迟值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



摘要

在此示例中，**DC 延迟** 为 751 毫秒，**WAN 延迟** 为 52 毫秒，**主机延迟** 为 6 秒。这表明用户由于服务器网络导致的平均延迟而遇到延迟。

场景 2

用户在 Citrix Virtual App 或 Desktop 上启动应用程序时遇到延迟

延迟可能由于服务器网络上的延迟、服务器网络导致的 ICA 流量延迟、客户端网络上的延迟或启动应用程序所需的时间。

要确定问题的根本原因，请分析以下指标：

- WAN 延迟
- DC 延迟
- 主机延迟

查看用户指标：

1. 导航到 **网关 > HDX Insight > 用户。**
2. 向下滚动并点击用户名。
3. 在图形表示中，记下特定会话的 WAN 延迟、DC 延迟和 RTT 值。
4. 在**当前会话**表中，请注意主机延迟较高。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

当前会话(/en-us/netscaler-application-delivery-management-software/media/nmas-hdxinsight-analytics-7.png)

摘要

在此示例中，**DC 延迟**为 1 毫秒，**WAN 延迟**为 12 毫秒，但**主机延迟**为 517 毫秒。高 RTT 而 DC 和 WAN 延迟较低表示主机服务器上存在应用程序错误。

注意 如果您使用的是运行软件 11.1 build 51.21 或更高版本的 NetScaler Console，HDX Insight 还会显示更多用户指标，例如 WAN 抖动和服务器端重传。要查看这些指标，请导航到 **Gateway > HDX Insight > Users**，然后选择一个用户名。用户指标将显示在图表旁边的表格中。

用户(/en-us/netscaler-application-delivery-management-software/media/nmas-hdxinsight-analytics-8.png)

HDX Insight 的地理地图

NetScaler Console 地理地图功能可在地图上显示应用程序在不同地理位置的使用情况。管理员可以使用此信息了解应用程序在各个地理位置的使用趋势。

您可以通过为特定地理位置或 LAN 指定私有 IP 范围（起始和结束 IP 地址）来配置 NetScaler Console 以显示该位置的地理地图。

您还可以从 HDX Insight 中的地理位置地图查看历史和活跃用户的详细信息。导航到 **Gateway > HDX Insight**，然后在地图的**世界**部分中，单击要查看详细信息的国家或地区。您可以进一步向下钻取以按城市和州查看信息。

配置数据中心地理地图：

导航到 **Settings > Analytics Settings > IP Blocks** 以配置特定位置的地理地图。

用例

设想一个场景，ABC 组织有两个分支机构，一个在圣克拉拉，另一个在印度。

圣克拉拉的用户使用 SClara.x.com 上的 NetScaler Gateway 设备访问 VPN 流量。印度用户使用 India.x.com 上的 NetScaler Gateway 设备访问 VPN 流量。

在特定时间段，例如上午 10 点到下午 5 点，圣克拉拉的用户连接到 SClara.x.com 访问 VPN 流量。大多数用户访问同一个 NetScaler Gateway，导致连接 VPN 出现延迟，因此一些用户转而连接到 India.x.com 而不是 SClara.x.com。

分析流量的 NetScaler 管理员可以使用地理地图功能来显示圣克拉拉办公室的流量。地图显示圣克拉拉办公室的响应时间很高，因为圣克拉拉办公室只有一个 NetScaler Gateway 设备供用户访问

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VPN 流量。因此，管理员可能会决定安装另一个 NetScaler Gateway，以便用户可以通过两个本地 NetScaler Gateway 设备访问 VPN。

HDX 分析2(/en-us/netscaler-application-delivery-management-software/media/nmas-hdxinsight-analytics-4.png)

限制

如果 NetScaler 实例具有 Advanced 许可证，则 NetScaler Console 上为 HDX Insight 设置的阈值将不会触发，因为分析数据仅收集 1 小时。

启用 HDX™ Insight 数据收集

HDX Insight 通过提供对通过 NetScaler 实例的 ICA 流量前所未有的端到端可见性，使 IT 能够提供卓越的用户体验，并且是 NetScaler Console Analytics 的一部分。HDX Insight 为网络、虚拟桌面、应用程序和应用程序结构提供引人注目且功能强大的商业智能和故障分析功能。HDX Insight 既可以即时分类用户问题，收集有关虚拟桌面连接的数据，还可以生成 AppFlow 记录并将其呈现为可视化报告。

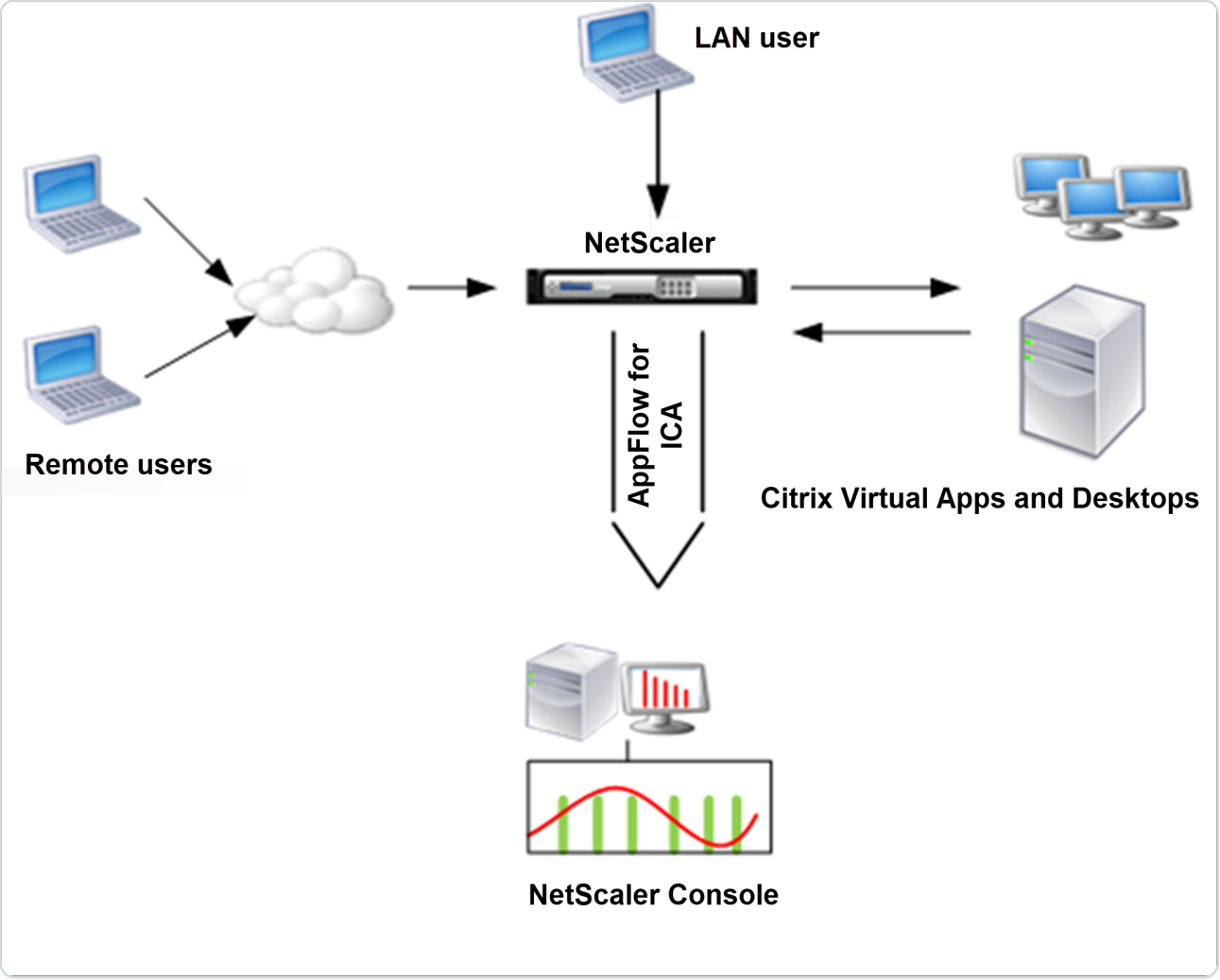
在 NetScaler 中启用数据收集的配置因设备在部署拓扑中的位置而异。

为以 LAN 用户模式部署的 NetScaler 启用数据收集

访问 Citrix Virtual App and Desktop 应用程序的外部用户必须在 NetScaler Gateway 上进行身份验证。但是，内部用户可能不需要重定向到 NetScaler Gateway。此外，在透明模式部署中，管理员必须手动应用路由策略，以便请求重定向到 NetScaler 设备。

为了克服这些挑战，并让 LAN 用户直接连接到 Citrix Virtual App and Desktop 应用程序，您可以通过配置一个缓存重定向虚拟服务器，将 NetScaler 设备部署在 LAN 用户模式下，该服务器在 NetScaler Gateway 设备上充当 SOCKS 代理。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

NetScaler Console 和 NetScaler Gateway 设备位于同一子网中。

要监控以此模式部署的 NetScaler 设备，首先将 NetScaler 设备添加到 NetScaler Insight 清单中，启用 AppFlow，然后查看仪表板上的报告。

将 NetScaler 设备添加到 NetScaler Console 清单后，您必须启用 AppFlow 进行数据收集。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

- 在 NetScaler 实例上，您可以导航到 **Settings > AppFlow > Collectors**，以检查收集器（即 NetScaler Console）是否已启动。NetScaler 实例使用 NSIP 将 AppFlow 记录发送到 NetScaler Console。但实例使用其 SNIP 来验证与 NetScaler Console 的连接。因此，请确保在实例上配置了 SNIP。
- 您无法通过使用 NetScaler Console 配置实用程序，在以 LAN 用户模式部署的 NetScaler 上启用数据收集。
- 有关命令及其用法的详细信息，请参阅 命令参考。
- 有关策略表达式的信息，请参阅 策略和表达式。

要使用命令行界面在 NetScaler 设备上配置数据收集，请执行以下操作：

在命令提示符下，执行以下操作：

1. 登录到设备。
2. 添加一个正向代理缓存重定向虚拟服务器，指定代理 IP 和端口，并将服务类型指定为 HDX。

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType
<cachetype>] [ - cltTimeout <secs>]
```

示例

```
add cr vserver cr1 HDX 10.12.2.2 443 –cacheType FORWARD –cltTimeout 180
```

注意：

如果您正在使用 NetScaler Gateway 设备访问 LAN 网络，请添加一个由与 VPN 流量匹配的策略应用的动作。

```
add vpn trafficAction <name> <qual> [-HDX ( ON or OFF )]



add vpn trafficPolicy <name> <rule> <action>
```

示例

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add vpn trafficAction act1 tcp -HDX ON



add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. 将 NetScaler Console 添加为 NetScaler 设备上的 AppFlow 收集器。

```
add appflow collector <name> -IPAddress <ip_addr>
```

示例：

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

4. 创建 AppFlow® 动作并将收集器与该动作关联。

```
add appflow action <name> -collectors <string>
```

示例：

```
add appflow action act -collectors MyInsight
```

5. 创建 AppFlow 策略以指定生成流量的规则。

```
add appflow policy <policyname> <rule> <action>
```

示例：

```
add appflow policy pol true act
```

6. 将 AppFlow 策略绑定到全局绑定点。

```
bind appflow global <policyname> <priority> -type <type>
```

示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

注意

type 的值必须是 ICA_REQ_OVERRIDE 或 ICA_REQ_DEFAULT 才能应用于 ICA® 流量。

7. 将 AppFlow 的 flowRecordInterval 参数值设置为 60 秒。

```
set appflow param -flowRecordInterval 60
```

示例：

```
set appflow param -flowRecordInterval 60
```

8. 保存配置。键入：`save ns config`

为以单跳模式部署的 NetScaler Gateway 设备启用数据收集

当您以单跳模式部署 NetScaler Gateway 时，它位于网络的边缘。Gateway 实例提供到桌面交付基础结构的代理 ICA 连接。单跳是最简单、最常见的部署。如果外部用户尝试访问组织中的内部网络，单跳模式可提供安全性。 在单跳模式下，用户通过虚拟专用网络 (VPN) 访问 NetScaler 设备。

要开始收集报告，您必须将 NetScaler Gateway 设备添加到 NetScaler Console 清单中并在 NetScaler Console 上启用 AppFlow。

要从 NetScaler Console 启用 AppFlow 功能：

1. 在 Web 浏览器中，键入 NetScaler Console 的 IP 地址（例如，`<http://192.168.100.1>`）。
2. 在“**用户名**”和“**密码**”中，输入管理员凭据。
3. 导航到“**基础结构 > 实例**”，然后选择要启用分析的 NetScaler 实例。
4. 从“**选择操作**”列表中，选择“**配置分析**”。
5. 选择 VPN 虚拟服务器，然后单击“**启用分析**”。
6. 选择“**HDX Insight**”，然后选择“**ICA**”。
7. 点击 **确定**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

当您在单跳模式下启用 AppFlow 时，以下命令在后台运行。此处明确指定这些命令是为了进行故障排除。

```
-  add appflow collector <name> -IPAddress <ip_addr>


-  add appflow action <name> -collectors <string>


-  set appflow param -flowRecordInterval <secs>


-  disable ns feature AppFlow


-  enable ns feature AppFlow


-  add appflow policy <name> <rule> <expression>


-  set appflow policy <name> -rule <expression>


-  bind vpn vserver <vsname> -policy <string> -type <type> -priority
<positive_integer>


-  set vpn vserver <name> -appflowLog ENABLED
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-  save ns config
```

EUEM 虚拟通道数据是 NetScaler Console 从 Gateway 实例接收的 HDX Insight 数据的一部分。EUEM 虚拟通道提供有关 ICA RTT 的数据。如果未启用 EUEM 虚拟通道，剩余的 HDX Insight 数据仍会显示在 NetScaler Console 上。

为以双跳模式部署的 NetScaler Gateway 设备启用数据收集

NetScaler Gateway 双跳模式为组织的内部网络提供了额外的保护，因为攻击者需要穿透多个安全区域或非军事区 (DMZ) 才能到达安全网络中的服务器。如果您想分析 ICA 连接经过的跳数（NetScaler Gateway 设备），以及每个 TCP 连接上的延迟详情以及它与客户端感知的总 ICA 延迟相比如何，您必须安装 NetScaler Console，以便 NetScaler Gateway 设备报告这些重要统计数据。

启用分析(/en-us/netscaler-application-delivery-management-software/media/double-hop-2.png)

第一个 DMZ 中的 NetScaler Gateway 处理用户连接并执行 SSL VPN 的安全功能。此 NetScaler Gateway 加密用户连接，确定用户如何进行身份验证，并控制对内部网络中服务器的访问。

第二个 DMZ 中的 NetScaler Gateway 用作 NetScaler Gateway 代理设备。此 NetScaler Gateway 使 ICA 流量能够穿过第二个 DMZ，以完成与服务器场的用户连接。

NetScaler Console 可以部署在属于第一个 DMZ 中 NetScaler Gateway 设备的子网中，也可以部署在属于第二个 DMZ 中 NetScaler Gateway 设备的子网中。在上图中，第一个 DMZ 中的 NetScaler Console 和 NetScaler Gateway 部署在同一子网中。

在双跳模式下，NetScaler Console 从一个设备收集 TCP 记录，并从另一个设备收集 ICA 记录。将 NetScaler Gateway 设备添加到 NetScaler Console 清单并启用数据收集后，每个设备都会通过跟踪跳数和连接链 ID 来导出报告。

为了让 NetScaler Console 识别哪个设备正在导出记录，每个设备都指定了一个跳数，每个连接都指定了一个连接链 ID。跳数表示流量从客户端流向服务器所经过的 NetScaler Gateway 设备数量。连接链 ID 表示客户端和服务器之间的端到端连接。

NetScaler Console 使用跳数和连接链 ID 来关联来自两个 NetScaler Gateway 设备的数据并生成报告。

要监控以这种模式部署的 NetScaler Gateway 设备，您必须首先将 NetScaler Gateway 添加到 NetScaler Console 清单中，在 NetScaler Console 上启用 AppFlow，然后才能在 NetScaler Console 仪表板上查看报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在用于 Optimal Gateway 的虚拟服务器上配置 HDX Insight

在用于 Optimal Gateway 的虚拟服务器上配置 HDX™ Insight 的步骤：

1. 导航到**基础架构 > 实例**，然后选择要启用分析的 NetScaler 实例。
2. 从**选择操作**列表中，选择**配置分析**。
3. 选择配置用于身份验证的 VPN 虚拟服务器，然后单击**启用分析**。
4. 选择 **HDX Insight**，然后选择 **ICA**。
5. 根据需要选择其他高级选项。
6. 单击**确定**。
7. 在其他 VPN 虚拟服务器上重复步骤 3 到 6。

在 NetScaler Console 上启用数据收集

如果您启用 NetScaler Console 从两台设备收集 ICA 详细信息，则收集到的详细信息将是冗余的。也就是说，两台设备会报告相同的指标。为了解决这种情况，您必须在第一台 NetScaler Gateway 设备上启用 ICA 的 AppFlow，然后在第二台设备上启用 TCP 的 AppFlow。通过这样做，一台设备导出 ICA AppFlow 记录，另一台设备导出 TCP AppFlow 记录。这还可以节省解析 ICA 流量的处理时间。

要从 NetScaler Console 启用 AppFlow 功能：

1. 在 Web 浏览器中，键入 NetScaler Console 的 IP 地址（例如，`<http://192.168.100.1>`）。
2. 在**用户名**和**密码**中，输入管理员凭据。
3. 导航到**基础架构 > 实例**，然后选择要启用分析的 NetScaler 实例。
4. 从**选择操作**列表中，选择**配置分析**。
5. 选择 VPN 虚拟服务器，然后点击 **启用分析**。
6. 选择 **HDX Insight**，然后分别选择 **ICA** 或 **TCP** 用于 ICA 流量或 TCP 流量。

   注意

   如果 NetScaler 设备上未为相应的服务或服务组启用 AppFlow 日志记录，则即使 Insight 列显示“已启用”，NetScaler Console 控制板也不会显示记录。

7. 点击 **确定**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置 NetScaler Gateway 设备以导出数据

安装 NetScaler Gateway 设备后，您必须在 NetScaler Gateway 设备上配置以下设置，才能将报告导出到 NetScaler Console：

- 配置第一和第二 DMZ 中的 NetScaler Gateway 设备的虚拟服务器，使其相互通信。
- 将第二 DMZ 中的 NetScaler Gateway 虚拟服务器绑定到第一 DMZ 中的 NetScaler Gateway 虚拟服务器。
- 在第二 DMZ 中的 NetScaler Gateway 上启用双跳。
- 禁用第二 DMZ 中的 NetScaler Gateway 虚拟服务器上的身份验证。
- 启用其中一个 NetScaler Gateway 设备以导出 ICA 记录
- 启用另一个 NetScaler Gateway 设备以导出 TCP 记录：
- 在两个 NetScaler Gateway 设备上启用连接链。

使用命令行界面配置 NetScaler Gateway：

1. 配置第一个 DMZ 中的 NetScaler Gateway 虚拟服务器，使其与第二个 DMZ 中的 NetScaler Gateway 虚拟服务器通信。

```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (ON or
OFF)] [-imgGifToPng]



add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
```

2. 将第二个 DMZ 中的 NetScaler Gateway 虚拟服务器绑定到第一个 DMZ 中的 NetScaler Gateway 虚拟服务器。在第一个 DMZ 中的 NetScaler Gateway 上运行以下命令：

```
bind vpn vserver <name> -nextHopServer <name>



bind vpn vserver vs1 -nextHopServer nh1
```

3. 在第二个 DMZ 中的 NetScaler Gateway 上启用双跳和 AppFlow。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set vpn vserver <name> [- doubleHop ( ENABLED or DISABLED )] [-
 appflowLog ( ENABLED or DISABLED )]



set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
```

4. 禁用第二个 DMZ 中的 NetScaler Gateway 虚拟服务器上的身份验证。

```
set vpn vserver <name> [-authentication (ON or OFF)]



set vpn vserver vs -authentication OFF
```

5. 启用其中一个 NetScaler Gateway 设备以导出 TCP 记录。

```
bind vpn vserver <name> [-policy <string> -priority <positive_integer>]
[-type <type>]



bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
OTHERTCP_REQUEST
```

6. 启用另一个 NetScaler Gateway 设备以导出 ICA 记录：

```
bind vpn vserver <name> [-policy <string> -priority <positive_integer>]
[-type <type>]



bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
ICA_REQUEST
```

7. 在两个 NetScaler Gateway 设备上启用连接链：

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set appflow param -connectionChaining ENABLED
```

使用配置实用程序配置 NetScaler Gateway：

1. 配置第一个 DMZ 中的 NetScaler Gateway 以与第二个 DMZ 中的 NetScaler Gateway 通信，并将第二个 DMZ 中的 NetScaler Gateway 绑定到第一个 DMZ 中的 NetScaler Gateway。
   a. 在“**配置**”选项卡上，展开“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。
   b. 在右侧窗格中，双击虚拟服务器，然后在“高级”组中，展开“**已发布的应用程序**”。
   c. 单击“**下一跳服务器**”，并将下一跳服务器绑定到第二个 NetScaler Gateway 设备。
2. 在第二个 DMZ 中的 NetScaler Gateway 上启用双跳。
   a. 在“**配置**”选项卡上，展开“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。
   b. 在右侧窗格中，双击虚拟服务器，然后在“**基本设置**”组中，单击编辑图标。
   c. 展开更多，选择 **双跳**，然后单击 **确定**。
3. 在第二个 DMZ 中的 NetScaler Gateway 上的虚拟服务器上禁用身份验证。
   a. 在 **配置** 选项卡上，展开 **NetScaler Gateway**，然后单击 **虚拟服务器**。
   b. 在右侧窗格中，双击虚拟服务器，然后在 **基本设置** 组中，单击编辑图标。
   c. 展开 **更多**，然后清除 **启用身份验证**。
4. 启用其中一个 NetScaler Gateway 设备以导出 TCP 记录。
   a. 在 **配置** 选项卡上，展开 **NetScaler Gateway**，然后单击 **虚拟服务器**。
   b. 在右侧窗格中，双击虚拟服务器，然后在高级组中，展开策略。
   c. 单击 + 图标，从 **选择策略** 列表中选择 **AppFlow**，然后从 **选择类型** 列表中选择 **其他 TCP 请求**。
   d. 单击 **继续**。
   e. 添加策略绑定，然后单击 **关闭**。
5. 启用另一个 NetScaler Gateway 设备以导出 ICA 记录：
   a. 在 **配置** 选项卡上，展开 **NetScaler Gateway**，然后单击 **虚拟服务器**。
   b. 在右侧窗格中，双击虚拟服务器，然后在 **高级** 组中， 展开 **策略**。
   c. 单击 + 图标，从 **选择策略** 列表中选择 AppFlow，然后从 Choose Type 列表中选择 **其他 TCP 请求**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. 单击“**继续**”。

e. 添加策略绑定，然后单击“**关闭**”。

6. 在两个 NetScaler Gateway 设备上启用连接链。

a. 在“**配置**”选项卡上，导航到“**系统**”>“**Appflow**”。

b. 在右侧窗格的“**设置**”组中，双击“**更改 Appflow 设置**”。

c. 选择“**连接链**”，然后单击“**确定**”。

7. 配置第一个 DMZ 中的 NetScaler Gateway 以与第二个 DMZ 中的 NetScaler Gateway 通信，并将第二个 DMZ 中的 NetScaler Gateway 绑定到第一个 DMZ 中的 NetScaler Gateway。

a. 在“配置”选项卡上，展开“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。

b. 在右侧窗格中，双击虚拟服务器，然后在“**高级组**”中，展开“**已发布的应用程序**”。

c. 单击“**下一跳服务器**”，并将下一跳服务器绑定到第二个 NetScaler Gateway 设备。

8. 在第二个 DMZ 中的 NetScaler Gateway 上启用双跳。

a. 在“配置”选项卡上，展开“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。

b. 在右侧窗格中，双击虚拟服务器，然后在“**基本设置**”组中，单击编辑图标。

c. 展开“更多”，选择“**双跳**”，然后单击“**确定**”。

9. 禁用第二个 DMZ 中 NetScaler Gateway 上虚拟服务器的身份验证。

a. 在“配置”选项卡上，展开“NetScaler Gateway”，然后单击“**虚拟服务器**”。

b. 在右侧窗格中，双击虚拟服务器，然后在“**基本设置**”组中，单击编辑图标。

c. 展开“**更多**”，然后清除“**启用身份验证**”。

10. 启用其中一个 NetScaler Gateway 设备以导出 TCP 记录。

a. 在“配置”选项卡上，展开“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。

b. 在右侧窗格中，双击虚拟服务器，然后在“高级”组中，展开“**策略**”。

c. 单击“**+**”图标，然后从“选择策略”列表中选择“AppFlow”，再从“**选择类型**”列表中选择“**其他 TCP 请求**”。

d. 单击“**继续**”。

e. 添加策略绑定，然后单击“**关闭**”。

11. 启用另一个 NetScaler Gateway 设备以导出 ICA 记录。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 在“配置”选项卡上，展开“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。

b. 在右侧窗格中，双击虚拟服务器，然后在“高级”组中，展开“**策略**”。

c. 单击“**+**”图标，然后从“**选择策略**”列表中选择“AppFlow”，再从“**选择类型**”列表中选择“**其他 TCP 请求**”。

d. 单击“**继续**”。

e. 添加策略绑定，然后单击“**关闭**”。

12. 在两台 NetScaler Gateway 设备上启用连接链。

启用数据收集以监控以透明模式部署的 NetScaler

当 NetScaler 以透明模式部署时，客户端可以直接访问服务器，无需中间的虚拟服务器。如果 NetScaler 设备在 Citrix Virtual Apps and Desktop 环境中以透明模式部署，ICA 流量不会通过 VPN 传输。

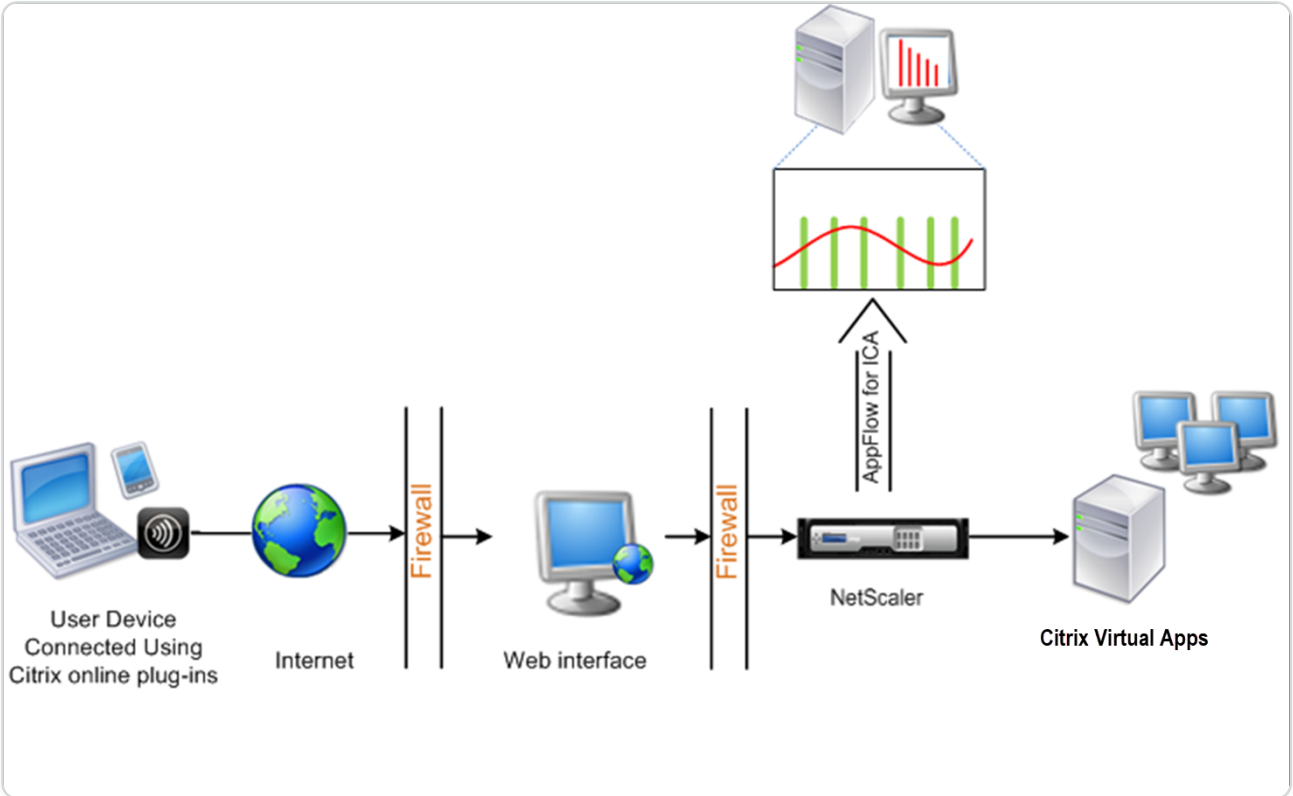
将 NetScaler 添加到 NetScaler Console 清单后，您必须启用 AppFlow 以进行数据收集。启用数据收集取决于设备和模式。在这种情况下，您必须将 NetScaler Console 添加为每台 NetScaler 设备上的 AppFlow 收集器，并且必须配置 AppFlow 策略以收集流经设备的所有或特定 ICA 流量。

注意

- 您无法使用 NetScaler Console 配置实用程序在以透明模式部署的 NetScaler 上启用数据收集。
- 有关命令及其用法的详细信息，请参阅命令参考。
- 有关策略表达式的信息，请参阅策略和表达式。

下图显示了 NetScaler 以透明模式部署时 NetScaler Console 的网络部署：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



要使用命令行界面在 NetScaler 设备上配置数据收集：

在命令提示符下，执行以下操作：

1. 登录到设备。
2. 指定 NetScaler 设备侦听流量的 ICA 端口。

```
set ns param --icaPorts <port>...
```

示例：

```
set ns param -icaPorts 2598 1494
```

注意

- 您可以使用此命令指定最多 10 个端口。
- 默认端口号为 2598。您可以根据需要修改端口号。

3. 将 NetScaler Insight Center 添加为 NetScaler 设备上的 AppFlow 收集器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add appflow collector <name> -IPAddress <ip_addr>
```

示例：

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

注意 要查看在 NetScaler 设备上配置的 AppFlow 收集器，请使用 **show appflow collector** 命令。

4. 创建 AppFlow 操作并将收集器与该操作关联。

```
add appflow action <name> -collectors <string> ...
```

示例：

添加 AppFlow 动作 act-collectors MyInsight

5. 创建 AppFlow 策略以指定生成流量的规则。

```
add appflow policy <policyname> <rule> <action>
```

示例：

```
add appflow policy pol true act
```

6. 将 AppFlow 策略绑定到全局绑定点。

```
bind appflow global <policyname> <priority> -type <type>
```

示例：

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

注意

type 的值必须是 ICA_REQ_OVERRIDE 或 ICA_REQ_DEFAULT 才能应用于 ICA 流量。

7. 将 AppFlow 的 flowRecordInterval 参数值设置为 60 秒。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set appflow param -flowRecordInterval 60
```

示例：

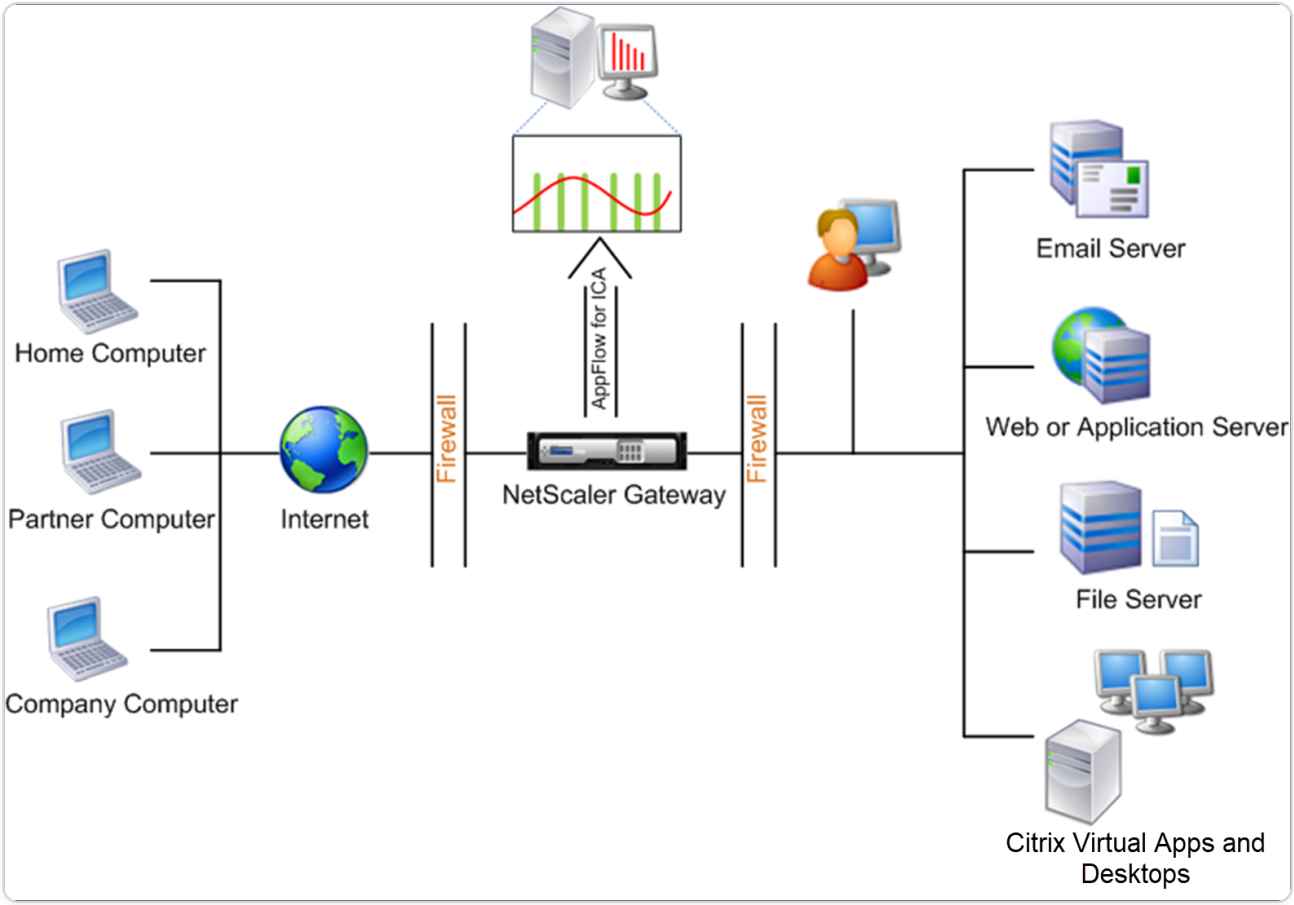
```
set appflow param -flowRecordInterval 60
```

8. 保存配置。键入：`save ns config`

为以单跳模式部署的 NetScaler Gateway 设备启用数据收集

当您以单跳模式部署 NetScaler Gateway 时，它位于网络的边缘。Gateway 实例为桌面交付基础架构提供代理 ICA 连接。单跳是最简单、最常见的部署方式。如果外部用户尝试访问组织内部网络，单跳模式可提供安全性。 在单跳模式下，用户通过虚拟专用网络 (VPN) 访问 NetScaler 设备。

要开始收集报告，您必须将 NetScaler Gateway 设备添加到 NetScaler Console 清单中，并在 NetScaler Console 上启用 AppFlow。



从 NetScaler Console 启用 AppFlow 功能：

1. 导航到 **Infrastructure** \> **Instances**，然后选择要启用分析的 NetScaler 实例。
2. 从 **Action** 列表中，选择 **Enable/Disable Insight**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 选择 **VPN virtual servers**，然后单击 **Enable AppFlow®**。
4. 在 **Enable AppFlow** 字段中，键入 **true**，然后选择 **ICA®**。
5. 单击 **OK**。

注意

在单跳模式下启用 AppFlow 时，以下命令在后台运行。此处明确指定这些命令是为了进行故障排除。

- `add appflow collector \<name\> -IPAddress \<ip\_addr\>`
- `add appflow action \<name\> -collectors \<string\>`
- `set appflow param -flowRecordInterval \<secs\>`
- `disable ns feature AppFlow`
- `enable ns feature AppFlow`
- `add appflow policy \<name\> \<rule\> \<expression\>`
- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

EUEM 虚拟通道数据是 NetScaler Console 从 Gateway 实例接收的 HDX Insight 数据的一部分。EUEM 虚拟通道提供有关 ICA RTT 的数据。如果未启用 EUEM 虚拟通道，剩余的 HDX Insight 数据仍会在 NetScaler Console 上显示。

启用数据收集以监控以透明模式部署的 NetScaler

当 NetScaler 以透明模式部署时，客户端可以直接访问服务器，无需中间虚拟服务器。如果 NetScaler 在 Citrix Virtual Apps and Desktops 环境中以透明模式部署，ICA 流量不会通过 VPN 传输。

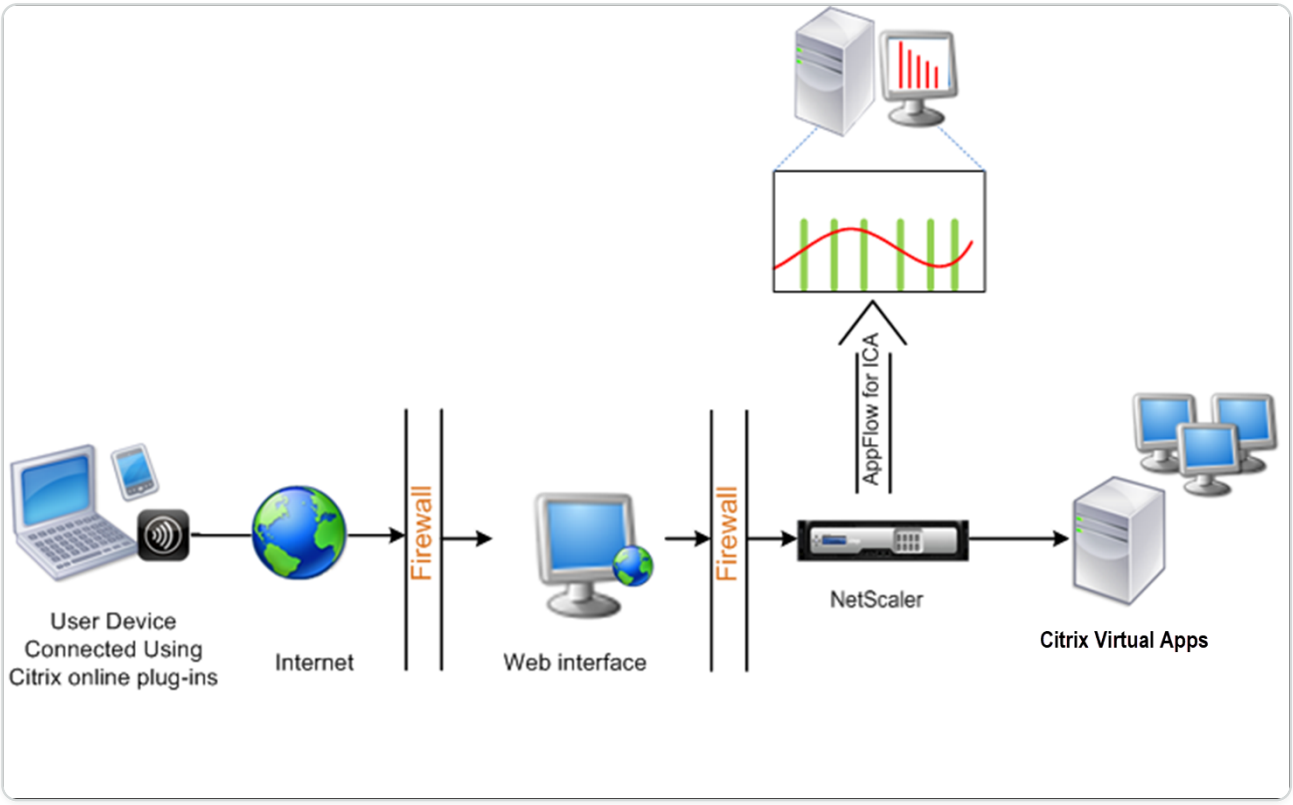
将 NetScaler 添加到 NetScaler Console 清单后，您必须启用 AppFlow 以进行数据收集。启用数据收集取决于设备和模式。在这种情况下，您必须将 NetScaler Console 添加为每个 NetScaler 实例上的 AppFlow 收集器，并且必须配置 AppFlow 策略以收集流经设备的全部或特定 ICA 流量。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

- 您无法使用 NetScaler Console 配置实用程序在以透明模式部署的 NetScaler 上启用数据收集。
- 有关命令及其用法的详细信息，请参阅 命令参考。
- 有关策略表达式的信息，请参阅 策略和表达式。

下图显示了当 NetScaler 以透明模式部署时 NetScaler Console 的网络部署：



要在 NetScaler 设备上配置数据收集，请使用命令行界面：

在命令提示符下，执行以下操作：

1. 登录到设备。
2. 指定 NetScaler 设备侦听流量的 ICA 端口。

```
set ns param --icaPorts \<port\>...
```

示例：

```
set ns param -icaPorts 2598 1494
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

- 您可以使用此命令指定最多 10 个端口。
- 默认端口号为 2598。您可以根据需要修改端口号。

3. 将 NetScaler Insight Center 添加为 NetScaler 实例上的 AppFlow 收集器。

```
add appflow collector <name> -IPAddress <ip_addr>
```

示例：

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

注意 要查看在 NetScaler 实例上配置的 AppFlow 收集器，请使用 **show appflow collector** 命令。

4. 创建 AppFlow® 操作并将收集器与该操作关联。

```
add appflow action <name> -collectors <string> ...
```

示例：

```
add appflow action act -collectors MyInsight
```

5. 创建 AppFlow 策略以指定生成流量的规则。

```
add appflow policy <policyname> <rule> <action>
```

示例：

```
add appflow policy pol true act
```

6. 将 AppFlow 策略绑定到全局绑定点。

```
bind appflow global <policyname> <priority> -type <type>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

示例：

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

注意

type 的值必须为 ICA_REQ_OVERRIDE 或 ICA_REQ_DEFAULT 才能应用于 ICA® 流量。

7. 将 AppFlow 的 flowRecordInterval 参数值设置为 60 秒。

```
set appflow param -flowRecordInterval 60
```

8. 保存配置。

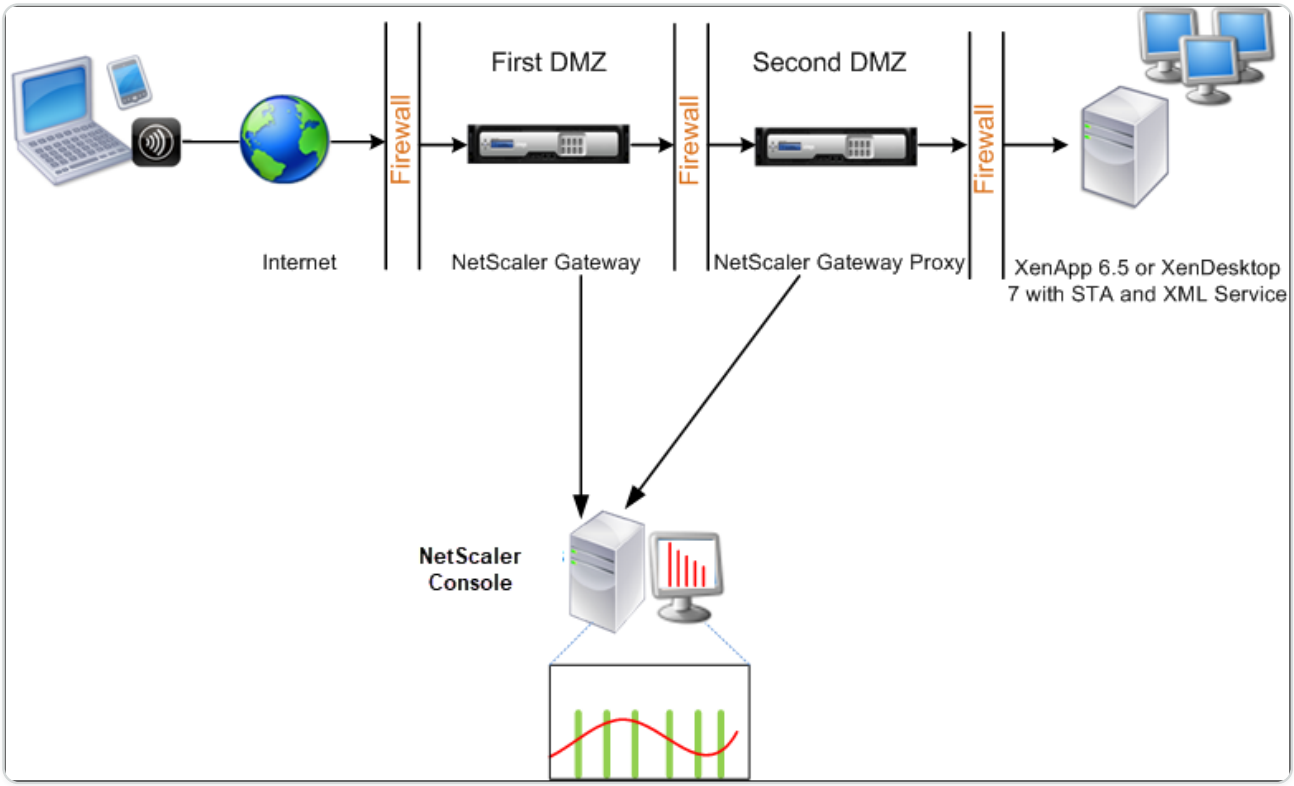
```
save ns config
```

为双跳模式下部署的 NetScaler Gateway 设备启用数据收集

NetScaler Gateway 双跳模式为组织的内部网络提供了额外保护，因为攻击者需要穿透多个安全区域或非军事区 (DMZ) 才能到达安全网络中的服务器。如果您想分析 ICA 连接经过的跳数 (NetScaler Gateway 设备)，以及每个 TCP 连接的延迟详情以及它与客户端感知的总 ICA 延迟相比的表现，则必须安装 NetScaler Console，以便 NetScaler Gateway 设备报告这些重要统计数据。

图 3. 以双跳模式部署的 NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.



第一个 DMZ 中的 NetScaler Gateway 处理用户连接并执行 SSL VPN 的安全功能。此 NetScaler Gateway 加密用户连接，确定用户如何进行身份验证，并控制对内部网络中服务器的访问。

第二个 DMZ 中的 NetScaler Gateway 充当 NetScaler Gateway 代理设备。此 NetScaler Gateway 使 ICA 流量能够穿过第二个 DMZ，以完成用户到服务器场的连接。

NetScaler Console 可以部署在属于第一个 DMZ 中的 NetScaler Gateway 设备的子网中，也可以部署在属于第二个 DMZ 中的 NetScaler Gateway 设备的子网中。在上面的图像中，第一个 DMZ 中的 NetScaler Console 和 NetScaler Gateway 部署在同一个子网中。

在双跳模式下，NetScaler Console 从一个设备收集 TCP 记录，从另一个设备收集 ICA 记录。将 NetScaler Gateway 设备添加到 NetScaler Console 清单并启用数据收集后，每个设备都会通过跟踪跳数和连接链 ID 来导出报告。

为了让 NetScaler Console 识别哪个设备正在导出记录，每个设备都指定了跳数，每个连接都指定了连接链 ID。跳数表示流量从客户端流向服务器所经过的 NetScaler Gateway 设备的数量。连接链 ID 表示客户端和服务器之间的端到端连接。

NetScaler Console 使用跳数和连接链 ID 来关联来自两个 NetScaler Gateway 设备的数据并生成报告。

要监控以这种模式部署的 NetScaler Gateway 设备，您必须首先将 NetScaler Gateway 添加到 NetScaler Console 清单，在 NetScaler Console 上启用 AppFlow，然后在 NetScaler Console 控制面板上查看报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 NetScaler Console 上启用数据收集

如果您启用 NetScaler Console 开始从两个设备收集 ICA 详细信息，则收集到的详细信息是冗余的。也就是说，两个设备都报告相同的指标。为了克服这种情况，您必须在第一个 NetScaler Gateway 设备之一上启用 TCP 的 AppFlow，然后在第二个设备上启用 ICA 的 AppFlow。通过这样做，其中一个设备导出 ICA AppFlow 记录，另一个设备导出 TCP AppFlow 记录。这还节省了解析 ICA 流量的处理时间。

要从 NetScaler Console 启用 AppFlow 功能：

1. 导航到 **基础架构 > 实例**，然后选择要启用分析的 NetScaler 实例。
2. 从“**操作**”列表中，选择“**启用/禁用 洞察**”。
3. 选择 VPN 虚拟服务器，然后单击“**启用 AppFlow®**”。
4. 在“**启用 AppFlow**”字段中，键入 **true**，并分别为 ICA 流量和 TCP 流量选择 **ICA/TCP**。

   注意

   如果 NetScaler 设备上的服务或服务组未启用 AppFlow 日志记录，NetScaler Console 仪表板将不显示记录，即使 Insight 列显示“已启用”。

5. 单击“**确定**”。

配置 NetScaler Gateway 设备以导出数据

安装 NetScaler Gateway 设备后，您必须在 NetScaler Gateway 设备上配置以下设置，才能将报告导出到 NetScaler Console：

- 配置第一个和第二个 DMZ 中的 NetScaler Gateway 设备的虚拟服务器以相互通信。
- 将第二个 DMZ 中的 NetScaler Gateway 虚拟服务器绑定到第一个 DMZ 中的 NetScaler Gateway 虚拟服务器。
- 在第二个 DMZ 中的 NetScaler Gateway 上启用双跳。
- 在第二个 DMZ 中的 NetScaler Gateway 虚拟服务器上禁用身份验证。
- 启用其中一个 NetScaler Gateway 设备以导出 ICA 记录
- 启用另一个 NetScaler Gateway 设备以导出 TCP 记录：
- 在两个 NetScaler Gateway 设备上启用连接链。

使用命令行界面配置 NetScaler Gateway：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 配置第一个 DMZ 中的 NetScaler Gateway 虚拟服务器，使其与第二个 DMZ 中的 NetScaler Gateway 虚拟服务器通信。

   add vpn nextHopServer \<name\> \<nextHopIP\> \<nextHopPort\> \[**-secure**(ON|OFF)\] \[**-imgGifToPng**\] ...

   ```
   add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
   ```

2. 将第二个 DMZ 中的 NetScaler Gateway 虚拟服务器绑定到第一个 DMZ 中的 NetScaler Gateway 虚拟服务器。在第一个 DMZ 中的 NetScaler Gateway 上运行以下命令：

   绑定 vpn vserver \<name\> **-下一跳服务器** \<name\>

   ```
   bind vpn vserver vs1 -nextHopServer nh1
   ```

3. 在第二个 DMZ 中的 NetScaler Gateway 上启用双跳和 AppFlow。

   设置 vpn vserver \<name\> \[**- 双跳** (启用 |禁用)\] \[**- AppFlow日志** (启用 |禁用)\]

   ```
   set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
   ```

4. 在第二个 DMZ 中的 NetScaler Gateway 虚拟服务器上禁用身份验证。

   set vpn vserver\<name\> \[**-authentication** (ON|OFF)\]

   ```
   set vpn vserver vs -authentication OFF
   ```

5. 启用其中一个 NetScaler Gateway 设备以导出 TCP 记录。

   bind vpn vserver\<name\> \[**-policy**\<string\> **-priority**\<positive_integer\>\] \[**-type**\<type\>\]

   ```
   bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
   OTHERTCP\_REQUEST
   ```

6. 启用另一个 NetScaler Gateway 设备以导出 ICA 记录：

   bind vpn vserver\<name\> \[**-policy**\<string\> **-priority**\<positive_integer\>\] \[**-type**\<type\>\]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
ICA\_REQUEST
```

7. 在两个 NetScaler Gateway 设备上启用连接链：

   set appFlow param

```
set appflow param -connectionChaining ENABLED
```

使用配置实用程序配置 NetScaler Gateway：

1. 配置第一个 DMZ 中的 NetScaler Gateway 以与第二个 DMZ 中的 NetScaler Gateway 通信，并将第二个 DMZ 中的 NetScaler Gateway 绑定到第一个 DMZ 中的 NetScaler Gateway。
   a. 在“**配置**”选项卡上，展开“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。
   b. 在右侧窗格中，双击虚拟服务器，然后在“高级”组中，展开“**已发布的应用程序**”。
   c. 单击“**下一跳服务器**”，并将下一跳服务器绑定到第二个 NetScaler Gateway 设备。
2. 在第二个 DMZ 中的 NetScaler Gateway 上启用双跳。
   a. 在“**配置**”选项卡上，展开“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。
   b. 在右侧窗格中，双击虚拟服务器，然后在“**基本设置**”组中，单击编辑图标。
   c. 展开“**更多**”，选择“**双跳**”，然后单击“**确定**”。
3. 在第二个 DMZ 中的 NetScaler Gateway 上的虚拟服务器上禁用身份验证。
   a. 在“**配置**”选项卡上，展开“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。
   b. 在右侧窗格中，双击虚拟服务器，然后在“**基本设置**”组中，单击编辑图标。
   c. 展开“**更多**”，然后清除“**启用身份验证**”。
4. 启用其中一个 NetScaler Gateway 设备以导出 TCP 记录。
   a. 在“**配置**”选项卡上，展开“**NetScaler Gateway**”，然后单击“**虚拟服务器**”。
   b. 在右侧窗格中，双击虚拟服务器，并在“高级”组中，展开“策略”。
   c. 单击 + 图标，并从“**选择策略**”列表中选择“**AppFlow**”，然后从“**选择类型**”下拉列表中选择“**其他 TCP 请求**”。
   d. 单击“**继续**”。
   e. 添加策略绑定，然后单击“**关闭**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 启用其他 NetScaler Gateway 设备以导出 ICA 记录：
   a. 在“**配置**”选项卡上，展开“**NetScaler Gateway**”并单击“**虚拟服务器**”。
   b. 在右侧窗格中，双击虚拟服务器，并在“**高级**”组中，展开“**策略**”。
   c. 单击 + 图标，并从“**选择策略**”下拉列表中选择“**AppFlow**”，然后从“选择类型”下拉列表中选择“**其他 TCP 请求**”。
   d. 单击“**继续**”。
   e. 添加策略绑定，然后单击“**关闭**”。
6. 在两个 NetScaler Gateway 设备上启用连接链。
   a. 在**Configuration**选项卡上，导航到**Settings > Appflow**。
   b. 在右侧窗格中，在“**设置**”组中，单击“**更改 Appflow 设置**”。
   c. 选择“**连接链**”，然后单击“**确定**”。

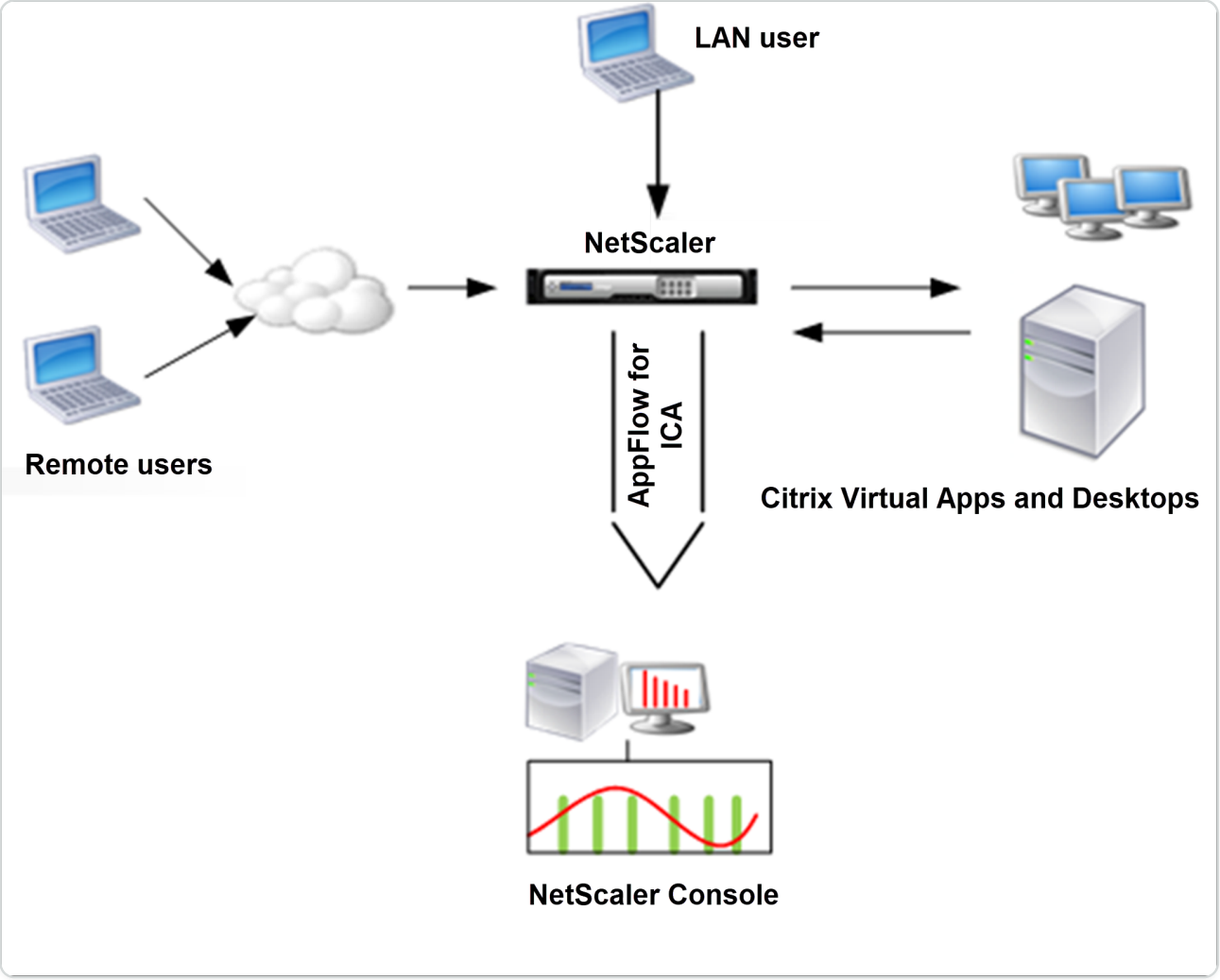
启用数据收集以监控以 LAN 用户模式部署的 NetScaler

访问 Citrix Virtual App 或 Desktop 应用程序的外部用户必须在 NetScaler Gateway 上进行身份验证。但是，内部用户可能不需要重定向到 NetScaler Gateway。此外，在透明模式部署中，管理员必须手动应用路由策略，以便将请求重定向到 NetScaler 设备。

为了克服这些挑战，并让 LAN 用户直接连接到 Citrix Virtual Apps and Desktops 应用程序，您可以通过配置缓存重定向虚拟服务器将 NetScaler 设备部署为 LAN 用户模式，该服务器在 NetScaler Gateway 设备上充当 SOCKS 代理。

图 4. 以 LAN 用户模式部署的 NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意 NetScaler Console 和 NetScaler Gateway 设备位于同一子网中。

要监控以此模式部署的 NetScaler 设备，首先将 NetScaler 设备添加到 NetScaler Insight 清单中，启用 AppFlow，然后查看控制板上的报告。

将 NetScaler 设备添加到 NetScaler Console 清单后，您必须启用 AppFlow 以进行数据收集。

注意

- 您无法通过使用 NetScaler Console 配置实用程序在以 LAN 用户模式部署的 NetScaler 上启用数据收集。
- 有关命令及其用法的详细信息，请参阅《命令参考》。
- 有关策略表达式的信息，请参阅《策略和表达式》。

要通过使用命令行界面在 NetScaler 设备上配置数据收集：

在命令提示符下，执行以下操作：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 登录到设备。
2. 添加一个前向代理缓存重定向虚拟服务器，使用代理IP和端口，并将服务类型指定为HDX。

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType
<cachetype>] [ - cltTimeout <secs>]
```

示例：

```
add cr vserver cr1 HDX 10.12.2.2 443 –cacheType FORWARD –cltTimeout 180
```

注意

如果您正在使用NetScaler Gateway设备访问LAN网络，请添加一个由匹配VPN流量的策略应用的动作。

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]



add vpn trafficPolicy** \<name\> \<rule\> \<action\>
```

示例：

```
add vpn trafficAction act1 tcp -HDX ON



add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. 在NetScaler设备上将NetScaler Console添加为AppFlow收集器。

```
add appflow collector** \<name\> **-IPAddress** \<ip\_addr\>
```

示例：

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

4. 创建AppFlow®动作并将收集器与该动作关联。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add appflow action** \<name\> **-collectors** \<string\> ...
```

示例：

```
add appflow action act -collectors MyInsight
```

5. 创建AppFlow策略以指定生成流量的规则。

```
add appflow policy** \<policyname\> \<rule\> \<action\>
```

示例：

```
add appflow policy pol true act
```

6. 将AppFlow策略绑定到全局绑定点。

```
bind appflow global** \<policyname\> \<priority\> **-type** \<type\>
```

示例：

```
bind appflow global pol 1 -type ICA\_REQ\_DEFAULT
```

注意

type 的值必须是 ICA_REQ_OVERRIDE 或 ICA_REQ_DEFAULT 才能应用于 ICA 流量。

7. 将AppFlow的flowRecordInterval参数值设置为60秒。

```
set appflow param -flowRecordInterval 60
```

示例：

```
set appflow param -flowRecordInterval 60
```

8. 保存配置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
save ns config
```

为 HDX™ Insight 创建阈值并配置警报

NetScaler Console 上的 HDX Insight 允许您监控通过 NetScaler 实例的 HDX 流量。NetScaler Console 允许您为用于监控 Insight 流量的各种计数器设置阈值。您还可以在 NetScaler Console 中配置规则和创建警报。

HDX 流量类型与各种实体相关联，例如应用程序、桌面、网关、许可证和用户。每个实体都可以包含与其关联的不同指标。例如，应用程序实体与各种点击量、应用程序消耗的带宽以及服务器响应时间相关联。用户实体可以与 WAN 延迟、DC 延迟、ICA® RTT 和用户消耗的带宽相关联。

NetScaler Console 中 HDX Insight 的阈值管理允许您在阈值被突破时主动创建规则和配置警报。现在，此阈值管理已扩展为配置一组阈值规则。您现在可以监控组而不是单个规则。阈值规则组包含一个或多个用户定义的阈值规则，这些规则针对从用户、应用程序和桌面等实体中选择的指标。每个规则都根据您在创建规则时输入的预期值进行监控。对于用户实体，阈值组也可以与地理位置相关联。

仅当配置的阈值组中的所有规则都被突破时，NetScaler Console 才会生成警报。例如，您可以将应用程序的总会话启动计数和应用程序启动计数作为一个阈值组进行监控。仅当两个规则都被突破时，才会生成警报。这允许您为实体设置更实际的阈值。

以下列出了一些示例：

- 阈值规则1：用户的 ICA RTT（指标）必须 \<= 100 毫秒
- 阈值规则2：用户的 WAN 延迟（指标）必须 \<= 100 毫秒

阈值组的示例可以是：{阈值规则 1 + 阈值规则 2}

要创建规则，您必须首先选择要监控的实体。然后，在创建规则时选择一个指标。例如，您可以选择应用程序实体，然后选择“总会话启动计数”或“应用程序启动计数”。您可以为实体和指标的每个组合创建一个规则。使用提供的比较器（\>、\<、\>= 和 \<=）并为每个指标键入阈值。

注意

如果您不想在单个组中监控多个实体，则必须为每个实体创建单独的阈值规则组。

当计数器的值超过阈值时，NetScaler Console 会生成一个事件以表示阈值突破，并为每个事件创建一个警报。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您必须配置接收警报的方式。您可以启用警报在 NetScaler Console 上显示，和/或通过电子邮件或短信在您的移动设备上接收警报。对于后两种操作，您必须在 NetScaler Console 上配置电子邮件服务器或短信服务器。

阈值组也可以绑定到地理位置，以实现用户实体的地理特定监控。

示例用例

ABC 公司是一家全球性公司，在 50 多个国家设有办事处。该公司有两个数据中心，一个在新加坡，另一个在加利福尼亚，托管 Citrix Virtual Apps and Desktops。公司员工通过 NetScaler Gateway 和基于 Citrix GSLB 的重定向在全球范围内访问 Citrix Virtual Apps and Desktops。ABC 公司的 Citrix Virtual Apps and Desktops 管理员 Eric 希望跟踪所有办事处的用户体验，以优化应用程序和桌面交付，实现随时随地访问。Eric 还希望检查用户体验指标，如 ICA RTT、延迟，并主动提出任何偏差。

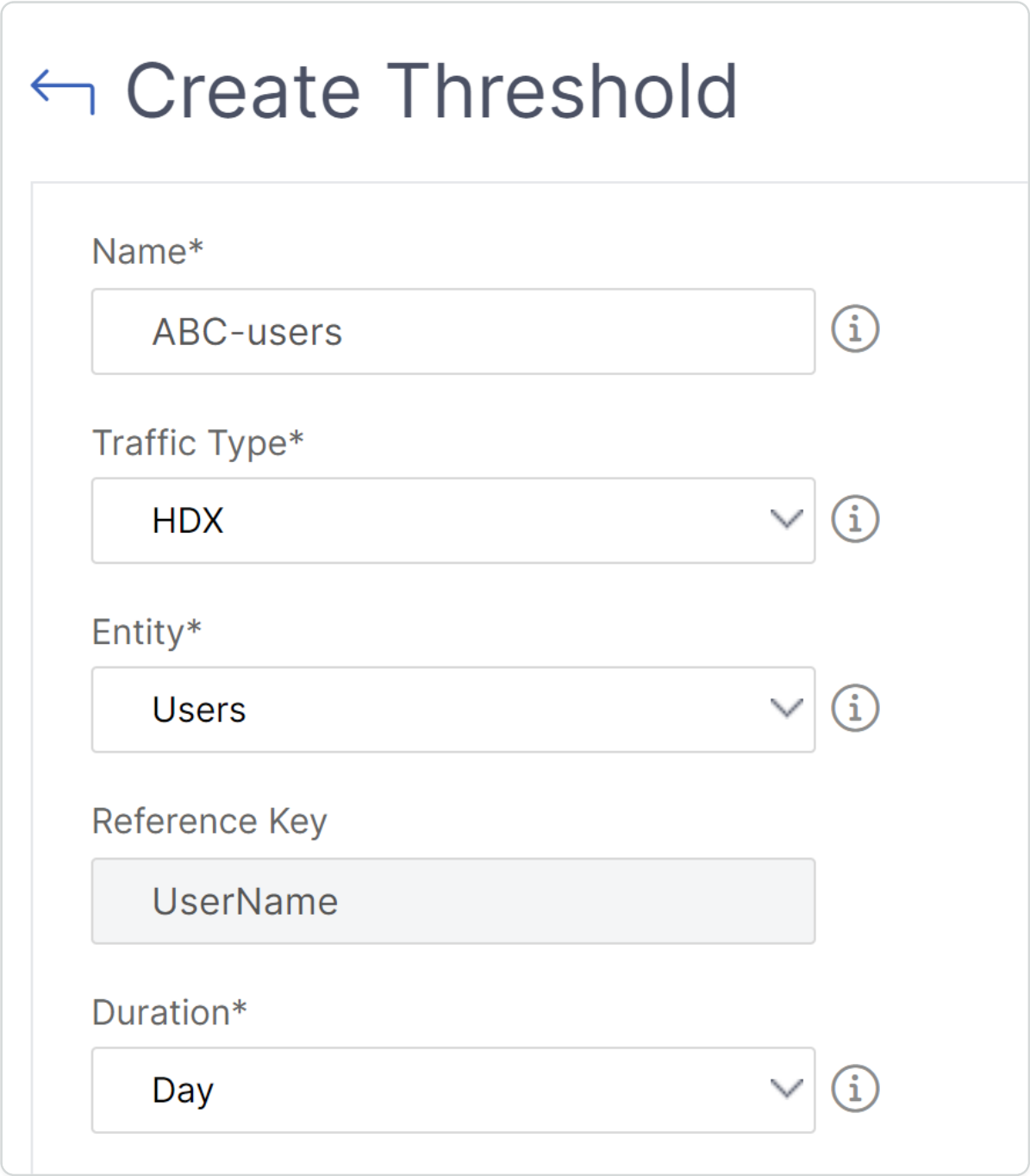
ABC 公司的用户分布广泛。有些用户靠近数据中心，而另一些用户则离数据中心较远。由于用户群分布广泛，这些位置的指标和相应的阈值也各不相同。例如，靠近数据中心的位置的 ICA RTT 可能为 5-10 毫秒，而远程位置的 ICA RTT 可能约为 100 毫秒。

通过 HDX Insight 的阈值规则组管理，Eric 可以为每个位置设置特定地理区域的阈值规则组，并通过电子邮件或短信接收每个区域的违规警报。Eric 还可以在一个阈值规则组中结合跟踪多个指标，并在出现容量问题时缩小根本原因。Eric 现在能够主动跟踪任何偏差，而无需担心手动查看所有 Citrix Virtual Apps and Desktops 组合指标的复杂性。

使用 NetScaler Console 创建 HDX Insight 的阈值规则组并配置警报：

1. 在 NetScaler Console 中，导航到 **Settings > Analytics Settings > Thresholds**。在打开的 **Thresholds** 页面上，单击 **Add**。
2. 在 **Create Thresholds and Alerts** 页面上，指定以下详细信息：
   a. **名称**。键入一个名称，用于创建 NetScaler Console 生成警报的事件。
   b. **流量类型**。从列表框中选择 HDX。
   c. **实体**。从列表框中选择类别或资源类型。实体因您之前选择的每种流量类型而异。
   d. **参考密钥**。参考密钥会根据您选择的流量类型和实体自动生成。
   e. **持续时间**。从列表框中，选择您要监视实体的时间间隔。您可以监视实体一小时、一天或一周。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 为所有实体创建阈值规则组：

   对于 HDX 流量，您必须通过单击 **Add Rule** 创建规则。在打开的 **Add Rules** 弹出窗口中输入值。

   添加规则(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-sla-management-2.png)

   您可以创建多个规则来监控每个实体。在一个组中创建多个规则，可以使您将这些实体作为一组阈值规则而不是单个规则进行监控。单击 **确定** 关闭窗口。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SLA 管理(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-sla-management-3.png)

4. 为用户实体配置地理位置标记

   您可以选择在 **配置地理详细信息** 部分为用户实体创建基于位置的警报。下图显示了一个创建基于地理位置的标记以监控美国西海岸用户 WAN 延迟性能的示例。

   地理详细信息(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-sla-management-4.png)

5. 单击 **启用阈值** 以允许 NetScaler Console 开始监控实体。
6. 或者，配置电子邮件通知和短信通知等操作。
7. 单击 **创建** 以创建阈值规则组。

查看 HDX™ Insight 报告和指标

HDX Insight 提供对您的 NetScaler 实例上与 HDX 流量相关的报告和指标的全面可见性。

您可以查看任何选定实体的 HDX 指标。视图包括以下类别的实体：

- **用户**：显示在选定时间间隔内访问 Citrix Virtual App 或 Desktop 的所有用户的报告。
- **应用程序**： 显示应用程序总数以及所有相关的有用信息（例如应用程序在指定时间间隔内启动的总次数）的报告。
- **实例**：显示关于充当传入流量网关的 NetScaler 实例的报告。
- **网关虚拟服务器**：显示所有虚拟服务器的报告。
- **桌面**：显示在选定时间范围内使用的桌面的报告。
- **许可证**：显示在指定时间段内使用的 SSL VPN 许可证总数的报告。

注意：

从版本 14.1 build 51.x 开始，您可以在 VPN 虚拟服务器级别监控关键指标，例如活动会话、桌面和已启动的应用程序。您可以在 **Gateway > HDX Insight > Gateway Virtual Servers** 下查看所有虚拟服务器的列表。

用户视图报告和指标

此视图中的报告和指标按 Citrix Virtual Apps and Desktops 用户显示。

导航到用户视图：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 导航到 **网关 > HDX Insight > 用户**

   用户图(/en-us/netscaler-application-delivery-management-software/media/analytics-hgx-users-graph.png)

用户视图报告和指标包含以下部分：

- 摘要视图
- 按用户视图
- 按用户会话视图

摘要视图

摘要视图显示在选定时间线内登录的所有用户的报告。此视图中的所有指标/报告都显示其在选定时间段内的对应值，除非另有说明。

要更改选定的时间段：

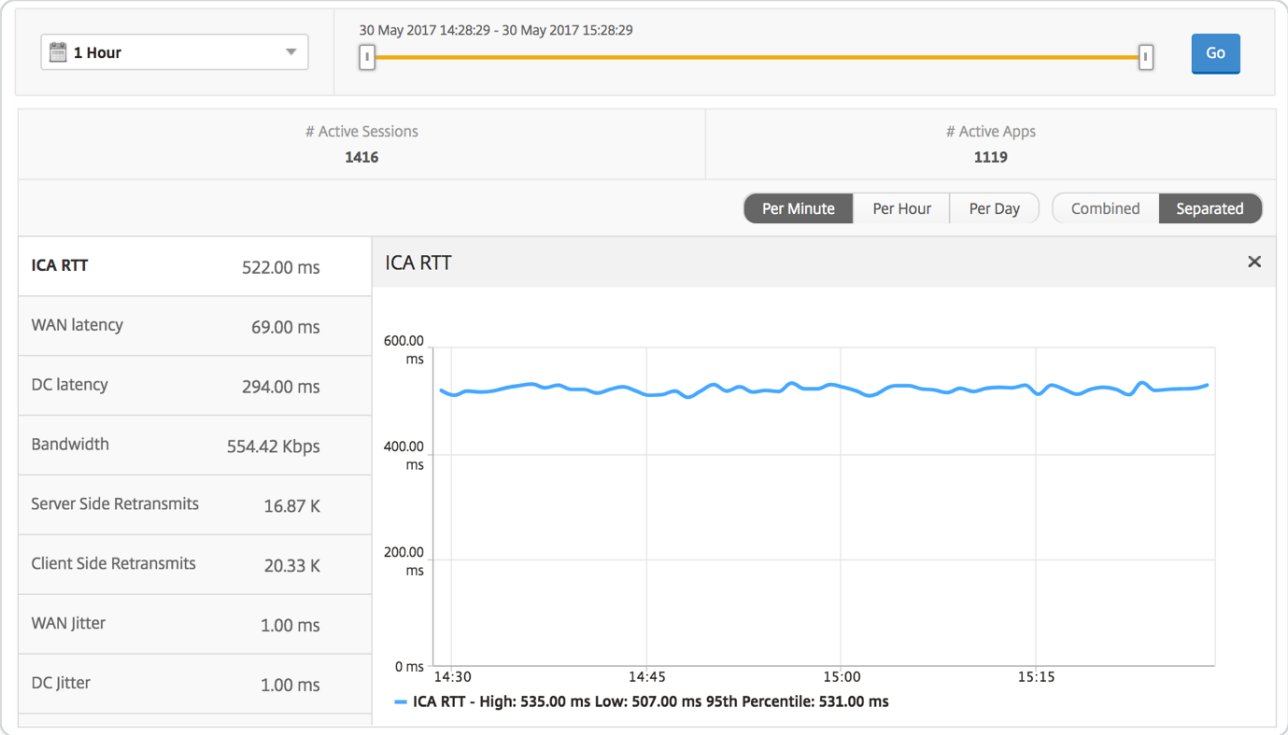
1. 使用时间段列表或时间滑块设置所需的时间间隔。
2. 单击 **Go**。

折线图

指标	描述
活动会话	此数字表示活动 Citrix Virtual Apps and Desktops 会话的数量。
活动应用程序	此数字表示活动 Citrix Virtual App 会话的数量。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual App 或 Desktop 上托管的应用程序或桌面交互时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。即在 NetScaler Gateway 与 VDI 或 CVAD 或 StoreFront 服务器之间。
带宽	在选定时间间隔内，端到端通信所占用的每秒总字节数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
服务器端重传	在 NetScaler 与后端服务器之间的连接上重传的数据包数量。
客户端重传	在 NetScaler 与最终用户之间的连接上重传的数据包数量。此指标的高值并不意味着用户体验不会是无缝的，但表示由于重传导致的高带宽利用率。
客户端快速 RTO	NetScaler 与最终用户之间的连接发生重传超时的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间的连接发生重传超时的次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。



用户摘要报告

以下是此报告特有的指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
活动会话	此数字指示活动 Citrix Virtual Apps and Desktops 会话的计数。
活动应用程序	这个数字表示活动 Citrix Virtual App 会话的数量。
ICA RTT	ICA RTT 是用户在使用分别托管在 Citrix Virtual App 或 Desktop 上的应用程序或桌面时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即，从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。即，在 NetScaler Gateway 与 VDI、CVAD 或 StoreFront 服务器之间。
带宽	在选定时间间隔内，端到端通信所占用的每秒总字节数。
服务器端重传	在 NetScaler 与后端服务器之间的连接上重传的数据包数量。
客户端重传	在 NetScaler 与最终用户之间的连接上重传的数据包数量。此指标的高值并不意味着用户体验不会是无缝的，但表示由于重传导致的高带宽利用率。
客户端快速 RTO	NetScaler 与最终用户之间的连接发生重传超时次数。
服务器端快速 RTO	NetScaler 与后端服务器之间连接上发生重传超时事件的次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
应用启动总次数	用户在选定时间段内启动的应用总数。
总字节数	用户在选定时间段内消耗的总字节数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
活动桌面	在给定时间间隔内活动 Citrix 虚拟桌面的总数。

Users

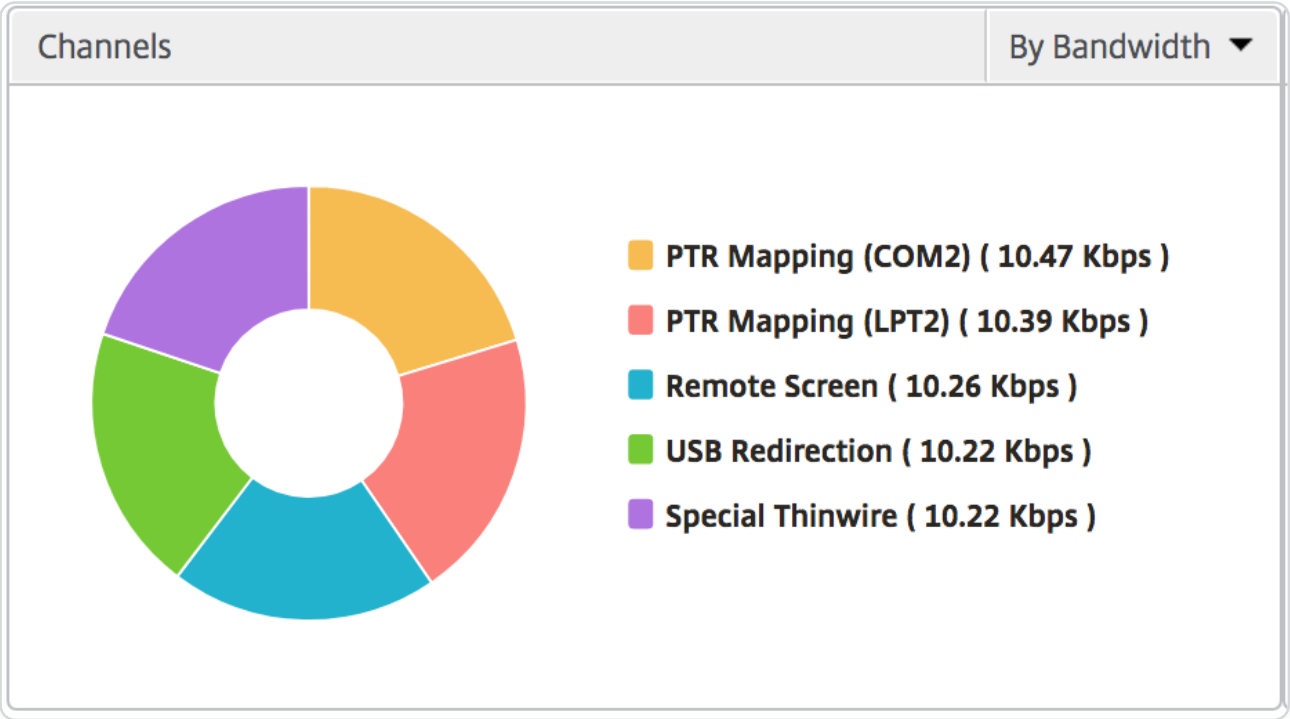
Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

通道

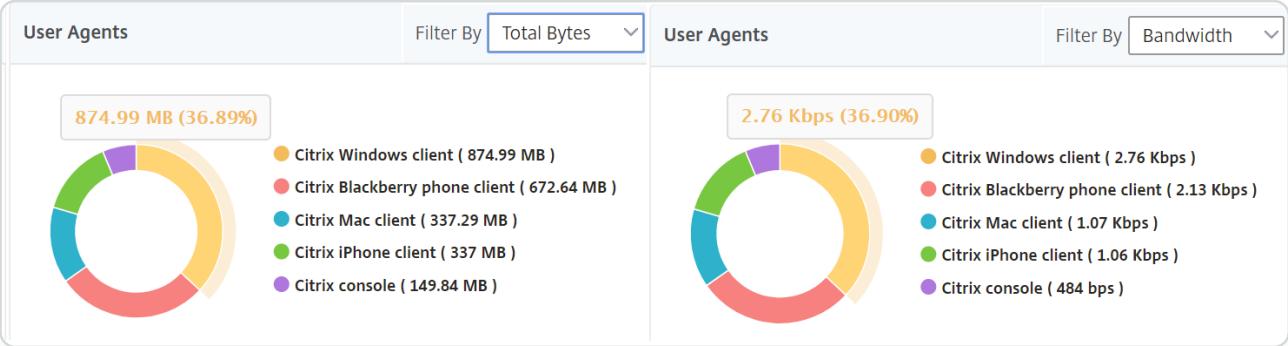
通道以甜甜圈图的形式表示每个 ICA® 虚拟通道消耗的总带宽或总字节数。您还可以按带宽或总字节数对指标进行排序。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

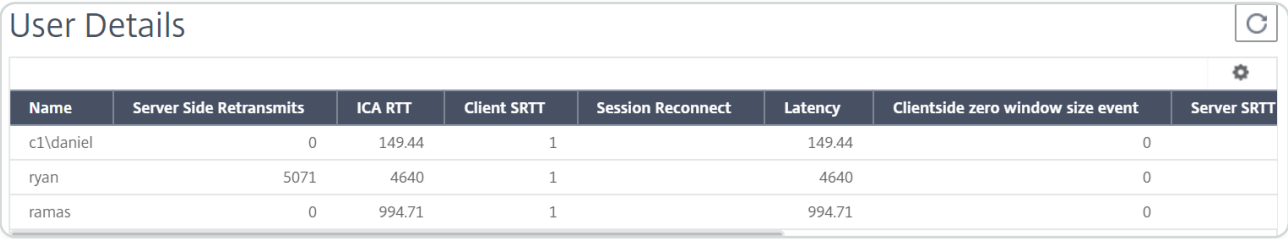


用户代理

用户代理以环形图的形式表示每个工作区客户端消耗的总带宽/总字节数。图表中的每个彩色分段代表一个工作区客户端。分段的长度取决于在该工作区客户端上启动应用程序的用户数量。您还可以按带宽或总字节数对指标进行排序。



单击每个分段以查看使用该工作区客户端的用户的详细信息。



Name	Server Side Retransmits	ICA RTT	Client SRTT	Session Reconnect	Latency	Clientside zero window size event	Server SRTT
c1\daniel	0	149.44	1		149.44	0	
ryan	5071	4640	1		4640	0	
ramas	0	994.71	1		994.71	0	

阈值违规计数

阈值违规计数指标表示在选定的时间段内违规阈值的计数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

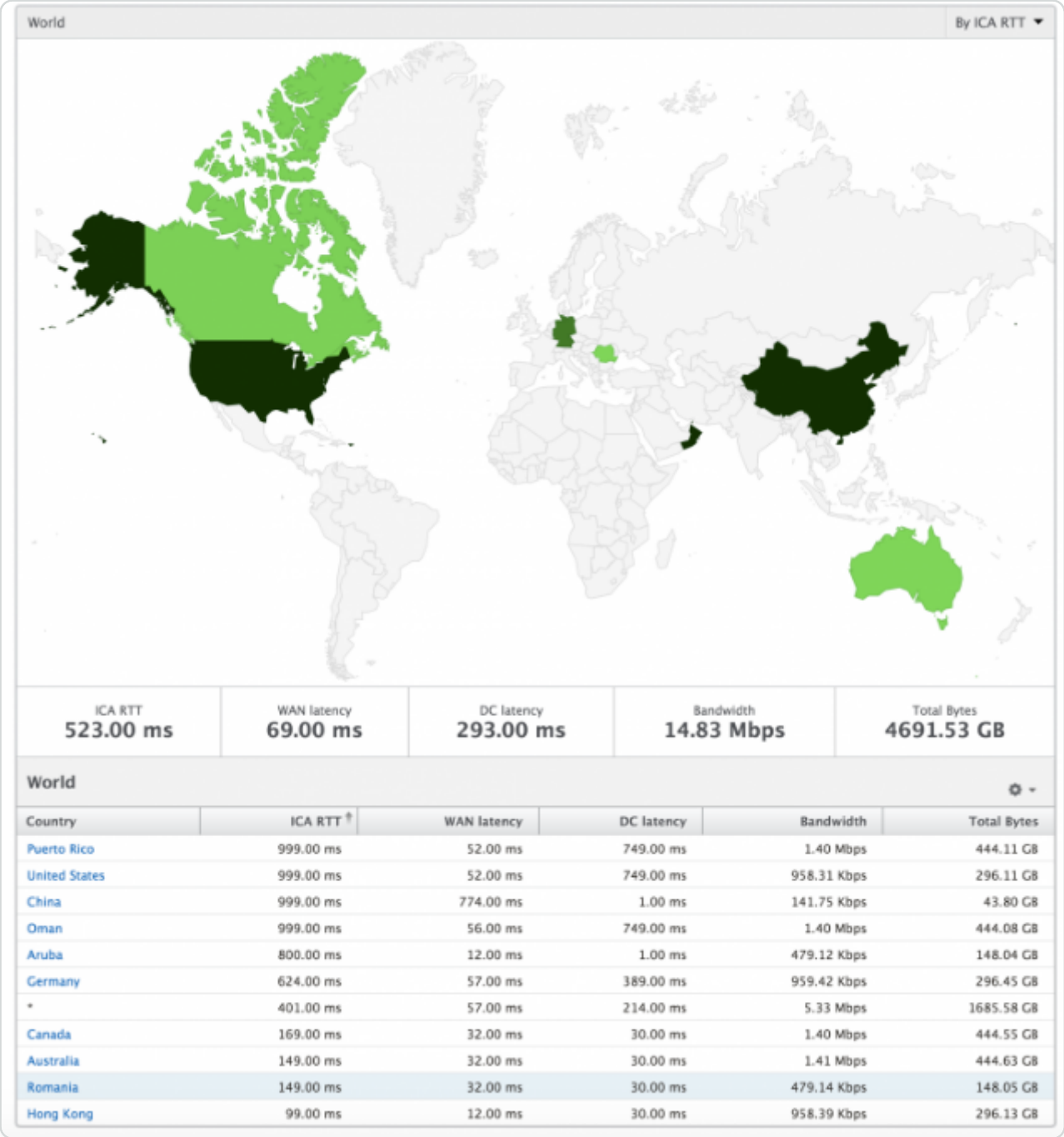
世界地图

HDX Insight 中的世界地图视图允许管理员从地理角度查看历史和活跃用户的详细信息。管理员可以拥有系统的世界视图，通过单击区域，可以深入到特定国家，甚至更深入到城市。管理员可以进一步深入查看按城市和州划分的信息。从 NetScaler Console 12.0 版及更高版本开始，您可以深入查看从地理位置连接的用户。

HDX Insight 世界地图中可查看以下详细信息，并且每个指标的密度以热图的形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- 带宽
- 总字节数

© 1997–2026 Citrix Systems, Inc. All rights reserved.



每个用户视图

每个用户视图为任何特定选定用户提供详细的最终用户体验报告。

导航到特定用户的指标：

1. 使用受支持的 Web 浏览器登录到您的 NetScaler Console。
2. 导航到 **网关 > HDX Insight > 用户**。
3. 从“用户摘要”报告中选择一个特定用户。

折线图

折线图显示了在选定时间段内特定选定用户的所有指标摘要。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

当前/已终止会话报告

此报告与所选用户的所有当前/已终止用户会话相关。这些指标可以按开始时间、会话重新连接和 ACR 计数进行排序。

指标	描述
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	活动/非活动会话显示绿色/红色。
主机延迟	通过 NetScaler 的 ICA 流量因服务器网络而导致的平均延迟。
每个间隔的带宽	会话在该特定时间间隔内消耗的带宽。
会话带宽	会话消耗的带宽，与时间间隔无关。
每个间隔的字节数	会话在该特定时间间隔内消耗的字节数。
开始时间	会话开始时间。
正常运行时间	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual App 服务器 IP。
NetScaler IP 地址	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows 客户端等
客户端版本	工作区版本。
MSI	布尔值（是/否）。指示会话是否为多流 ICA。
会话重新连接	会话重新连接的次数。
ACR 计数	客户端自动将用户重新连接到断开的会话的总次数。
用户访问类型	显示 ICA 会话的访问模式。例如，NetScaler Gateway 用户/透明模式。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
国家/地区	建立会话的国家/地区。
区域	建立会话的区域。
城市	建立会话的城市。
USB 状态	活动/非活动 - 绿色/红色。
接受的 USB 实例数	接受的 USB 实例计数。
USB 实例拒绝数量	被拒绝的 USB 实例数量。
USB 实例停止数量	已停止的 USB 实例数量。
客户端主机名	客户端的主机名。
HA 故障转移计数	HA 故障转移发生的次数。
终止原因	显示会话终止的原因。例如，ICA 会话超时、用户终止会话。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual App 或 Desktop 上托管的应用程序或桌面交互时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。即，在 NetScaler Gateway 与 VDI、CVAD 或 StoreFront 服务器之间。
总字节数	用户在选定时间段内消耗的总字节数。
服务器端重传	在 NetScaler 与后端服务器之间的连接上重传的数据包数量。
客户端重传	在 NetScaler 与最终用户之间的连接上重传的数据包数量。此指标的高值并不意味着用户体验不会是无缝的，但表示由于重传导致的高带宽利用率。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
客户端快速 RTO	在 NetScaler 与最终用户之间的连接上发生重传超时的次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
服务器端快速 RTO	在 NetScaler 与后端服务器之间的连接上发生重传超时的次数。

在 HDX Insight 中对 EDT 的支持

NetScaler Console 现在支持开明数据传输 (EDT)，用于显示 HDX Insight 的分析数据。也就是说，NetScaler Console 现在同时支持 UDP 和 TCP 协议。NetScaler Gateway 对 EDT 的支持可确保运行 Citrix Workspace 的用户获得高清的会话内虚拟桌面用户体验。

HDX Insight 现在将 EDT 会话和非 EDT 会话的数量显示为活动会话报告的一部分。“用户”表显示系统中所有用户的详细报告。该表显示了 WAN 延迟、DC 延迟、重传、RTO 等指标，其中一些指标对于具有 EDT 会话的用户不可用，因为它们目前是从 TCP 堆栈计算的。因此，它们显示为“NA”。

EDT(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-edt-support-1.png)

引入了一个新的环形图，让您查看用户消耗的带宽，以及根据用户使用的协议类型显示的总字节数。

EDT1(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-edt-support-2.png)

注意

HDX Insight 中的 EDT 从版本 12.1 build 50.28 开始在 NetScaler Console 上受支持，并从版本 12.1 build 49.23 开始在 ADC 实例上可用。

从 NetScaler Console 12.0 及更高版本开始提供的 HDX Insight 指标：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L7 客户端延迟	在 ICA 客户端和 NETSCALER 实例之间观察到的平均 L7 延迟。当交付路径中存在非 CITRIX 设备时，此指标非常有用。
L7 服务器端延迟	在 NetScaler 设备和 Citrix Virtual App 之间观察到的平均 L7 延迟。当交付路径中存在非 Citrix 设备时，此指标非常有用。
最大违规延迟	当在设定的时间间隔内发生违反定义阈值的情况时，L7 延迟的最高值。
平均违规延迟	当系统处于“L7 延迟违规”状态时，L7 延迟的平均值。
L7 阈值违规计数	L7 阈值违规发生的次数。

Current Sessions

By Start Time

Diagram	Session ID	Total Bytes	Bandwidth per Interval	Session Type	ICA RTT	Bytes per Interval	WAN latency	DC latency	Host Delay
	0000...000001	209.84 KB	11.58 Kbps	Application	854 ms	209.84 KB	83.00 ms	771 ms	4.00 ms
	0000...000001	127.18 KB	40.70 Kbps	Application	848 ms	127.18 KB	65.00 ms	710 ms	4.00 ms

Terminated Sessions

By Start Time

Session ID	Session Type	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Session Bandwidth	Total Bytes	Bytes per Interval
0000...000001	Application	1.01 s	59.00 ms	763.00 ms	9.40 Kbps	9.40 Kbps	1.38 MB	1.38 MB
0000...000001	Desktop	971.00 ms	59.00 ms	733.00 ms	8.82 Kbps	8.82 Kbps	1.29 MB	1.29 MB
0000...000001	Application	998.00	51.00 ms	732.00 ms	9.91 Kbps	9.91 Kbps	1.45 MB	1.45 MB

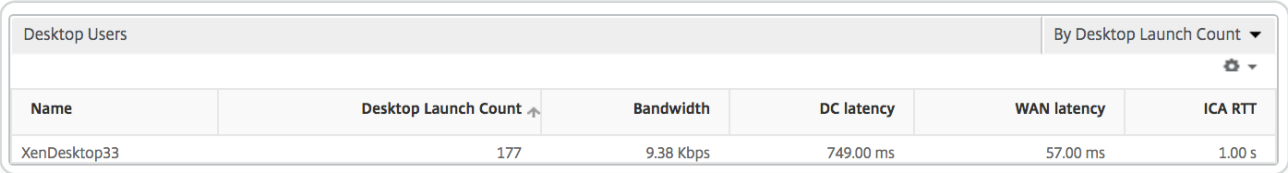
桌面用户

此表提供了特定用户的 Citrix Virtual Desktop 会话的详细信息。这些指标可以按桌面启动计数和带宽进行排序。

指标	描述
名称	Citrix 虚拟桌面的名称。
桌面启动计数	桌面已启动的次数。
带宽	在选定时间间隔内，端到端通信每秒消耗的总字节数。

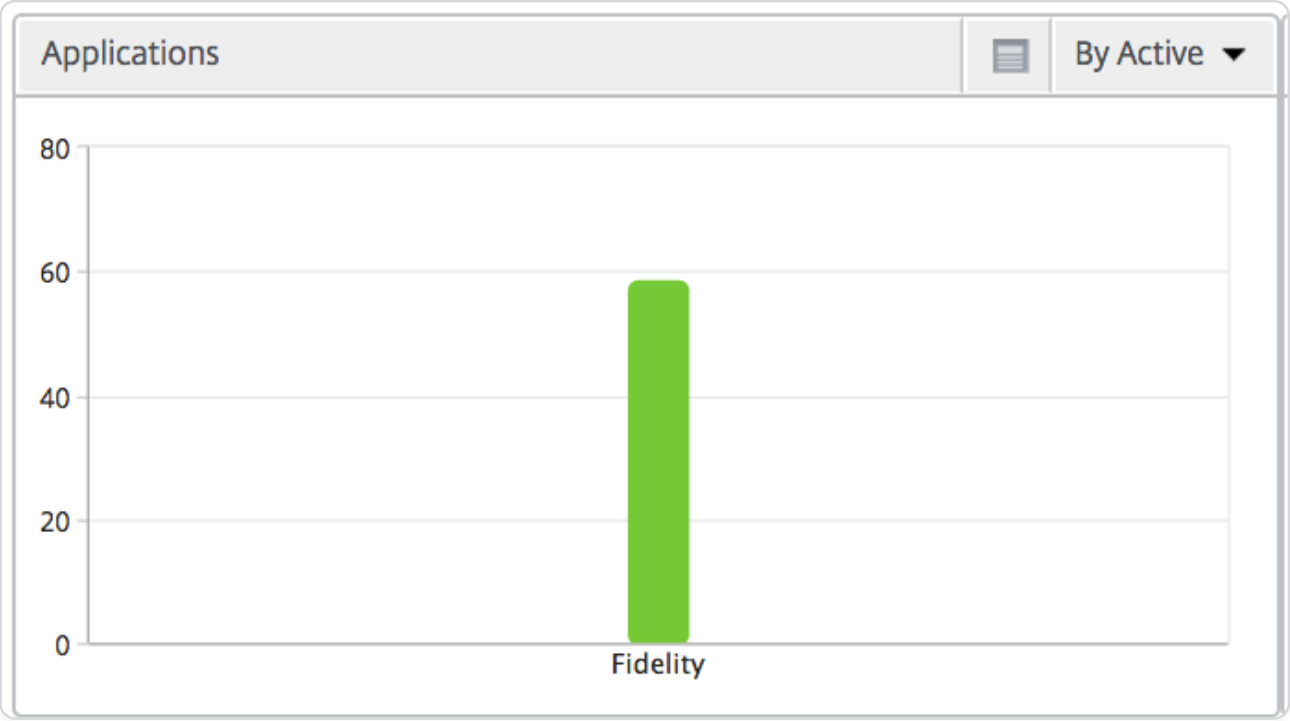
© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
DC 延迟	由网络服务器端引起的延迟。在 NetScaler Gateway 与 VDI、CVAD 或 StoreFront 服务器之间。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual App 或 Desktop 上托管的应用程序或桌面交互时所经历的屏幕延迟。



应用程序

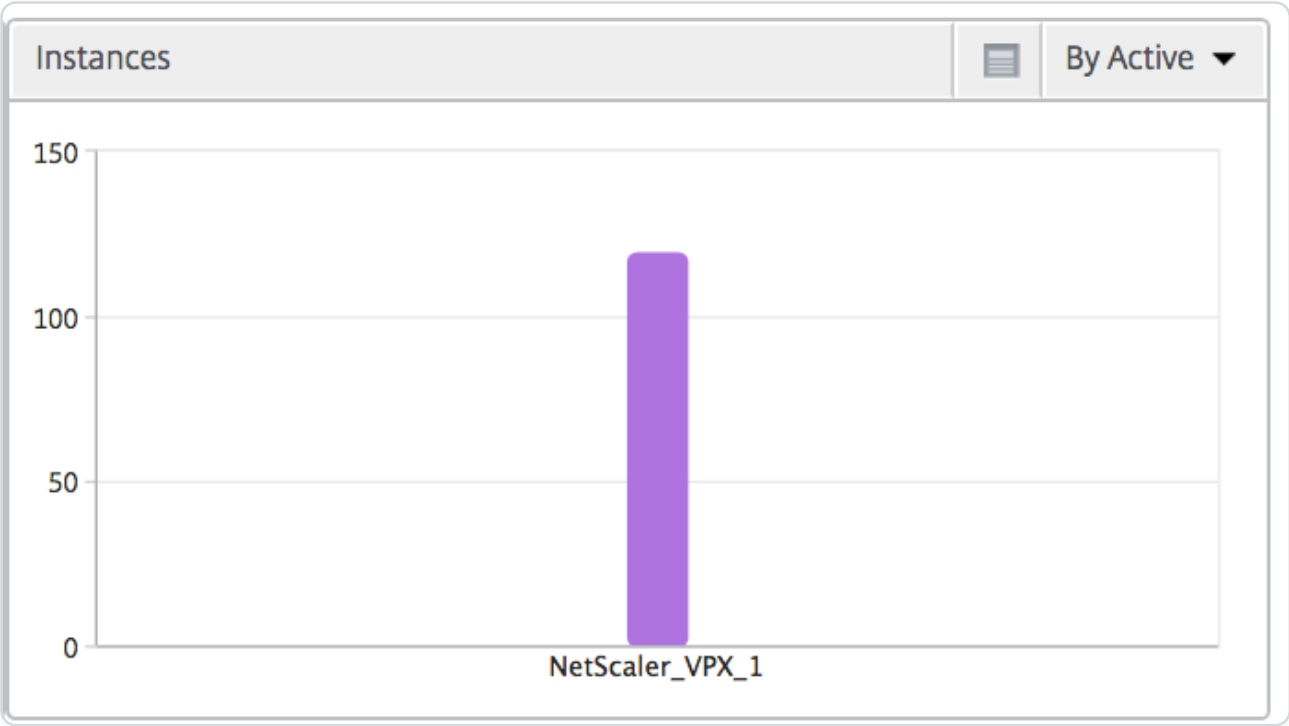
一个条形图，表示按活动状态、总会话启动次数、总应用程序启动次数和启动持续时间排序的应用程序。



实例

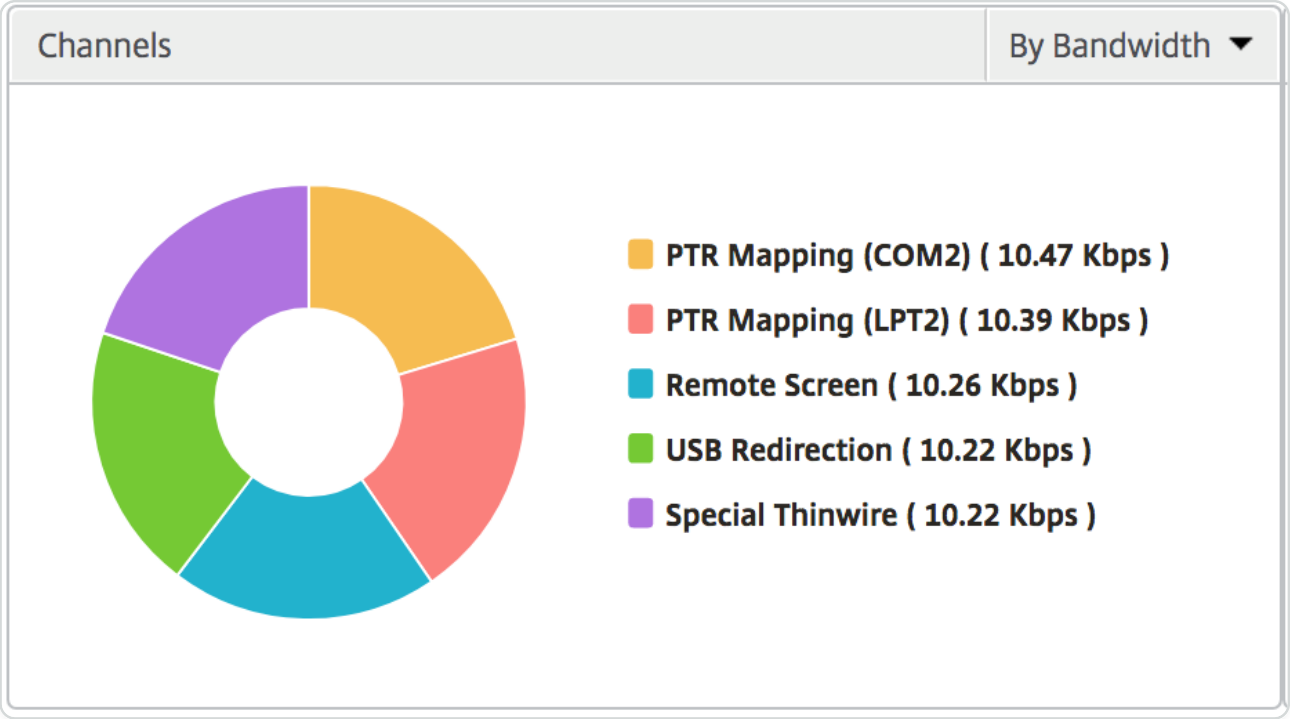
一个条形图，表示按活动状态和总应用程序排序的 NetScaler 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



通道

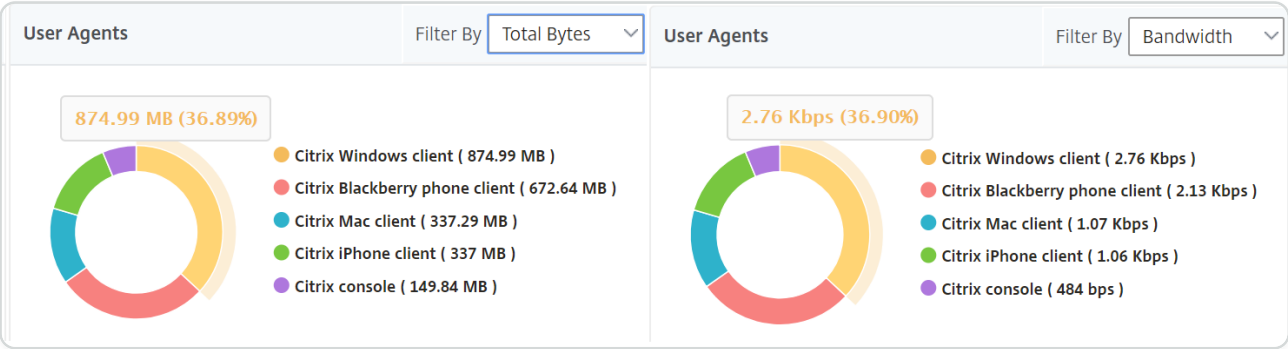
通道以环形图的形式表示每个 ICA 虚拟通道消耗的总带宽或总字节数。您还可以按带宽或总字节数对指标进行排序。



用户代理

用户代理以环形图的形式表示每个端点消耗的总带宽/总字节数。您还可以按带宽或总字节数对指标进行排序。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



按用户会话视图

按用户会话视图提供特定选定用户会话的报告。

要查看选定用户会话的指标：

1. 导航到 **Gateway > HDX Insight > 用户**。
2. 从“**用户摘要报告**”部分选择特定用户。
3. 从“**当前会话**”或“**已终止会话**”列中选择一个会话。

时间线图表

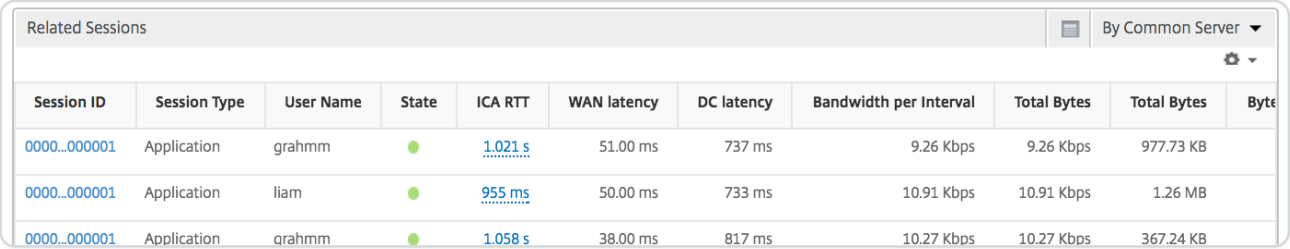
指标	描述
会话重新连接	这个数字表示活动 Citrix Virtual Apps and Desktops 会话的数量。
ACR 计数	这个数字表示活动 Citrix Virtual App 会话的数量。
ICA RTT	ICA RTT 是用户在使用 Citrix Virtual Apps 或 Desktops 上托管的应用程序或桌面时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。在 NetScaler Gateway 与 VDI、CVAD 或 StoreFront 服务器之间。
会话带宽	会话消耗的带宽，与时间间隔无关。
服务器端重传	NetScaler 与后端服务器之间连接上重传的数据包数量。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
客户端重传	NetScaler 与最终用户之间连接上重传的数据包数量。此指标的高值并不意味着用户体验不会无缝，但表示由于重传导致的高带宽利用率。
客户端快速 RTO	NetScaler 与最终用户之间连接上发生重传超时事件的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间连接上发生重传超时事件的次数。
每个间隔的带宽	会话在该特定时间间隔内消耗的带宽。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。

折线图(/en-us/netscaler-application-delivery-management-software/media/hdx-timeline-chart.png)
活动应用程序
“**活动应用程序**”部分显示所选用户的活动应用程序。这些应用程序还可以按活动会话数和启动持续时间进行排序。

应用程序(/en-us/netscaler-application-delivery-management-software/media/hdx-active-application.png)
相关会话
“相关会话”部分显示所选用户会话的相关会话。关系可以选为“通用服务器”或“通用 NetScaler”。



应用程序视图报告和指标

此视图中的报告和指标侧重于 Citrix Virtual Apps。

导航到应用程序视图：

1. 导航到 **Gateway > HDX Insight > 应用程序**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

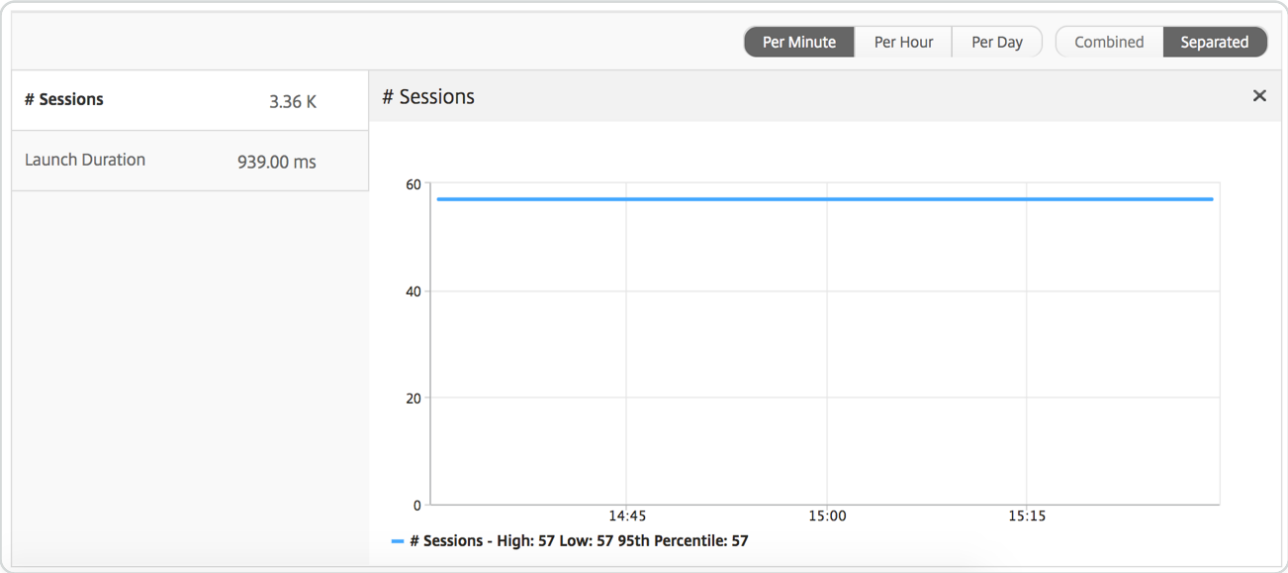
摘要视图

摘要视图显示在选定时间线内登录的所有应用程序的报告。

除非另有明确说明，否则所有指标/报告都将具有与所选时间段相对应的值。

折线图

指标	描述
# 会话	在给定时间间隔内的会话总数。
启动持续时间	启动应用程序的平均时间。



应用程序摘要报告

指标	描述
名称	Citrix Virtual App 的名称。
会话启动总数	在给定时间间隔内，Citrix Virtual App 活动会话的总数。
应用程序启动总数	在给定时间间隔内，Citrix Virtual App 应用程序启动的总数。
启动持续时间	启动 Citrix Virtual App 的平均时间。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Applications

Name	Total App Launch Count	Launch Duration	Total Session Launch count
Microsoft Outlook	531	514.00 ms	531
Microsoft Visio	354	555.00 ms	354
Microsoft Word	354	557.00 ms	354
Microsoft Excel	354	555.00 ms	354

活动应用程序报告

指标	描述
名称	Citrix 虚拟应用程序的名称。
状态	显示应用程序的状态：绿色-活动，红色-非活动
#活动会话	在给定时间间隔内使用此应用程序的活动用户会话数。
#活动应用程序	此应用程序的活动会话数。

Active Applications

Name	State	# Active Sessions	# Active Apps
Communicator	●	60	60
Fidelity	●	60	60
GoToMeeting	●	60	60

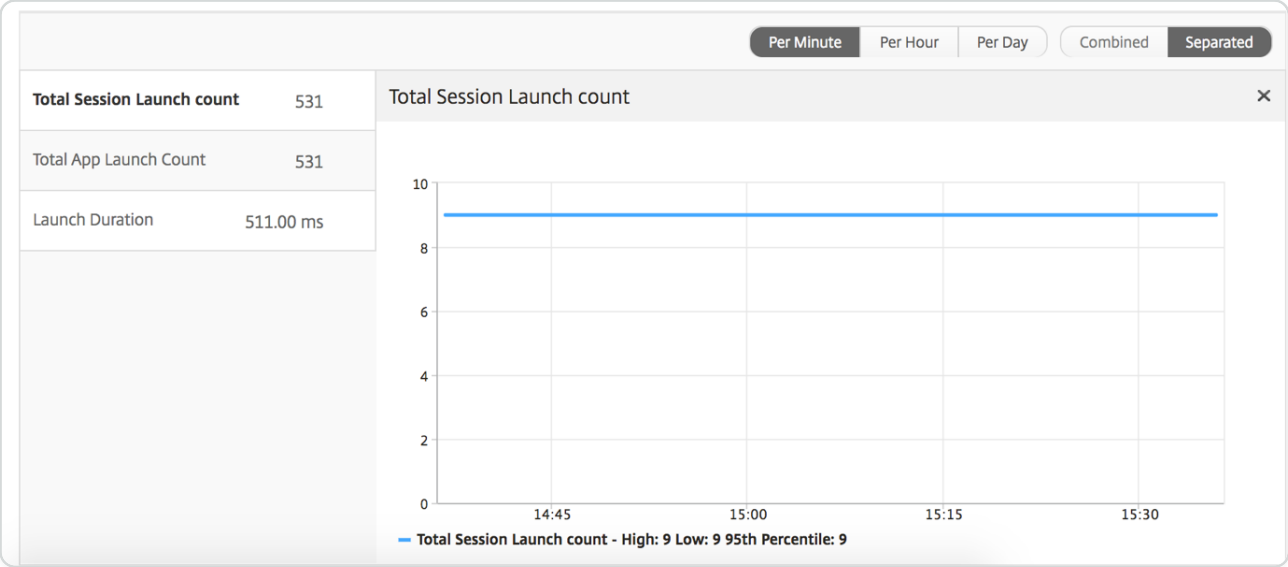
阈值报告

阈值报告表示在选定期间内，当*实体*选择为应用程序时，阈值被突破的次数。有关更多信息，请参阅如何创建阈值。

折线图

指标	描述
# 活动会话数	此数字表示活动 Citrix Virtual Apps and Desktops 会话的数量。
启动持续时间	启动应用程序所需的平均时间。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



当前会话报告

指标	描述
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	活动/非活动会话的绿色/红色指示。
主机延迟	由服务器网络引起的通过 NetScaler 的 ICA 流量的平均延迟。
每间隔带宽	会话在该特定时间间隔内消耗的带宽。
会话带宽	会话消耗的带宽，与时间间隔无关。
每间隔字节数	会话在该特定时间间隔内消耗的字节数。
开始时间	会话开始时间。
运行时间	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual App 服务器 IP。
NetScaler IP 地址	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows 客户端等

© 1997–2026 Citrix Systems, Inc. All rights reserved.

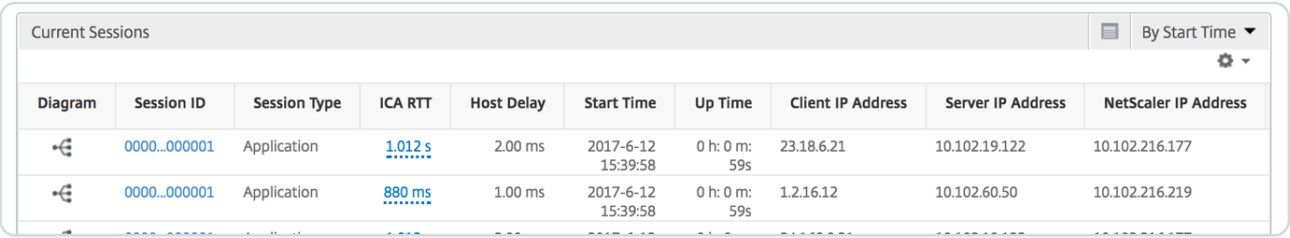
指标	描述
客户端版本	工作区版本。
MSI	布尔值（是/否）。指示会话是否为多流 ICA。
会话重新连接次数	会话重新连接的次数。
ACR 计数	客户端自动将用户重新连接到断开连接的会话的总次数。
用户访问类型	显示 ICA 会话的访问模式。例如，NetScaler Gateway 用户/透明模式。
国家	建立会话的国家。
区域	建立会话的区域。
城市	建立会话的城市。
USB 状态	活动/非活动 - 绿色/红色。
接受的 USB 实例数	接受的 USB 实例计数。
拒绝的 USB 实例数	拒绝的 USB 实例计数。
已停止的 USB 实例数	已停止的 USB 实例计数。
客户端主机名	客户端的主机名。
HA 故障转移计数	HA 故障转移发生的次数。
终止原因	显示会话终止的原因。例如，ICA 会话超时、用户终止会话。
ICA RTT	ICA RTT 是用户在使用分别托管在 Citrix Virtual Apps 或 Desktops 上的应用程序或桌面时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
DC 延迟	由网络服务器端引起的延迟。即在 NetScaler Gateway 与 VDI、CVAD 或 StoreFront 服务器之间。
总字节数	用户在选定时间段内消耗的总字节数。
服务器端重传	NetScaler 与后端服务器之间连接上重传的数据包数量。
客户端重传	NetScaler 与最终用户之间连接上重传的数据包数量。此指标的高值并不意味着用户体验不会是无缝的，但表示由于重传导致的高带宽利用率。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
客户端快速 RTO	NetScaler 与最终用户之间连接上发生重传超时次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间连接上发生重传超时次数。
用户名	访问此特定 Citrix Virtual App 的用户的用户名。
会话 ID	Citrix Virtual App 会话的唯一标识符。
会话类型	将是“应用程序”。
状态	会话状态：绿色表示活动，红色表示非活动。
最大违规延迟	当在设定的时间间隔内发生定义的阈值违规时，L7 延迟的最高值。
平均违规延迟	当系统处于“L7 延迟违规”状态时，L7 延迟的平均值。
L7 阈值违规计数	L7 阈值违规发生的次数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
L7 客户端延迟	在 ICA 客户端和 NetScaler 实例之间观察到的平均 L7 延迟。当交付路径中存在非 Citrix 设备时，此指标非常有用。
L7 服务器端延迟	在 NetScaler 设备和 Citrix Virtual App 之间观察到的平均 L7 延迟。当交付路径中存在非 Citrix 设备时，此指标非常有用。



按应用程序会话视图

每个应用程序会话视图显示特定选定应用程序会话的报告。

查看会话报告：

1. 使用受支持的 Web 浏览器登录到您的 NetScaler Console。
2. 导航到 **网关 > HDX Insight > 应用程序**。
3. 从应用程序摘要报告中选择特定用户。
4. 从当前会话报告中选择一个会话。

折线图

指标	描述
会话重新连接	会话重新连接的次数。
ACR 计数	客户端自动将用户重新连接到断开连接的会话的总次数。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual Apps 和 Desktops 上托管的应用程序或桌面交互时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即，从 NetScaler 到最终用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
服务器端零窗口大小事件	由网络服务器端引起的延迟。即，从 NetScaler 到后端服务器。
每间隔带宽	会话在该特定时间间隔内消耗的带宽。
服务器端重传	在 NetScaler 与后端服务器之间的连接上重传的数据包数量。
客户端重传	在 NetScaler 与最终用户之间的连接上重传的数据包数量。此指标的高值并不意味着用户体验不会无缝，但表示由于重传导致的高带宽利用率。
会话带宽	会话消耗的带宽，无论时间间隔如何。
服务器端零窗口大小事件	此计数器表示服务器通告零 TCP 窗口的次数。
客户端快速 RTO	NetScaler 与最终用户之间的连接发生重传超时次数。
服务器端快速 RTO	NetScaler 与后端服务器之间的连接发生重传超时次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。

折线图(/en-us/netscaler-application-delivery-management-software/media/hdx-line-chart-2.png)

用户柱状图

用户柱状图表示登录到此特定应用程序的用户。

柱状图(/en-us/netscaler-application-delivery-management-software/media/hdx-user-bar-graph.png)

桌面视图报告和指标

此视图中的报告和指标侧重于 Citrix Virtual Desktops。

导航到桌面视图：

1. 使用受支持的 Web 浏览器登录到您的 NetScaler Console。
2. 导航到 **网关 > HDX Insight > 桌面**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

摘要视图

摘要视图显示在选定时间线内登录的所有 Citrix Virtual Desktops 的报告。

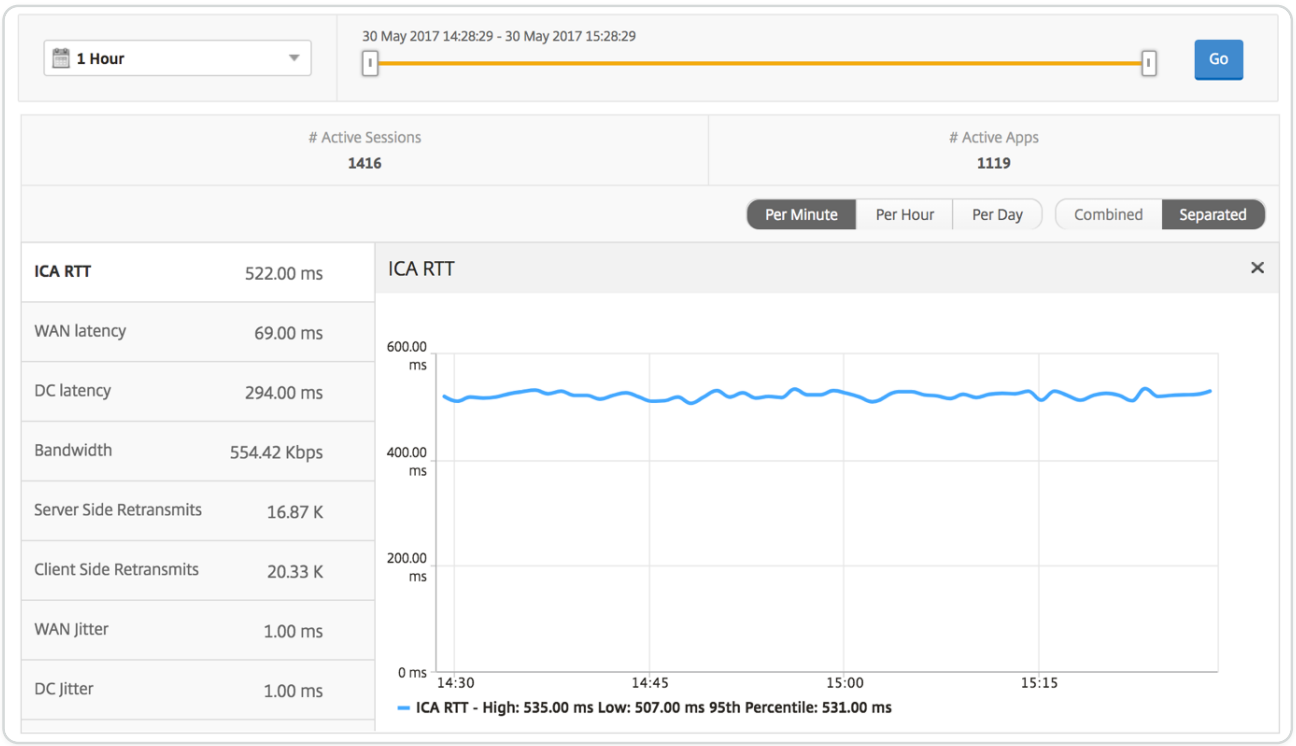
除非另有明确说明，否则所有指标/报告都将包含所选时间段内对应的值。

折线图

指标	描述
# 活动会话	此数字表示活动 Citrix Virtual Apps and Desktops 会话的数量。
# 活动应用程序	此数字表示活动 Citrix Virtual App 会话的数量。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual Apps and Desktops 上托管的应用程序或桌面交互时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。即在 NetScaler Gateway 与 VDI、CVAD 或 StoreFront 服务器之间。
带宽	在选定时间间隔内，端到端通信每秒消耗的总字节数。
服务器端重传	NetScaler 与后端服务器之间连接上重传的数据包数量。
客户端重传	NetScaler 与最终用户之间连接上重传的数据包数量。此指标的高值并不意味着用户体验不会无缝，但表示由于重传导致的高带宽利用率。
客户端快速 RTO	NetScaler 与最终用户之间连接上发生重传超时事件的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间连接上发生重传超时事件的次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。

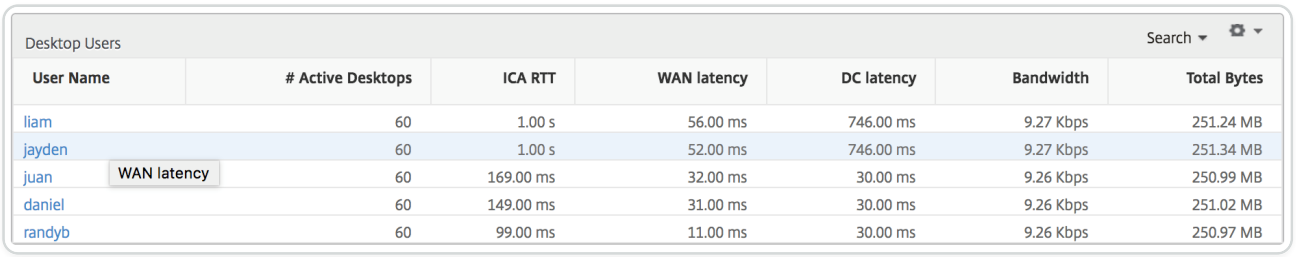


桌面摘要报告

指标	描述
活动会话	在给定时间间隔内，Citrix Virtual Desktop 活动会话的总数。
活动桌面	在给定时间间隔内，Citrix Virtual Desktops 活动桌面的总数。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual Apps 和 Desktops 上托管的应用程序或桌面交互时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。即在 NetScaler Gateway 与 VDI、CVAD 或 StoreFront 服务器之间。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
带宽	在选定时间间隔内，端到端通信每秒占用的总字节数。
总字节数	用户在选定时间段内消耗的总字节数。



User Name	# Active Desktops	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
liam	60	1.00 s	56.00 ms	746.00 ms	9.27 Kbps	251.24 MB
jayden	60	1.00 s	52.00 ms	746.00 ms	9.27 Kbps	251.34 MB
juan	60	169.00 ms	32.00 ms	30.00 ms	9.26 Kbps	250.99 MB
daniel	60	149.00 ms	31.00 ms	30.00 ms	9.26 Kbps	251.02 MB
randyb	60	99.00 ms	11.00 ms	30.00 ms	9.26 Kbps	250.97 MB

阈值报告

阈值报告显示了在选定期间内，当*实体*被选为桌面时，阈值被突破的次数。有关更多信息，请参阅如何创建阈值。

每个桌面视图

每个桌面视图为选定的 Citrix 虚拟桌面提供详细的最终用户体验报告。

要导航到特定桌面视图：

1. 使用受支持的 Web 浏览器登录到您的 NetScaler Console。
2. 导航到 **分析 \> HDX Insight \> 桌面**。
3. 从**桌面摘要报告**中选择一个特定的**桌面**。

折线图

指标	描述
# 活动会话	此数字表示活动 Citrix Virtual Apps and Desktops 会话的数量。
# 活动应用程序	此数字表示活动 Citrix Virtual App 会话的数量。
ICA RTT	ICA RTT 是用户在与 Citrix Virtual Apps and Desktops 上托管的应用程序或桌面交互时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
DC 延迟	由网络服务器端引起的延迟。即在 NetScaler Gateway 与 VDI 或 CVAD 或 StoreFront 服务器之间。
带宽	在选定时间间隔内，端到端通信所占用的每秒总字节数。
服务器端重传	NetScaler 与后端服务器之间连接上重传的数据包数量。
客户端重传	NetScaler 与最终用户之间连接上重传的数据包数量。此指标的高值并不意味着用户体验不会无缝，但表示由于重传导致的高带宽利用率。
客户端快速 RTO	NetScaler 与最终用户之间连接发生重传超时事件的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间连接发生重传超时事件的次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。

线形图(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-line-chart.png)

桌面用户报告

此表提供了特定用户的 Citrix Virtual Desktop 会话的深入信息。这些指标可以按桌面启动计数和带宽进行排序。

指标	描述
名称	思杰虚拟桌面的名称。
桌面启动次数	桌面已启动的次数。
带宽	在选定时间间隔内，端到端通信每秒消耗的总字节数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
数据中心延迟	由网络服务器端引起的延迟。即，NetScaler Gateway 与 VDI、CVAD 或 StoreFront 服务器之间的延迟。
广域网延迟	由网络客户端引起的延迟。即，从 NetScaler 到最终用户的延迟。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual Apps and Desktops 上托管的应用程序或桌面交互时所经历的屏幕延迟。

桌面用户(/en-us/netscaler-application-delivery-management-software/media/hdx-dekstop-user.png)

用户桌面活动/非活动报告

以下指标可以按每个间隔的带宽、会话重新连接和 ACR 计数进行排序。

指标	描述
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	活动/非活动会话显示为绿色/红色。
主机延迟	通过 NetScaler 的 ICA 流量因服务器网络引起的平均延迟。
每个间隔的带宽	会话在该特定时间间隔内消耗的带宽。
会话带宽	会话消耗的带宽，与时间间隔无关。
每个间隔的字节数	会话在该特定时间间隔内消耗的字节数。
开始时间	会话开始时间。
运行时间	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual App 服务器 IP。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
NetScaler IP 地址	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows 客户端等
客户端版本	工作区版本。
MSI	布尔值（是/否）。指示会话是否为多流 ICA。
会话重新连接	会话重新连接的次数。
ACR 计数	客户端自动将用户重新连接到已断开会话的总次数。
用户访问类型	显示 ICA 会话的访问模式。例如，NetScaler Gateway 用户/透明模式。
国家/地区	建立会话的国家/地区。
区域	建立会话的区域。
城市	建立会话的城市。
USB 状态	活动/非活动 - 绿色/红色。
接受的 USB 实例数	接受的 USB 实例计数。
拒绝的 USB 实例数	拒绝的 USB 实例计数。
已停止的 USB 实例数	已停止的 USB 实例计数。
客户端主机名	客户端的主机名。
HA 故障转移计数	HA 故障转移发生的次数。
终止原因	显示会话终止的原因。例如，ICA 会话超时、用户终止会话。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual Apps 和 Desktops 上托管的应用程序或桌面交互时所经历的屏幕延迟。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
WAN 延迟	由网络客户端引起的延迟。即，从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。即 NetScaler Gateway 与 VDI、CVAD 或 StoreFront 服务器之间的延迟。
总字节数	用户在选定时间段内消耗的总字节数。
服务器端重传	NetScaler 与后端服务器之间连接上重传的数据包数量。
客户端重传	NetScaler 与最终用户之间连接上重传的数据包数量。此指标的高值并不意味着用户体验不会无缝，但表示由于重传导致的高带宽利用率。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
客户端快速 RTO	NetScaler 与最终用户之间连接上发生重传超时事件的次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间连接上发生重传超时的次数。
VDI 映像名称	用户连接到的 Citrix Virtual Desktop 名称
图表	

非活动用户(/en-us/netscaler-application-delivery-management-software/media/hdx-user-dekstop-active-inactive.png)

按桌面会话视图

按桌面会话视图提供特定选定 Citrix Virtual Desktop 会话的报告。

导航到桌面会话视图：

1. 使用受支持的 Web 浏览器登录到 NetScaler Console。
2. 导航到 **分析 \> HDX Insight \> 桌面**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 从 **Desktop Summary Report** 中选择一个特定的桌面。
4. 从当前会话报告中选择一个会话。

时间线图表

按用户会话视图提供特定选定用户会话的报告。

要查看所选用户会话的指标：

1. 使用受支持的 Web 浏览器登录到您的 NetScaler Console。
2. 导航到 **网关 > HDX Insight > 用户**。
3. 从 **User Summary Report** 部分选择特定用户。
4. 从 **Current Sessions** 或 **Terminated Sessions** 列中选择一个会话。

指标	描述
会话重新连接	此数字表示活动 Citrix Virtual Apps and Desktops 会话的数量。
ACR 计数	此数字表示活动 Citrix Virtual App 会话的数量。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual Apps and Desktops 上托管的应用程序或桌面交互时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即，从 NetScaler 到最终用户。
DC 延迟	网络服务器端引起的延迟。即，NetScaler Gateway 与 VDI、CVAD 或 StoreFront 服务器之间的延迟。
会话带宽	会话消耗的带宽，与时间间隔无关。
服务器端重传	NetScaler 与后端服务器之间连接上重传的数据包数量。
客户端重传	NetScaler 与最终用户之间连接上重传的数据包数量。此指标的高值并不意味着用户体验不会无缝，但表示由于重传导致的高带宽利用率。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
客户端快速 RTO	NetScaler 与最终用户之间连接上发生重传超时事件的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间连接上发生重传超时事件的次数。
每间隔带宽	会话在该特定时间间隔内消耗的带宽。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。

时间线图表(/en-us/netscaler-application-delivery-management-software/media/hdx-timeline-chart.png)

相关桌面会话报告

以下指标可以按每个间隔的带宽、会话重新连接和 ACR 计数进行排序。

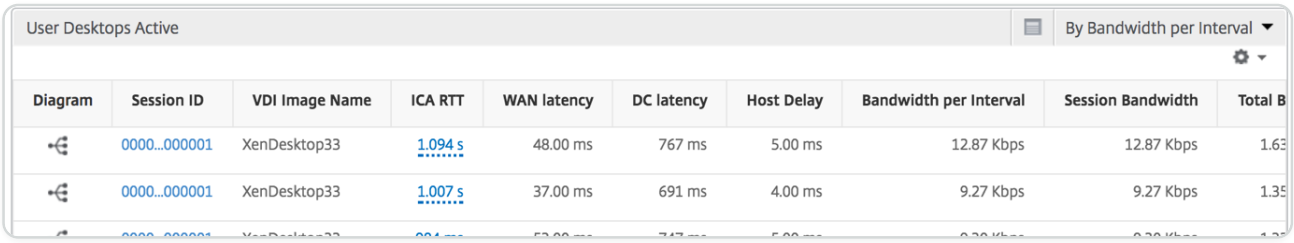
指标	描述
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色表示活动/非活动会话。
主机延迟	由于服务器网络导致通过 NetScaler 的 ICA 流量的平均延迟。
每个时间间隔的带宽	会话在该特定时间间隔内消耗的带宽。
会话带宽	会话消耗的带宽，与时间间隔无关。
每个时间间隔的字节数	会话在该特定时间间隔内消耗的字节数。
开始时间	会话开始时间。
运行时间	会话持续时间。
客户端 IP 地址	最终用户 IP。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
服务器 IP 地址	后端/Citrix Virtual App 服务器 IP。
NetScaler IP 地址	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows 客户端等
客户端版本	工作区版本。
MSI	布尔值（是/否）。指示会话是否为多流 ICA。
会话重新连接	会话重新连接的次数。
ACR 计数	客户端自动将用户重新连接到已断开会话的总次数。
用户访问类型	显示 ICA 会话的访问模式。例如，NetScaler Gateway 用户/透明模式。
国家/地区	建立会话的国家/地区。
区域	建立会话的区域。
城市	建立会话的城市。
USB 状态	活动/非活动 - 绿色/红色。
接受的 USB 实例数	接受的 USB 实例计数。
拒绝的 USB 实例数	拒绝的 USB 实例计数。
停止的 USB 实例数	停止的 USB 实例计数。
客户端主机名	客户端的主机名。
HA 故障转移计数	HA 故障转移发生的次数。
终止原因	显示会话终止的原因。例如，ICA 会话超时、用户终止会话。
ICA RTT	ICA RTT 是用户在使用分别托管在 Citrix Virtual Apps 和 Desktops 上的应用程序或桌面时所经历的屏幕延迟。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。即在 NetScaler Gateway 与 VDI 或 CVAD 或 StoreFront 服务器之间。
总字节数	用户在选定时间段内消耗的总字节数。
服务器端重传	在 NetScaler 与后端服务器之间的连接上重传的数据包数量。
客户端重传	在 NetScaler 与最终用户之间的连接上重传的数据包数量。此指标的高值并不意味着用户体验不会是无缝的，但表示由于重传导致的高带宽利用率。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
客户端快速 RTO	NetScaler 与最终用户之间连接发生重传超时事件的次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间连接发生重传超时事件的次数。



实例视图报告和指标

实例视图中的报告和指标侧重于 NetScaler 实例。

导航到实例视图：

1. 使用受支持的 Web 浏览器登录到您的 NetScaler Console。
2. 导航到 **分析 \> HDX Insight \> 实例**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

实例视图报告和指标包含以下部分：

- 实例摘要视图
- 按实例视图

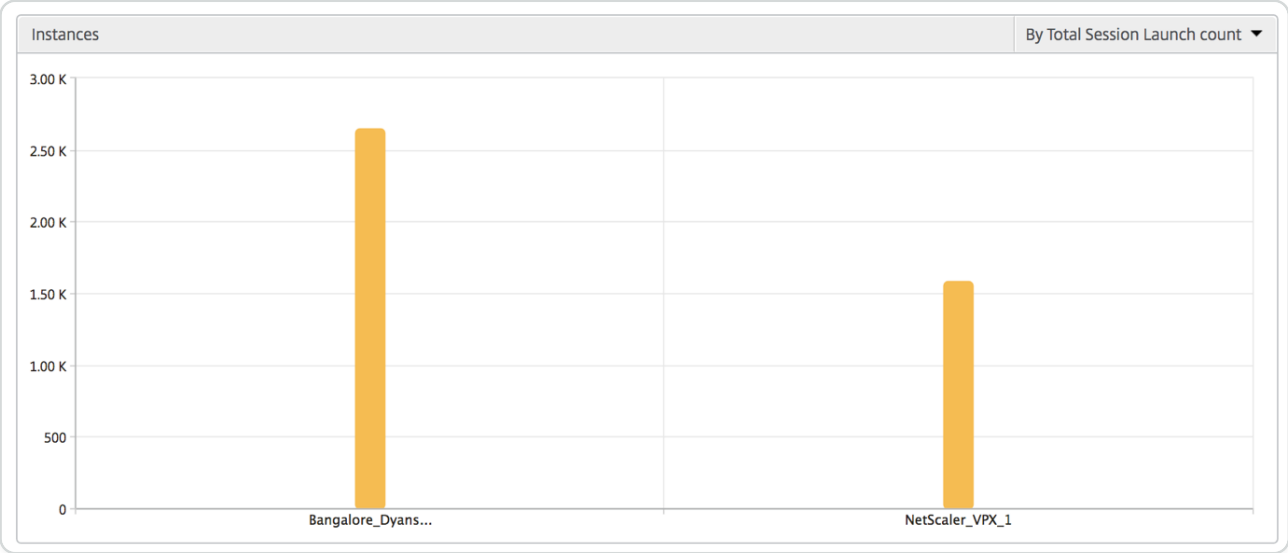
实例摘要视图

此视图称为摘要视图，因为它显示了所有已添加到 NetScaler Console 的 NetScaler 实例的报告。

除非另有明确说明，否则以下所有指标/报告都将显示在选定时间段内与其对应的数值。

实例柱状图

此图显示实例与总会话启动计数 | 总应用程序，这些可以从图表画布右上角的列表中选择。



实例/活动实例摘要报告

指标	描述
名称	NetScaler 实例的主机名。
IP 地址	NetScaler IP 地址。
会话启动总数	在给定时间间隔内创建的唯一用户会话总数。
应用程序总数	在给定时间间隔内启动的唯一应用程序总数。
类型	不适用

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Instances

Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

阈值报告

阈值报告表示在选定期间内，*实体*被选为实例时，阈值被突破的次数。有关更多信息，请参阅如何创建阈值。

跳过的流

跳过的流是跳过解析 ICA 连接的记录。这可能由于多种原因发生，例如使用不受支持的 Citrix Virtual Apps and Desktops 版本、不受支持的工作区版本或工作区类型等。此表显示了 IP 地址和跳过的流计数。这些工作区可能不属于白名单工作区。因此，这些会话将从监视中跳过。

Skipped Flows

IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

全球视图

HDX Insight 中的世界地图视图允许管理员从地理角度查看历史和活动用户详细信息。管理员可以拥有系统的全球视图，通过简单地单击区域，可以向下钻取到特定国家/地区，甚至进一步钻取到城市。管理员还可以进一步向下钻取以按城市和州查看信息。从 NetScaler Console 12.0 版及更高版本开始，您可以向下钻取到从地理位置连接的用户。

可以在 HDX Insight 的世界地图上查看以下详细信息，并且每个指标的密度以热图的形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- 带宽
- 总字节数

世界视图(/en-us/netscaler-application-delivery-management-software/media/hdx-world-map-1.png)

按实例视图

按实例视图为特定选定的 NetScaler 实例提供详细的最终用户体验报告。

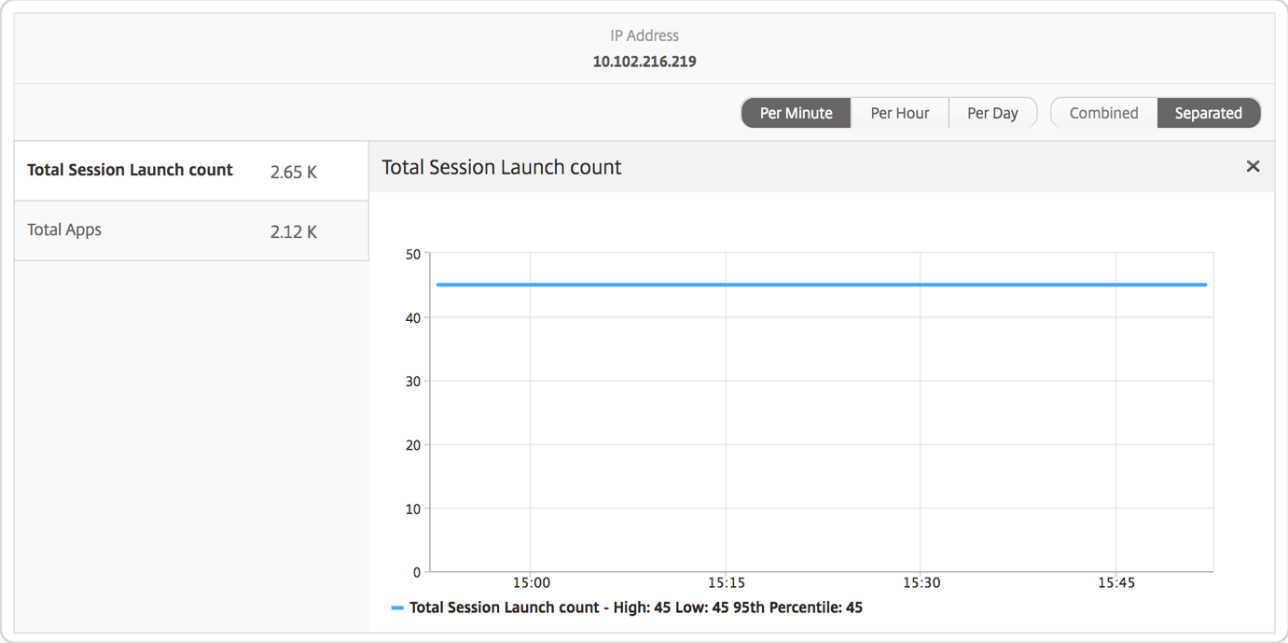
© 1997–2026 Citrix Systems, Inc. All rights reserved.

导航到实例视图：

1. 使用受支持的 Web 浏览器登录到您的 NetScaler Console。
2. 导航到 **分析 \> HDX Insight \> 实例**。
3. 从 **实例摘要报告** 中选择一个特定实例。

折线图

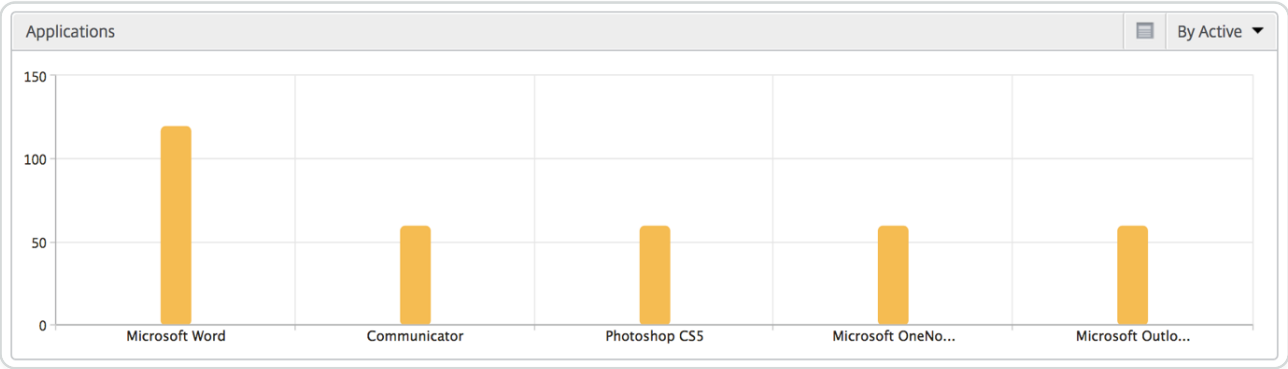
指标	描述
IP 地址	这表示所选实例的 NetScaler IP 地址。
会话启动总数	在给定时间间隔内处于活动状态的 Citrix Virtual App 会话总数。
应用程序总数	在给定时间间隔内启动的唯一应用程序总数。



应用程序柱状图

根据以下条件显示前 5 个应用程序：按活动应用程序、会话启动总数、应用程序启动总数或启动持续时间。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



用户柱状图

用户柱状图根据以下条件显示前 5 个用户

- 带宽
- WAN 延迟
- DC 延迟
- ICA RTT

用户图(/en-us/netscaler-application-delivery-management-software/media/hdx-users-bar-graph.png)

桌面用户报告

此表提供了特定用户的 Citrix Virtual Desktop 会话的详细信息。这些指标可以按桌面启动计数和带宽进行排序。

指标	描述
名称	Citrix 虚拟桌面的名称。
桌面启动计数	桌面已启动的次数。
带宽	在选定的时间间隔内，端到端通信每秒占用的总字节数。
DC 延迟	由网络服务器端引起的延迟。即，在 NetScaler Gateway 与 VDI、CVAD 或 StoreFront 服务器之间。
WAN 延迟	客户端网络引起的延迟。即从 NetScaler 到最终用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
ICA RTT	ICA RTT 是用户在使用分别托管在 Citrix Virtual Apps 和 Desktops 上的应用程序或桌面时所经历的屏幕延迟。

桌面用户(/en-us/netscaler-application-delivery-management-software/media/hdx-dekstop-user.png)

世界视图

HDX Insight 中的世界地图视图允许管理员从地理角度查看历史和活跃用户详细信息。管理员可以查看系统的世界视图，通过单击区域深入到特定国家，并进一步深入到城市。管理员还可以进一步深入查看按城市和州划分的信息。从 NetScaler Console 12.0 版及更高版本开始，您可以深入查看从地理位置连接的用户。

可以在 HDX Insight 的世界地图上查看以下详细信息，并且每个指标的密度以热图的形式显示：

- ICA RTT
- 广域网延迟
- 数据中心延迟
- 带宽
- 总字节数

世界视图(/en-us/netscaler-application-delivery-management-software/media/hdx-world-map-1.png)

许可证视图报告和指标

许可证视图提供 NetScaler Gateway 许可证信息的详细信息。

要导航到许可证视图：

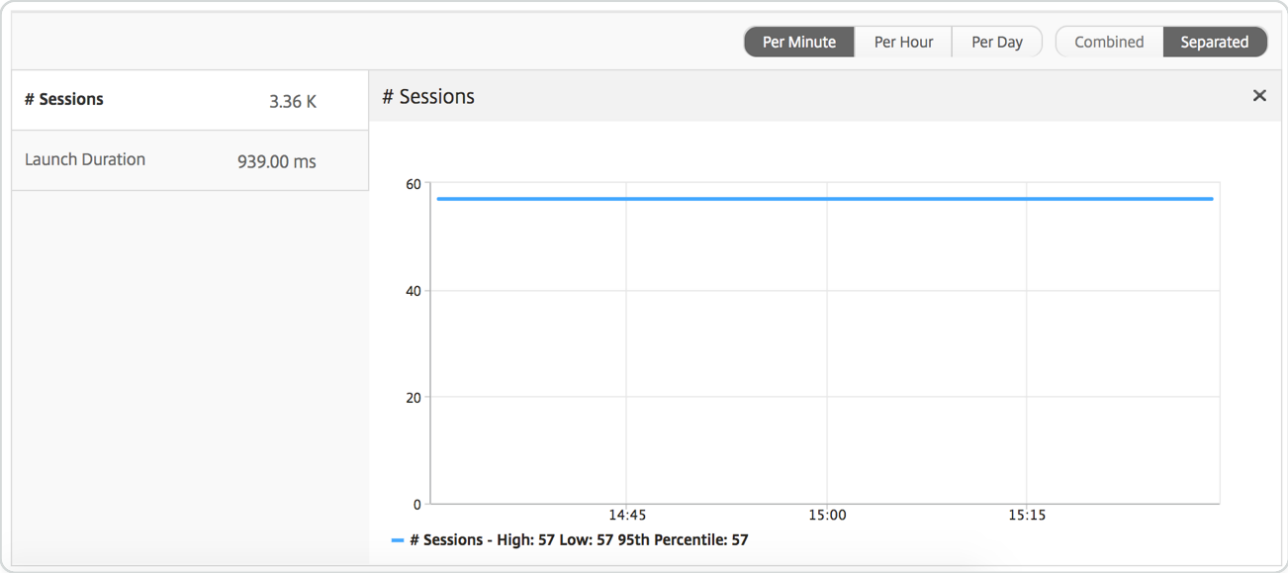
1. 使用受支持的 Web 浏览器登录到您的 NetScaler Console。
2. 导航到 **Analytics \> HDX Insight \> 许可证**。

折线图

指标	描述
正在使用的许可证	在选定时间段内使用的 NetScaler Gateway CCU 许可证。每个计数表示用户会话数。这与该用户启动的应用程序和桌面会话无关。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
总许可证数	客户可使用的 NetScaler Gateway CCU 许可证总数。



阈值报告

阈值报告表示在选定期间内，当*实体*选择为“许可证”时，超出阈值的计数。有关更多信息，请参阅如何创建阈值。

应用程序视图报告和指标

此视图中的报告和指标侧重于 Citrix Virtual Apps。

导航到应用程序视图：

1. 导航到 **网关 > HDX™ Insight > 应用程序**。

摘要视图

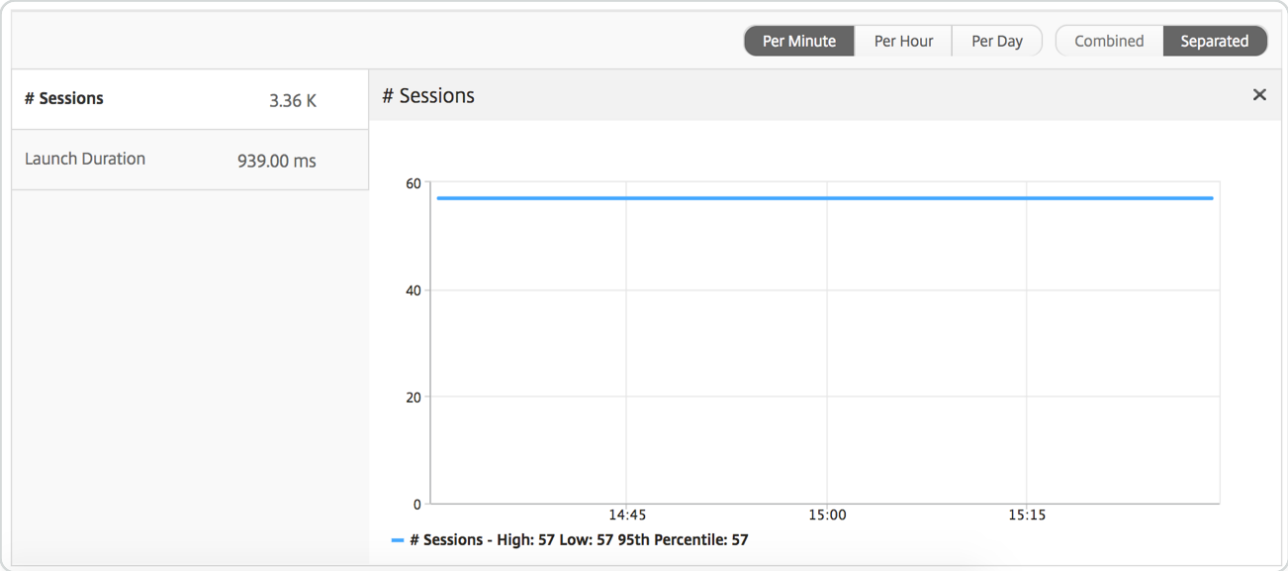
摘要视图显示在选定时间线内登录的所有应用程序的报告。

除非另有明确说明，否则以下所有指标/报告都将具有在选定时间段内与其对应的值。

折线图

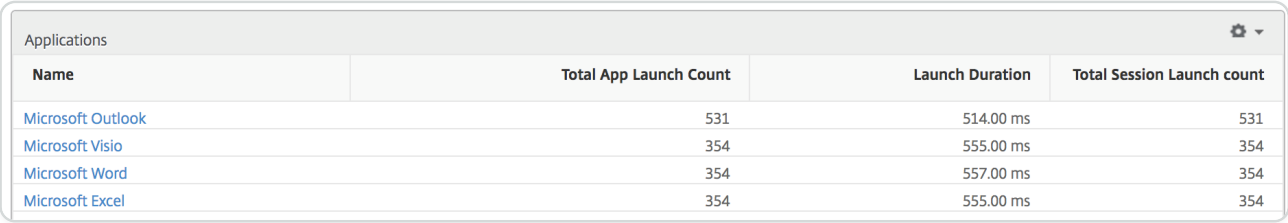
指标	描述
# 会话	在给定时间间隔内的会话总数。
启动持续时间	启动应用程序的平均耗时。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



应用程序摘要报告

指标	描述
名称	Citrix Virtual App 的名称。
会话启动总数	在给定时间间隔内，Citrix Virtual App 活动会话的总数。
应用程序启动总数	在给定时间间隔内，Citrix Virtual App 应用程序启动的总数。
启动持续时间	启动 Citrix Virtual App 所需的平均时间。



活动应用程序报告

指标	描述
名称	Citrix 虚拟应用程序的名称。
状态	显示应用程序的状态：绿色-活动，红色-非活动
#活动会话	在给定时间间隔内使用此应用程序的活动用户会话数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

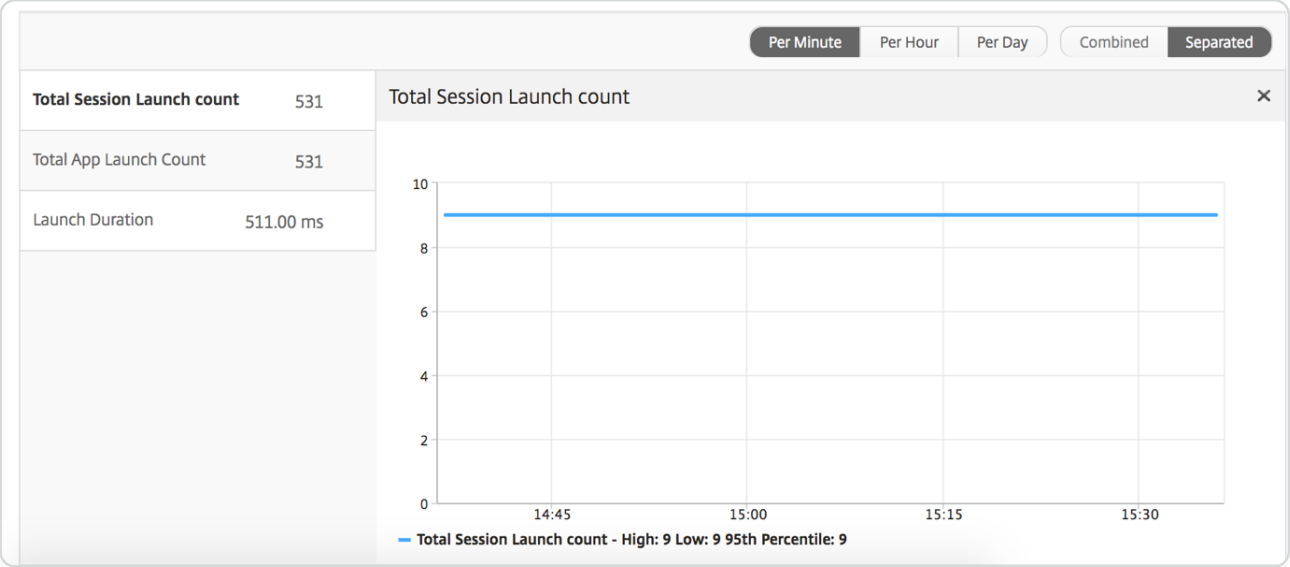
指标	描述
#活动应用程序	此应用程序的活动会话数。

阈值报告

阈值报告表示在选定期间内，当*实体*选择为应用程序时，已突破的阈值数量。有关更多信息，请参阅如何创建阈值和警报。

折线图

指标	描述
# 活动会话	此数字表示活动 Citrix Virtual Apps and Desktops 会话的数量。
启动持续时间	启动应用程序所需的平均时间。



当前会话报告

指标	描述
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

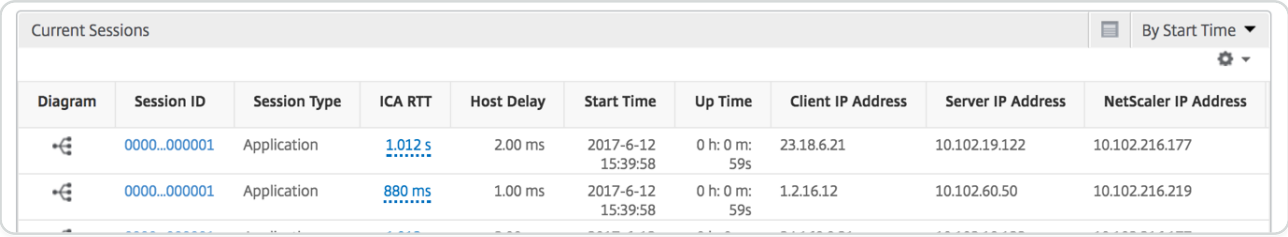
指标	描述
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	通过 NetScaler 的 ICA 流量因服务器网络引起的平均延迟。
每个时间间隔的带宽	会话在该特定时间间隔内消耗的带宽。
会话带宽	会话消耗的带宽，与时间间隔无关。
每个时间间隔的字节数	会话在该特定时间间隔内消耗的字节数。
开始时间	会话开始时间。
运行时间	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual App 服务器 IP。
NetScaler IP 地址	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows 客户端等
客户端版本	工作区版本。
MSI	布尔值（是/否）。指示会话是否为多流 ICA。
会话重新连接次数	会话重新连接的次数。
ACR 计数	客户端自动将用户重新连接到断开连接的会话的总次数。
用户访问类型	显示 ICA 会话的访问模式。例如，NetScaler Gateway 用户/透明模式。
国家/地区	建立会话的国家/地区。
区域	建立会话的区域。
城市	建立会话的城市。
USB 状态	活动/非活动 - 绿色/红色。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
接受的 USB 实例数	接受的 USB 实例计数。
拒绝的 USB 实例数	拒绝的 USB 实例计数。
停止的 USB 实例数	停止的 USB 实例计数。
客户端主机名	客户端的主机名。
HA 故障转移计数	HA 故障转移发生的次数。
终止原因	显示会话终止的原因。例如，ICA 会话超时、用户终止会话。
ICA RTT	ICA RTT 是用户在使用分别托管在 Citrix Virtual Apps 和 Desktops 上的应用程序或桌面时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。即从 NetScaler 到后端服务器。
总字节数	用户在选定时间段内消耗的总字节数。
服务器端重传	NetScaler 与后端服务器之间连接上重传的数据包数量。
客户端重传	NetScaler 与最终用户之间连接上重传的数据包数量。此指标的高值并不意味着用户体验不会是无缝的，但表示由于重传导致的高带宽利用率。
客户端零窗口大小事件	此计数器表示客户端通告零 TCP 窗口的次数。
客户端快速 RTO	NetScaler 与最终用户之间的连接发生重传超时的次数。
服务器端零窗口大小事件	此计数器表示服务器通告零 TCP 窗口的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间的连接发生重传超时的次数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
用户名	访问此特定 Citrix Virtual App 的用户的用户名。
会话 ID	Citrix Virtual App 会话的唯一标识符。
会话类型	将是“应用程序”。
状态	会话状态：绿色表示活动，红色表示非活动。
最大违规延迟	当在设定的时间间隔内发生定义的阈值违规时，L7 延迟的最高值。
平均违规延迟	当系统处于“L7 延迟违规”状态时，L7 延迟的平均值。
L7 阈值违规计数	L7 阈值违规发生的次数。
L7 客户端延迟	在 ICA 客户端和 NetScaler 实例之间观察到的平均 L7 延迟。当交付路径中存在非 Citrix 设备时，此指标很有用。
L7 服务器端延迟	在 NetScaler 设备和 Citrix Virtual App 之间观察到的平均 L7 延迟。当交付路径中存在非 Citrix 设备时，此指标很有用。



按应用程序会话视图

按应用程序会话视图显示特定选定的应用程序会话的报告。

查看会话报告：

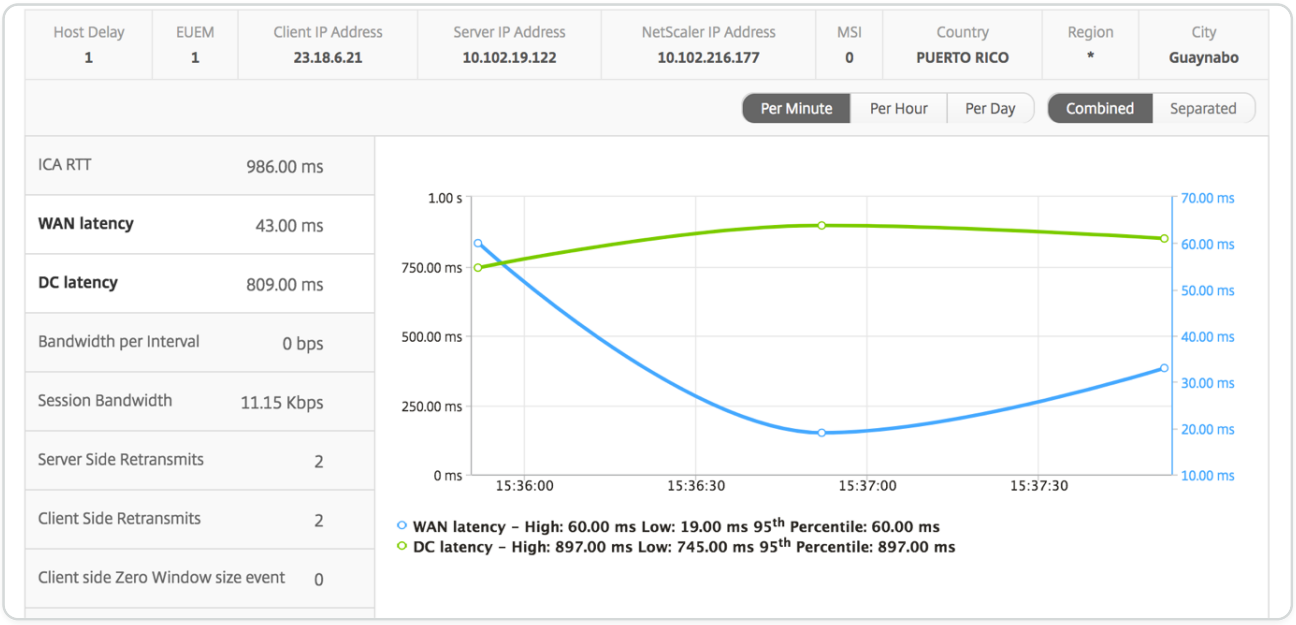
1. 导航到 **网关 > HDX Insight > 应用程序**。
2. 从应用程序摘要报告中选择特定用户。
3. 从当前会话报告中选择一个会话。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

折线图

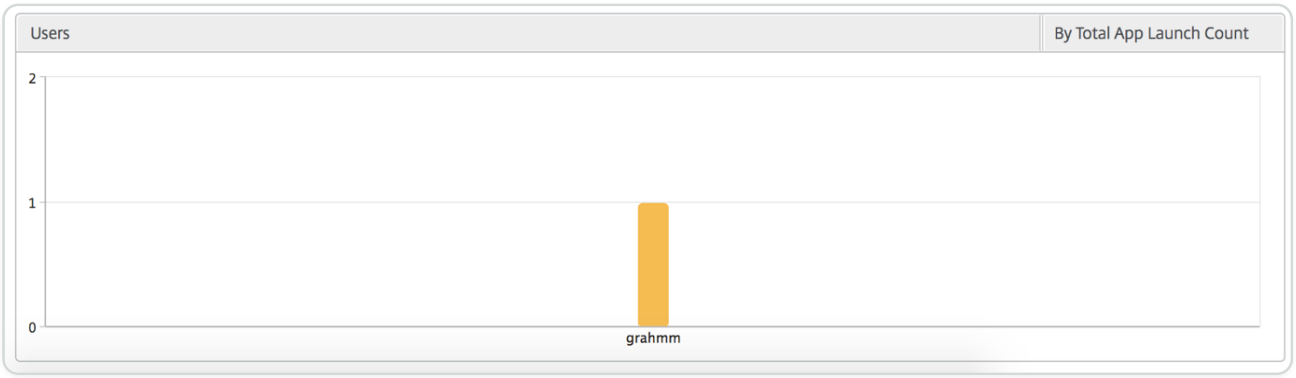
指标	描述
会话重新连接	会话重新连接的次数。
ACR 计数	客户端自动将用户重新连接到断开会话的总次数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps 和 Desktops 上的应用程序或桌面交互时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即，从 NetScaler 到最终用户。
服务器端零窗口大小事件	由网络服务器端引起的延迟。即从 NetScaler 到后端服务器的延迟。
每个间隔的带宽	会话在该特定时间间隔内消耗的带宽。
服务器端重传	在 NetScaler 与后端服务器之间的连接上重传的数据包数量。
客户端重传	在 NetScaler 与最终用户之间的连接上重传的数据包数量。此指标的高值并不意味着用户体验不会无缝，但表示由于重传导致的高带宽利用率。
会话带宽	会话消耗的带宽，与时间间隔无关。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
客户端快速 RTO	NetScaler 与最终用户之间的连接上发生重传超时事件的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间的连接上发生重传超时事件的次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



用户条形图

用户条形图表示登录到此特定应用程序的用户。



桌面视图报告和指标

此视图中的报告和指标侧重于 Citrix Virtual Desktops。

导航到桌面视图：

1. 导航到 **网关 > HDX™ Insight > 桌面**。

摘要视图

摘要视图显示在选定时间线内登录的所有 Citrix Virtual Desktops 的报告。

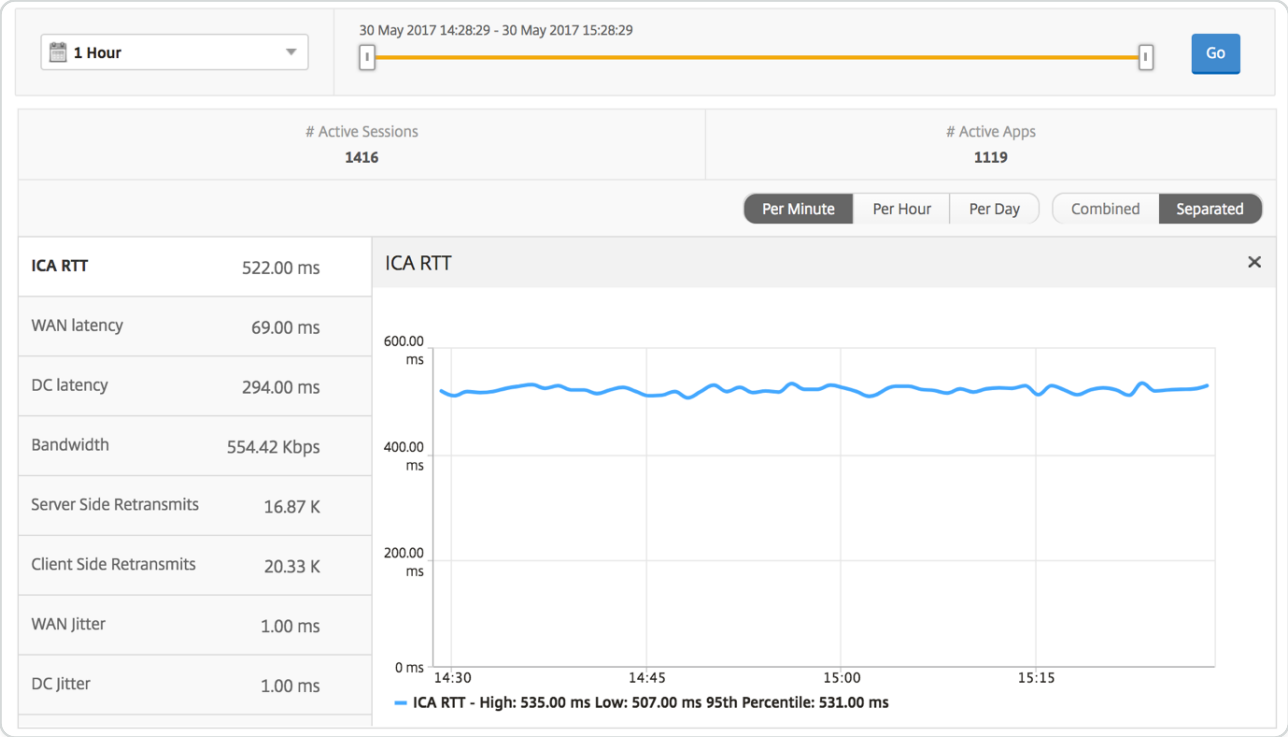
除非另有明确说明，否则所有指标/报告都将显示其在选定时间段内的相应值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

折线图

指标	描述
# 活动会话	此数字表示活动 Citrix Virtual Apps and Desktops 会话的数量。
# 活动应用程序	此数字表示活动 Citrix Virtual App 会话的数量。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps 和 Desktops 上的应用程序或桌面交互时所体验到的屏幕延迟。
广域网延迟	由网络客户端引起的延迟。即，从 NetScaler 到最终用户。
数据中心延迟	由网络服务器端引起的延迟。即，从 NetScaler 到后端服务器。
带宽	在选定的时间间隔内，端到端通信所占用的每秒总字节数。
服务器端重传	在 NetScaler 与后端服务器之间的连接上重传的数据包数量。
客户端重传	在 NetScaler 与最终用户之间的连接上重传的数据包数量。此指标的高值并不意味着用户体验不会是无缝的，但表示由于重传导致的高带宽利用率。
客户端快速 RTO	在 NetScaler 与最终用户之间的连接上发生重传超时的次数。
服务器端快速 RTO	在 NetScaler 与后端服务器之间的连接上发生重传超时的次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。

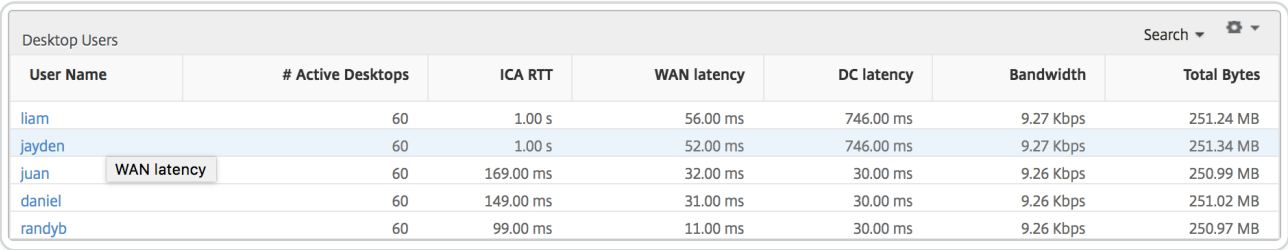
© 1997–2026 Citrix Systems, Inc. All rights reserved.



桌面摘要报告

指标	描述
活动会话	在给定时间间隔内，Citrix Virtual Desktop 活动会话的总数。
活动桌面	在给定时间间隔内，Citrix Virtual Desktops 活动桌面的总数。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual Apps 和 Desktops 上托管的应用程序或桌面交互时所经历的屏幕延迟。
广域网延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。即从 NetScaler 到后端服务器。
带宽	在选定时间间隔内，端到端通信每秒消耗的总字节数。
总字节数	用户在选定时间段内消耗的总字节数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



User Name	# Active Desktops	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
liam	60	1.00 s	56.00 ms	746.00 ms	9.27 Kbps	251.24 MB
jayden	60	1.00 s	52.00 ms	746.00 ms	9.27 Kbps	251.34 MB
juan	60	169.00 ms	32.00 ms	30.00 ms	9.26 Kbps	250.99 MB
daniel	60	149.00 ms	31.00 ms	30.00 ms	9.26 Kbps	251.02 MB
randyb	60	99.00 ms	11.00 ms	30.00 ms	9.26 Kbps	250.97 MB

阈值报告

阈值报告显示了在选定期间内，当*实体*选择为桌面时，被突破的阈值数量。有关更多信息，请参阅如何创建阈值和警报。

按桌面视图

按桌面视图为选定的 Citrix Virtual Desktop 提供详细的最终用户体验报告。

要导航到特定桌面视图：

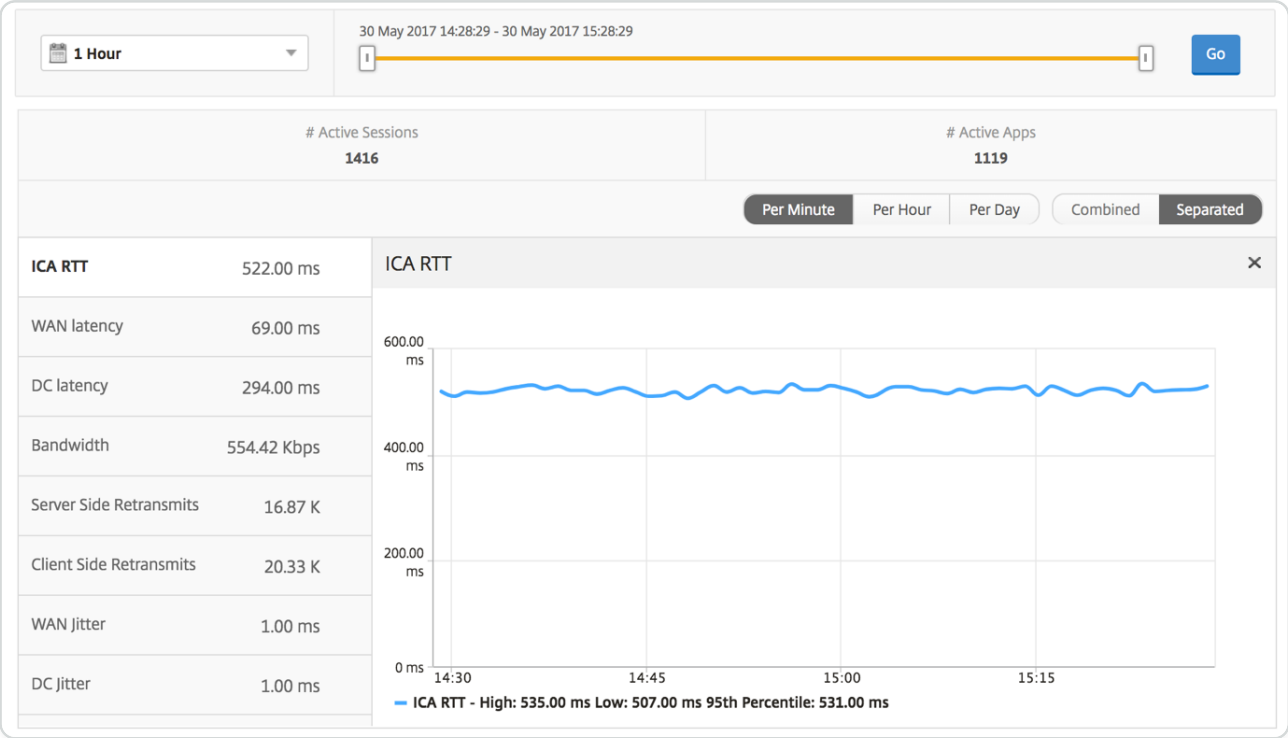
1. 导航到 **分析 \> HDX Insight \> 桌面**。
2. 从**桌面摘要报告**中选择一个特定的**桌面**。

折线图

指标	描述
# 活动会话	此数字表示活动 Citrix Virtual Apps and Desktops 会话的数量。
# 活动应用程序	此数字表示活动 Citrix Virtual App 会话的数量。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual Apps and Desktops 上托管的应用程序或桌面交互时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。即从 NetScaler 到后端服务器。
带宽	在选定时间间隔内，端到端通信每秒消耗的总字节数。
服务器端重传	NetScaler 与后端服务器之间连接上重传的数据包数量。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
客户端重传	NetScaler 与最终用户之间连接上重传的数据包数量。此指标的高值并不意味着用户体验不会是无缝的，但表示由于重传导致的高带宽利用率。
客户端快速 RTO	NetScaler 与最终用户之间的连接上发生重传超时的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间的连接上发生重传超时的次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。



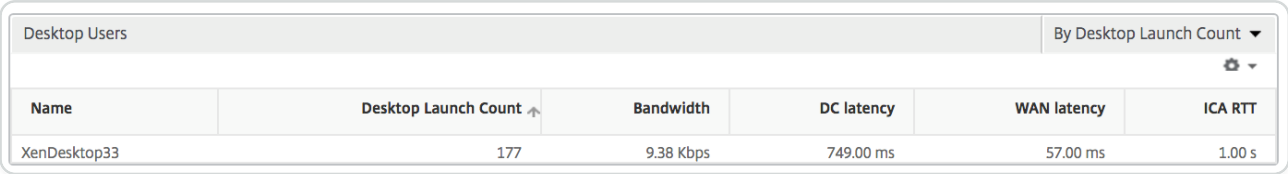
桌面用户报告

此表提供了对特定用户的 Citrix Virtual Desktop 会话的深入了解。这些指标可以按桌面启动计数和带宽进行排序。

指标	描述
名称	Citrix 虚拟桌面的名称。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
桌面启动计数	桌面已启动的次数。
带宽	在选定时间间隔内，端到端通信每秒消耗的总字节数。
DC 延迟	由网络服务器端引起的延迟。即从 NetScaler 到后端服务器的延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户的延迟。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual Apps 和 Desktops 上托管的应用程序或桌面交互时所经历的屏幕延迟。



用户桌面活跃/非活跃报告

以下指标可以按每间隔带宽、会话重新连接次数和 ACR 计数进行排序。

指标	描述
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色表示活动/非活动会话。
主机延迟	通过 NetScaler 实例的 ICA 流量中，由服务器网络引起的平均延迟。
每间隔带宽	会话在该特定时间间隔内消耗的带宽。
会话带宽	会话消耗的带宽，与时间间隔无关。
每间隔字节数	会话在该特定时间间隔内消耗的字节数。
开始时间	会话开始时间。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
运行时间	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual App 服务器 IP。
NetScaler IP 地址	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows 客户端等
客户端版本	Workspace 版本。
MSI	布尔值（是/否）。指示会话是否为多流 ICA。
会话重新连接	会话重新连接的次数。
ACR 计数	客户端自动将用户重新连接到断开连接的会话的总次数。
用户访问类型	显示 ICA 会话的访问模式。例如，NetScaler Gateway 用户/透明模式。
国家/地区	建立会话的国家/地区。
区域	建立会话的区域。
城市	会话建立的城市。
USB 状态	活动/非活动 - 绿色/红色。
接受的 USB 实例数	接受的 USB 实例计数。
拒绝的 USB 实例数	拒绝的 USB 实例计数。
停止的 USB 实例数	停止的 USB 实例计数。
客户端主机名	客户端的主机名。
HA 故障转移计数	HA 故障转移发生的次数。
终止原因	显示会话终止的原因。例如，ICA 会话超时、用户终止会话。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps 或 Desktops 上的应用程序或桌面交互时所体验到的屏幕延迟。
广域网延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
数据中心延迟	由网络服务器端引起的延迟。即从 NetScaler 到后端服务器。
总字节数	用户在选定时间段内消耗的总字节数。
服务器端重传	NetScaler 和后端服务器之间连接上重传的数据包数量。
客户端重传	NetScaler 和最终用户之间连接上重传的数据包数量。此指标的高值并不意味着用户体验不会是无缝的，但表示由于重传导致的高带宽利用率。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
客户端快速 RTO	NetScaler 与最终用户之间的连接发生重传超时次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间的连接发生重传超时次数。
VDI 映像名称	用户连接到的 Citrix 虚拟桌面名称
图表	

非活动报告(/en-us/netscaler-application-delivery-management-software/media/hdx-user-dekstop-active-inactive.png)

按桌面会话视图

按桌面会话视图提供特定选定 Citrix 虚拟桌面会话的报告。

导航到桌面会话视图：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 导航到 **网关 > HDX Insight > 桌面**。
2. 从 **Desktop Summary Report** 中选择一个特定桌面。
3. 从当前会话报告中选择一个会话。

时间线图表

每个用户会话视图提供特定选定用户会话的报告。

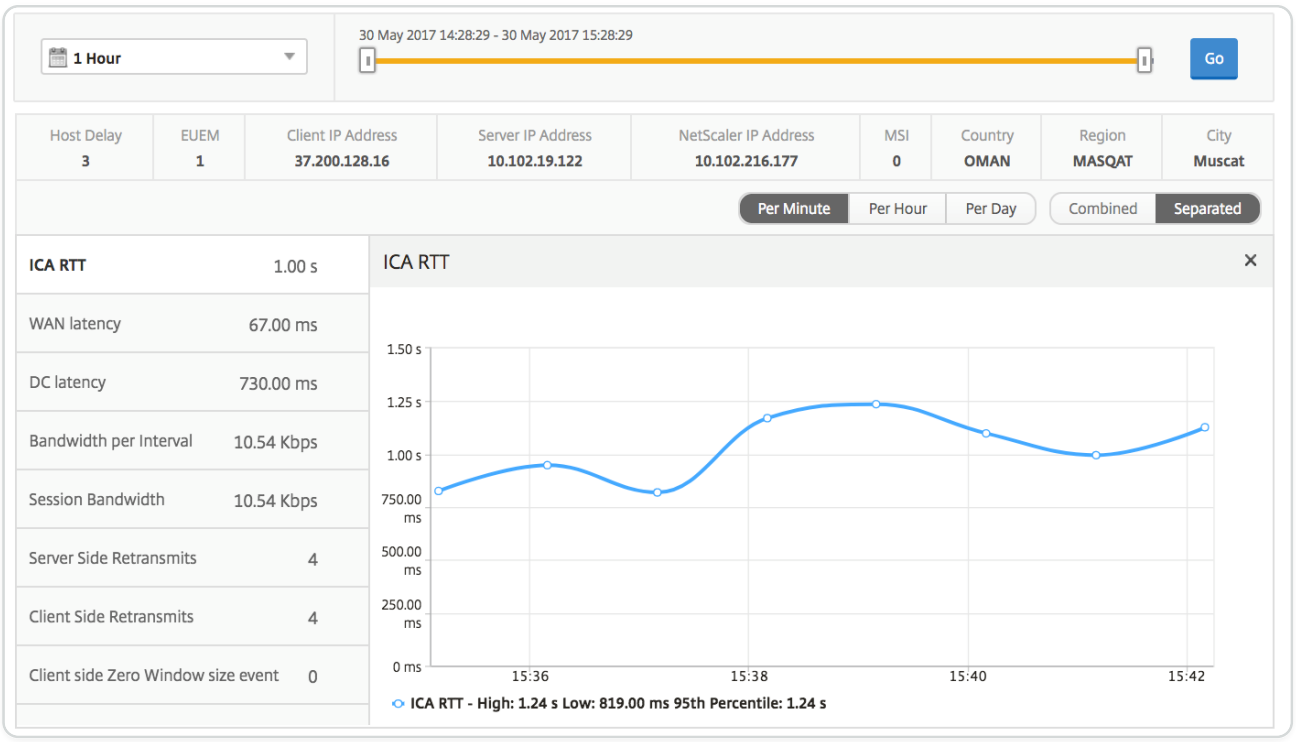
查看所选用户会话的指标：

1. 导航到 **网关 > HDX Insight > 用户**。
2. 从 **User Summary Report** 部分选择特定用户。
3. 从 **Current Sessions** 或 **Terminated Sessions** 列中选择一个会话。

指标	描述
会话重新连接	此数字表示活动 Citrix Virtual App and Desktop 会话的数量。
ACR 计数	此数字表示活动 Citrix Virtual App 会话的数量。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual App 和 Desktop 上的应用程序或桌面交互时所经历的屏幕延迟。
WAN 延迟	网络客户端引起的延迟。即，从 NetScaler 到最终用户。
DC 延迟	网络服务器端引起的延迟。即，从 NetScaler 到后端服务器。
会话带宽	会话消耗的带宽，与时间间隔无关。
服务器端重传	NetScaler 与后端服务器之间连接上重传的数据包数量。
客户端重传	NetScaler 与最终用户之间连接上重传的数据包数量。此指标的高值并不意味着用户体验不会无缝，但表示由于重传导致的高带宽利用率。
客户端快速 RTO	NetScaler 与最终用户之间连接上发生重传超时次数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
服务器端快速 RTO	NetScaler 与后端服务器之间连接上发生重传超时次数。
每间隔带宽	会话在该特定时间间隔内消耗的带宽。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。



相关桌面会话报告

以下指标可以按每个间隔的带宽、会话重新连接和 ACR 计数进行排序。

指标	描述
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色表示活动/非活动会话。
主机延迟	通过 NetScaler 的 ICA 流量因服务器网络而导致的平均延迟。

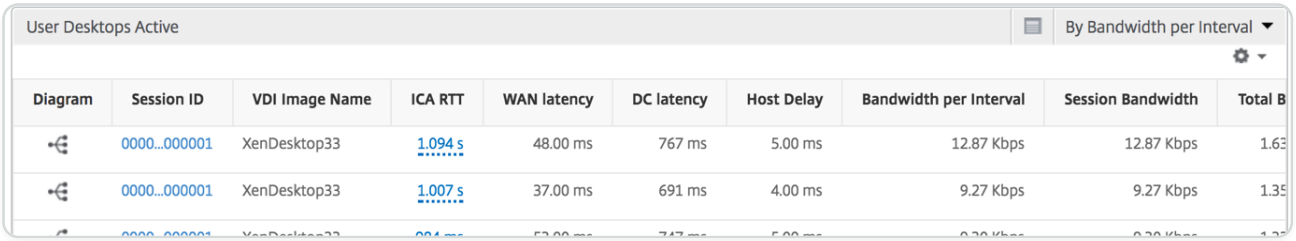
© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
每个间隔的带宽	会话在该特定时间间隔内消耗的带宽。
会话带宽	会话消耗的带宽，与时间间隔无关。
每个间隔的字节数	会话在该特定时间间隔内消耗的字节数。
开始时间	会话开始时间。
运行时间	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual App 服务器 IP。
NetScaler IP 地址	NetScaler 管理 IP (NSIP)。
客户端类型	Receiver 类型 - Citrix Windows 客户端等
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否为多流 ICA。
会话重新连接次数	会话重新连接的次数。
ACR 计数	客户端自动将用户重新连接到已断开连接的会话的总次数。
用户访问类型	显示 ICA 会话的访问模式。例如，NetScaler Gateway 用户/透明模式。
国家	建立会话的国家。
区域	建立会话的区域。
城市	建立会话的城市。
USB 状态	活动/非活动 - 绿色/红色。
接受的 USB 实例数	接受的 USB 实例计数。
拒绝的 USB 实例数	拒绝的 USB 实例计数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
停止的 USB 实例数	停止的 USB 实例计数。
客户端主机名	客户端的主机名。
HA 故障转移计数	HA 故障转移发生的次数。
终止原因	显示会话终止的原因。例如，ICA 会话超时，用户终止会话。
ICA RTT	ICA RTT 是用户在使用分别托管在 Citrix Virtual App 或 Desktop 上的应用程序或桌面时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。即从 NetScaler 到后端服务器。
总字节数	用户在选定时间段内消耗的总字节数。
服务器端重传	NetScaler 与后端服务器之间连接上重传的数据包数量。
客户端重传	NetScaler 与最终用户之间连接上重传的数据包数量。此指标的高值并不意味着用户体验不会无缝，但表示由于重传导致的高带宽利用率。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
客户端快速 RTO	NetScaler 与最终用户之间连接上发生重传超时事件的次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间连接上发生重传超时事件的次数。
VDI 映像名称	用户连接到的 Citrix 虚拟桌面名称

© 1997–2026 Citrix Systems, Inc. All rights reserved.

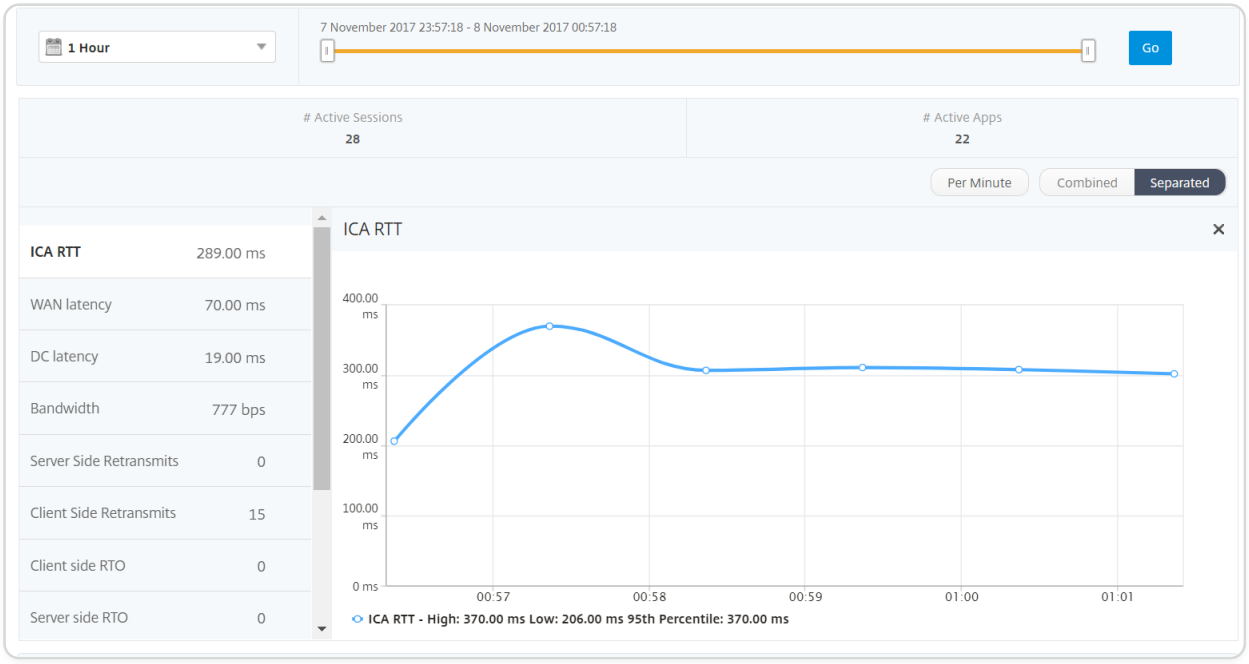


用户视图报告和指标

此视图中的报告和指标按 Citrix Virtual Apps™ 和 Desktop 用户显示。

导航到“用户”视图：

1. 导航到 **Gateway > HDX™ Insight > 用户**



摘要视图

摘要视图显示在选定时间线内登录的所有用户的报告。除非另有说明，此视图中的所有指标/报告都显示其在选定时间段内的相应值。

更改选定的时间段：

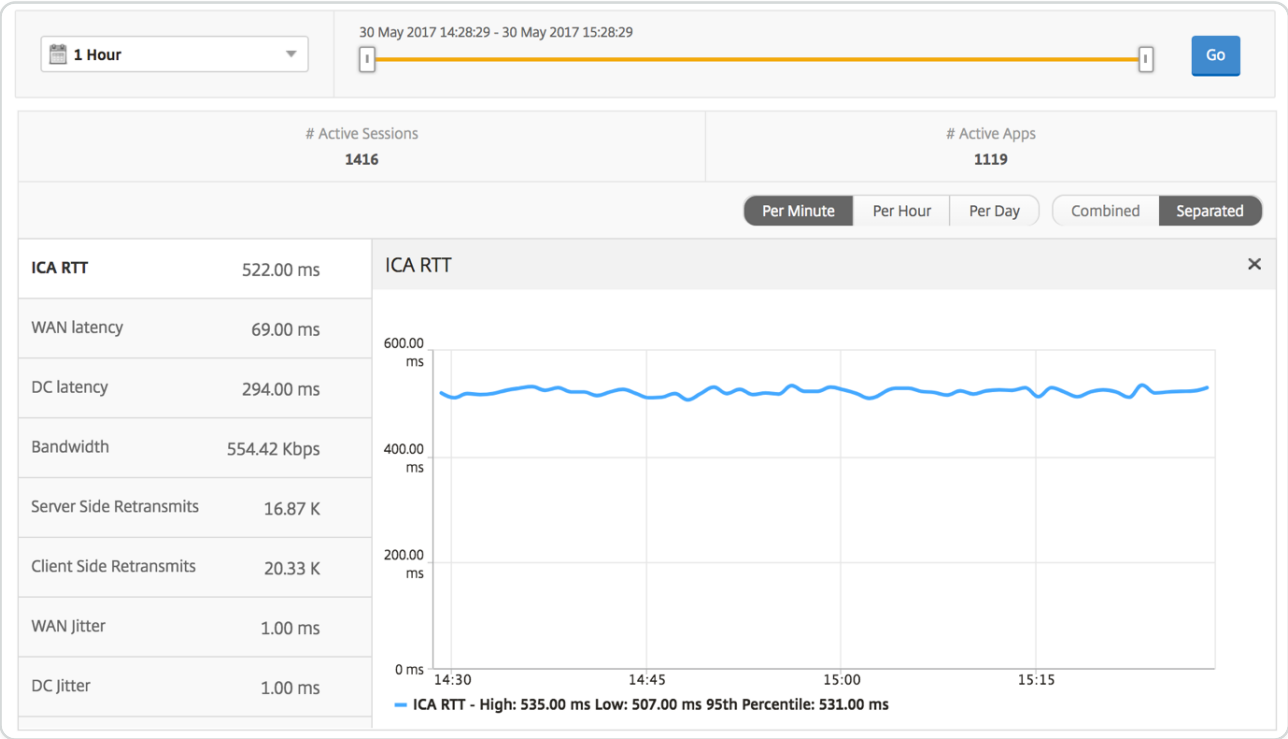
1. 使用时间段列表或时间滑块设置所需的时间间隔。
2. 单击 **Go**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

折线图

指标	描述
# 活动会话	此数字表示活动 Citrix Virtual App 和 Desktop 会话的数量。
# 活动应用程序	此数字表示活动 Citrix Virtual App 会话的数量。
ICA RTT	ICA RTT 是用户分别与 Citrix Virtual App 或 Desktop 上托管的应用程序或桌面交互时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
数据中心延迟	由网络服务器端引起的延迟。即从 NetScaler 到后端服务器。
带宽	在选定时间间隔内，端到端通信每秒占用的总字节数。
服务器端重传	NetScaler 与后端服务器之间连接上重传的数据包数量。
客户端重传	NetScaler 与最终用户之间连接上重传的数据包数量。此指标的高值并不意味着用户体验不会无缝，但表示由于重传导致的高带宽利用率。
客户端快速 RTO	NetScaler 与最终用户之间的连接发生重传超时次数。
服务器端快速 RTO	NetScaler 与后端服务器之间的连接发生重传超时次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



用户摘要报告

以下是此报告特有的指标。

指标	描述
# 活动会话	此数字指示活动 Citrix Virtual App and Desktop 会话的计数。
# 活动应用程序	此数字表示活动 Citrix Virtual App 会话的数量。
ICA RTT	ICA RTT 是用户在使用 Citrix Virtual App 或 Desktop 上托管的应用程序或桌面时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即，从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。即，从 NetScaler 到后端服务器。
带宽	在选定时间间隔内，端到端通信每秒消耗的总字节数。
服务器端重传	NetScaler 与后端服务器之间连接上重传的数据包数量。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
客户端重传	NetScaler 与最终用户之间连接上重传的数据包数量。此指标的高值并不意味着用户体验不会是无缝的，但表示由于重传导致的高带宽利用率。
客户端快速 RTO	NetScaler 与最终用户之间连接上发生重传超时事件的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间的连接上发生重传超时的次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
总应用程序启动计数	用户在选定时间段内启动的应用程序总数。
总字节数	用户在选定时间段内消耗的总字节数。
活动桌面	在给定时间间隔内活动 Citrix 虚拟桌面的总数。

Users

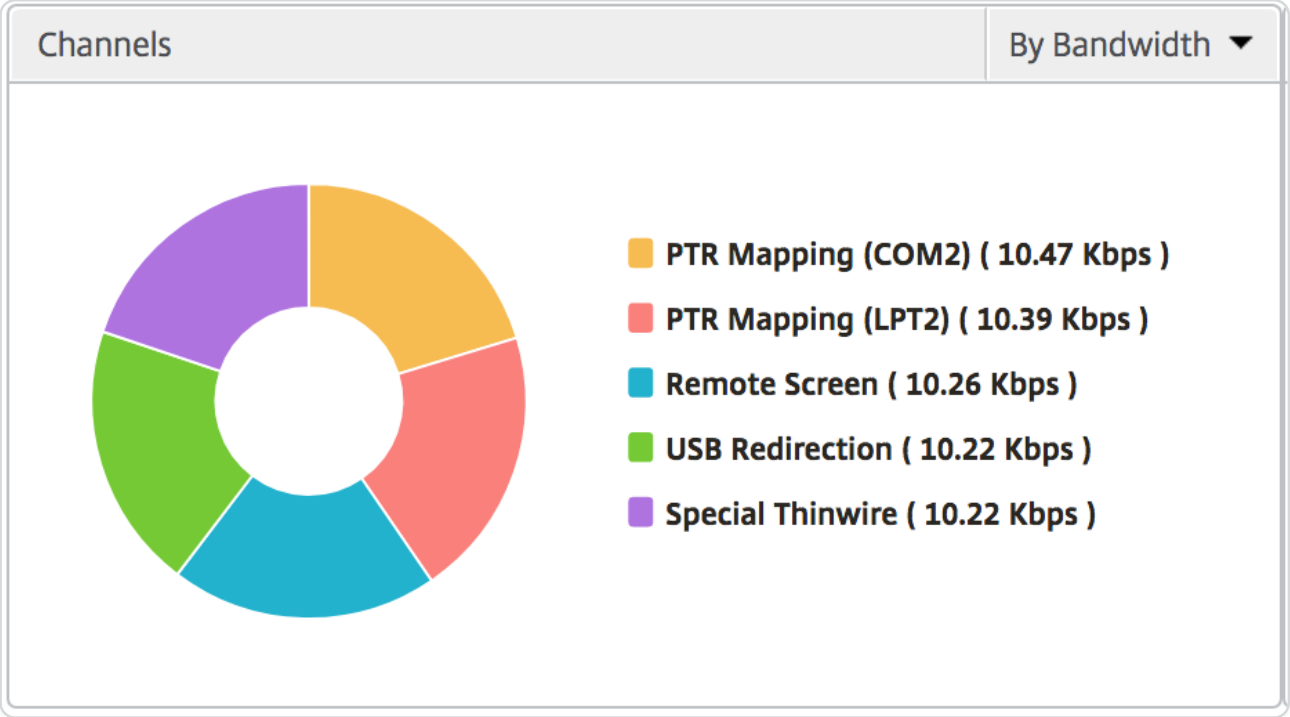
Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

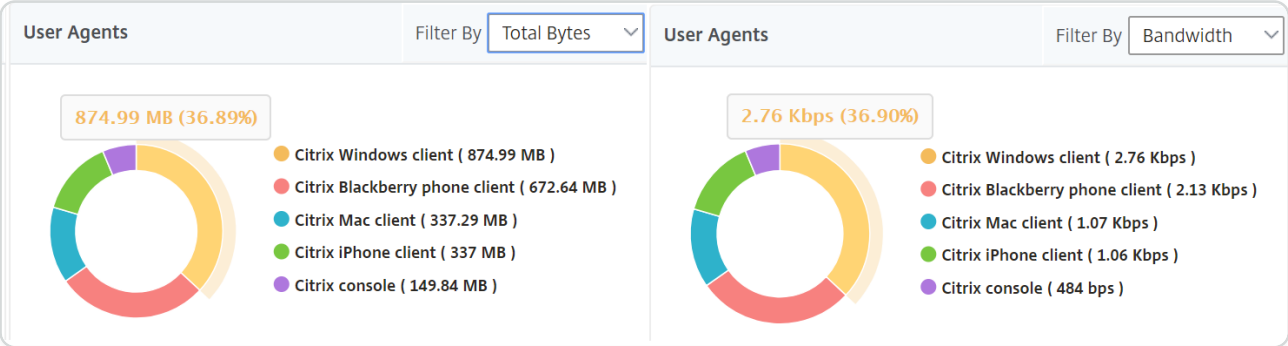
通道

通道以环形图的形式表示每个 ICA® 虚拟通道消耗的总带宽或总字节数。您还可以按带宽或总字节数对指标进行排序。



用户代理

用户代理以环形图的形式表示每个端点消耗的总带宽/总字节数。您还可以按带宽或总字节数对指标进行排序。



阈值违规计数

阈值违规计数指标表示在选定时间段内违规的阈值数量。有关详细信息，请参阅如何创建阈值和警报。

世界地图

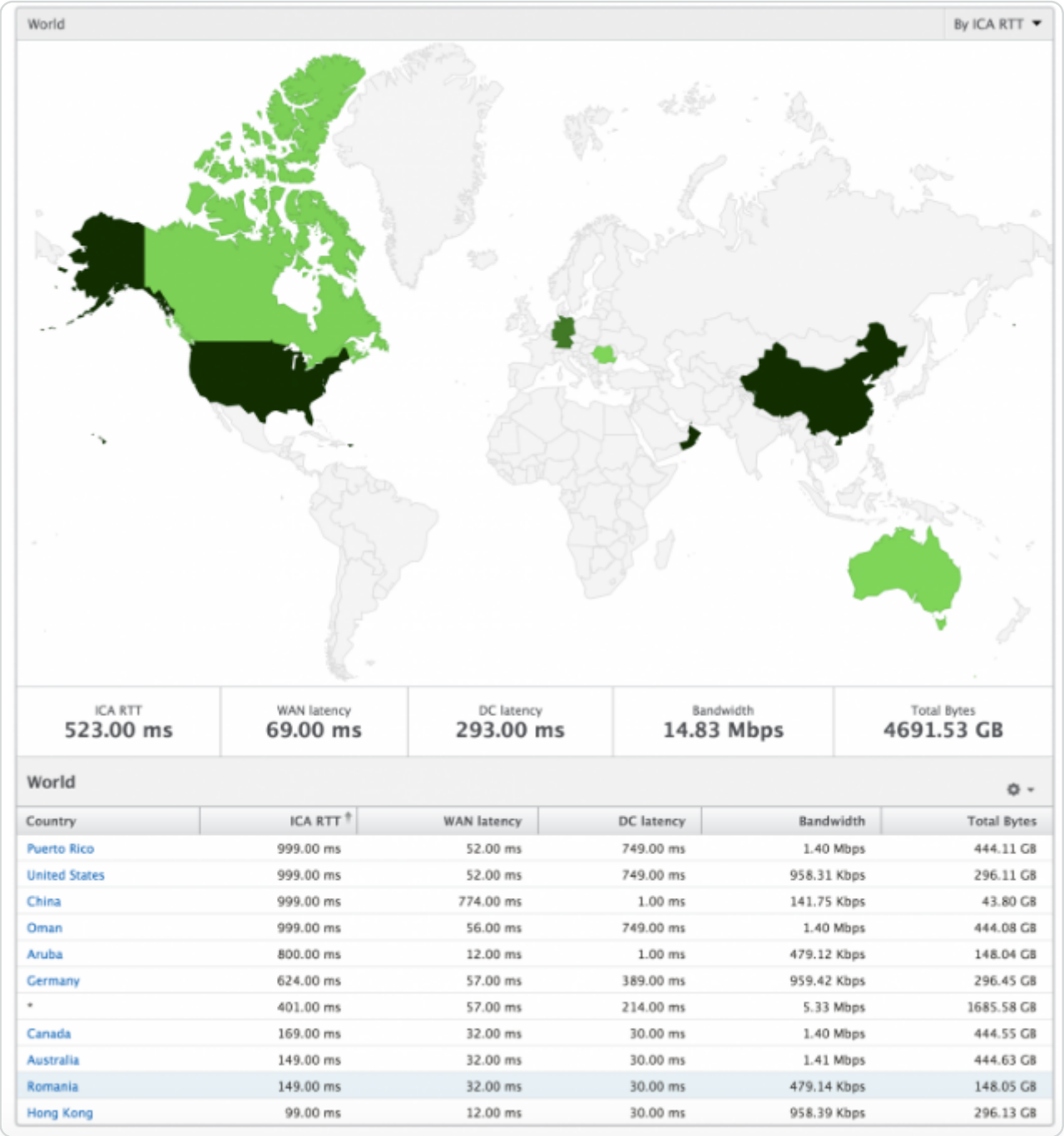
HDX Insight 中的世界地图视图允许管理员从地理角度查看历史和活动用户详细信息。管理员可以查看系统的世界视图，通过单击区域深入到特定国家/地区，甚至深入到城市。管理员可以进一步深入

© 1997–2026 Citrix Systems, Inc. All rights reserved.

查看按城市和州划分的信息。从 NetScaler Console 12.0 版及更高版本开始，您可以深入查看从地理位置连接的用户。

可以在 HDX Insight 的世界地图上查看以下详细信息，并且每个指标的密度以热图的形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- 带宽
- 总字节数



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

© 1997–2026 Citrix Systems, Inc. All rights reserved.

按用户视图

按用户视图为任何特定选定用户提供详细的最终用户体验报告。

导航到特定用户的指标：

1. 导航到 **Gateway > HDX Insight > 用户**。
2. 从用户摘要报告中选择特定用户。

折线图

折线图显示了在选定时间段内特定选定用户的所有指标摘要。

当前/已终止会话报告

此报告与所选用户的所有当前/已终止用户会话相关。这些指标可以按开始时间、会话重新连接和 ACR 计数进行排序。

指标	描述
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	活动/非活动会话的绿色/红色状态。
主机延迟	由于服务器网络原因，通过 NetScaler 实例的 ICA 流量的平均延迟。
每个间隔的带宽	会话在该特定时间间隔内消耗的带宽。
会话带宽	会话消耗的带宽，与时间间隔无关。
每个间隔的字节数	会话在该特定时间间隔内消耗的字节数。
开始时间	会话开始时间。
运行时间	会话持续时间。
客户端 IP 地址	终端用户 IP。
服务器 IP 地址	后端/Citrix Virtual App 服务器 IP。
NetScaler IP 地址	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows Client 等

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
客户端版本	工作区版本。
MSI	布尔值（是/否）。指示会话是否为多流 ICA。
会话重新连接	会话重新连接的次数。
ACR 计数	客户端自动将用户重新连接到断开连接的会话的总次数。
用户访问类型	显示 ICA 会话的访问模式。例如，NetScaler Gateway 用户/透明模式。
国家/地区	会话建立的国家/地区。
区域	会话建立的区域。
城市	会话建立的城市。
USB 状态	活动/非活动 - 绿色/红色。
接受的 USB 实例数	接受的 USB 实例计数。
拒绝的 USB 实例数	拒绝的 USB 实例计数。
停止的 USB 实例数	停止的 USB 实例数量。
客户端主机名	客户端的主机名。
HA 故障转移计数	HA 故障转移发生的次数。
终止原因	显示会话终止的原因。例如，ICA 会话超时、用户终止会话。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual App 或 Desktop 上的应用程序或桌面交互时所经历的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
DC 延迟	由网络服务器端引起的延迟。即从 NetScaler 到后端服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

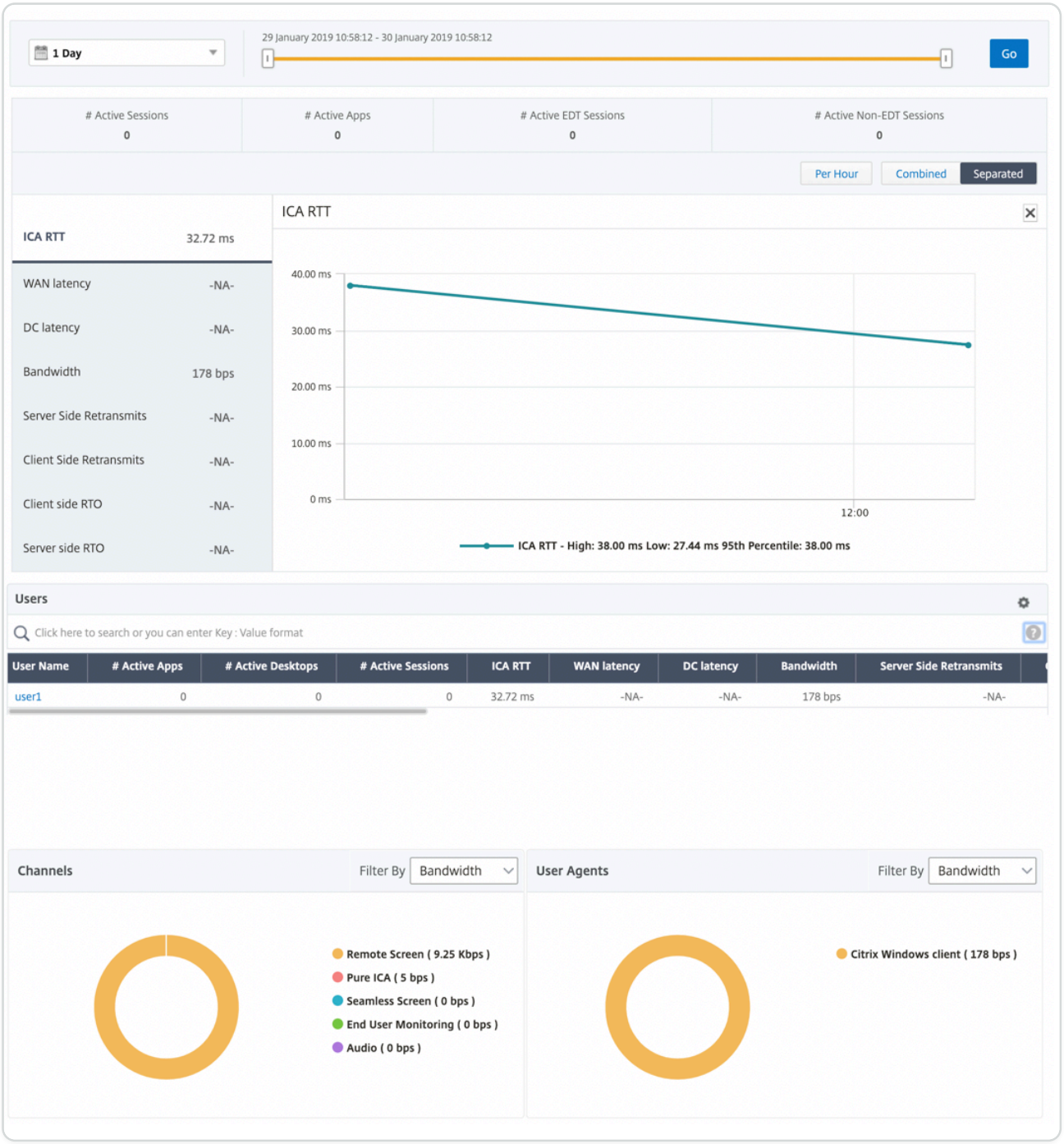
指标	描述
总字节数	用户在选定时间段内消耗的总字节数。
服务器端重传	在 NetScaler 与后端服务器之间的连接上重传的数据包数量。
客户端重传	在 NetScaler 与最终用户之间的连接上重传的数据包数量。此指标的高值并不意味着用户体验不会无缝，但表示由于重传导致的高带宽利用率。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。
客户端快速 RTO	在 NetScaler 与最终用户之间的连接上发生重传超时的次数。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
服务器端快速 RTO	在 NetScaler 与后端服务器之间的连接上发生重传超时的次数。

HDX INSIGHT 中对 EDT 的支持

NetScaler Console 现在支持开明数据传输 (EDT)，用于显示 HDX Insight 的分析数据。也就是说，NetScaler Console 现在同时支持 UDP 和 TCP 协议。NetScaler Gateway 对 EDT 的支持确保了运行 Citrix Workspace 的用户获得虚拟桌面会话内的高清用户体验。

HDX Insight 现在将 EDT 会话和非 EDT 会话的数量显示为活动会话报告的一部分。“用户”表显示系统中所有用户的详细报告。该表显示了 WAN 延迟、DC 延迟、重传和 RTO 等指标。其中一些指标不适用于具有 EDT 会话的用户，因为它们目前是从 TCP 堆栈计算的。因此，它们显示为“不适用”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



引入了一个新的环形图，让您能够查看用户消耗的带宽以及根据用户使用的协议类型计算的总字节数。

EDT(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-edt-support-2.png)

适用于 NetScaler Console 12.0 及更高版本的 HDX Insight 指标：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L7 客户端延迟	在 ICA 客户端和 NETSCALER 实例之间观察到的平均 L7 延迟。当交付路径中存在非 CITRIX 设备时，此指标非常有用。
L7 服务器端延迟	在 NetScaler 设备和 Citrix Virtual App 之间观察到的平均 L7 延迟。当交付路径中存在非 Citrix 设备时，此指标非常有用。
最大违规延迟	当在设定的时间间隔内发生定义的阈值违规时，L7 延迟的最高值。
平均违规延迟	当系统处于“L7 延迟违规”状态时，L7 延迟的平均值。
L7 阈值违规计数	L7 阈值违规发生的次数。

当前会话(/en-us/netscaler-application-delivery-management-software/media/hdx-current-sessions-1.png)

已终止的会话(/en-us/netscaler-application-delivery-management-software/media/hdx-teminated-sessions-1.png)

桌面用户

此表提供了特定用户的 Citrix Virtual Desktop 会话的深入信息。这些指标可以按桌面启动计数和带宽进行排序。

指标	描述
名称	Citrix 虚拟桌面的名称。
桌面启动计数	桌面已启动的次数。
带宽	在选定时间间隔内，端到端通信每秒占用的总字节数。
DC 延迟	由网络服务器端引起的延迟。即从 NetScaler 到后端服务器。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
ICA RTT	ICA RTT 是用户在使用分别托管在 Citrix Virtual App 或 Desktop 上的应用程序或桌面时遇到的屏幕延迟。

桌面用户(/en-us/netscaler-application-delivery-management-software/media/hdx-dekstop-user.png)

应用程序

一个条形图，表示按活动状态、会话启动总次数、应用程序启动总次数和启动持续时间排序的应用程序。

应用程序(/en-us/netscaler-application-delivery-management-software/media/hdx-application-graph.png)

实例

一个条形图，表示按活动状态和应用程序总数排序的 NetScaler 实例

实例(/en-us/netscaler-application-delivery-management-software/media/hdx-instances-graph.png)

通道

通道以环形图的形式表示每个 ICA 虚拟通道消耗的总带宽或总字节数。您还可以按带宽或总字节数对指标进行排序。

通道(/en-us/netscaler-application-delivery-management-software/media/hdx-insight-channel-1.png)

用户代理

用户代理以环形图的形式表示每个端点消耗的总带宽/总字节数。您还可以按带宽或总字节数对指标进行排序。

用户代理(/en-us/netscaler-application-delivery-management-software/media/hdx-user-agents.png)

按用户会话视图

按用户会话视图提供特定选定用户的会话报告。

要查看选定用户的会话指标：

1. 导航到 **网关 > HDX Insight > 用户**。
2. 从“**用户摘要报告**”部分选择特定用户。
3. 从“**当前会话**”或“**已终止会话**”列中选择一个会话。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

时间线图表

指标	描述
会话重新连接	此数字表示活动 Citrix Virtual App 和 Desktop 会话的数量。
ACR 计数	此数字表示活动 Citrix Virtual App 会话的数量。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual App 或 Desktop 上的应用程序或桌面交互时遇到的屏幕延迟。
WAN 延迟	由网络客户端引起的延迟。即从 NetScaler 到最终用户。
数据中心延迟	由网络服务器端引起的延迟。即从 NetScaler 到后端服务器。
会话带宽	会话消耗的带宽，与时间间隔无关。
服务器端重传	在 NetScaler 与后端服务器之间的连接上重传的数据包数量。
客户端重传	在 NetScaler 与最终用户之间的连接上重传的数据包数量。此指标的高值并不意味着用户体验不会无缝，但表示由于重传导致的高带宽利用率。
客户端快速 RTO	NetScaler 与最终用户之间的连接上发生重传超时的次数。
服务器端快速 RTO	NetScaler 与后端服务器之间的连接上发生重传超时的次数。
每间隔带宽	会话在该特定时间间隔内消耗的带宽。
服务器端零窗口大小事件	此计数器指示服务器通告零 TCP 窗口的次数。
客户端零窗口大小事件	此计数器指示客户端通告零 TCP 窗口的次数。

时间线图表(/en-us/netscaler-application-delivery-management-software/media/hdx-timeline-chart.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

活动应用程序

“**活动应用程序**”部分显示所选用户的活动应用程序。这些应用程序还可以按活动会话数和启动持续时间进行排序。

活动应用程序(/en-us/netscaler-application-delivery-management-software/media/hdx-active-application.png)

相关会话

“相关会话”部分显示所选用户会话的相关会话。关系可以选为通用服务器或通用 NetScaler。

相关会话(/en-us/netscaler-application-delivery-management-software/media/hdx-related-sessions.png)

实例视图报告和指标

实例视图中的报告和指标侧重于 NetScaler 实例。

导航到实例视图：

1. 导航到 **网关 > HDX™ Insight > 实例**。

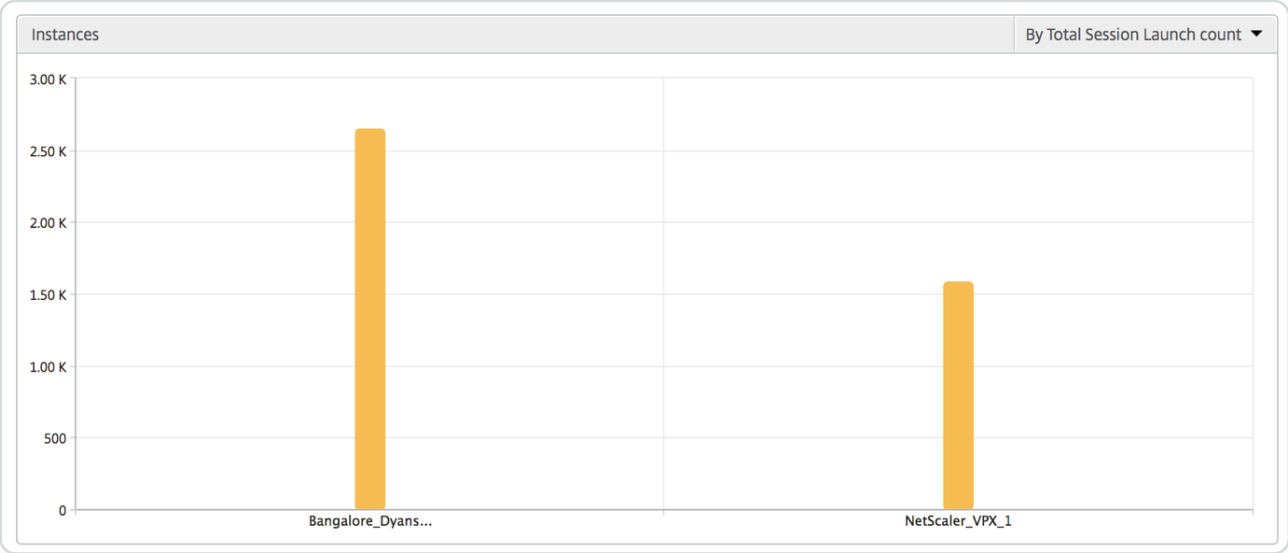
实例摘要视图

此视图称为摘要视图，因为它显示了添加到 NetScaler Console 的所有 NetScaler 实例的报告。

除非另有明确说明，否则所有指标/报告都将显示所选时间段的相应值。

实例柱状图

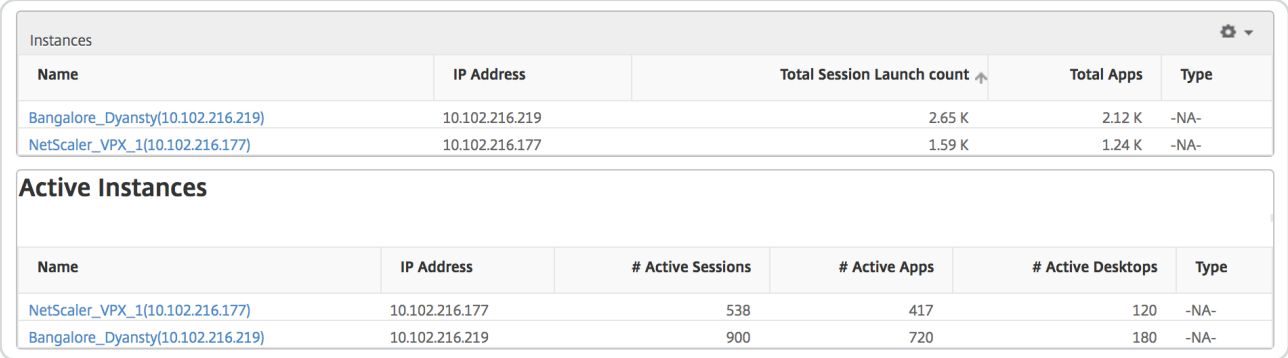
此图表显示实例与总会话启动计数和总应用程序，这些可以从图表画布右上角的列表中选择。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

实例/活动实例摘要报告

指标	描述
名称	NetScaler 实例的主机名。
IP 地址	NetScaler IP 地址。
会话启动总数	在给定时间间隔内创建的唯一用户会话总数。
应用程序总数	在给定时间间隔内启动的唯一应用程序总数。
类型	不适用



Instances

Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

阈值报告

阈值报告表示在选定期间，当*实体*选择为实例时，已突破的阈值数量。有关详细信息，请参阅如何创建阈值和警报。

跳过的流

跳过的流是跳过解析 ICA 连接的记录。这可能由于多种原因而发生，例如使用不受支持的 Citrix Virtual Apps and Desktops 版本、不受支持的工作区版本或工作区类型等。此表显示 IP 地址和跳过的流计数。这些工作区可能不属于白名单工作区。因此，这些会话将从监视中跳过。

有关 ICA 解析相关问题的更多详细信息，请参阅 **错误\! 超链接引用无效**。

Skipped Flows

IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

世界视图

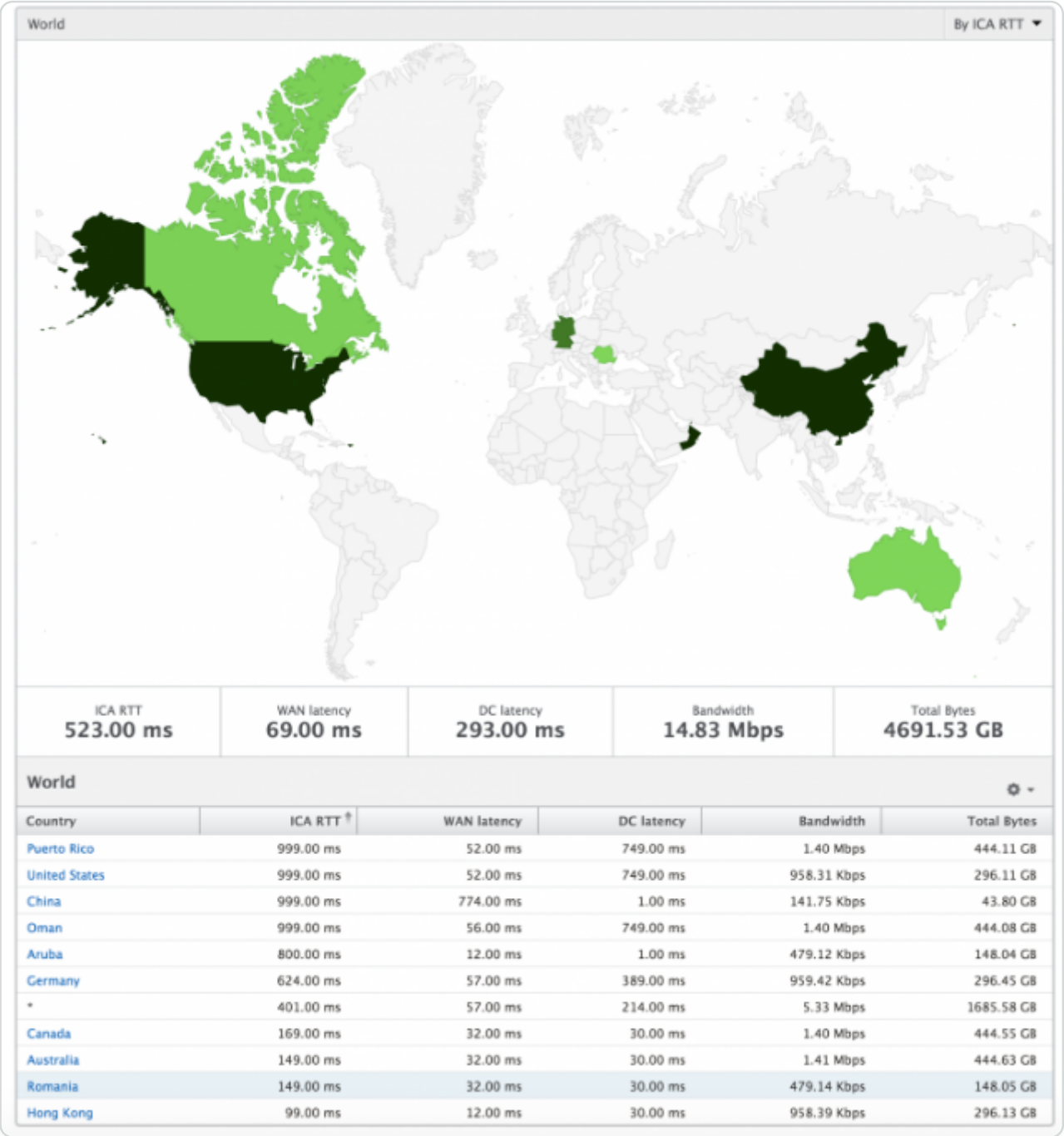
HDX Insight 中的世界地图视图允许管理员从地理角度查看历史和活跃用户详细信息。管理员可以查看系统的世界视图，通过单击区域深入到特定国家/地区，甚至城市。管理员可以进一步深入查看按

© 1997–2026 Citrix Systems, Inc. All rights reserved.

城市和州划分的信息。从 NetScaler 12.0 版及更高版本开始，您可以深入查看从地理位置连接的用户。

可以在 HDX Insight 的世界地图上查看以下详细信息，每个指标的密度以热图形式显示：

- ICA® RTT
- WAN 延迟
- DC 延迟
- 带宽
- 总字节数



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

© 1997–2026 Citrix Systems, Inc. All rights reserved.

按实例视图

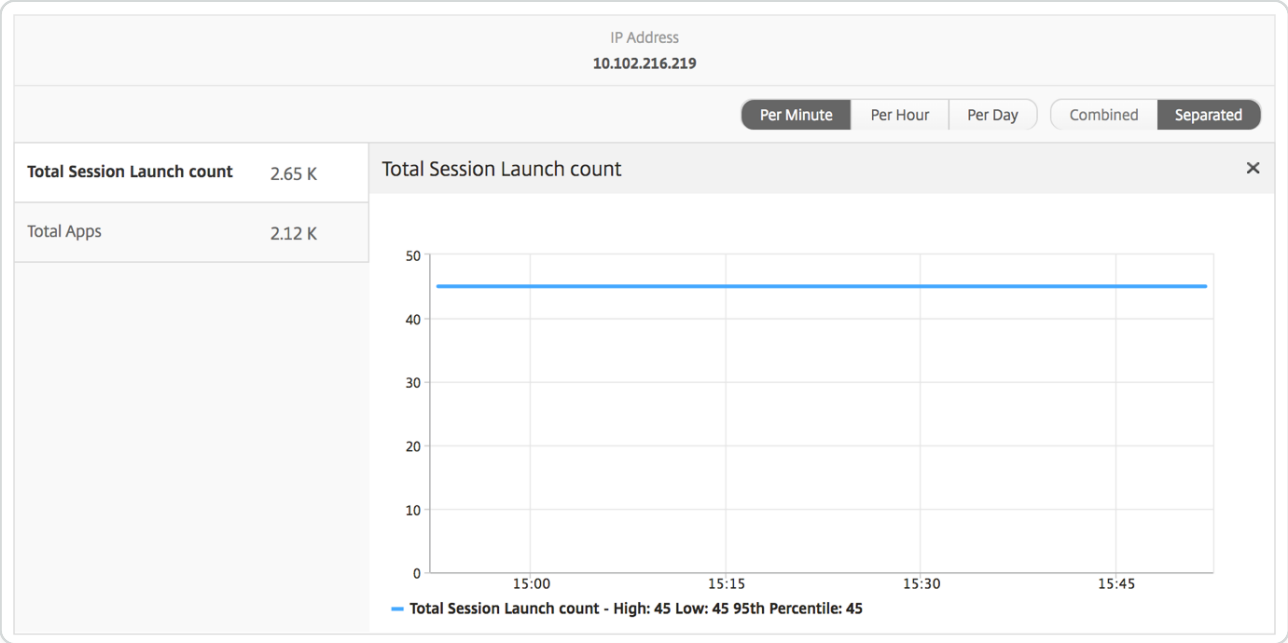
按实例视图为特定选定的 NetScaler 实例提供详细的最终用户体验报告。

导航到实例视图：

1. 导航到 **网关 > HDX Insight > 实例**。
2. 从 **实例摘要报告** 中选择一个特定实例。

折线图

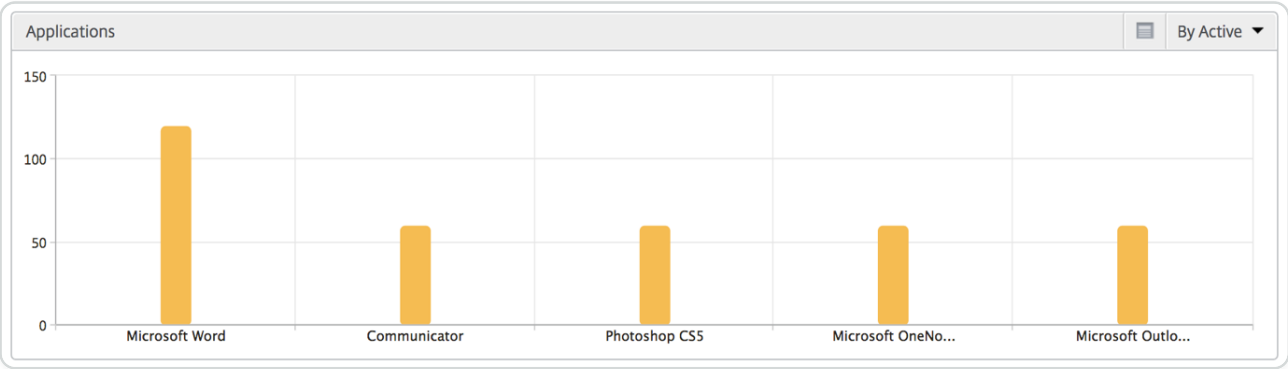
指标	描述
IP 地址	这表示所选实例的 NetScaler IP 地址。
会话启动总数	在给定时间间隔内，Citrix Virtual App 活动会话的总数。
应用程序总数	在给定时间间隔内启动的唯一应用程序总数。



应用程序条形图

根据以下条件显示前 5 个应用程序：活动应用程序、会话启动总数、应用程序启动总数或启动持续时间。

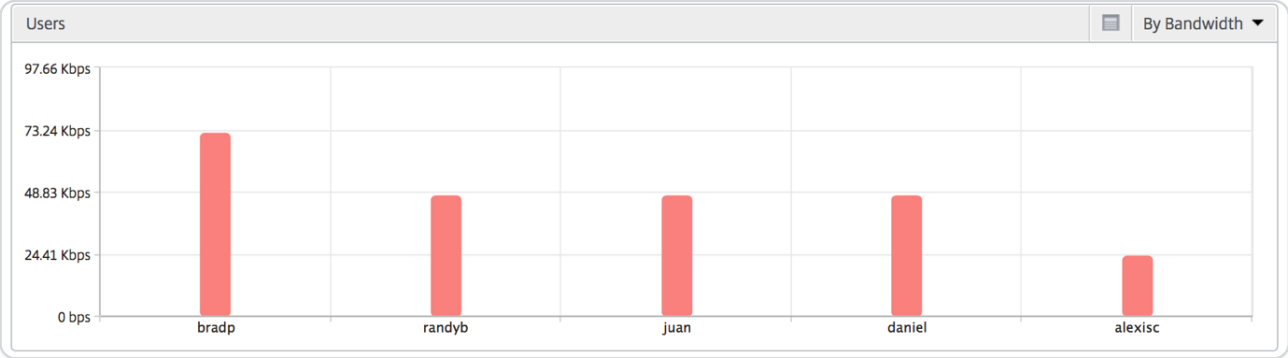
© 1997–2026 Citrix Systems, Inc. All rights reserved.



用户条形图

用户条形图根据以下条件显示前 5 名用户

- 带宽
- WAN 延迟
- DC 延迟
- ICA RTT



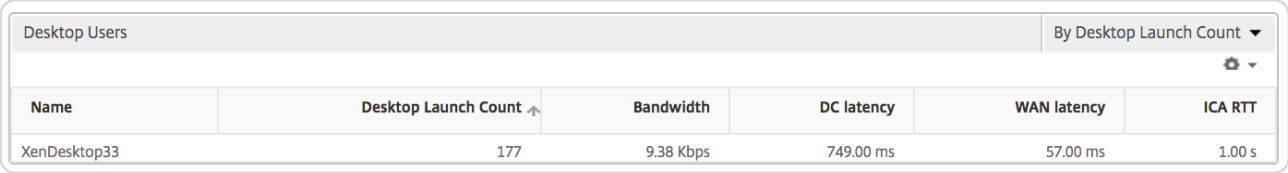
桌面用户报告

此表提供了特定用户的 Citrix Virtual Desktop 会话的深入信息。这些指标可以按桌面启动计数和带宽进行排序。

指标	描述
名称	Citrix 虚拟桌面的名称。
桌面启动计数	桌面已启动的次数。
带宽	在选定时间间隔内，端到端通信每秒消耗的总字节数。
DC 延迟	网络服务器端引起的延迟。即从 NetScaler 到后端服务器的延迟。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指标	描述
WAN 延迟	网络客户端引起的延迟。即从 NetScaler 到最终用户的延迟。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual App 或 Desktop 上的应用程序或桌面交互时所经历的屏幕延迟。



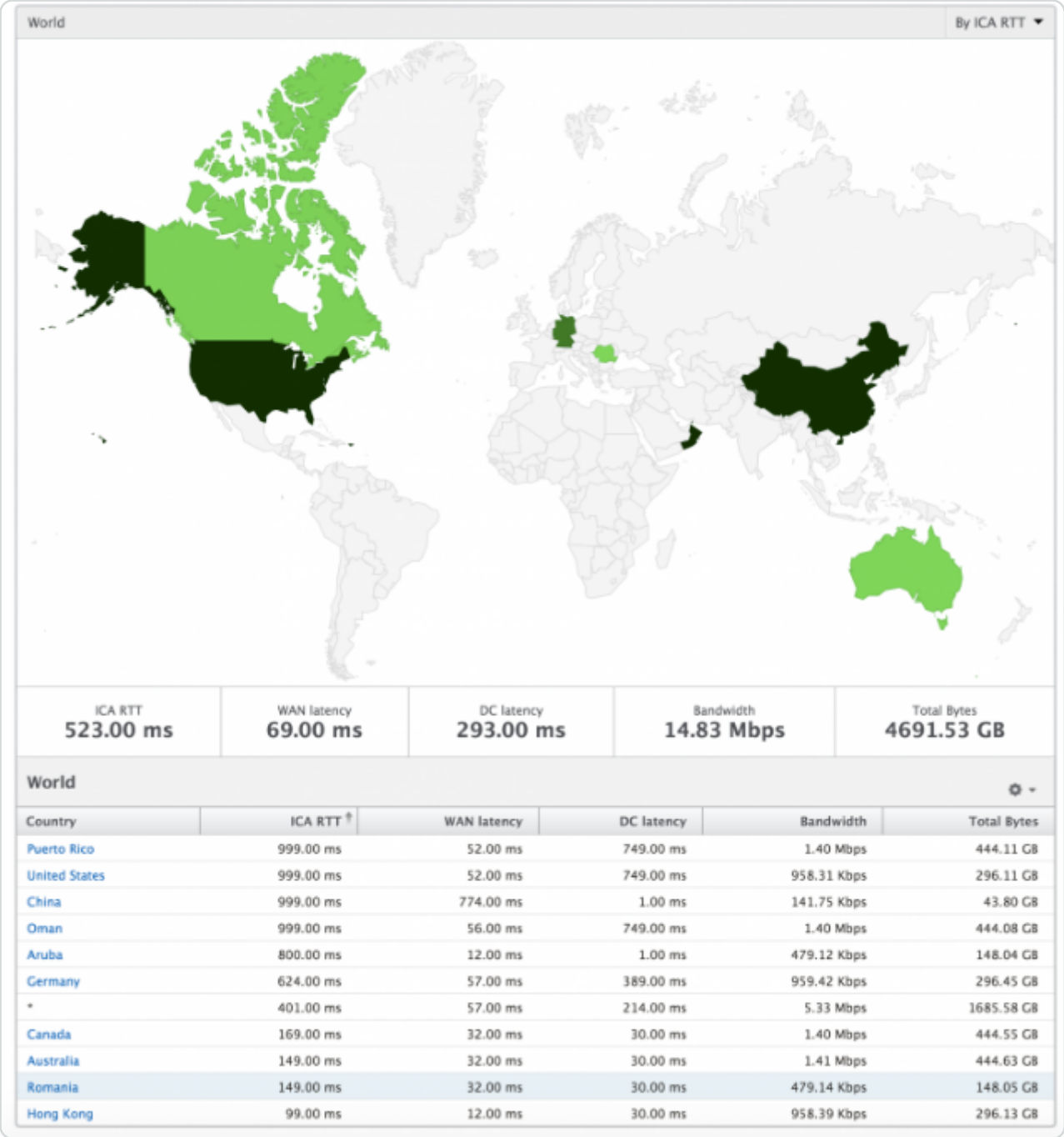
世界视图

HDX Insight 中的世界地图视图允许管理员从地理角度查看历史和活跃用户详细信息。管理员可以查看系统的世界视图，通过单击区域深入到特定国家，甚至更深入到城市。管理员还可以进一步深入查看按城市和州划分的信息。从 NetScaler Console 12.0 版及更高版本开始，您可以深入查看从地理位置连接的用户。

可以在 HDX Insight 的世界地图上查看以下详细信息，并且每个指标的密度以热图形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- 带宽
- 总字节数

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

许可证视图报告和指标

许可证视图提供有关 NetScaler Gateway 许可证信息的详细信息。

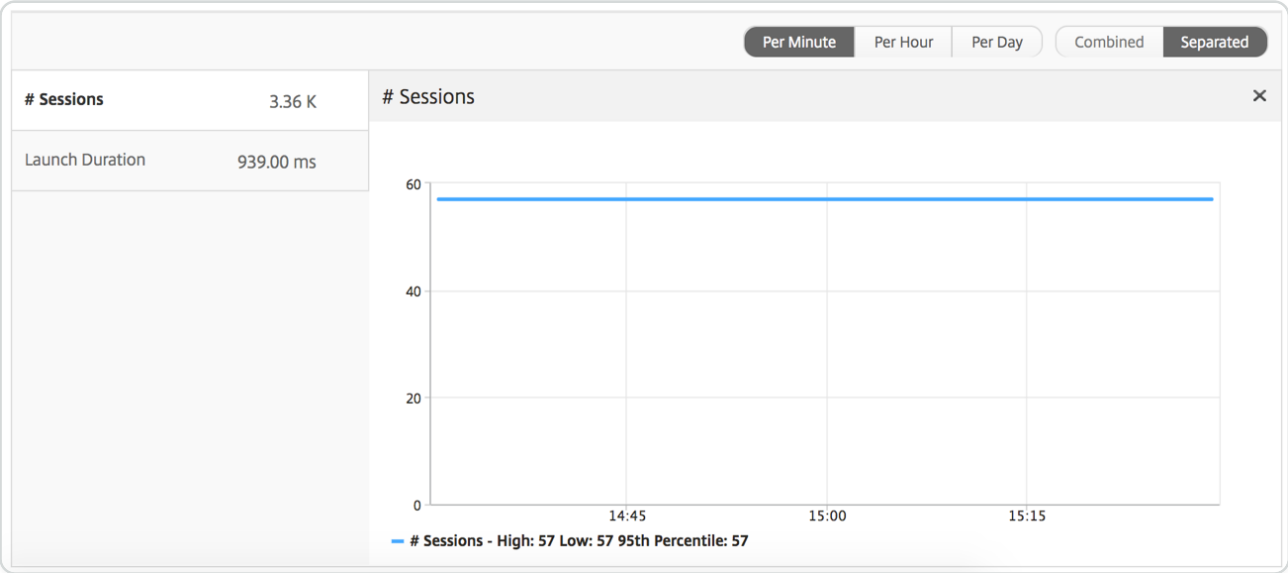
导航到许可证视图：

1. 导航到 **Gateway > HDX™ Insight > 许可证**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

折线图

指标	描述
正在使用的许可证	在选定时间线内使用的 NetScaler Gateway CCU 许可证。每个计数表示用户会话的数量。这与该用户启动的应用程序和桌面会话无关。
总许可证数	客户可用的 NetScaler Gateway CCU 许可证总数。



阈值报告

阈值报告表示在选定期间内，当*实体*选择为“许可证”时，已突破的阈值计数。有关更多信息，请参阅如何创建阈值和警报。

排查 HDX™ Insight 问题

如果 HDX Insight 解决方案未按预期运行，问题可能出在以下某个方面。有关故障排除，请参阅相应部分中的清单。

- HDX Insight 配置。
- NetScaler 与 NetScaler Console 之间的连接。
- 在 NetScaler 中生成 HDX/ICA 流量记录。
- 在 NetScaler Console 中填充记录。

HDX Insight 配置清单

- 确保在 NetScaler 中启用了 AppFlow 功能。有关详细信息，请参阅 启用 AppFlow。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 检查 NetScaler 运行配置中的 HDX Insight 配置。

  运行 `show running | grep -i <appflow_policy>` 命令以检查 HDX Insight 配置。确保绑定类型为 ICA REQUEST。例如；

  `bind vpn vserver afsanity -policy afp -priority 100 -type ICA_REQUEST`

  对于透明模式，绑定类型必须为 ICA_REQ_DEFAULT。例如；

  `bind appflow global afp 100 END -type ICA_REQ_DEFAULT`

- 对于单跳/Access Gateway 或双跳部署，请确保 HDX Insight AppFlow 策略绑定到 HDX/ICA 流量流经的 VPN 虚拟服务器。
- 对于透明模式或 LAN 用户模式，请确保已设置 ICA® 端口 1494 和 2598。
- 检查 `appflowlog` 参数在 NetScaler Gateway 或 VPN 虚拟服务器中是否为 Access Gateway 或双跳部署启用。有关详细信息，请参阅 为虚拟服务器启用 AppFlow。
- 检查“连接链”是否在双跳 NetScaler 中启用。有关详细信息，请参阅 配置 NetScaler Gateway 设备以导出数据。
- HA 故障转移后，如果 HDX Insight 详细信息被跳过解析，请检查 ICA 参数“enableSRonHAFailover”是否已启用。有关详细信息，请参阅 NetScaler 高可用性对上的会话可靠性。

NetScaler 与 NetScaler Console 之间的连接清单

- 检查 NetScaler 中的 AppFlow 收集器状态。有关详细信息，请参阅 如何检查 NetScaler 与 AppFlow 收集器之间的连接状态。
- 检查 HDX Insight AppFlow® 策略命中情况。

  运行命令 `show appflow policy <policy_name>` 以检查 AppFlow 策略命中情况。

  您还可以导航到 GUI 中的**设置 > AppFlow > 策略**以检查 AppFlow 策略命中情况。

- 验证是否有任何防火墙阻止 AppFlow 端口 4739 或 5557。

NetScaler 中 HDX/ICA 流量的记录生成清单

运行命令 `tail -f /var/log/ns.log | grep -i "default ICA Message"` 进行日志验证。根据生成的日志，您可以使用此信息进行故障排除。

- 日志：**跳过解析 ICA 连接 - 此主机不支持 HDX Insight**

  原因：不支持的 Citrix Virtual Apps and Desktops 版本

© 1997–2026 Citrix Systems, Inc. All rights reserved.

解决方法：将 Citrix Virtual Apps and Desktops 服务器升级到支持的版本。

- 日志：**客户端类型 0x53，不支持**

  原因：Citrix Workspace 版本不受支持

  解决方案：将 Citrix Workspace 升级到受支持的版本。有关详细信息，请参阅 Citrix Workspace 应用程序。

- 日志：**来自扩展数据包的错误 - 跳过此流的所有 HDX 处理**

  原因：解压缩 ICA 流量时出现问题

  解决方案：在此 ICA 会话建立新会话之前，没有可用的报告。

- 日志：**无效转换: NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT"**

  原因：解析 ICA 握手时出现问题

  解决方案：在此特定 ICA 会话建立新会话之前，没有可用的报告。

- 日志：**缺少 EUEM ICA RTT**

  原因：无法解析最终用户体验监控通道数据

  解决方案：确保在 Citrix Virtual Apps and Desktops 服务器上启动了最终用户体验监控服务。确保您使用的是受支持的 Citrix Workspace 应用程序版本。

- 日志：**无效通道标头**

  原因：无法识别通道标头

  解决方案：在此特定 ICA 会话建立新会话之前，没有可用的报告。

- 日志：**跳过代码**

  如果您看到跳过代码的以下任何值，则 Insight 详细信息将被跳过解析。

  跳过代码 0 表示记录已成功从 NetScaler 导出。

跳过代码	错误消息	错误原因
100	NS_ICA_ERR_NULL_FRAG	处理 ICA 片段时出错，可能是由于内存条件导致
101	NS_ICA_ERR_INVALID_HS_CMD	收到无效的握手命令

© 1997–2026 Citrix Systems, Inc. All rights reserved.

跳过代码	错误消息	错误原因
102	NS_ICA_ERR_REDUC_PARAM_CNT	为 V3 扩展器初始化指定了无效参数
103	NS_ICA_ERR_REDUC_INIT	无法正确初始化 V3 扩展器
104	NS_ICA_ERR_REDUC_PARAM_BYTES	分配编码器到通道的字节数不足
105	NS_ICA_ERR_INVALID_CHANNEL	ICA 通道号无效
106	NS_ICA_ERR_INVALID_DECODER	为通道指定了无效的解码器
107	NS_ICA_ERR_INVALID_TW_PARAM	在 Thinwire 通道上指定了无效的参数计数
108	NS_ICA_ERR_INVALID_TW_DECODER	用于 Thinwire 通道的无效解码器
109	NS_ICA_ERR_REDUC_NO_DECODER	通道未定义解码器
110	NS_ICA_ERR_REDUC_V3_EXPANDER	展开通道数据失败
111	NS_ICA_ERR_REDUC_BYTES_V3_OOR	扩展器错误：消耗的字节数超过可用字节数
112	NS_ICA_ERR_REDUC_BYTES_OOR	错误：未压缩数据溢出
113	NS_ICA_ERR_REDUC_INVALID_CMD	未定义的扩展器命令
114	NS_ICA_ERR_CGP_FILL_HOLE	处理拆分 CGP 帧时出错
115	NS_ICA_ERR_MEM_NSB_ALLOC	NSB 分配错误 – 由于内存不足

© 1997–2026 Citrix Systems, Inc. All rights reserved.

跳过代码	错误消息	错误原因
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	扩展器上下文的内存分配错误
117	NS_ICA_ERR_ICA_OLD_SERVER	旧服务器，不支持功能块
118	NS_ICA_ERR_PIR_MANY_FRAG	数据包初始化请求已分段，无法处理
119	NS_ICA_ERR_INIT_ICA_CAPS	ICA 功能初始化错误
120	NS_ICA_ERR_NO_MSI_SUPPORT	主机不支持 MSI 功能。表示 XenApp 版本低于 6.5 或 XenDesktop 版本低于 5.0
121	NS_ICA_ERR_CGP_INVALID_CMD	遇到无效的 CGP 命令
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	通道字节不足
123	NS_ICA_ERR_CHANNEL_DATA	EUEM、CONTROL 或 SEAMLESS 通道上的数据不正确
124	NS_ICA_ERR_INVALID_PURE_CMD	处理纯 ICA 通道数据时收到无效命令
125	NS_ICA_ERR_INVALID_PURE_LEN0	处理纯 ICA 通道数据时遇到无效长度
126	NS_ICA_ERR_INVALID_PURE_LEN	处理 PURE ICA 通道数据时遇到无效长度
127	NS_ICA_ERR_INVALID_CLNT_DATA	从客户端收到的数据长度无效
128	NS_ICA_ERR_MSI_GUID_SZ	MSI GUID 大小错误

© 1997–2026 Citrix Systems, Inc. All rights reserved.

跳过代码	错误消息	错误原因
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	检测到无效通道头
130	NS_ICA_ERR_CGP_PARSE_RECONNECT_ID	重新连接会话检索失败
131	NS_ICA_ERR_DISABLE_SR_NON_NS_RECONNECT	禁用 SR 时出错
132	NS_ICA_ERR_REDUC_NOT_V3	不支持的 ICA Reducer 版本
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	压缩已禁用，主机未接受
134	NS_ICA_ERR_IDENT_PROTO	无法识别 ICA 或 CGP 协议，在不正确的工作区中发现
135	NS_ICA_ERR_INVALID_SIGNATURE	ICA 签名或魔术字符串不正确
136	NS_ICA_ERR_PARSE_RAW	解析 ICA 握手数据包时出错
137	NS_ICA_ERR_INCOMPLETE_PKT	握手时收到不完整的数据包
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	ICA 帧过大，超过 1460 字节
139	NS_ICA_ERR_FORWARD	转发 ICA 数据时出错
140	NS_ICA_ERR_MAX_HOLES	无法处理 CGP 命令，因为它拆分超出了支持的限制
141	NS_ICA_ERR_ASSEMBLE_FRAME	无法正确重新组装 ICA 帧
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	已跳过此工作区（客户端）的 ICA 解析，因为它不在允许列表中

© 1997–2026 Citrix Systems, Inc. All rights reserved.

跳过代码	错误消息	错误原因
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	无法检测到客户端重新连接 Cookie 的解析状态
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	客户端重新连接后检测到无效的重新连接 Cookie 长度
145	NS_ICA_ERR_INVALID_RECONNECT_ID	客户端重新连接 Cookie 未满足所需约束
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	从客户端接收到无效的工作区版本字符串
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	从客户端接收到无效的产品 ID
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	扩展后通道长度无效
149	NS_ICA_ERR_SPECIAL_THINWIRE	解压缩错误
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	无缝命令的字节数不足
151	NS_ICA_ERR_EUEM_INSUFFBYTE	EUEM 命令的字节数不足
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	无缝通道解析的事件无效
153	NS_ICA_ERR_CTRL_INVALID_EVENT	用于 CTRL 通道解析的无效事件
154	NS_ICA_ERR_EUEM_INVALID_EVENT	用于 EUEM 通道解析的无效事件
155	NS_ICA_ERR_USB_INVALID_EVENT	用于 USB 通道解析的无效事件
156	NS_ICA_ERR_PURE_INVALID_EVENT	用于纯通道解析的无效事件

© 1997–2026 Citrix Systems, Inc. All rights reserved.

跳过代码	错误消息	错误原因
157	NS_ICA_ERR_VCP_INVALID_EVENT	用于虚拟通道解析的无效事件
158	NS_ICA_ERR_ICAP_INVALID_EVENT	用于 ICA 数据解析的无效事件
159	NS_ICA_ERR_CGPP_INVALID_EVENT	用于 CGP 数据解析的无效事件
160	NS_ICA_ERR_BASICCRYPT_INVALIDSTATE	基本加密中加密命令的无效状态
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	基本加密中的无效加密命令
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	RC5 加密中加密命令的无效状态
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	RC5 加密中的加密命令无效
164	NS_ICA_ERR_ADVCRYPT_ENC	RC5 加密/解密错误
165	NS_ICA_ERR_ADVCRYPT_DEC	RC5 加密/解密错误
166	NS_ICA_ERR_SERVER_NOT_REDUCER_V3	VDA 不支持 Reducer 版本 3
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Workspace 不支持 Reducer 版本 3
168	NS_ICA_ERR_ICAP_INSUFFBYTE	ICA 握手中的字节数异常
169	NS_ICA_ERR_HIGHER_RECONSEQ	重新连接后，对等方发送的 CGP 恢复序列号更高
170	NS_ICA_ERR_DESCSRINFO_ABSENT	重新连接后无法恢复 ICA 解析状态

© 1997–2026 Citrix Systems, Inc. All rights reserved.

跳过代码	错误消息	错误原因
171	NS_ICA_ERR_NSAP_PARSING	解析 Insight 通道数据时出错
172	NS_ICA_ERR_NSAP_APP	从 Insight 通道数据解析应用程序详细信息时出错
173	NS_ICA_ERR_NSAP_ACR	解析 Insight 通道数据中的 ACR 详细信息时出错
174	NS_ICA_ERR_NSAP_SESSION_END	解析 Insight 通道数据中的会话结束详细信息时出错
175	NS_ICA_ERR_NON_NSAP_SN	由于缺少 Insight 通道支持，跳过了服务节点上的 ICA 解析
176	NS_ICA_ERR_NON_NSAP_CLIENT	客户端不支持 NSAP
177	NS_ICA_ERR_NON_NSAP_SERVER	VDA 不支持 NSAP
178	NS_ICA_ERR_NSAP_NEG_FAIL	NSAP 数据协商时出错
179	NS_ICA_ERR_SN_RECONNECT_TKT_FETCH	在服务节点中获取服务重新连接票证时出错
180	NS_ICA_ERR_SN_HIGHER_RECONSEQ	在服务节点中接收到更高的重新连接序列号时出错
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONNSAP	禁用非 NSAP 连接的 HDX Insight 时出错

示例日志：

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49 GMT], Client Type [0x0052], Receiver Version [19.12.0.23],
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
User [user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]"
```

```
Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41 GMT ns-223 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow: Session GUID [4e3a91175ebcbe686baf175eec7e0200], Client IP/Port [10.105.232.40/60059], Server IP/Port [10.106.40.219/2598], MSI Client Cookie [Non-MSI], Session setup time [01/09/2020:22:55:39 GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [10.106.40.219], Ctx Flags [0x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

错误计数器

ICA 解析会捕获各种计数器。下表列出了 ICA 解析的各种计数器。 运行命令 `nsconmsg -g hdx -d statswt0` 以查看计数器详细信息。

HDX 计数器名称	用途	类别（统计/错误/诊断）
hdx_tot_ica_conn	指示 NS 检测到的纯 ICA 连接总数。每当检测到基于客户端 PCB 上的 ICA 签名的 ICA 连接时，此计数器会递增。	统计
hdx_tot_cgp_conn	指示 NS 检测到的 CGP 连接总数（会话可靠性开启）。每当检测到基于客户端 PCB 上的 CGP 签名的 CGP 连接时，此计数器会递增。	统计
hdx_dbg_tot_udt_conn	指示 NS 检测到的 UDP ICA 连接总数	统计
hdx_dbg_tot_nsap_conn	指示 NS 检测到的 NSAP 支持的连接总数	统计信息
hdx_tot_skip_conn	指示解析器因无效的 ICA 或 CGP 签名而跳过了多少 ICA 连接。	统计信息
hdx_dbg_active_conn	该时刻的总活动 EDT/CGP/ICA 连接数。	统计信息

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX 计数器名称	用途	类别（统计/错误/诊断）
hdx_dbg_active_nsap_conn	该时刻的总活动 EDT/CGP/ICA NSAP 连接数。	统计信息
hdx_dbg_skip_appflow_disabled	由于禁用 AppFlow 而导致 AppFlow 从会话中分离的总实例数	统计信息/诊断
hdx_dbg_transparent_user	透明用户访问总数	统计/诊断
hdx_dbg_ag_user	Access Gateway 用户访问总数	统计/诊断
hdx_dbg_lan_user	LAN 用户模式访问总数	统计/诊断
hdx_basic_enc	指示使用基本加密的 ICA 连接数	统计/诊断
hdx_advanced_enc	指示使用基于高级 RC5 加密的 ICA 连接数	统计/诊断
hdx_dbg_reconnected_session	客户端在没有任何 NetScaler 错误的情况下重新连接请求的总数	统计/诊断
hdx_dbg_host_rejected_ns_reconnect	客户端拒绝重新连接请求的主机总数	统计/诊断
hdx_euem_available	指示具有可用最终用户体验监控通道的连接数。最终用户体验监控通道是收集诸如 ICA RTT 等统计信息所必需的。	统计/诊断
hdx_err_disabled_sr	会话可靠性已使用 `nsapimgr` 旋钮禁用。此会话无法正常工作。	错误
hdx_err_skip_no_msi	XA/XD 服务器缺少 MSI 功能。这表示服务器版本较旧，HDX Insight 将跳过此连接。	错误
hdx_err_skip_old_server	旧的不受支持的服务器版本	错误

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX 计数器名称	用途	类别（统计/错误/诊断）
hdx_err_clnt_not_whitelist	客户端工作区不在允许列表中，HDX Insight 跳过此连接	错误
hdx_sm_ica_cam_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CAM_CHANNEL 总数	诊断
hdx_sm_ica_usb_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_USB_CHANNEL 总数	诊断
hdx_sm_ica_clip_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CLIP_CHANNEL 总数	诊断
hdx_sm_ica_ccm_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CCM_CHANNEL 总数	诊断
hdx_sm_ica_cdm_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CDM_CHANNEL 总数	诊断
hdx_sm_ica_com1_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_COM1_CHANNEL 总数	诊断
hdx_sm_ica_com2_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_COM2_CHANNEL 总数	诊断
hdx_sm_ica_cpm_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CPM_CHANNEL 总数	诊断
hdx_sm_ica_lpt1_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_LPT1_CHANNEL 总数	诊断

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX 计数器名称	用途	类别（统计/错误/诊断）
hdx_sm_ica_lpt2_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_LPT2_CHANNEL 总数	诊断
dx_dbg_sm_ica_msi_disabled	通过 SmartAccess 策略禁用 MSI 的情况总数	诊断
hdx_sm_ica_file_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_FILE_CHANNEL 总数	诊断
hdx_dbg_usb_accept_device	接受的 USB 设备总数	诊断
hdx_dbg_usb_reject_device	拒绝的 USB 设备总数	诊断
hdx_dbg_usb_reset_endpoint	USB 端点重置总数	诊断
hdx_dbg_usb_reset_device	USB 设备重置总数	诊断
hdx_dbg_usb_stop_device	USB 设备停止总数	诊断
hdx_dbg_usb_stop_device_response	已停止 USB 设备的响应总数	诊断
hdx_dbg_usb_device_gone	USB 设备丢失总数	诊断
hdx_dbg_usb_device_stopped	已停止的 USB 设备总数	诊断

nstrace 验证

检查 CFLOW 协议以查看所有从 NetScaler 发出的 AppFlow 记录。

NetScaler Console 清单中的记录填充

- 运行命令 `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` 并检查日志以确认 NetScaler Console 正在接收 AppFlow 记录。
- 确认 NetScaler 实例已添加到 NetScaler Console。
- 验证 NetScaler Gateway/VPN 虚拟服务器是否已在 NetScaler Console 中获得许可。
- 确保为双跳启用了多跳参数设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 确保在双跳部署中，NetScaler Gateway 已为第二跳清除。

联系 Citrix 技术支持之前

为了快速解决问题，请在联系 Citrix 技术支持之前确保您拥有以下信息：

- 部署和网络拓扑的详细信息。
- NetScaler 和 NetScaler Console 版本。
- Citrix Virtual Apps and Desktops 服务器版本。
- 客户端 Workspace 版本。
- 问题发生时活动 ICA 会话的数量。
- 通过在 NetScaler 命令提示符下运行 `show techsupport` 命令捕获的技术支持包。
- 为 NetScaler Console 捕获的技术支持包。
- 在所有 NetScaler 上捕获的数据包跟踪。 要启动数据包跟踪，请键入 `start nstrace -size 0'` 要停止数据包跟踪，请键入 `stop nstrace`
- 通过运行 `show arp` 命令收集系统 ARP 表中的条目。

已知问题

有关 HDX Insight 的已知问题，请参阅 NetScaler 发行说明。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

基础架构

NetScaler Console 提供基础架构管理和分析功能，用于发现、监控和管理您的 NetScaler 实例。以下主题可帮助您管理 NetScaler 基础架构：

- 基础架构分析
- 实例管理
- SSL 证书管理
- 事件
- 网络功能
- 网络报告
- 配置
- 安全建议
- 升级建议
- 编排

基础架构分析

网络管理员的一个主要目标是监控 NetScaler 实例。NetScaler 实例提供了通过它访问的应用程序和桌面的使用情况和性能的有趣见解。管理员必须监控 NetScaler 实例并分析每个 NetScaler 实例处理的应用程序流。他们能够修复配置、设置、连接、证书以及其他可能影响应用程序使用或性能的任何可能问题。例如，应用程序流量模式的突然变化可能是由于 SSL 配置更改（例如禁用 SSL 协议）造成的。管理员必须能够快速识别这些数据点之间的关联，以确保以下各项：

- 应用程序可用性处于最佳状态
- 不存在资源消耗、硬件、容量或配置更改问题
- 不存在未使用的库存
- 不存在过期证书

基础架构分析功能通过关联多个数据源并将其量化为可衡量分数（定义实例的运行状况）来简化数据分析过程。借助此功能，管理员可以获得一个单一接触点，以了解是否存在问题、问题的根源以及他们可以执行的可能补救措施。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

基础架构分析

NetScaler Console 基础架构分析功能整理从 NetScaler 实例收集的所有数据，并将其量化为定义实例运行状况的**实例分数**。实例分数以表格视图或圆形打包可视化形式进行汇总。基础架构分析功能可帮助您可视化导致或可能导致实例出现问题的因素。此可视化还有助于您确定为防止问题及其再次发生而必须执行的操作。

实例分数

实例分数表示 NetScaler 实例的运行状况。分数为 100 表示实例完全健康，没有任何问题。实例分数捕获实例上不同级别的潜在问题。它是实例运行状况的可量化度量，多个“运行状况指标”有助于该分数。

运行状况指标是实例分数的构建块，其中，分数会根据该时间窗口中检测到的所有指标，在预定义的“监控周期”内定期计算。目前，基础架构分析每小时根据从实例收集的数据计算一次实例分数。 指标可以定义为实例上属于以下类别之一的任何活动（事件或问题）。

- 系统资源指标
- 关键事件指标
- SSL 配置指标
- 配置偏差指示器

运行状况指示器

- 系统资源指示器

  以下是 NetScaler 实例上可能发生并由 NetScaler Console 监控的关键系统资源问题。

  - **CPU 使用率高**。NetScaler 实例中的 CPU 使用率已超过较高阈值。
  - **内存使用率高**。NetScaler 实例中的内存使用率已超过较高阈值。
  - **磁盘使用率高**。NetScaler 实例中的磁盘使用率已超过较高阈值。
  - **磁盘错误**。安装 NetScaler 实例的虚拟机管理程序上的硬盘 0 或硬盘 1 存在错误。
  - **电源故障**。电源已失效或与 NetScaler 实例断开连接。
  - **SSL 卡故障**。实例上安装的 SSL 卡已失效。
  - **闪存错误**。NetScaler 实例上出现 Compact Flash 错误。
  - **NIC 丢弃**。NetScaler 实例中 NIC 卡丢弃的数据包已超过较高阈值。

有关这些系统资源错误的更多信息，请参阅实例仪表板。

- 关键事件指示器

© 1997–2026 Citrix Systems, Inc. All rights reserved.

以下关键事件由 NetScaler Console 事件管理功能下配置为严重级别的事件识别。

- **HA 同步失败**。高可用性模式下 NetScaler 实例之间的配置同步在辅助服务器上失败。
- **HA 无心跳**。高可用性模式下 NetScaler 实例对中的主服务器未从辅助服务器接收到心跳。
- **HA 辅助状态异常**。高可用性模式下 NetScaler 实例对中的辅助服务器处于“关闭”、“未知”或“保持辅助”状态。
- **HA 版本不匹配**。高可用性模式下 NetScaler 实例对上安装的 NetScaler 软件映像版本不匹配。
- **群集同步失败**。群集模式下 NetScaler 实例之间的配置同步失败。
- **群集版本不匹配**。群集模式下 NetScaler 实例上安装的 NetScaler 软件映像版本不匹配。
- **群集传播失败**。配置传播到群集中所有实例失败。

> **注意**
>
> 您可以通过更改事件的严重级别来获取关键 SNMP 事件列表。有关如何更改严重级别的更多信息，请参阅修改 NetScaler 实例上发生的事件的报告严重级别。

有关 NetScaler Console 中事件的更多信息，请参阅事件。

- SSL 配置指示器
  - **不推荐的密钥强度**。SSL 证书的密钥强度不符合 NetScaler® 标准
  - **不推荐的颁发者**。Citrix 不推荐此 SSL 证书的颁发者。
  - **SSL 证书已过期**。NetScaler 实例中安装的 SSL 证书已过期。
  - **SSL 证书即将过期**。NetScaler 实例中安装的 SSL 证书将在未来一周内过期。
  - **不推荐的算法**。NetScaler 实例中安装的 SSL 证书的签名算法不符合 NetScaler 标准。

有关 SSL 证书的更多信息，请参阅 SSL 仪表板。

- 配置偏差指示器
  - **配置漂移模板**。配置与您创建的审计模板存在漂移（未保存的更改），这些模板包含您希望在某些实例上审计的特定配置。
  - **配置漂移默认值**。配置与默认配置文件存在漂移（未保存的更改）。

有关配置偏差以及如何运行审计报告以检查配置偏差的更多信息，请参阅 查看审计报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

查看 NetScaler 容量问题

当 NetScaler 实例消耗了大部分可用容量时，在处理客户端流量时可能会发生丢包。此问题会导致 NetScaler 实例的性能低下。通过了解此类 NetScaler 容量问题，您可以主动分配额外的许可证以稳定 NetScaler 性能。

要查看 NetScaler 容量问题，

1. 导航到 **基础架构 > 基础架构分析**。
2. 展开要查看容量问题的实例。

NetScaler Console 每五分钟从 NetScaler 实例轮询这些事件，并显示是否存在丢包或速率限制计数器增量。这些问题根据以下容量参数进行分类：

- **达到吞吐量限制** – 达到吞吐量限制后，实例中丢弃的数据包数量。
- **达到 PE CPU 限制** - 达到 PE CPU 限制后，所有 NIC 上丢弃的数据包数量。
- **达到 PPS 限制** – 达到 PPS 限制后，实例中丢弃的数据包数量。
- **SSL 吞吐量速率限制** – SSL 吞吐量达到限制的次数。
- **SSL TPS 速率限制** – SSL TPS 达到限制的次数。

NetScaler Console 根据定义的容量阈值计算实例分数。

- 低阈值 – 1 个数据包丢弃或速率限制计数器递增
- 高阈值 – 10000 个数据包丢弃或速率限制计数器递增

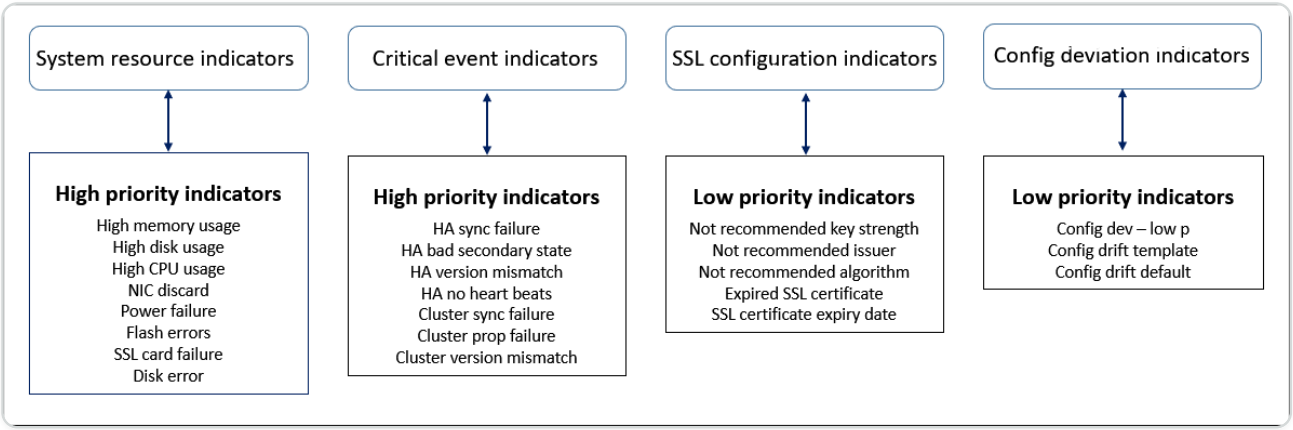
因此，当 NetScaler 实例超出容量阈值时，实例分数会受到影响。

当数据包丢弃或速率限制计数器递增时，会在 `NetScalerCapacityBreach` 类别下生成一个事件。要查看这些事件，请导航到**帐户 > 系统事件**。

运行状况指示器值

指示器根据其值分为高优先级指示器和低优先级指示器，如下所示：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



同一组指示器中的运行状况指示器具有不同的权重。一个指示器对降低实例分数的影响可能比另一个指示器更大。例如，高内存使用率对实例分数的影响比高磁盘使用率、高 CPU 使用率和 NIC 丢弃更大。如果实例上检测到的指示器数量越多，则实例分数越低。

指示器的值根据以下规则计算。指示器通过以下三种方式之一进行检测：

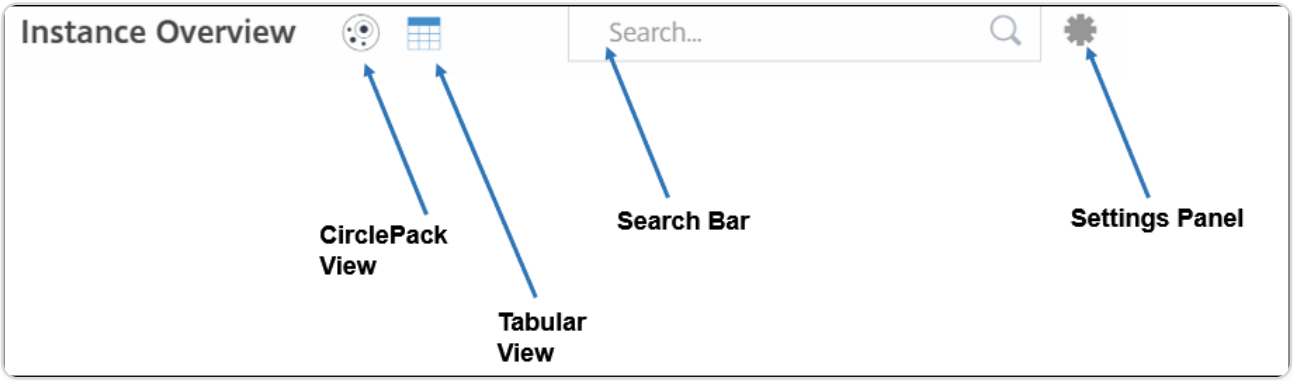
1. **基于活动**。例如，当实例发生电源故障时，会触发系统资源指示器，此指示器会降低实例分数。当指示器清除时，惩罚也会清除，实例分数会增加。
2. **基于阈值违规**。例如，当网卡丢弃数据包且超出阈值级别时，会触发系统资源指示器。
3. **基于低阈值和高阈值违规**。在此，指示器可以通过两种方式触发：
   - 当指标值介于低阈值和高阈值之间时，将对实例分数施加部分惩罚。
   - 当值超过高阈值时，将对实例分数施加全部惩罚。
   - 如果值低于低阈值，则不对实例分数施加任何惩罚。

例如，CPU 使用率是一个系统资源指标，当使用率值超过低阈值和高阈值时都会触发。

基础架构分析仪表板

导航到 **基础架构 > 基础架构分析**。

基础架构分析可以以**圆形打包**格式或**表格**格式查看。您可以在这两种格式之间切换。



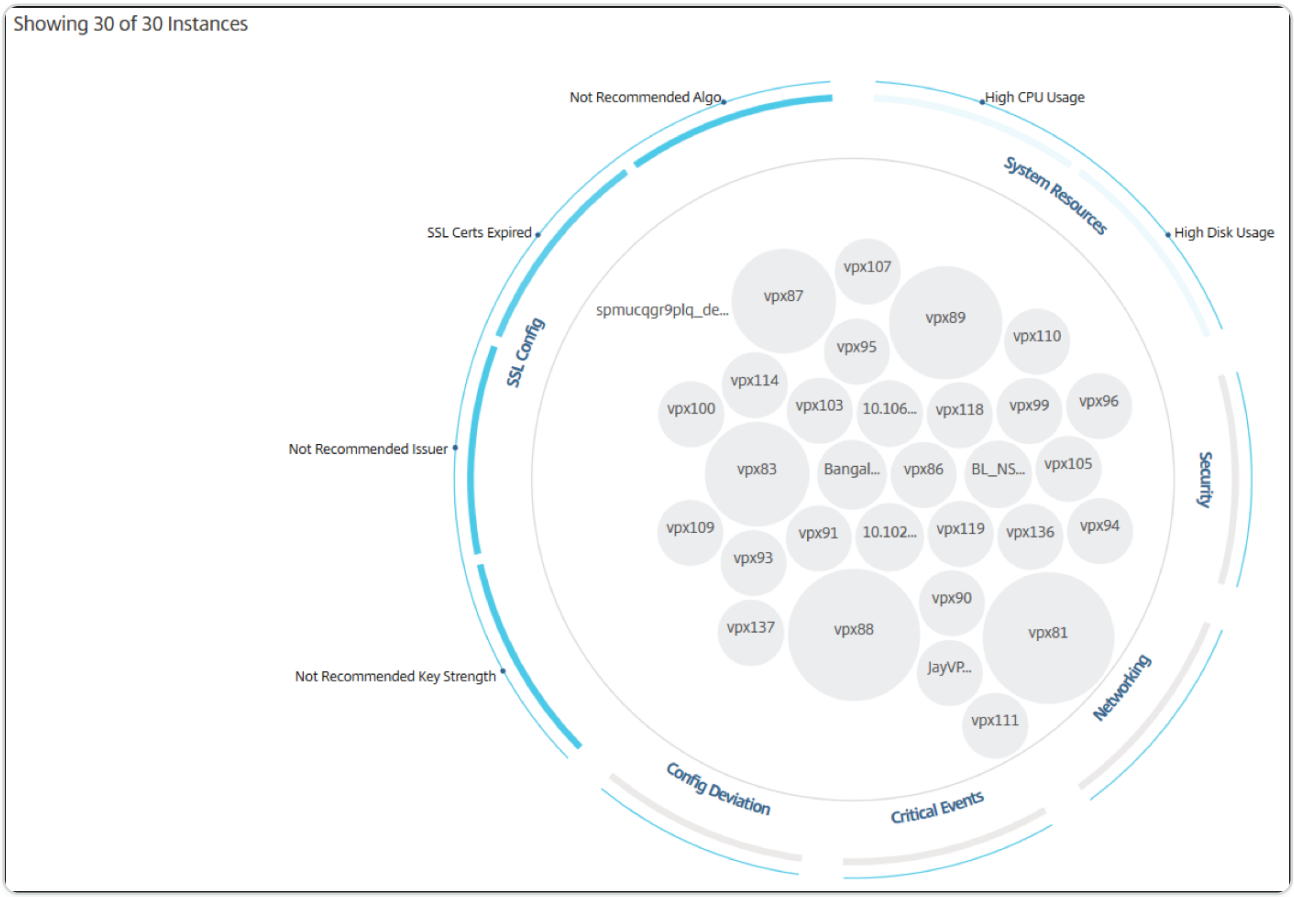
- 在表格视图中，您可以通过在搜索栏中键入主机名或 IP 地址来搜索实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 默认情况下，“基础架构分析”页面在页面右侧显示“摘要”面板。
- 单击**设置**图标以显示**设置**面板。
- 在两种视图格式中，“摘要”面板都显示网络中所有实例的详细信息。

圆形打包视图

圆形打包图将实例组显示为紧密组织的圆形。它们通常显示层次结构，其中较小的实例组要么与同一类别中的其他组颜色相似，要么嵌套在较大的组中。圆形打包表示分层数据集，并显示层次结构中的不同级别以及它们如何相互作用。



实例圆圈

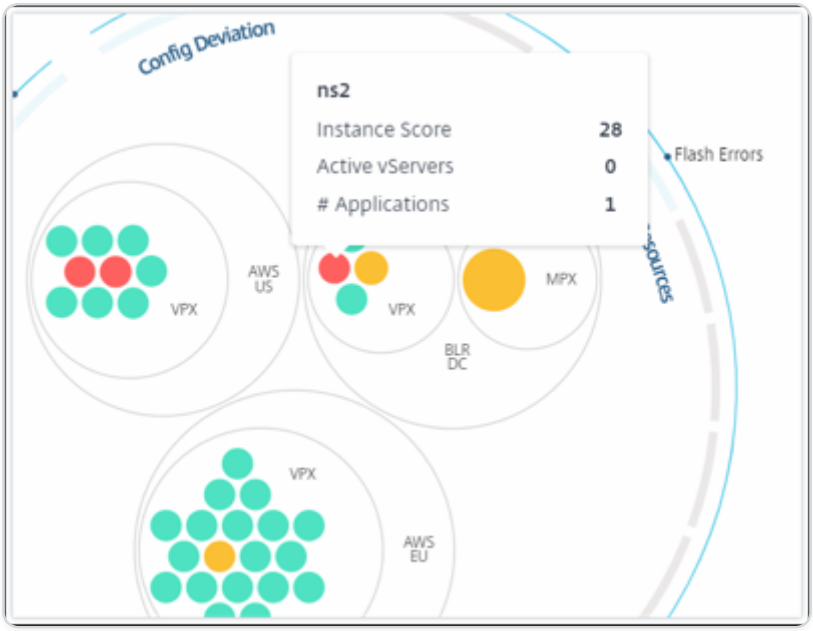
颜色。在圆圈包中，每个实例都表示为一个彩色圆圈。圆圈的颜色表示该实例的健康状况。

- **绿色** - 实例分数在 100 到 80 之间。实例健康。
- **黄色** - 实例分数在 80 到 50 之间；已发现一些问题，需要审查。
- **红色** - 实例分数低于 50。该实例处于危急阶段，因为在该实例上发现了多个问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

大小。这些彩色圆圈的大小表示在该实例上配置的虚拟服务器数量。更大的圆圈表示虚拟服务器数量更多。

您可以将鼠标指针悬停在每个实例圆圈（彩色圆圈）上以查看摘要。悬停工具提示会显示实例的主机名、活动虚拟服务器的数量以及在该实例上配置的应用程序数量。



分组实例圆圈

最初的圆圈包包含根据以下标准分组、嵌套或封装在另一个圆圈内的实例圆圈：

- 它们部署的站点
- 部署的实例类型 - VPX、MPX、SDX 和 CPX
- NetScaler 实例的虚拟或物理模型
- 实例上安装的 NetScaler 映像版本

© 1997–2026 Citrix Systems, Inc. All rights reserved.

下图显示了一个圆形打包图，其中实例首先按部署它们的站点或数据中心进行分组，然后根据它们的类型、VPX 和 MPX 进一步分组。

分组的圆圈(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-5.png)

所有这些嵌套的圆圈都由两个最外层的圆圈包围。这两个外层圆圈代表 NetScaler Console 监控的四类事件（系统资源、关键事件、SSL 配置和配置偏差）以及相关的健康指标。

集群实例圆圈

NetScaler Console 监控许多实例。为了简化这些实例的监控和维护，基础设施分析允许您在两个级别上对它们进行集群。也就是说，实例分组可以嵌套在另一个分组中。

例如，BLR 数据中心部署了两种类型的 NetScaler 实例——VPX 和 MPX。您可以首先按类型对 NetScaler 实例进行分组，然后按它们所属的站点对所有实例进行分组。现在您可以轻松识别您管理的站点中部署了多少种类型的实例。

集群(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-6.png)

选择圆形打包图(/en-us/netscaler-application-delivery-management-software/media/circle-pack-select.png)

以下是双层集群的几个示例：

站点和型号：

站点(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-7.png)

类型和版本：

型号(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-8.png)

站点和版本：

版本(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-9.png)

如何使用环形图包

单击每个彩色圆圈以突出显示该实例。

环形图包使用方法(/en-us/netscaler-application-delivery-management-software/media/circle-pack-how-to.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

根据该实例中发生的事件，只有那些健康指标会在外圈突出显示。例如，以下两张环形图包的图像显示了不同的风险指标集，尽管两个实例都处于关键状态。

环形图包(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-10.png)

您还可以单击健康指标，以获取有关报告该风险指标的实例数量的更多详细信息。例如，单击 `Not recommended Algo` 可查看该风险指标的摘要报告。

环形图包(/en-us/netscaler-application-delivery-management-software/media/infra-analytics-11.png)

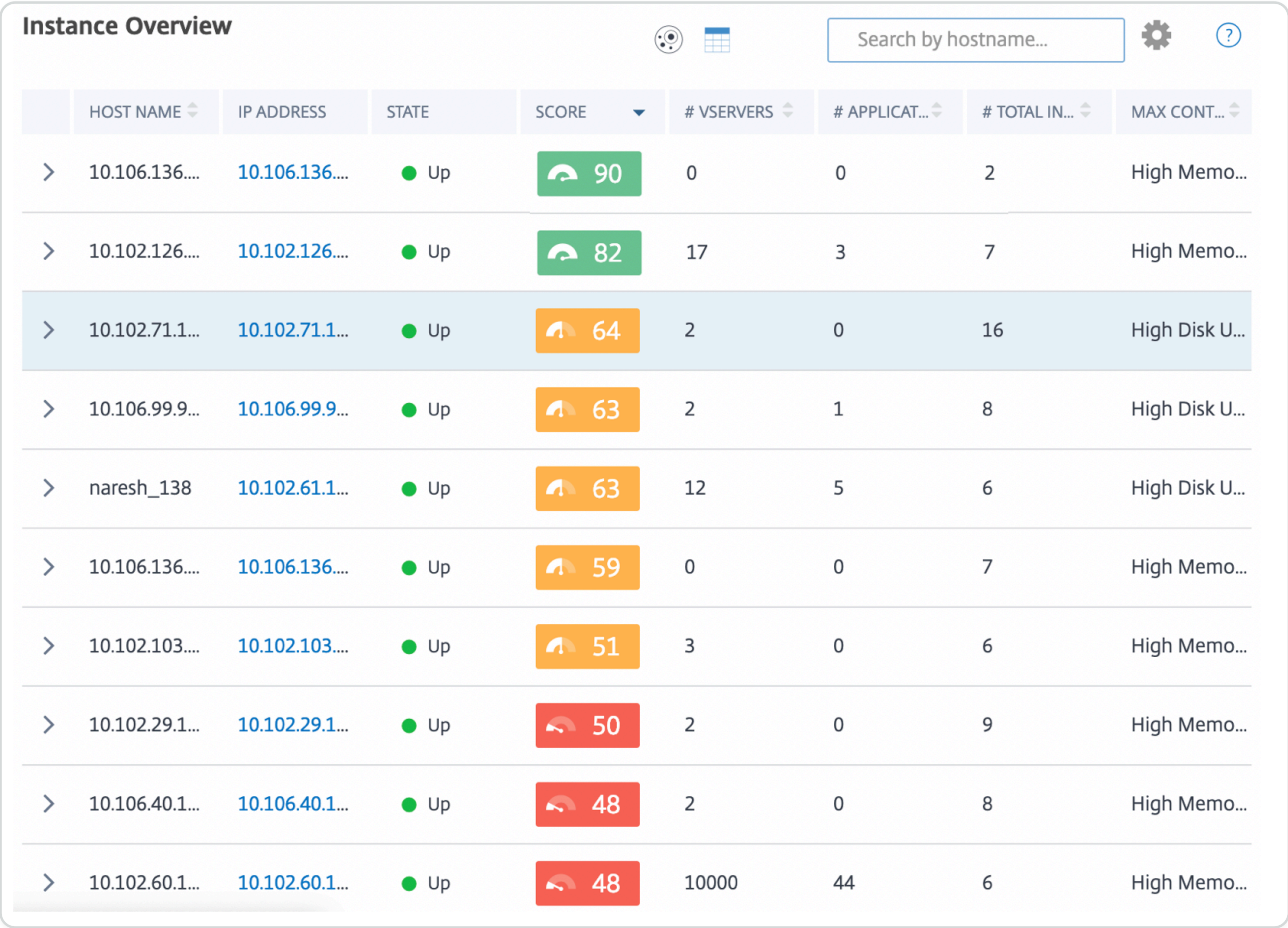
表格视图

表格视图以表格形式显示实例及其详细信息。显示的详细信息如下：

- 实例的主机名
- 实例的 IP 地址
- 实例的状态
- 实例分数
- 在该实例上配置的虚拟服务器数量
- 在该实例上配置的应用程序数量
- 风险指标总数
- 对实例分数降低贡献更大的事件

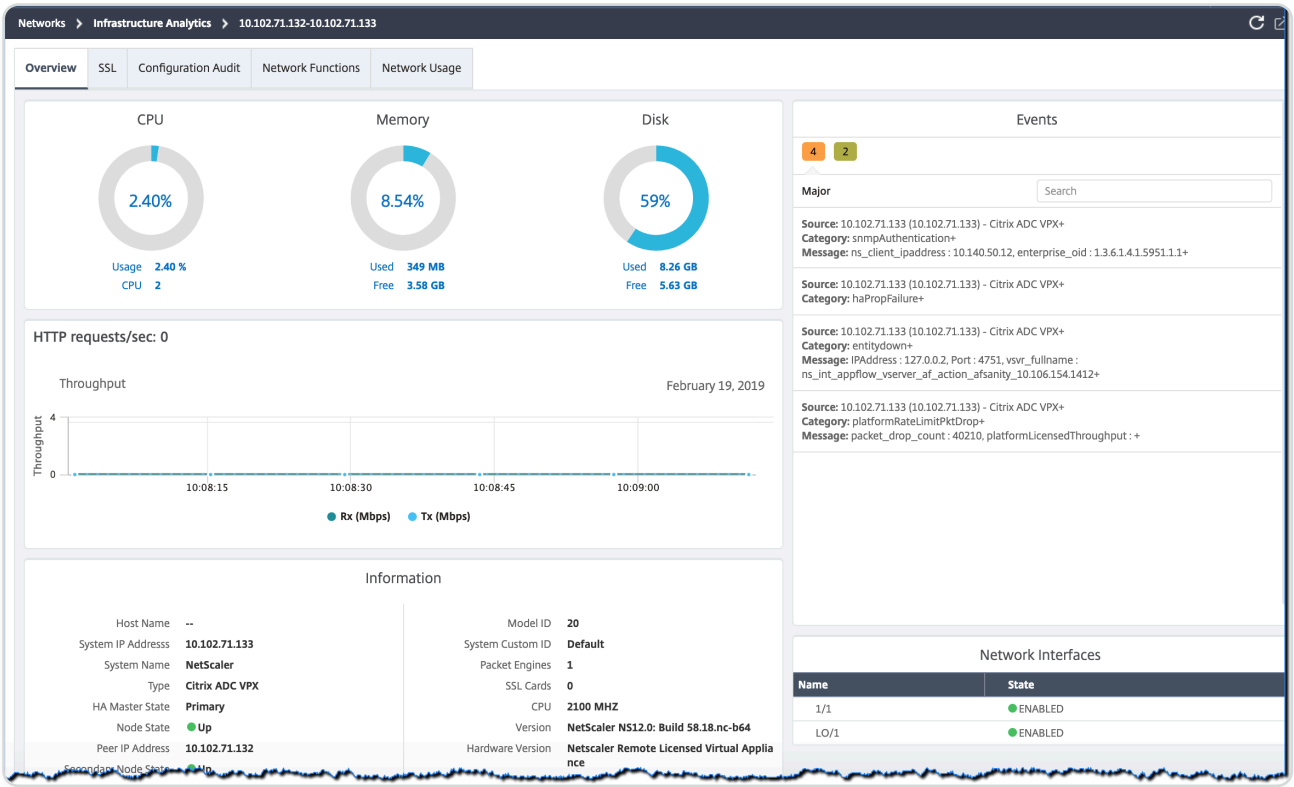
处于危急状态的实例位于表格顶部，其次是需要审查的实例，然后是更健康的实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

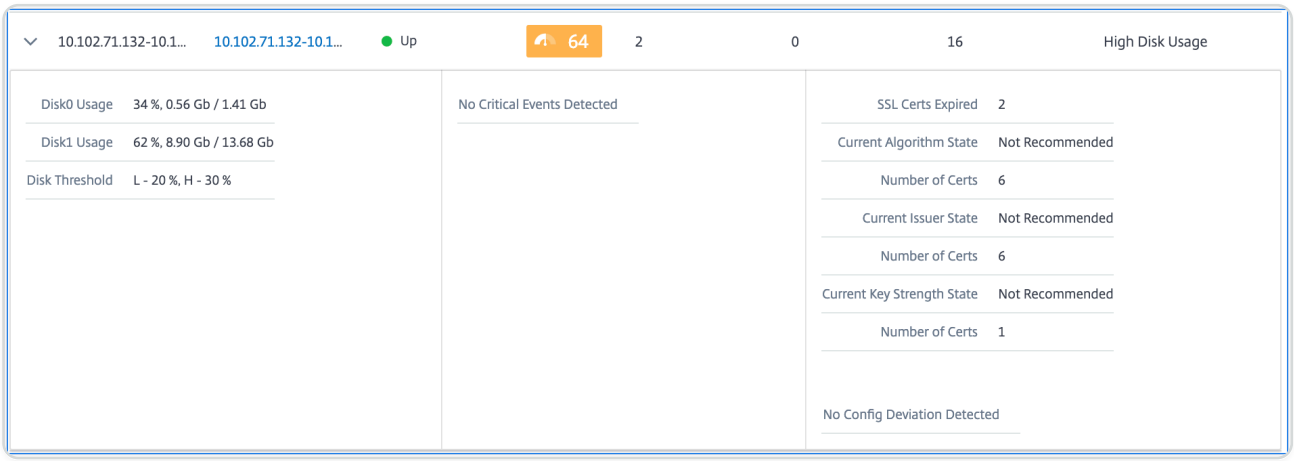


在表格视图中单击实例 IP 地址，以仪表板显示形式查看该实例的更多详细信息。实例仪表板提供了实例的概览，您可以在其中查看实例的 CPU、内存和磁盘使用情况。您还可以查看与 SSL 证书管理、配置审计、网络功能以及显示实例详细网络使用情况的网络报告相关的详细信息。继续向下滚动可查看此实例上启用的功能和模式列表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您还可以单击每行开头的箭头以展开该行，查看更多详细信息。



展开的表格行显示了实例在所有类别中发生的错误。在上面的示例中，您可以看到系统资源、SSL 配置和配置文件偏差方面存在错误。但实例未报告任何严重事件。

如何使用摘要面板

摘要面板可帮助您高效快速地关注需要审查或处于危急状态的实例。该面板分为三个选项卡：概览、实例信息和流量配置文件。您在此面板中所做的更改会修改圆形打包和表格视图格式的显示。以下部分将更详细地描述这些选项卡。以下部分中的示例可帮助您有效地使用不同的选择标准来分析实例报告的问题。

概览：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

概览选项卡允许您根据实例中可能出现的硬件错误、使用情况、过期证书和类似指标来监控实例。您可以在此处监控的指标如下：

- CPU 使用率
- 内存使用率
- 磁盘使用情况
- 系统故障
- 严重事件
- SSL 证书过期

以下示例说明了如何与“**概览**”面板交互，以隔离报告错误的实例。

示例 1：查看处于审核状态的实例：

选中“**审核**”复选框，仅查看未报告严重错误但仍需要关注的实例。

“**概览**”面板中的直方图表示基于高 CPU 使用率、高内存使用率和高磁盘使用率事件的聚合实例数。直方图按 10%、20%、30%、40%、50%、60%、70%、80%、90% 和 100% 分级。将鼠标指针悬停在其中一个条形图上。图表底部的图例显示了使用范围和该范围内的实例数。您还可以单击条形图以显示该范围内的所有实例。

示例 2：查看占用分配内存 10% 到 20% 的实例：

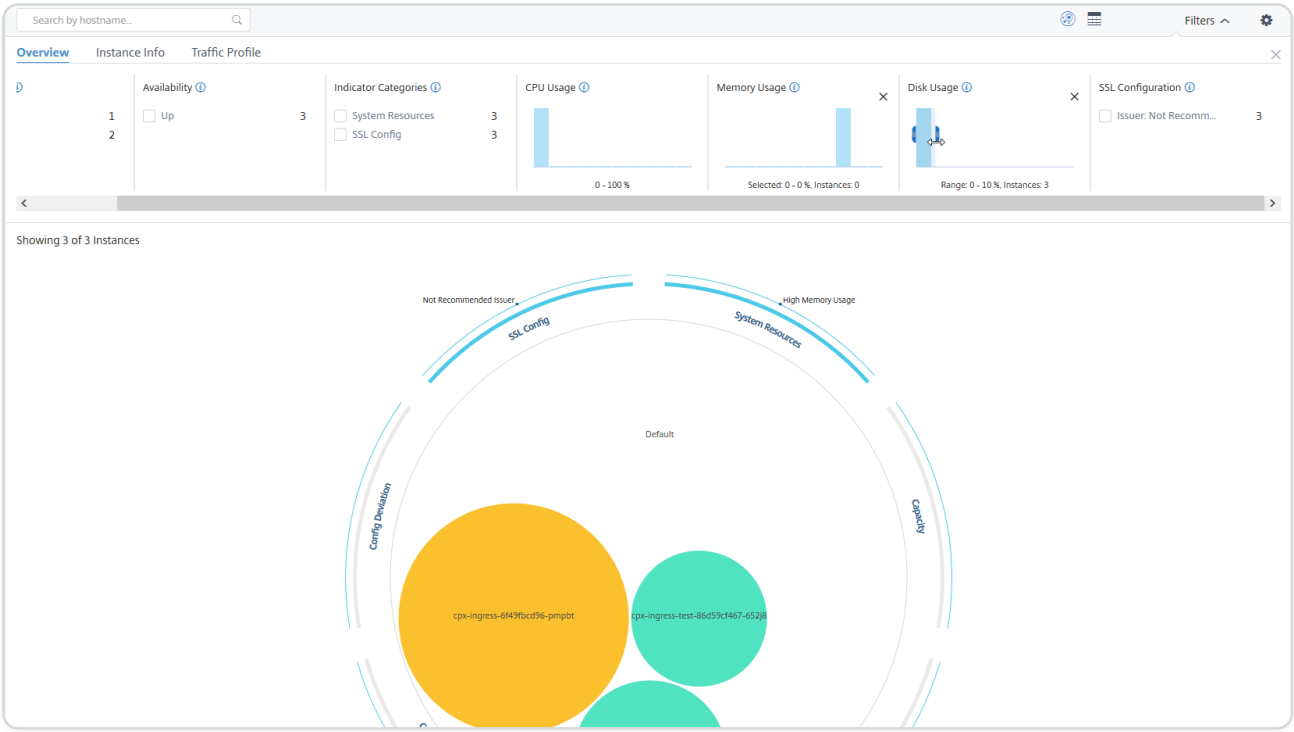
在内存使用情况部分，单击条形图。图例显示所选范围为 10–20%，并且有 29 个实例在该范围内运行。

您还可以在这些直方图中选择多个范围。

示例 3：查看在多个范围内占用高磁盘空间的实例：

要查看已占用 0% 到 10% 之间磁盘空间的实例，请将鼠标指针拖动到这两个范围上。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意

单击“X”以移除选择。您也可以单击**重置**以移除多个选择。

概览面板中的水平条形图指示报告系统错误、关键事件以及 SSL 证书过期状态的实例数量。选中复选框以查看这些实例。

示例 4：查看过期 SSL 证书的实例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1 - 单击**筛选器**列表。

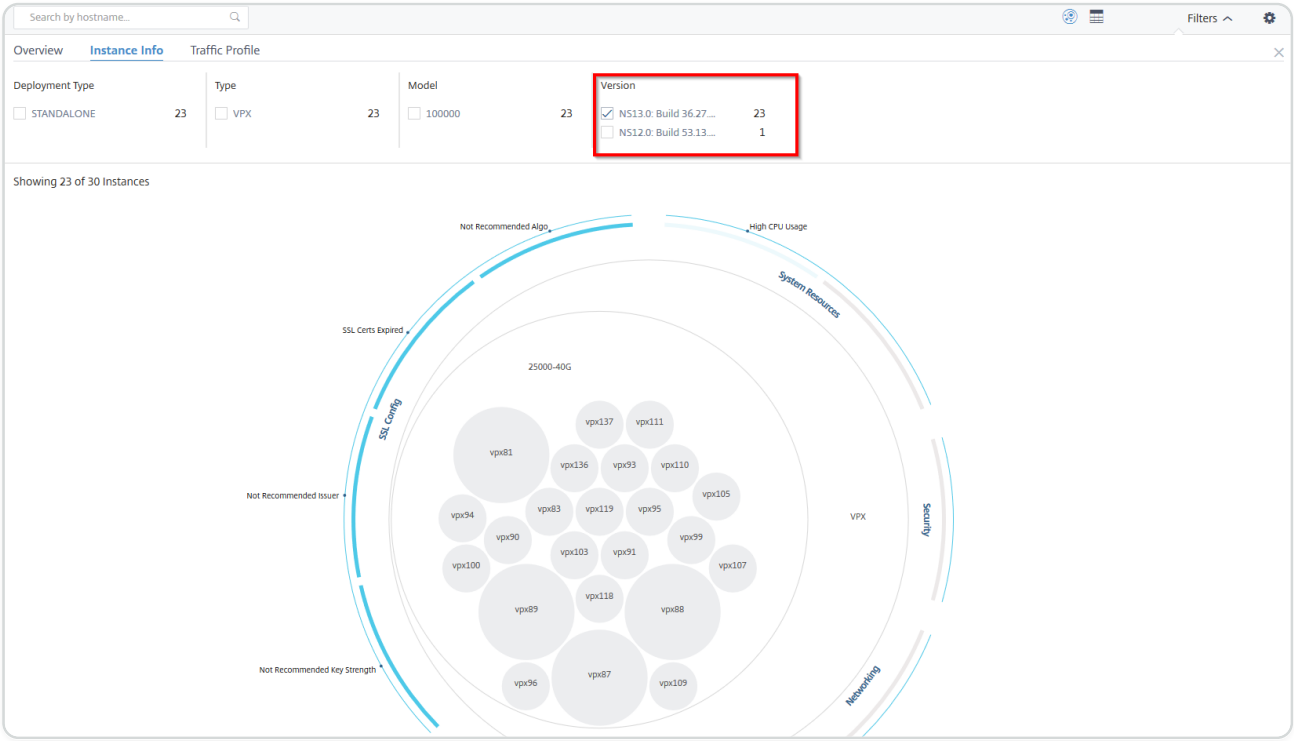
2 - 在 **SSL 证书过期**部分中，选中**已过期**复选框以查看实例。

实例信息

实例信息面板允许您根据部署类型、实例类型、型号和软件版本查看实例。您可以选择多个复选框以缩小选择范围。

示例 5：查看具有特定内部版本号的 NetScaler VPX 实例：

选择您要查看的版本。



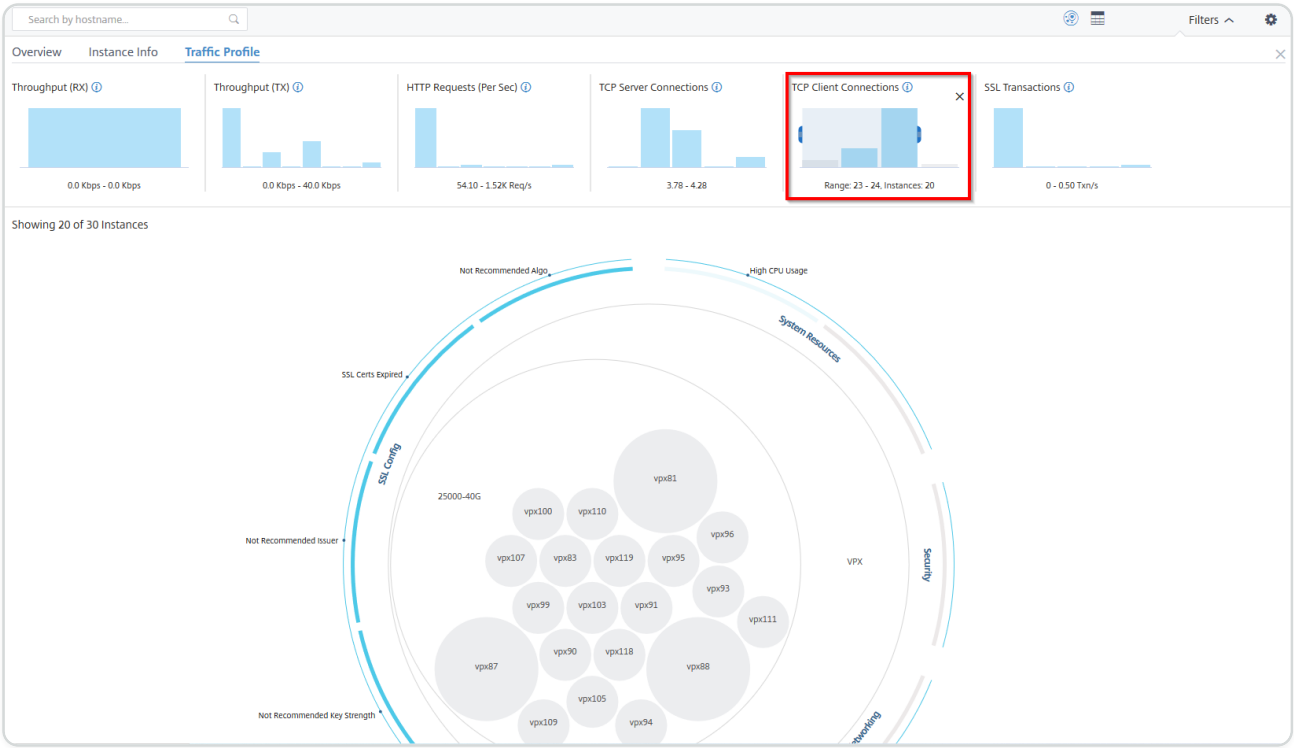
流量配置文件

流量配置文件面板中的直方图表示基于实例上的许可吞吐量、请求数、连接数以及实例处理的事务数的聚合实例数量。选择条形图以查看该范围内的实例。

示例 6：查看支持 TCP 连接的实例：

下图显示了支持 TCP 连接的实例数量。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



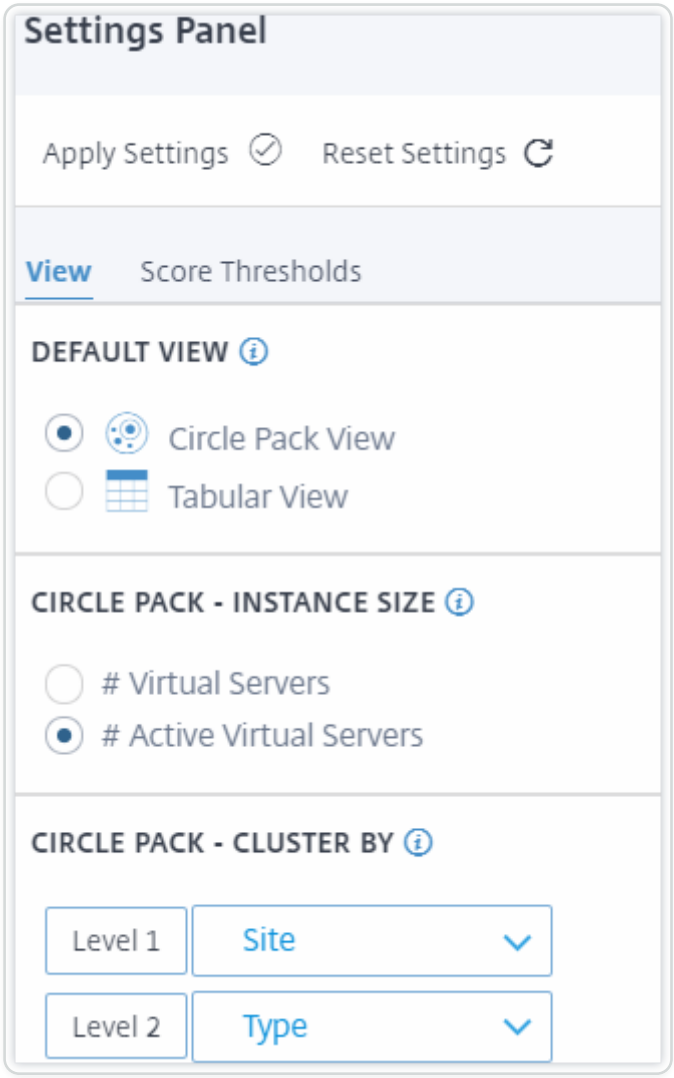
如何使用设置面板

设置面板允许您设置基础架构分析的默认视图。它还允许您设置高 CPU 使用率、高磁盘使用率和高内存使用率的低阈值和高阈值。设置面板分为两个选项卡 - 视图和分数阈值。

视图

- **默认视图**。选择**圆圈包**或表格格式作为分析页面上的默认视图。您选择的格式是您在 NetScaler Console 中访问页面时看到的格式。
- **圆圈包 - 实例大小**。允许实例圆圈的大小由虚拟服务器数量或活动虚拟服务器数量决定。
- **圆圈包 - 聚类依据**。决定实例圆圈的两级聚类。有关实例聚类的更多信息，请参阅聚类实例圆圈。

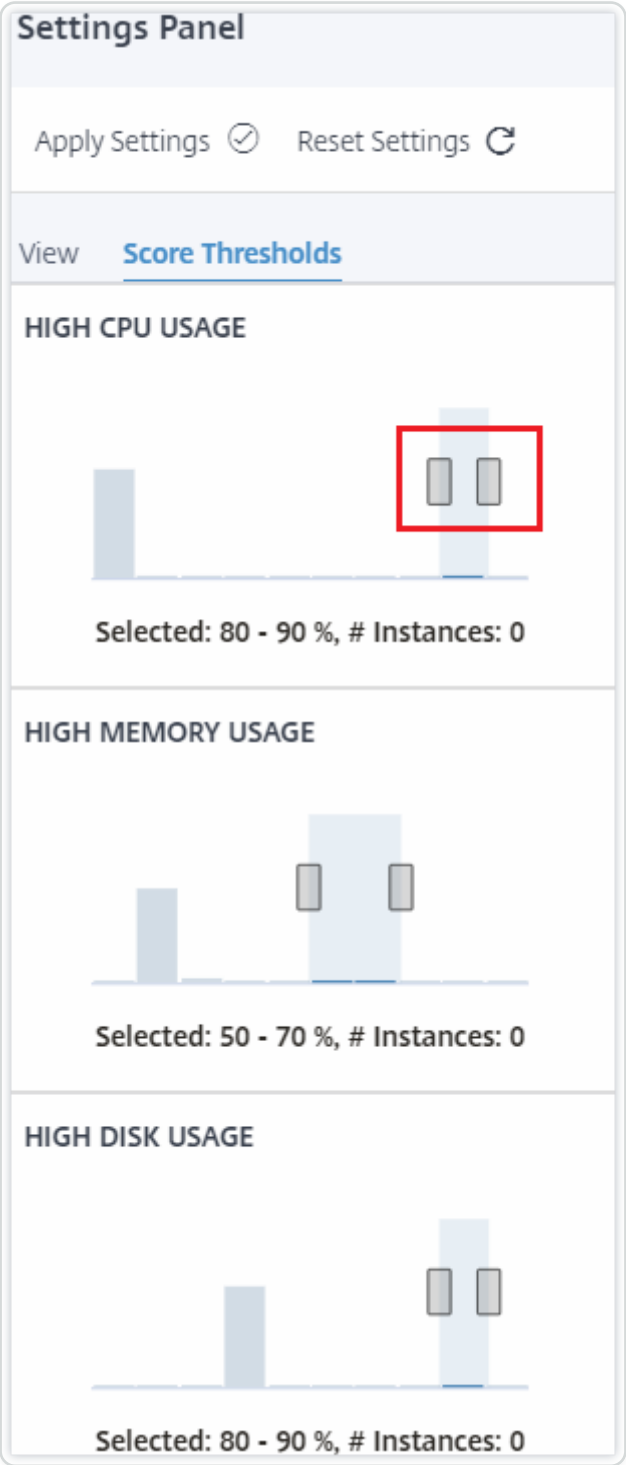
© 1997–2026 Citrix Systems, Inc. All rights reserved.



分数阈值

您可以根据组织中的流量要求修改高 CPU、内存和磁盘使用率的低阈值和高阈值。拖动每个选择直方图中的手柄以设置值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意

单击**应用设置**以应用这些更改，或单击**重置**以删除所有更改。

如何在仪表板上可视化数据

使用基础架构分析，网络管理员现在可以在几秒钟内识别出需要最多关注的实例。为了更详细地了解数据可视化，让我们考虑一下 ExampleCompany 的网络管理员 Chris 的案例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Chris 在组织中维护许多 NetScaler 实例。其中一些实例处理高流量，Chris 需要密切监控它们。Chris 注意到，一些高流量实例不再处理通过它们的全部流量。为了分析这种下降，Chris 之前不得不阅读来自各种来源的多个数据报告。Chris 不得不花费更多时间手动关联数据，并确定哪些实例未处于最佳状态且需要关注。

Chris 使用基础设施分析功能以可视化方式查看所有实例的运行状况。

以下两个示例说明了基础设施分析如何协助 Chris 进行维护活动：

示例 1 - 监控 SSL 流量：

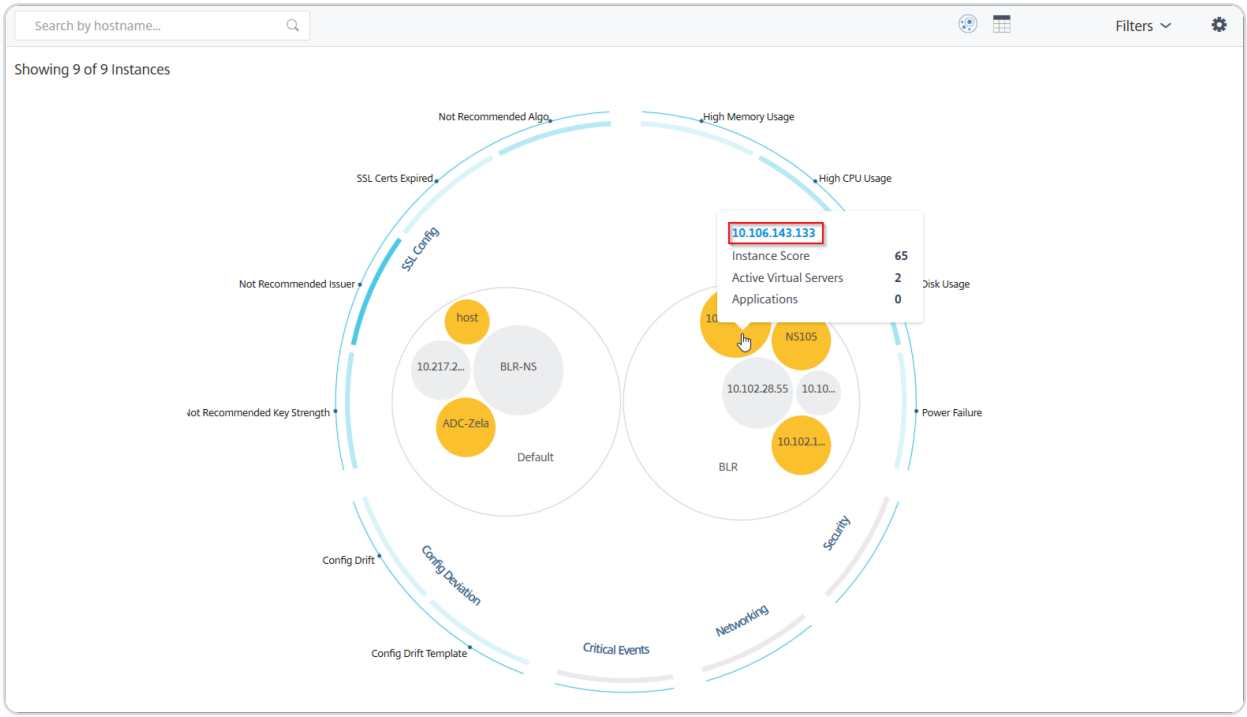
Chris 在 Circle Pack 上注意到一个实例的实例分数较低，并且该实例处于“关键”状态。Chris 单击该实例以查看问题所在。实例摘要显示该实例存在 SSL 卡故障，并且该实例无法处理 SSL 流量（SSL 流量已减少）。Chris 提取该信息并向团队发送报告，要求立即调查该问题。

示例 2 - 监控配置更改：

Chris 还注意到另一个实例处于“审核”状态，并且最近出现了配置偏差。当 Chris 单击配置偏差风险指示器时，Chris 注意到已进行了与 RC4 密码、SSL v3、TLS 1.0 和 TLS 1.1 相关的配置更改，这可能是出于安全考虑。Chris 还注意到此实例的 SSL 事务流量配置文件已下降。Chris 导出此报告并将其发送给管理员以进一步查询。

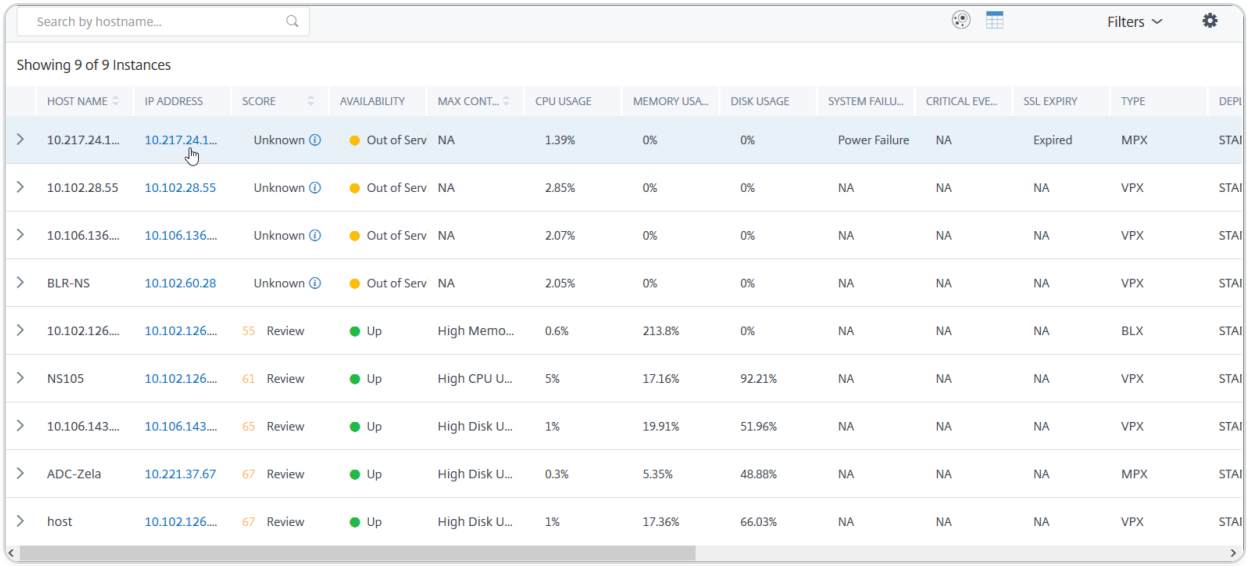
在基础设施分析中查看实例详细信息

1. 导航到 **基础设施 > 基础设施分析**
2. 单击圆包视图并选择 IP 地址。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

您也可以从表格视图中单击 IP 地址。



- **主机名** – 表示分配给 NetScaler 实例的主机名
- **IP 地址** – 表示 NetScaler 实例的 IP 地址
- **分数** – 表示 NetScaler 实例的分数以及状态，例如“严重”、“良好”和“一般”
- **可用性** – 表示 NetScaler 实例的状态，例如 **正常**、**关闭** 或 **停止服务**。
- **最大贡献** – 表示 NetScaler 实例错误计数最多的问题类别。
- **CPU 使用率** – 表示实例当前使用的 CPU 百分比
- **内存使用率** – 表示实例当前使用的内存百分比
- **磁盘使用率** – 表示实例当前使用的磁盘百分比
- **系统故障** – 表示实例系统的错误总数
- **关键事件** – 表示 NetScaler 实例具有最多事件的事件类别
- **SSL 过期** – 表示 NetScaler 实例上安装的 SSL 证书的状态
- **类型** – 表示 NetScaler 实例类型，例如 VPX、SDX、MPX 或 CPX
- **部署** – 表示 NetScaler 实例是作为独立实例还是 HA 对部署
- **型号** – 表示 NetScaler 实例的型号
- **版本** – 表示 NetScaler 实例的版本和内部版本号
- **吞吐量** – 表示 NetScaler 实例的当前网络吞吐量
- **HTTPS 请求/秒** – 表示 NetScaler 实例当前接收的 HTTPS 请求/秒
- **TCP 连接** – 表示当前建立的 TCP 连接数
- **SSL 事务** – 表示 NetScaler 实例当前处理的 SSL 事务

© 1997–2026 Citrix Systems, Inc. All rights reserved.

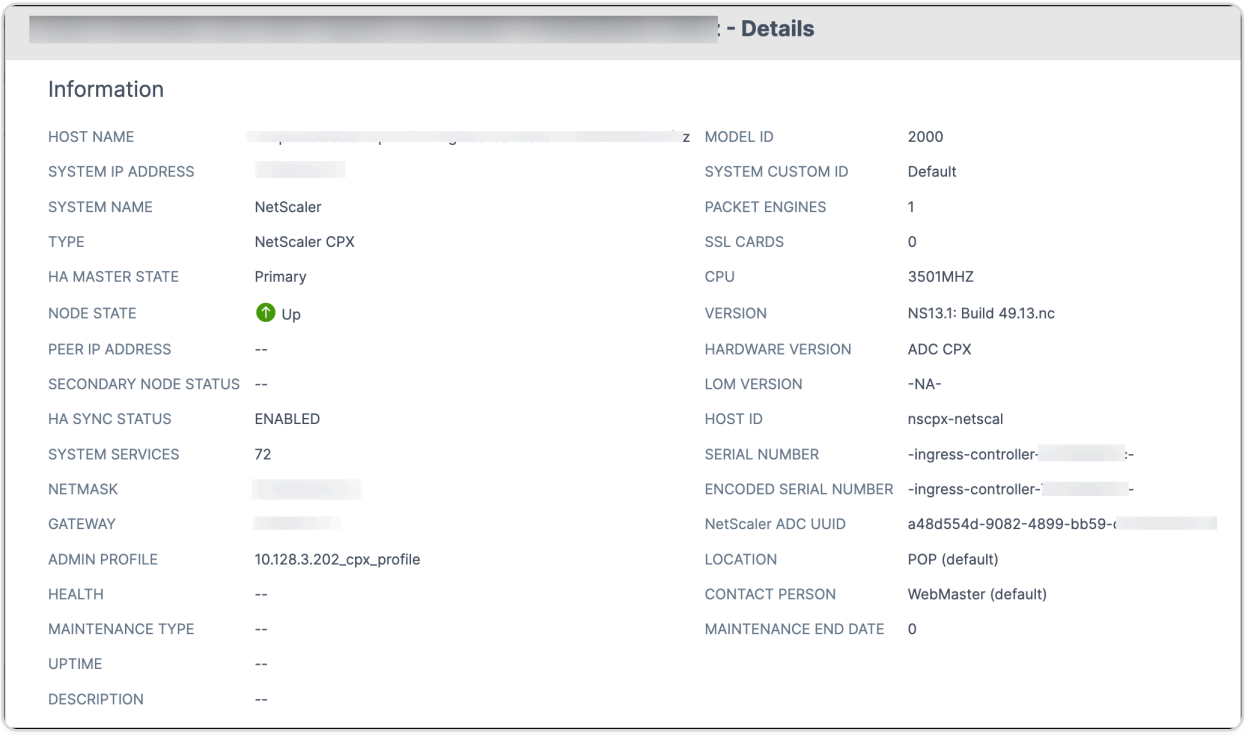
- **站点** – 表示部署 NetScaler 实例的站点名称。

> **注意**
>
> 每 5 分钟更新一次 CPU 使用率、内存使用率、磁盘使用率、吞吐量等当前值。

单击“**实例详细信息**”以查看详细信息。

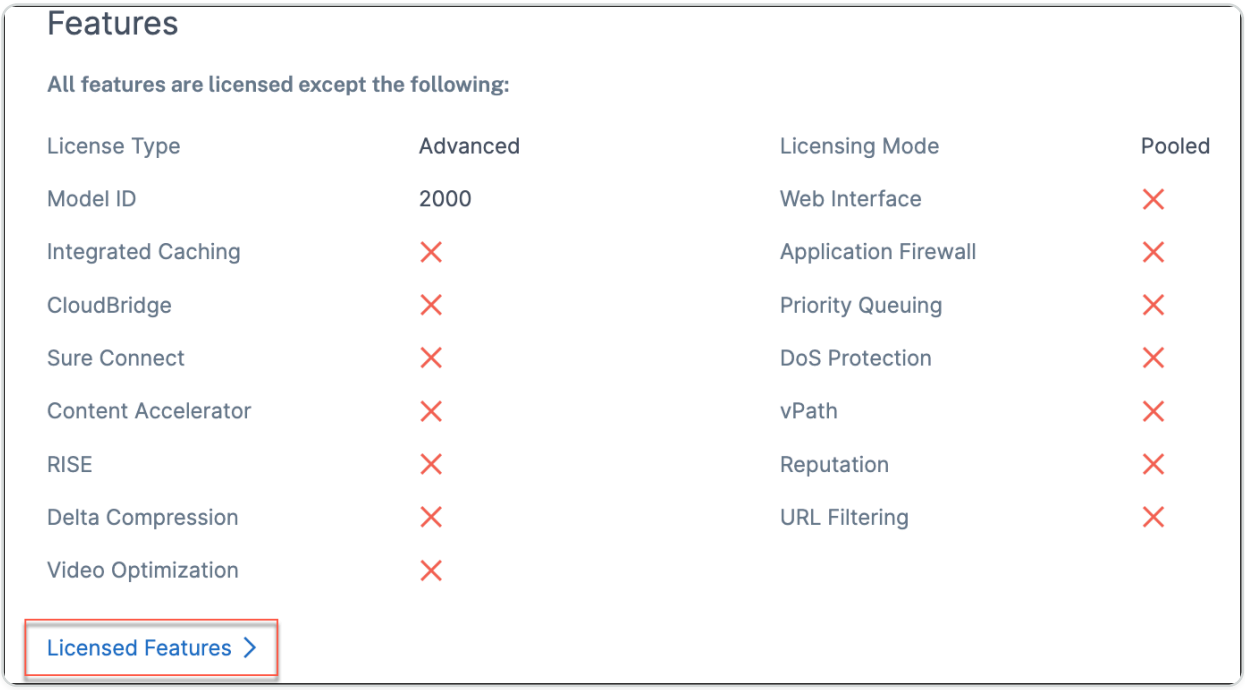
显示以下详细信息：

- **信息** - 实例详细信息，例如实例类型、部署类型、版本、型号。



- **功能** – 默认情况下，显示未授权的功能。单击**已授权功能**以查看已授权的功能。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

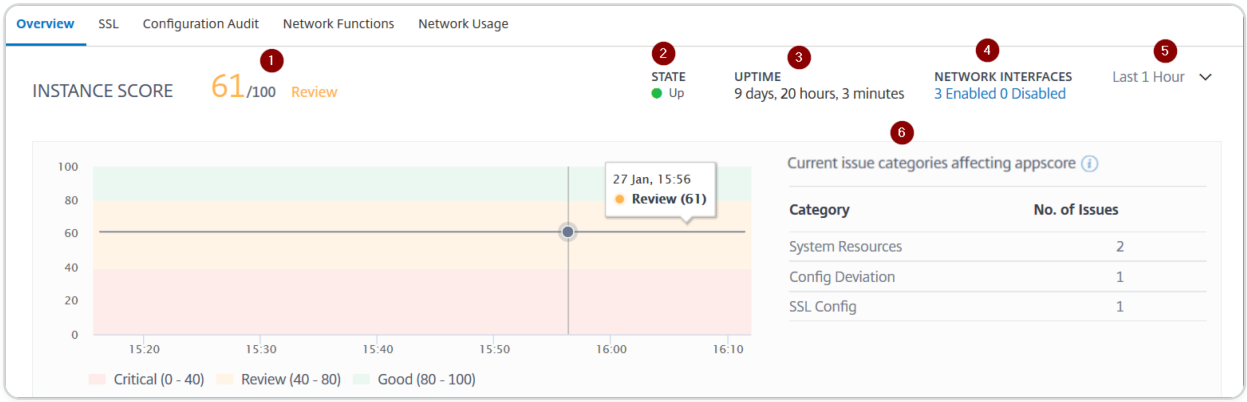


- **模式** – 默认情况下，显示实例上所有已禁用的模式。单击**查看已启用模式**以查看实例上已启用的模式。

实例仪表板提供实例概览，您可以在其中查看以下详细信息：

- **实例分数**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1 – 表示所选时间段内当前的 NetScaler 实例分数。最终分数计算为**100 减去总罚分**。图表显示了所选时间段的分数范围。

2 – 表示 NetScaler 实例的状态，例如**正常**、**关闭**和**停止服务**。

3 – 表示 NetScaler 实例已启动并运行的持续时间。

4 – 表示实例已启用和禁用的网络接口总数。单击以查看详细信息，例如网络接口名称和状态（已启用或已禁用）。

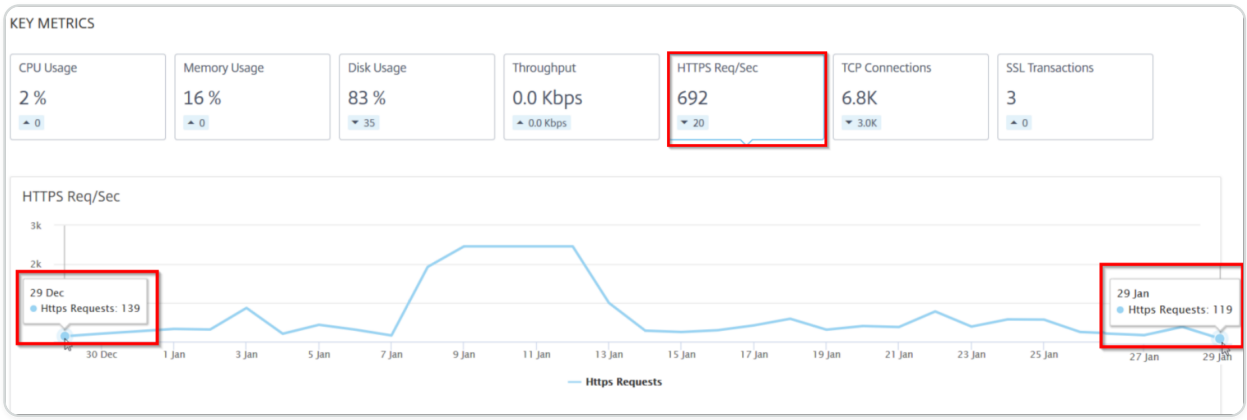
5 – 从列表中选择时间段以查看实例详细信息。

6 – 显示 NetScaler 实例的总问题数和问题类别。

- **关键指标**

单击每个选项卡可查看详细信息。在每个指标中，您可以查看所选时间的平均值和差值。

下图是 HTTPS 请求/秒的示例，所选时间段为 1 小时。值 **692** 是 1 个月期间的平均 HTTPS 请求/秒，值 **20** 是差值。在图中，第一个值是 **139**，最后一个值是 **119**。差值为 **139 – 119 = 20**。



您可以以图表形式查看所选时间段的以下实例指标：

- **CPU 使用率** – 实例在所选持续时间内的平均 CPU 百分比（同时显示数据包 CPU 和管理 CPU）。
- **内存使用率** – 实例在所选持续时间内的平均内存使用百分比。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **磁盘使用率** – 实例在所选持续时间内的平均磁盘空间百分比。
- **吞吐量** – 实例在所选持续时间内的平均网络吞吐量。
- **HTTPS 请求/秒** – 实例在所选持续时间内的平均 HTTPS 请求数。
- **TCP 连接** – 客户端和服务器在所选持续时间内的平均 TCP 连接数。
- **SSL 事务** – 实例在所选持续时间内的平均 SSL 事务数。

- **问题**

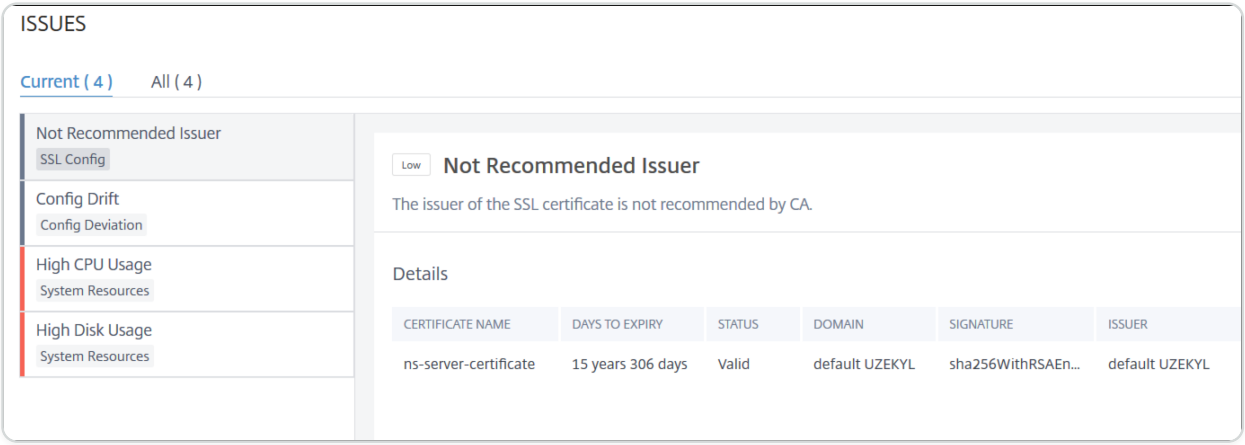
  您可以查看 NetScaler 实例中出现的以下问题：

问题类别	描述	问题
系统资源	显示与 NetScaler 系统资源（例如 CPU、内存、磁盘使用情况）相关的所有问题。	- CPU 使用率高
		- 内存使用率高
		- 磁盘使用率高
		- SSL 卡故障
		- 电源故障
		- 磁盘错误
		- 闪存错误
		- NIC 丢弃
SSL 配置	显示与 NetScaler 实例上的 SSL 配置相关的所有问题。	- SSL 证书过期
		- 不推荐的颁发者
		- 不推荐的算法
		- 不推荐的密钥强度
配置偏差	显示与 NetScaler 实例中应用的配置作业相关的所有问题。	- 配置漂移

© 1997–2026 Citrix Systems, Inc. All rights reserved.

问题类别	描述	问题
		- 运行中与模板
关键事件	显示与配置为 HA 对和集群的 NetScaler 实例相关的所有关键事件。	- 集群属性传播失败
		- 集群同步失败
		- 集群版本不匹配
		- HA 辅助状态异常
		- HA 无心跳
		- HA 同步失败
		- HA 版本不匹配
网络	显示实例中出现的操作问题。	有关详细信息，请参阅具有新指标的增强型基础架构分析。

单击每个选项卡以分析和排查问题。例如，假设实例在选定的时间段内出现以下错误：



- “**当前**”选项卡显示当前影响实例分数的问题。
- “**所有**”选项卡显示在选定持续时间内检测到的所有基础架构问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

查看 NetScaler 实例中的容量问题

当 NetScaler 实例已消耗其大部分可用容量时，在处理客户端流量时可能会发生数据包丢弃。此问题会导致 NetScaler 实例的性能低下。通过了解此类 NetScaler 容量问题，您可以主动分配额外的许可证以稳定 NetScaler 性能。

在**圆包视图**中，您可以查看 NetScaler 实例的容量问题（如果存在）。

要查看 NetScaler 容量问题，

1. 导航到**基础架构 > 基础架构分析**。
2. 选择圆包视图。

注意

在**基础架构分析**中，圆包视图和表格视图显示在过去一小时内发生的事件和问题。

下图显示所选实例中存在容量问题：

问题根据以下容量参数进行分类：

- **吞吐量限制已达到** – 达到吞吐量限制后，实例中丢弃的数据包数量。
- **PE CPU 限制已达到** – 达到 PE CPU 限制后，所有 NIC 上丢弃的数据包数量。

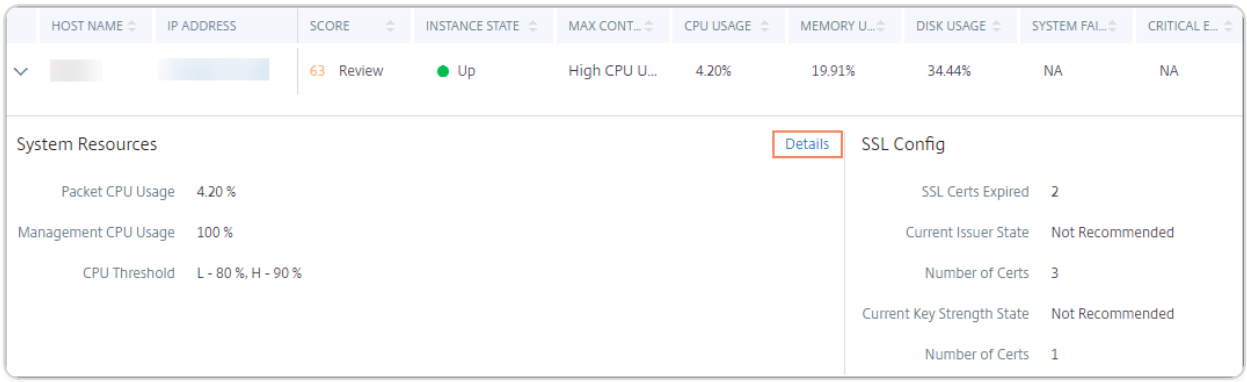
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **PPS 限制已达到** – 达到 PPS 限制后，实例中丢弃的数据包数量。
- **SSL 吞吐量速率限制** – 达到 SSL 吞吐量限制的次数。
- **SSL TPS 速率限制** – 达到 SSL TPS 限制的次数。

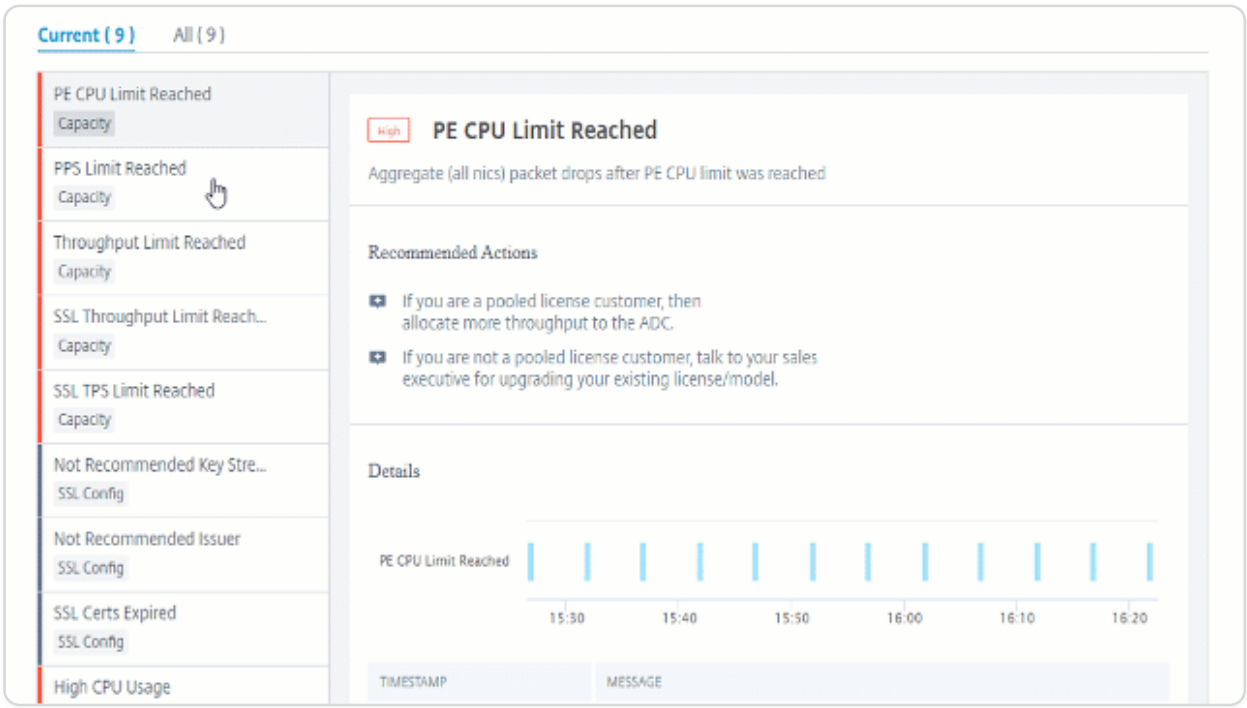
查看解决容量问题的建议操作

NetScaler Console 建议可以解决容量问题的操作。要查看建议的操作，请执行以下步骤：

1. 在 **Infrastructure > Infrastructure Analytics** 中，选择表格视图。
2. 选择存在容量问题的实例，然后单击**详细信息**。



3. 在实例页面中，向下滚动到**问题**部分。
4. 选择每个问题并查看解决容量问题的建议操作。



NetScaler Console 每五分钟从 NetScaler 实例轮询这些事件，并显示是否存在数据包丢弃或速率限制计数器增量。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console 根据定义的容量阈值计算实例分数。

- **低阈值** – 1 个数据包丢弃或速率限制计数器增量
- **高阈值** – 10000 个数据包丢弃或速率限制计数器增量

因此，当 NetScaler 实例超出容量阈值时，实例分数会受到影响。

当数据包丢弃或速率限制计数器增量时，会在 `ADCCapacityBreach` 类别下生成一个事件。要查看这些事件，请导航到 **Accounts > System Events**。

增强型基础架构分析，带新指标

使用 NetScaler Console 基础架构分析，您可以：

- 查看 NetScaler 实例中出现的一组新的操作问题。
- 查看错误消息并检查建议以解决问题。

作为管理员，您可以快速识别问题的根本原因分析。

注意

规则指标不支持以下情况：

- 配置为群集模式的 NetScaler 实例。
- 配置了管理分区的 NetScaler 实例。

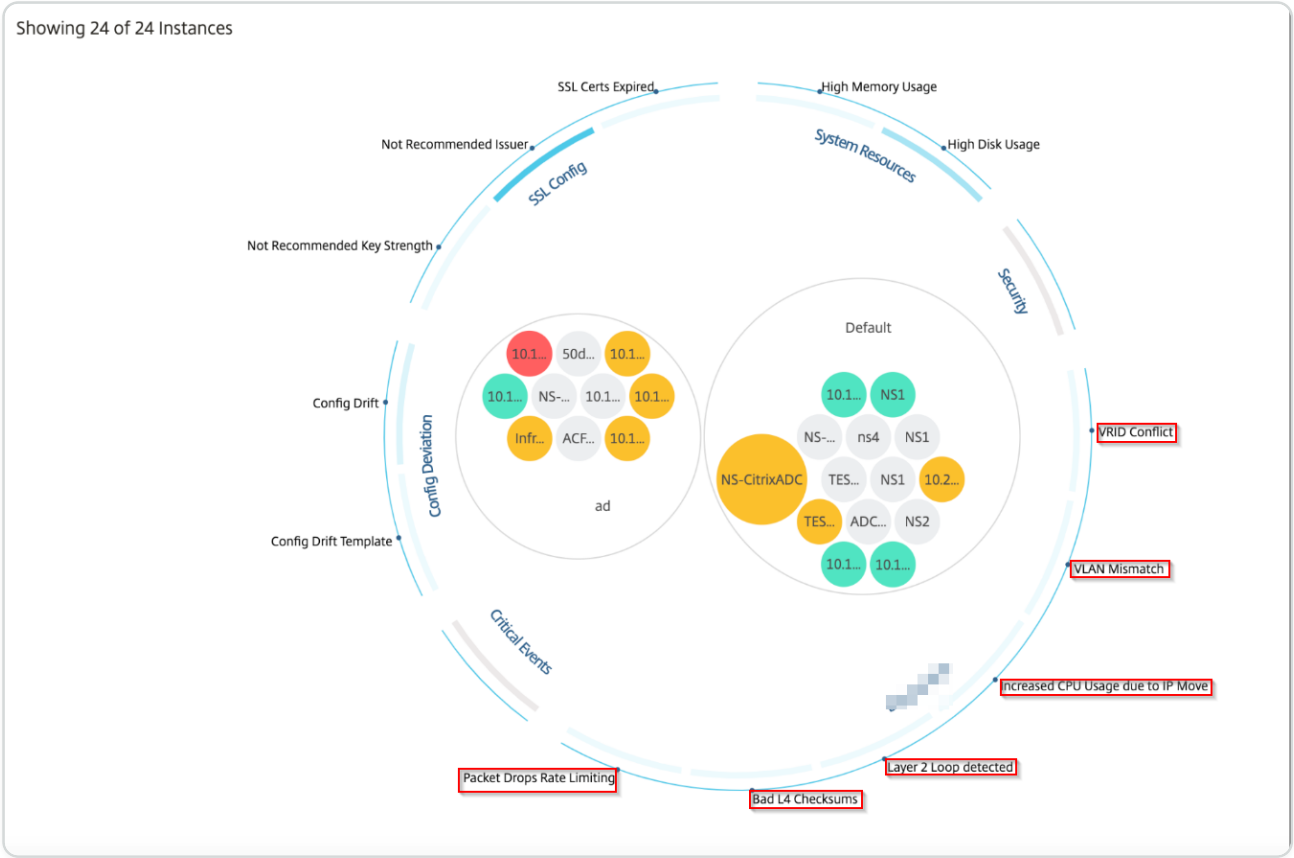
在 NetScaler Console 中，导航到 **基础架构 > 基础架构分析** 以查看以下指标：

基础架构分析中的指标名称	描述
端口分配失败	检测 NetScaler 何时使用 SNIP 与新的服务器连接进行通信，以及该 SNIP 上可用的总端口已耗尽。建议的操作是在同一子网中添加另一个 SNIP。
无默认路由配置	检测到由于路由不可用而导致流量丢弃的情况。
IP 冲突	检测到网络中两个或更多实例上配置或应用了相同的 IP 地址。
VRID 冲突	检测到指定 VRID 出现间歇性访问问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

基础架构分析中的指标名称	描述
VLAN 不匹配	检测到绑定到 IP 子网的 VLAN 配置过程中是否发生任何错误。
TCP 小窗口攻击	检测到可能正在进行的小窗口攻击。此警报仅供参考，因为 NetScaler 已缓解此攻击。
速率控制阈值	检测到根据配置的速率控制阈值丢弃数据包的情况。
持久性限制	检测到 NetScaler 内存达到最大命中数的情况。
GSLB 站点名称不匹配	检测到由于站点名称不匹配而导致 GSLB 配置同步失败的情况。
格式错误的 IP 报头	检测 IPv4 数据包的完整性检查失败时的情况。
错误的 L4 校验和	检测 TCP 数据包的校验和验证失败时的情况。
IP 移动导致的 CPU 使用率增加	检测是否需要更新大量 MAC 地址。
过度的包转向	检测由于使用非对称 RSS 密钥类型而导致的软件数据包转向级别过高的情况。
二层环路	检测网络中是否存在二层环路。
标记 VLAN 不匹配	检测在未标记接口上接收到标记 VLAN 数据包时的情况。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

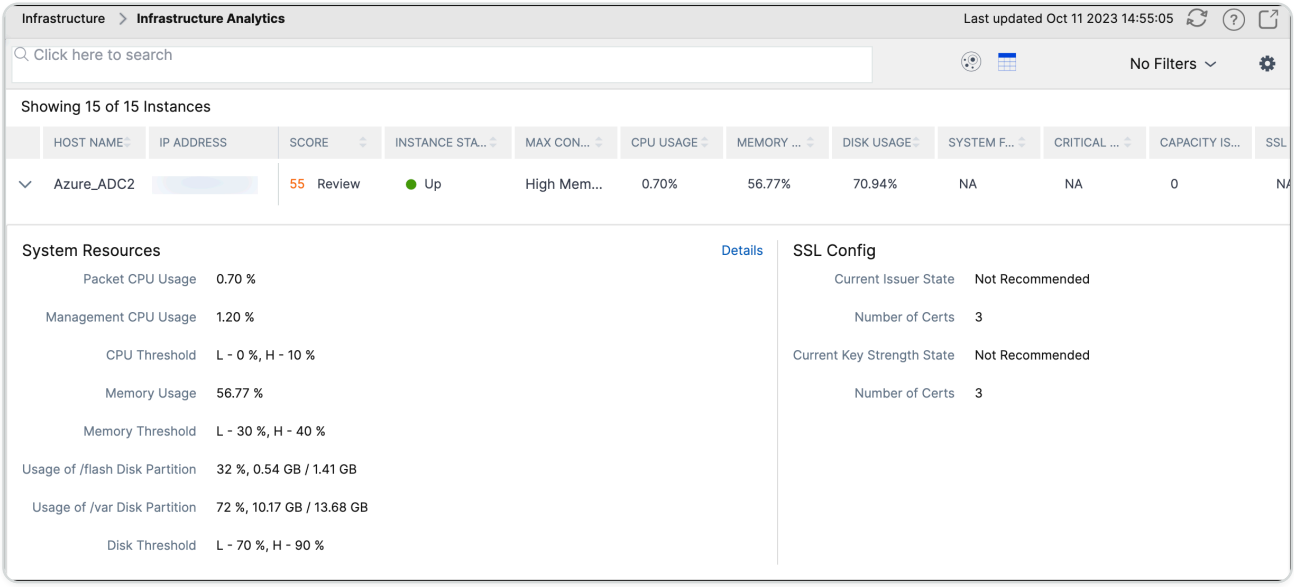


表格视图

您还可以使用**基础设施分析**中的表格视图选项查看异常。导航到**基础设施 > 基础设施分析**，然后单击

以显示所有托管实例。单击

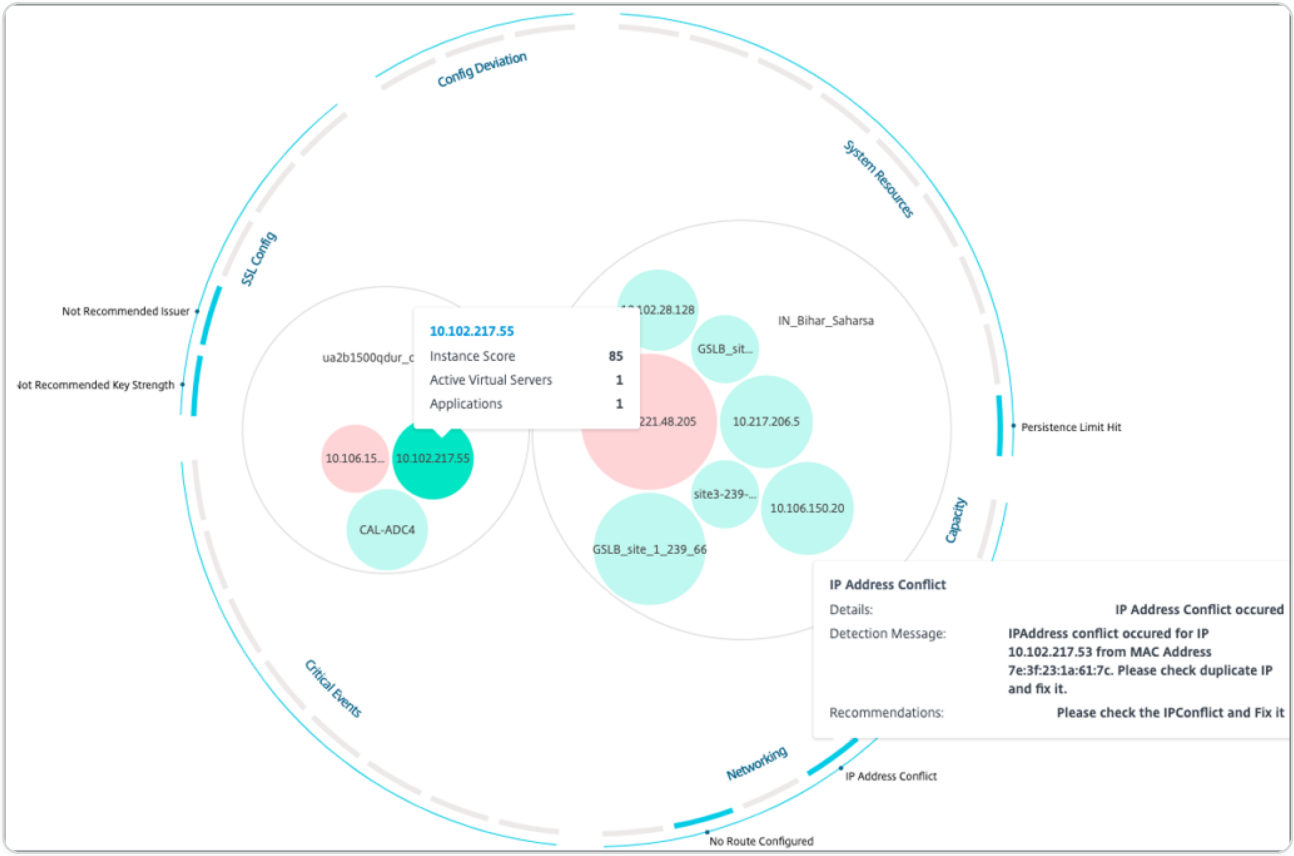
以展开查看详细信息。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

查看异常详情

例如，如果您想查看网络中**IP地址冲突**的详细信息，请点击显示IP地址冲突的异常以查看详细信息。



- **详细信息** - 指示检测到什么异常
- **检测消息** - 指示发生IP地址冲突的MAC地址
- **建议** - 指示解决此IP地址冲突的操作项

实例管理

实例是 Citrix NetScaler 设备，您可以使用 NetScaler Console 对其进行管理、监视和故障排除。您必须将实例添加到 NetScaler Console 才能对其进行监视。实例可以在设置 NetScaler Console 时添加，也可以稍后添加。将实例添加到 NetScaler Console 后，系统会持续轮询它们以收集信息，这些信息以后可用于解决问题或作为报告数据。

实例可以分组为静态组或私有 IP 块。当您想要运行特定任务（例如配置作业等）时，静态实例组会很有用。私有 IP 块根据地理位置对您的实例进行分组。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

添加实例

您可以在首次设置 NetScaler Console 服务器时添加实例，也可以稍后添加。要添加实例，您必须指定每个 NetScaler 实例的主机名或 IP 地址，或者指定一个 IP 地址范围。

要了解如何将实例添加到 NetScaler Console，请参阅 将实例添加到 NetScaler Console。

当您将实例添加到 NetScaler Console 服务器时，服务器会隐式地将自身添加为该实例的陷阱目标，并收集该实例的清单。要了解更多信息，请参阅 NetScaler Console 如何发现实例。

添加实例后，您可以通过导航到 **Infrastructure > Instances** 并单击 **All Instances** 来删除它。在“实例”页面上，选择要删除的实例，然后单击 **Remove**。

如何使用实例仪表板

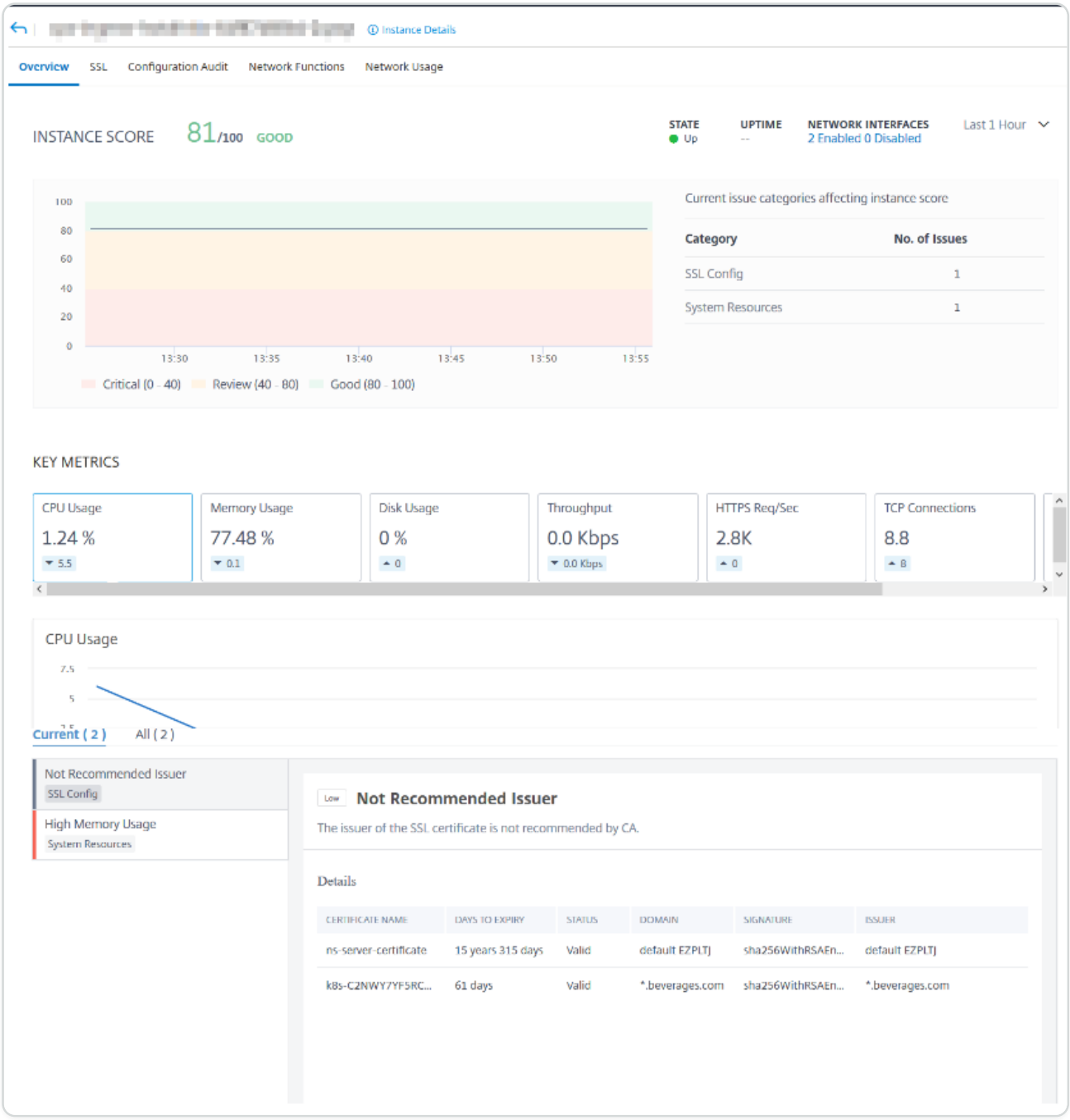
NetScaler Console 中的每个实例仪表板以表格和图形格式显示所选实例的数据。在轮询过程中从您的实例收集的数据会显示在仪表板上。

默认情况下，每分钟轮询一次托管实例以收集数据。状态、每秒 HTTP 请求数、CPU 使用率、内存使用率和吞吐量等统计信息通过 NITRO 调用持续收集。作为管理员，您可以在单个页面上查看所有这些收集到的数据，识别实例中的问题，并立即采取措施纠正它们。

要查看特定实例的仪表板，请导航到 **Infrastructure > Instances**。从摘要中，选择实例类型，然后选择要查看的实例，再单击 **Dashboard**。

下图概述了每个实例仪表板上显示的各种数据：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **概览**。概览选项卡显示所选实例的 CPU 和内存使用情况。您还可以查看实例生成的事件和吞吐量数据。实例特定信息，例如 IP 地址、其硬件和 LOM 版本、配置文件详细信息、序列号、联系人等，也在此处显示。继续向下滚动，还会显示所选实例上可用的许可功能以及其上配置的模式。

  有关更多信息，请参阅 Instance details。

- **SSL 控制板**。您可以使用每个实例控制板上的“SSL”选项卡来查看或监控所选实例的 SSL 证书、SSL 虚拟服务器和 SSL 协议的详细信息。您可以单击图表中的“数字”以显示更多详细信息。

- **配置审计**。您可以使用配置审计选项卡查看所选实例上发生的所有配置更改。控制板上的“**NetScaler® 配置保存状态**”和“**NetScaler 配置漂移**”图表显示了已保存配置与未保存配置中配置更改的高级详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **网络功能**。使用网络功能控制板，您可以监控所选 NetScaler 实例上配置的实体的状态。您可以查看虚拟服务器的图表，这些图表显示客户端连接、吞吐量和服务器连接等数据。
- **网络使用情况**。您可以在“网络使用情况”选项卡上查看所选实例的网络性能数据。您可以显示一小时、一天、一周或一个月的报告。时间轴滑块功能可用于自定义生成的网络报告的持续时间。默认情况下，只显示八个报告，但您可以单击屏幕右下角的“加号”图标以添加更多性能报告。

监控全球分布式站点

作为网络管理员，您可能需要监控和管理部署在不同地理位置的网络实例。然而，在管理地理分布式数据中心中的网络实例时，评估网络需求并非易事。

NetScaler Console 中的地理地图为您提供了站点的图形表示，并按地理位置细分了您的网络监控体验。借助地理地图，您可以按位置可视化网络实例分布并监控网络问题。

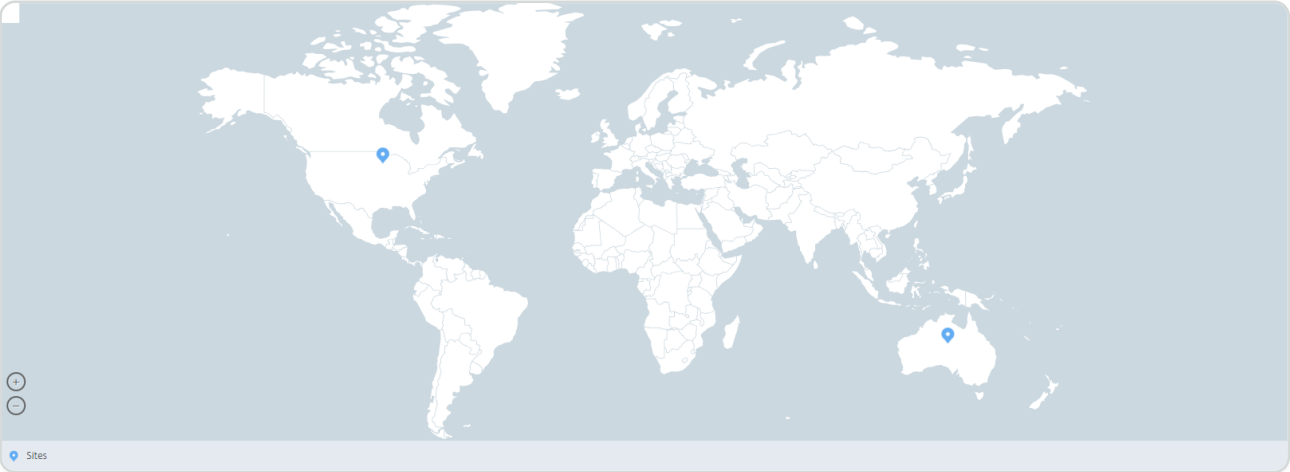
以下部分说明了如何在 NetScaler Console 中监控数据中心。

NetScaler Console 站点是特定地理位置中 Citrix NetScaler 实例的逻辑分组。例如，一个站点可能分配给 Amazon Web Services (AWS)，而另一个站点可能分配给 Azure。还有另一个站点托管在租户的本地。NetScaler Console 管理和监控连接到所有站点的所有 NetScaler 实例。您可以使用 NetScaler Console 监控和收集来自受管实例的 syslog、AppFlow、SNMP 以及任何此类数据。

NetScaler Console 中的地理地图为您提供了站点的图形表示。地理地图还按地理位置细分了您的网络监控体验。借助地理地图，您可以按位置可视化网络实例分布并监控所有网络问题。您可以导航到 **Infrastructure > Instances** 页面，以查看世界地图上创建的站点的可视化表示。

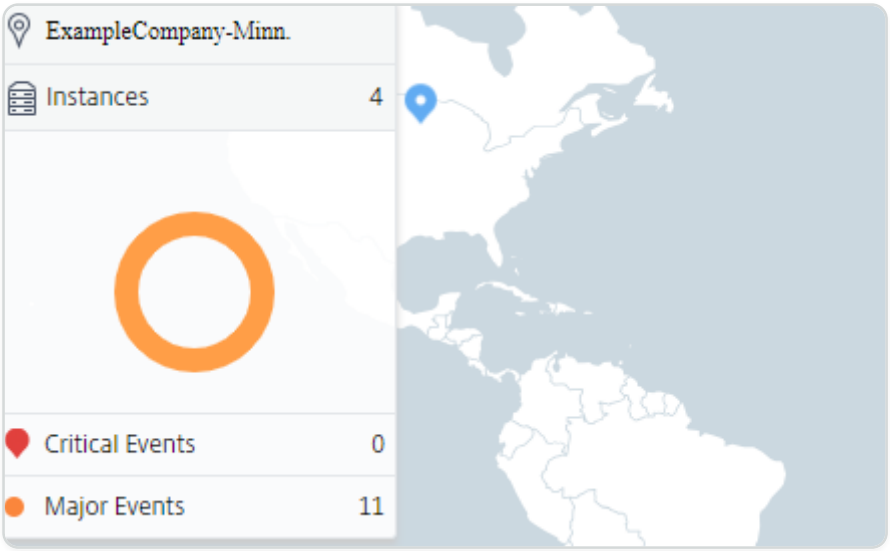
用例

一家领先的移动运营商公司 ExampleCompany 依靠私有服务提供商来托管其资源和应用程序。该公司已经有两个站点——一个在美国明尼阿波利斯，另一个在澳大利亚爱丽斯泉。在此图像中，您可以看到两个标记代表两个现有站点。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

标记还显示一个数字，表示每个站点中的应用程序数量。您可以单击这些标记以获取有关每个站点的更多信息。



单击选项卡以查看更多信息：

- **实例**选项卡：在此选项卡中查看以下内容：
  - 每个网络实例的 IP 地址
  - 实例类型
  - 它们上面的严重事件数量
  - NetScaler 实例上引发的重要事件和所有事件。
- **事件**选项卡：查看实例上引发的严重事件和重要事件列表。
- **证书**选项卡：在此选项卡中查看以下内容：
  - 所有实例的证书列表
  - 过期状态
  - 重要信息以及按使用中证书数量排名前 10 的实例。
- **代理**选项卡：查看实例所绑定的代理列表。

  查看代理(/en-us/netscaler-application-delivery-management-software/media/nmaservice-global-datacenters-3.png)

配置地理地图

ExampleCompany 决定在印度班加罗尔创建第三个站点。该公司希望通过将一些不太关键的内部 IT 应用程序卸载到班加罗尔办事处来测试云。该公司决定使用 AWS 云计算服务。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

作为管理员，您必须首先创建一个站点，然后将 NetScaler 实例添加到 NetScaler Console 中。您还必须将实例添加到站点，添加代理，并将代理绑定到站点。然后，NetScaler Console 会识别 NetScaler 实例和代理所属的站点。

有关添加 NetScaler 实例的更多信息，请参阅 添加实例。

创建站点：

在 NetScaler Console 中添加实例之前创建站点。提供位置信息可让您精确地定位站点。

导航到 **基础架构 > 实例 > 站点**，然后点击 **添加**。

1. 在 **创建站点** 页面中，指定以下信息：

   a. **站点类型**：选择 **数据中心**。

   > **注意**
   >
   > 站点可以作为主数据中心或分支机构。请相应选择。

   b. **类型**：从列表中选择 AWS 作为云提供商。

   > **注意**
   >
   > 相应地勾选 **将现有 VPC 用作站点** 复选框。

   c. **站点名称**：键入站点名称。

   d. **城市**：键入城市。

   e. **邮政编码**：键入邮政编码。

   f. **区域**：键入区域。

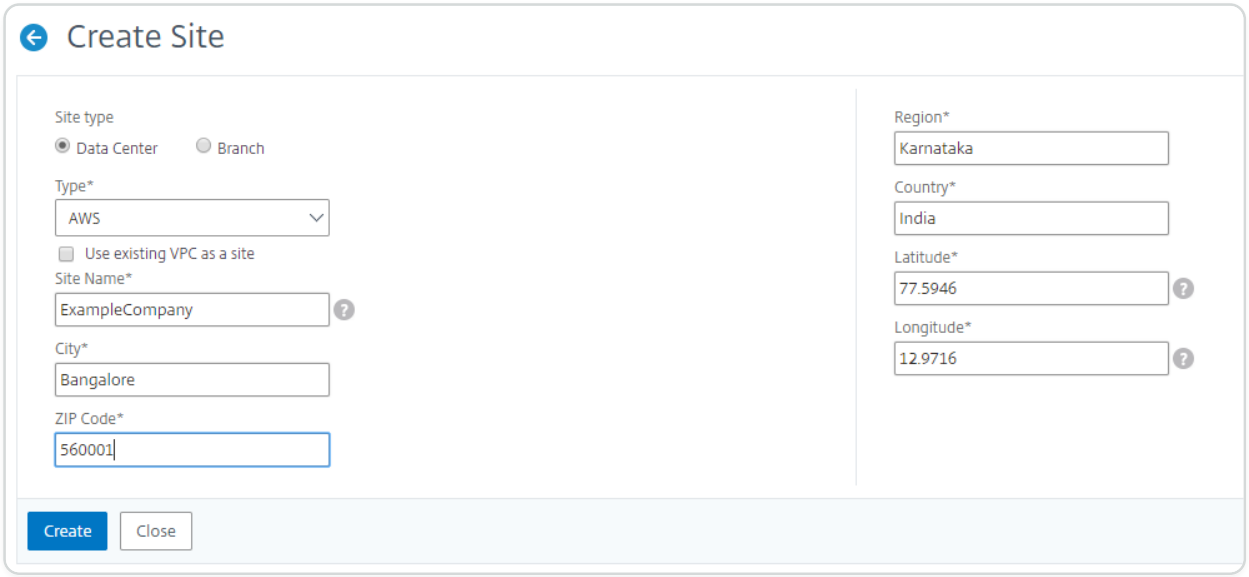
   g. **国家/地区**：键入国家/地区。

   h. **纬度**：键入位置的纬度。

   i. **经度**：键入位置的经度。

2. 点击**创建**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



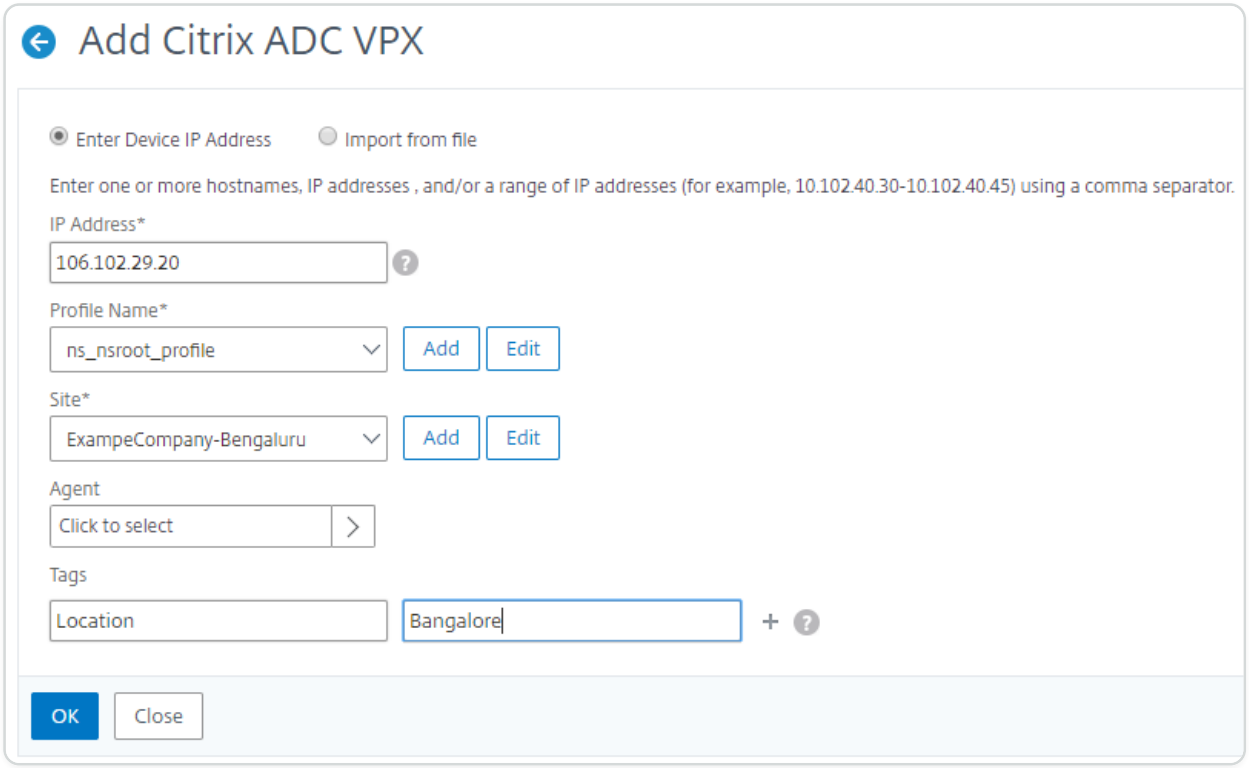
添加实例并选择站点：

创建站点后，您必须在 NetScaler Console 中添加实例。您可以选择之前创建的站点，也可以创建一个站点并关联该实例。

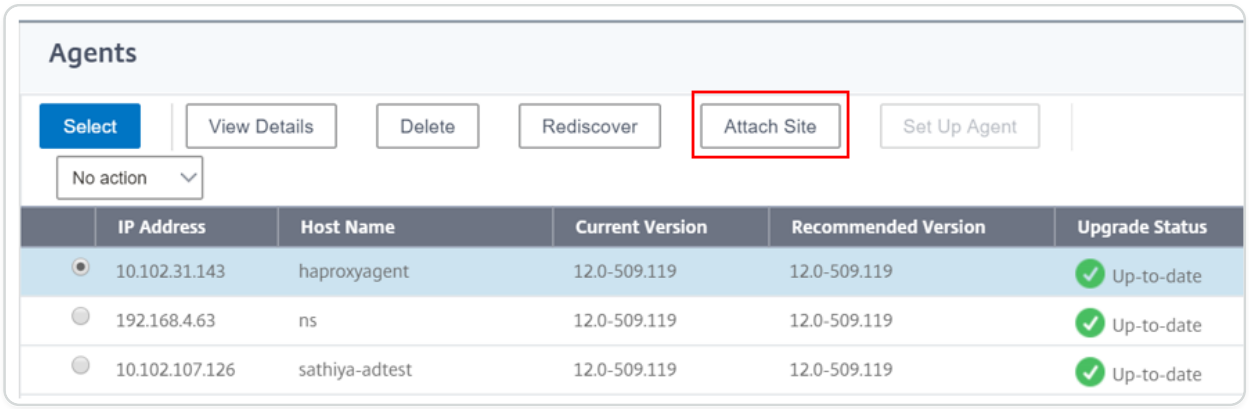
创建站点后，您必须在 NetScaler Console 中添加实例。您可以选择之前创建的站点，也可以创建一个站点并关联该实例。

1. 在 NetScaler Console 中，导航到**基础架构 > 实例**。
2. 选择要创建的实例类型，然后点击**添加**。
3. 在**添加 NetScaler VPX**页面上，键入 IP 地址并从列表中选择配置文件。
4. 从列表中选择站点。您可以点击**站点**字段旁边的“+”号来创建站点，或点击编辑图标来更改默认站点的详细信息。
5. 点击右箭头，并从显示的列表中选择代理。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 选择代理后，您必须将代理与站点关联。此步骤允许代理绑定到站点。选择代理，然后点击**附加站点**。



\1. 从列表中选择站点，然后点击**保存**。

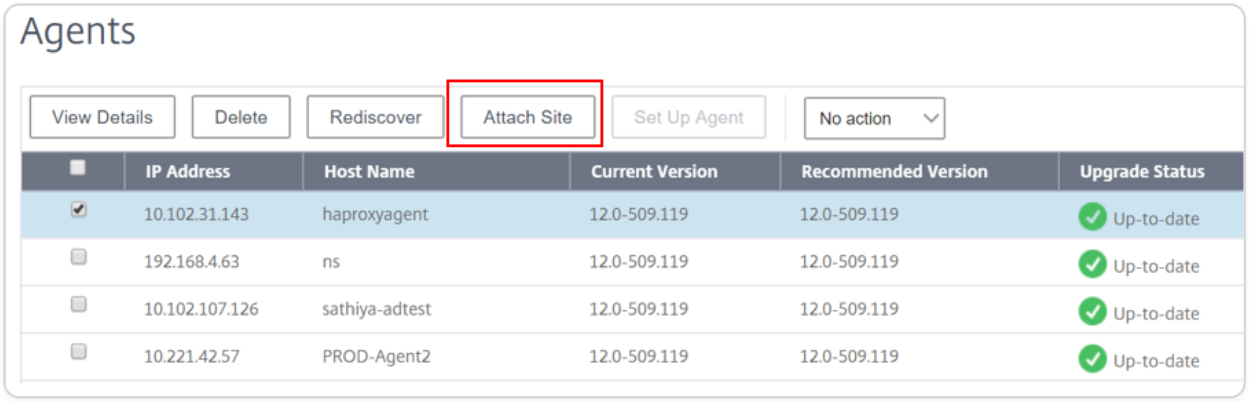
\1. 点击**确定**。

您还可以通过导航到 **基础设施 > 实例 > 代理** 来将代理附加到站点。

将 NetScaler 代理与站点关联：

1. 在 NetScaler Console 中，导航到 **基础设施 > 实例 > 代理**。
2. 选择代理，然后单击 **附加站点**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



\1. 您可以关联站点并单击 **保存**。

NetScaler Console 开始监控班加罗尔站点中添加的 NetScaler 实例以及其他两个站点的实例。

如何创建标签并将其分配给实例

NetScaler Console 现在允许您将 Citrix NetScaler 实例与标签关联。标签是您可以分配给实例的关键字或一个词的术语。标签添加了有关实例的一些附加信息。标签可以被视为有助于描述实例的元数据。标签允许您根据这些特定关键字对实例进行分类和搜索。您还可以将多个标签分配给单个实例。

以下用例可帮助您了解实例标记如何帮助您更好地监控它们。

- **用例 1**：您可以创建一个标签来标识英国的所有实例。在这里，您可以创建一个键为“Country”，值为“UK”的标签。此标签可帮助您搜索和监控英国的所有这些实例。
- **用例 2**：您想要搜索处于暂存环境中的实例。在这里，您可以创建一个键为“Purpose”，值为“Staging_NS”的标签。此标签可帮助您将暂存环境中使用的所有实例与正在运行客户端请求的实例区分开来。
- **用例 3**：假设您想找出位于英国“Swindon”地区且由您（David T.）拥有的 NetScaler 实例列表。您可以为所有这些要求创建标签，并将其分配给满足这些条件的所有实例。

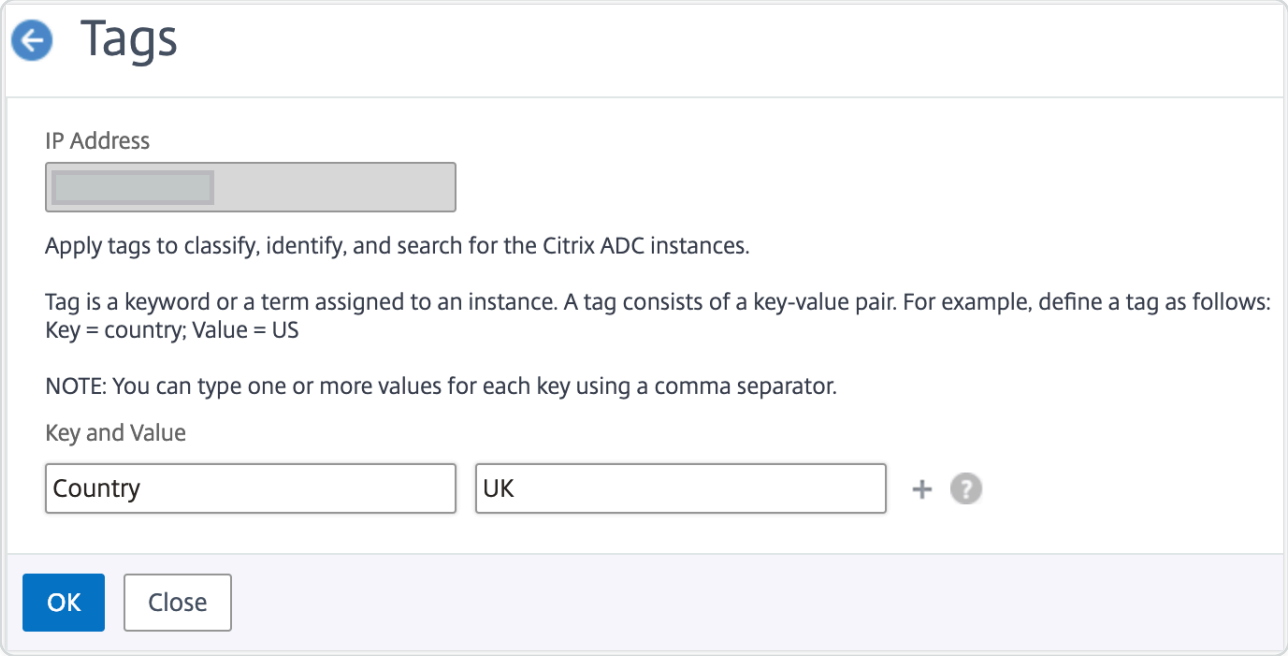
将标签分配给 NetScaler VPX 实例：

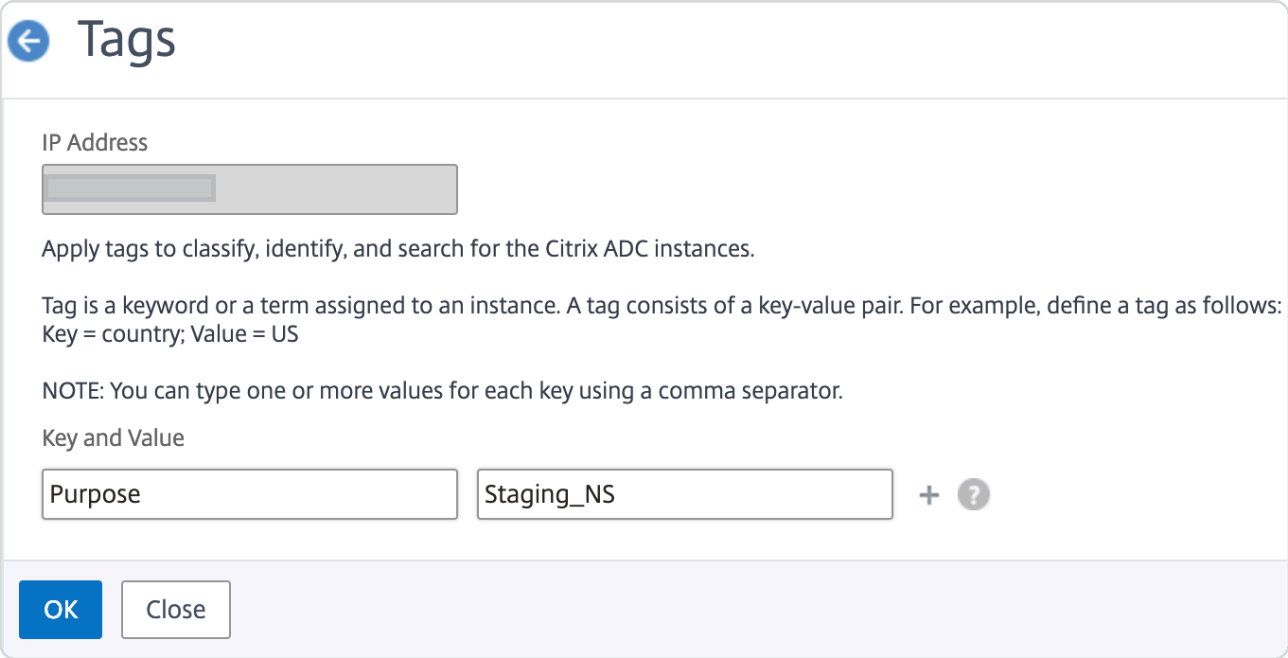
1. 在 NetScaler 控制台 中，导航到 **基础架构 > 实例 > NetScaler**。
2. 选择 **NetScaler VPX** 选项卡。
3. 选择所需的 NetScaler VPX。
4. 单击 **Tags**。
5. 创建标签并单击 **OK**。

出现的“**标签**”窗口允许您通过为创建的每个关键字分配值来创建自己的“键值”对。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

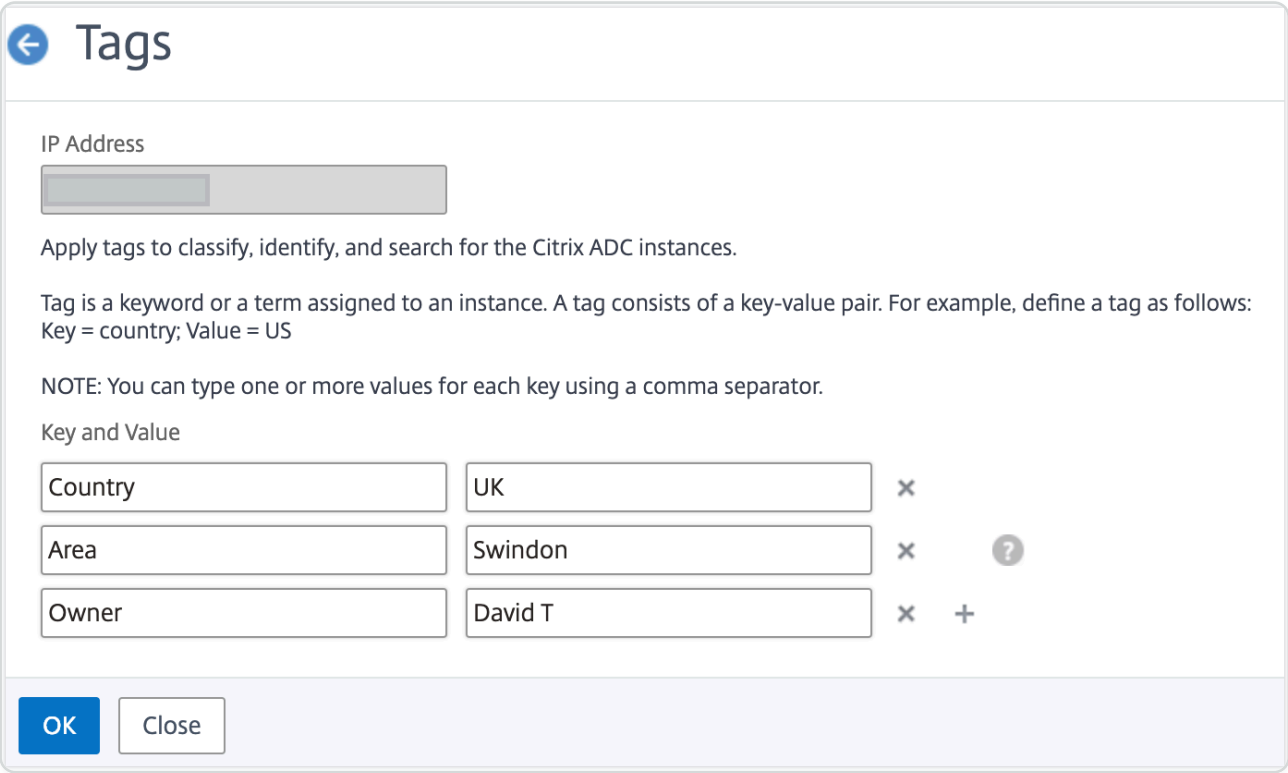
例如，以下图像显示了一些已创建的关键字及其值。您可以添加自己的关键字并为每个关键字键入一个值。





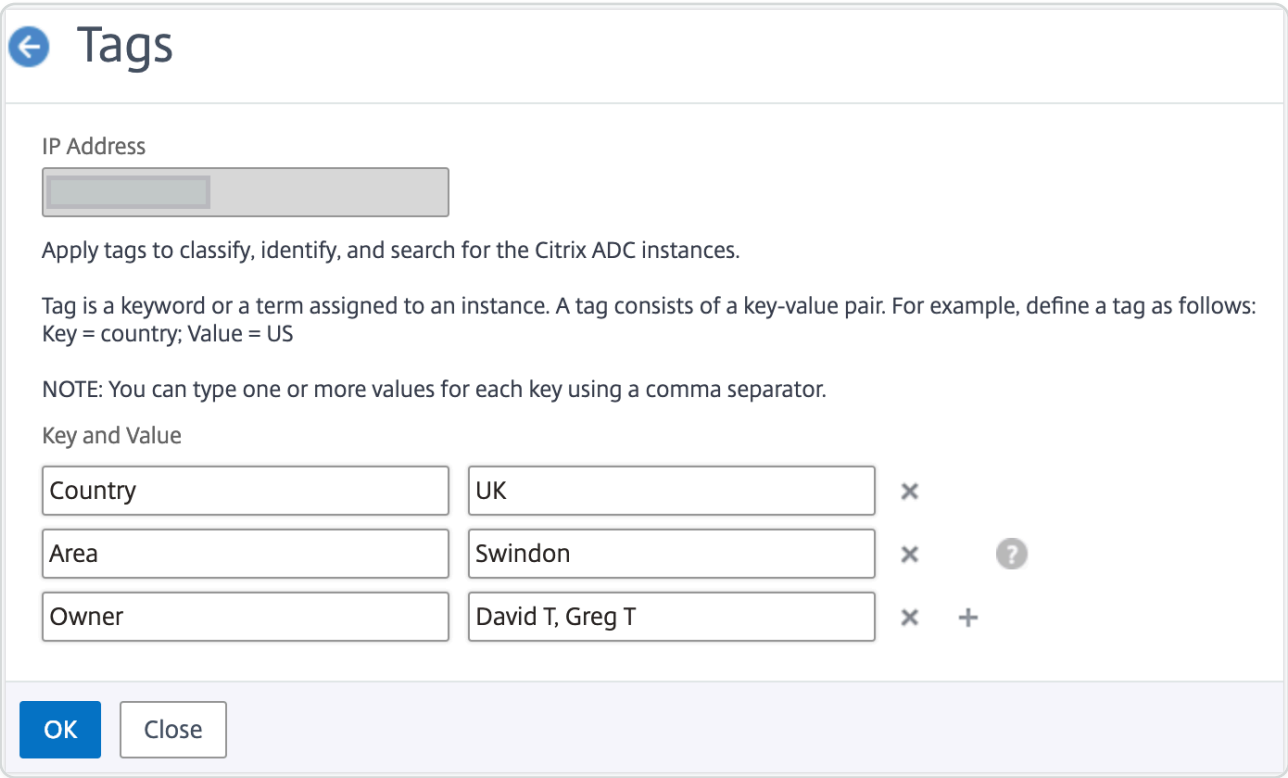
您还可以通过单击“+”添加多个标签。添加多个有意义的标签可以帮助您高效地搜索实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以通过用逗号分隔的方式为一个关键字添加多个值。

例如，您正在将管理员角色分配给另一位同事 Greg T。您可以添加他的姓名并用逗号分隔。添加多个姓名有助于您通过其中一个姓名或两个姓名进行搜索。NetScaler Console 会将逗号分隔的值识别为两个不同的值。



要了解有关如何根据标签搜索实例的更多信息，请参阅如何使用标签和属性值搜索实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

您可以稍后添加新标签或删除现有标签。您可以创建的标签数量没有限制。

如何使用标签和属性值搜索实例

NetScaler Console 可能管理着许多 NetScaler 实例。作为管理员，您可能希望能够根据特定参数灵活地搜索实例清单。NetScaler Console 现在提供改进的搜索功能，可以根据您在搜索字段中定义的参数搜索 NetScaler 实例的子集。您可以根据两个条件搜索实例：标签和属性。

- **标签**。标签是您可以分配给 NetScaler 实例的术语或关键字，用于添加有关 NetScaler 实例的额外描述。您现在可以将 NetScaler 实例与标签关联。这些标签可用于更好地识别和搜索 NetScaler 实例。
- **属性**。NetScaler Console 中添加的每个 NetScaler 实例都具有与该实例关联的一些默认参数或属性。例如，每个实例都有自己的主机名、IP 地址、版本、主机 ID、硬件型号 ID 等。您可以通过为这些属性中的任何一个指定值来搜索实例。

例如，假设您想找出版本为 12.0 且处于 UP 状态的 NetScaler 实例列表。在这里，实例的版本和状态由默认属性定义。

除了 12.0 版本和实例的 UP 状态外，您还可以搜索您拥有的那些实例。您可以创建一个“所有者”标签，并为该标签分配值“David T”。有关如何创建和分配标签的更多信息，请参阅如何创建标签并分配给实例。

您可以使用标签和属性的组合来创建自己的搜索条件。

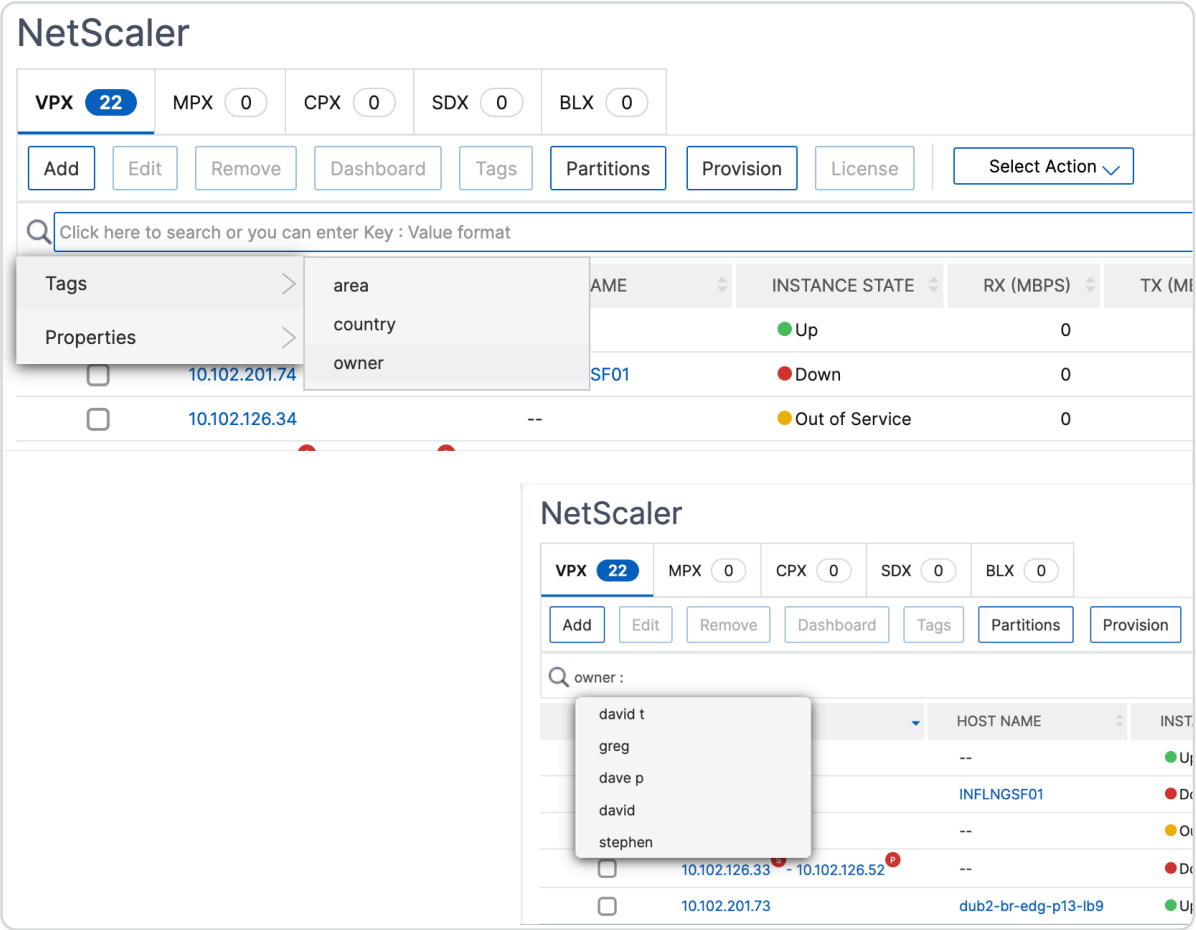
搜索 NetScaler VPX 实例

1. 在 NetScaler Console 中，导航到 **Infrastructure > Instances > NetScaler** > **VPX** 选项卡。
2. 单击搜索字段。您可以通过使用标签或属性，或通过组合两者来创建搜索表达式。

   以下示例展示了如何高效地使用搜索表达式来搜索实例。

   a. 选择 **Tags** 选项并选择 **Owner**。选择“David T.”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler Console 支持在搜索表达式中使用正则表达式和通配符。

b. 您可以使用正则表达式进一步扩展搜索条件。例如，您想搜索由 David 或 Stephen 拥有的实例。在这种情况下，您可以通过使用“\|”表达式分隔值来键入这些值。

   使用常规实例搜索实例(/en-us/netscaler-application-delivery-management-software/media/instance-search-tags-properties-3.png)

c. 您还可以使用通配符来替换或表示一个或多个字符。例如，您可以键入 `Dav*` 来搜索 David T 和 Dave P 拥有的所有实例。

   使用通配符搜索实例(/en-us/netscaler-application-delivery-management-software/media/instance-search-tags-properties-4.png)

注意

有关正则表达式和通配符以及如何使用它们的更多信息，请单击搜索栏中的“信息”图标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

通过 NetScaler® Console 集中式 GeoIP 数据库更新

NetScaler Console 允许管理员直接通过 NetScaler Console 从 MaxMind 上传 GeoIP 数据库（地理位置数据库）文件。您可以立即将 GeoIP 数据库文件推送到受管 NetScaler 实例，也可以安排稍后更新。这些文件对于准确的 IP 到位置映射至关重要，常用于 GSLB 和安全策略。

借助此增强功能，您还可以获得更新历史记录跟踪，这使您能够查看更新是成功还是失败。此外，您可以从 NetScaler Console 查看、删除或下载以前上传或推送的 GeoIP 数据库版本。此增强功能还引入了 NetScaler Console 中 GeoIP 数据库文件的手动更新、版本控制和自动化更新工作流，从而实现无缝的 GeoIP 数据库更新，而不会影响 GSLB 服务。

以前，NetScaler 没有用于管理 NetScaler 上 GeoIP 数据库更新的集中式机制。管理员必须在每个设备上手动执行更新，这在生产环境中既耗时又容易出错，并且具有破坏性。

此增强功能提供以下优势：

- **自动化**：更新过程是自动化的，并且在没有计划停机的情况下执行，因此减少了运营开销。
- **有效可扩展性**：管理多个 NetScaler 实例的更新效率高且易于扩展。
- **版本控制**：如果出现问题，您可以跟踪历史版本、上传并同步较旧的 GeoIP 数据库文件。

限制

- **格式转换支持仅限于 MaxMind**：自动格式转换仅支持 MaxMind 文件。对于其他供应商，文件必须已采用支持的格式。
- **删除限制**：不允许删除正在使用的文件。在删除之前，请确保没有活动的依赖项。

通过 NetScaler Console 配置集中式 GeoIP 数据库更新

先决条件

- 确保您拥有使用 GeoIP 数据库文件所需的有效 MaxMind 许可证。
- 如果您正在使用其他供应商的文件格式，请确保文件采用支持的格式。

执行以下步骤以上传来自 MaxMind 或任何其他供应商的 GeoIP DB 文件：

1. 导航到 **Infrastructure > GeoIP DB Sync**，然后单击 **Get Started**。

   集中式 GeoIP DB 入门(/en-us/netscaler-application-delivery-management-software/media/centralized-geodb-get-started.png)

2. 选择以下选项之一：

   - **上传新文件**：您可以从本地系统上传文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **使用现有文件**：您可以选择 NetScaler Console 上已存在的文件。

> **注意：**
>
> - 如果您是首次上传 GeoIP DB 文件，则不会看到 **使用现有文件** 选项。只有在文件已上传后，**使用现有文件** 选项才会在后续上传中出现。
> - 如果您上传 MaxMind 文件，NetScaler Console 服务会在上传期间自动将文件转换为 NetScaler 推荐的格式。如果您上传来自其他提供商的文件，则该文件必须为 CSV 格式，并遵循 NetScaler 推荐的以下字段顺序：IP 范围、国家/地区代码、区域、城市。

3. 文件上传后，您可以执行以下操作之一：

   - 单击 **Sync Now**，然后单击 **Start Sync**：所有 NetScaler 实例将立即更新。
   - 单击 **Create Schedule** - 您可以选择将来的日期和时间来更新 NetScaler 实例。

   集中式 GeoIP DB 同步选项(/en-us/netscaler-application-delivery-management-software/media/centralized-geodb-sync-options.png)

4. 在 **GeoIP DB Sync** 页面上查看同步进度和按实例的同步状态。

   集中式 GeoIP DB 同步进度(/en-us/netscaler-application-delivery-management-software/media/centralized-geodb-view-sync-progress.png)

5. 根据您的要求，您可以执行以下操作：

   - **选择新文件**：单击**选择新文件**以上传本地 GeoIP DB 文件或从 NetScaler Console 中选择一个已上传的文件。
   - **查看文件信息**：单击**查看文件信息**以查看以前上传的文件。如果出现问题，您可以跟踪历史版本、上传并同步较旧的 GeoIP DB 文件。
   - **活动计划**：单击**活动计划**以查看尚未执行的即将到来的计划。
   - **历史计划**：单击**历史计划**以查看已完成的以前的 GeoIP DB 同步活动。

   集中式 GeoIP DB 同步进度(/en-us/netscaler-application-delivery-management-software/media/centralized-geodb-other-options.png)

管理 NetScaler 实例的管理员分区

您可以在 Citrix NetScaler 实例上配置管理员分区，以便组织中的不同组在同一 NetScaler 实例上分配到不同的分区。网络管理员可以被分配管理多个 NetScaler 实例上的多个分区。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console 提供了一种无缝的方式，可以通过一个控制台管理管理员拥有的所有分区。您可以在不中断其他分区配置的情况下管理这些分区。

要允许多个用户管理不同的管理员分区，您必须创建组，然后将用户和分区分配给这些组。每个用户只能查看和管理其所属组中的分区。在 NetScaler Console 中，每个管理员分区都被视为一个实例。当您发现一个 NetScaler 实例时，在该 NetScaler 实例上配置的管理员分区会自动添加到系统中。

假设您有两个 NetScaler VPX 实例，每个实例上配置了两个分区。例如，NetScaler 实例 10.102.216.49 具有 Partition_1、Partition_2 和 Partition_3，NetScaler 实例 10.102.29.120 具有 p1 和 p2，如下图所示。

要查看分区，请导航到“**基础结构 > 实例 > NetScaler > VPX**”，然后单击“**分区**”。

您可以为 user-p1 分配以下分区：10.102.29.120-p1 和 10.102.216.49-Partition_1。并且，您可以将 user-p2 分配给管理分区 10.102.29.80-p2、10.102.216.49-Partition_2 和 10.102.216.49-Partition_3。

然后，您必须创建两个用户 user-p1 和 user-p2，并将这些用户分配给您为他们创建的组。

首先，您必须创建两个具有适当权限（例如：管理员权限）的组，并在每个组中包含所需的管理员分区实例。例如，创建系统组 partition1-admin，并将 NetScaler 管理员分区 10.102.29.120-p1 和 10.102.216.49-Partition_1 添加到此组。同时创建系统组 partition2-admin，并将 NetScaler 管理员分区 10.102.29.120-p2、10.102.216.49-Partition_2 和 10.102.216.49-Partition_3 添加到此组。

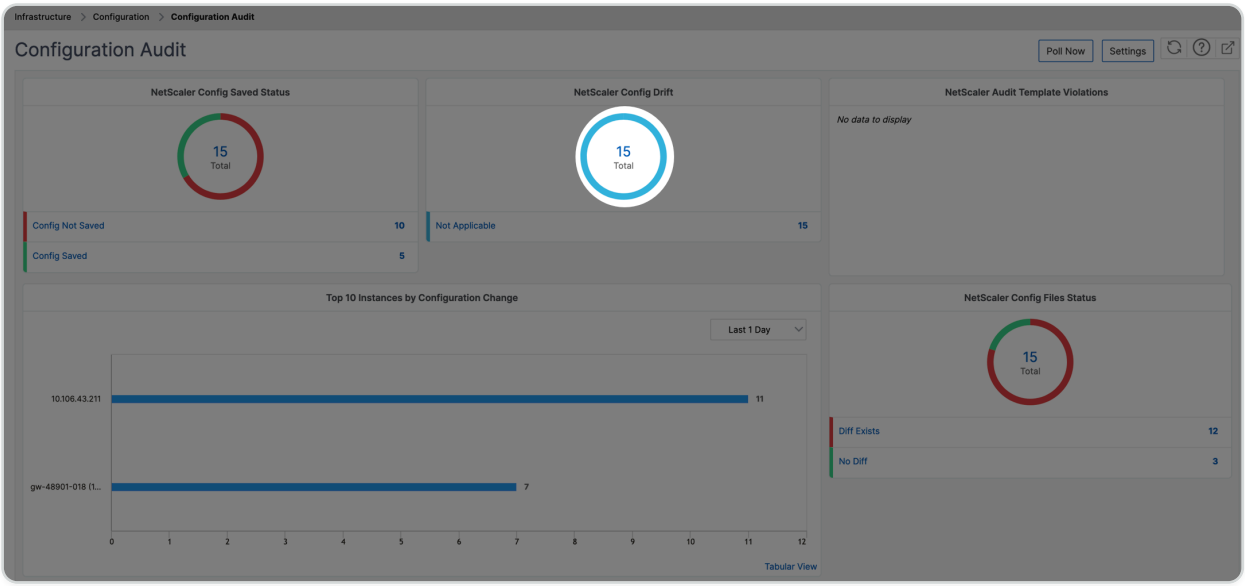
创建管理员分区后，您还可以使用修订历史记录差异功能和管理员分区功能的审计模板进行审计。

管理员分区的**修订历史记录差异**允许您查看分区 NetScaler 实例的五个最新配置文件之间的差异。您可以将配置文件相互比较（例如，配置修订版 - 1 与配置修订版 - 2），或将当前运行/保存的配置与配置修订版进行比较。除了配置差异之外，还会显示更正配置。您可以将所有更正命令导出到本地文件夹并更正配置。

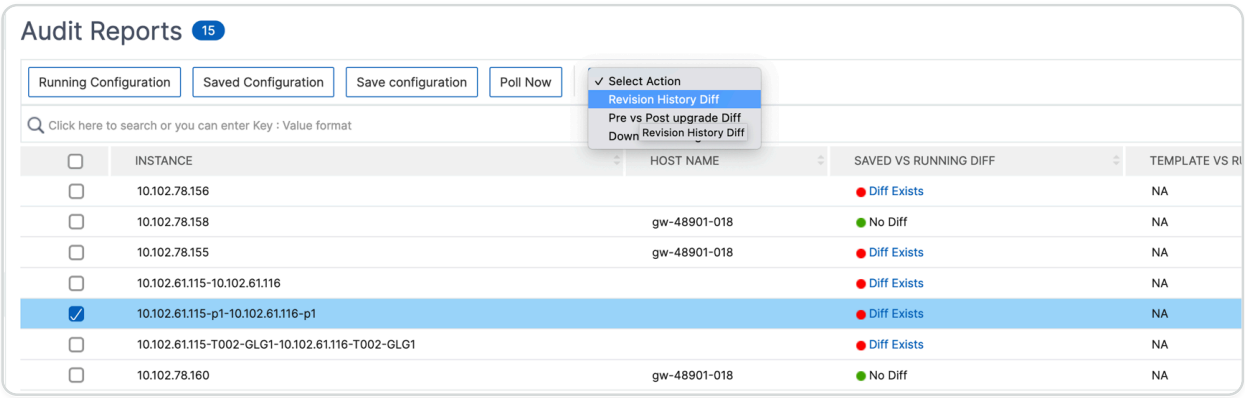
查看修订历史记录差异：

1. 导航到“**基础结构 > 配置审计**”。单击表示实例配置状态的圆环图。在打开的“**审计报告**”页面中，单击分区 NetScaler 实例。

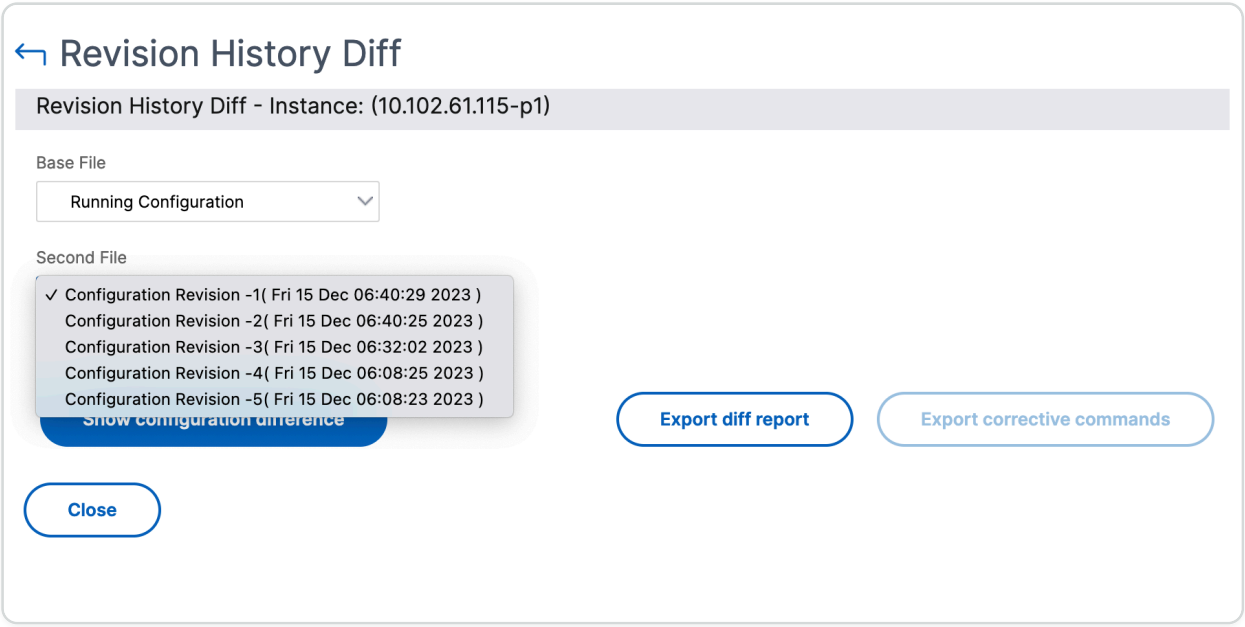
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 从“**操作**”菜单中，单击“**修订历史记录差异**”。



3. 在**修订历史差异**页面上，选择要比较的文件。例如，将“已保存配置”与“配置修订版 -1”进行比较，然后单击**显示配置差异**。



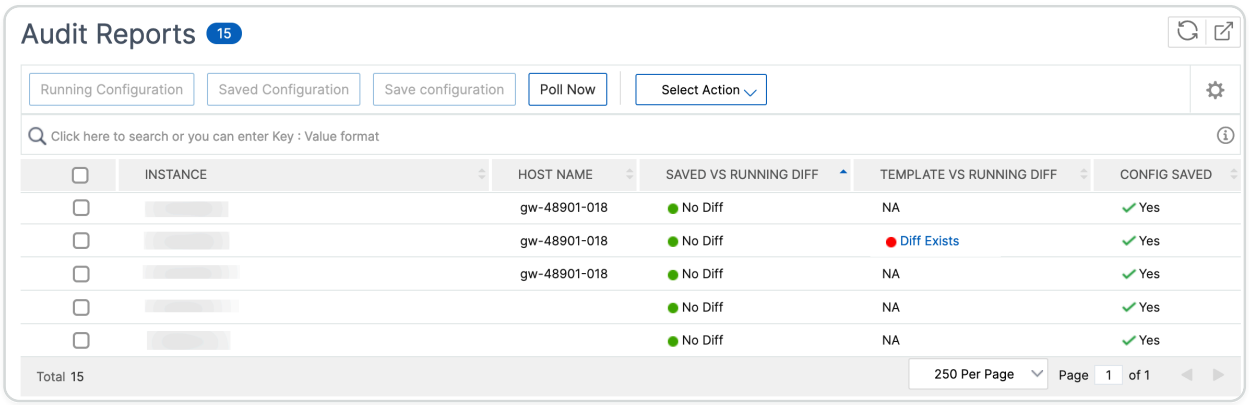
© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 然后，您可以查看所选分区 NetScaler 实例的五个最新配置文件之间的差异，如下所示。您还可以查看纠正性配置命令，并将这些纠正性命令导出到本地文件夹。这些纠正性命令是需要在基本文件上运行的命令，以便将配置恢复到所需状态（用于比较的配置文件）。

分区的审核模板允许您创建自定义配置模板并将其与分区实例关联。实例的运行配置与审核模板之间的任何差异都显示在**审核报告**页面的**模板与运行差异**列中。除了配置差异之外，还会显示纠正配置。您还可以将所有纠正命令导出到本地文件夹并纠正配置。

查看模板与运行差异：

1. 在**审核报告**页面上，单击分区 NetScaler 实例。



2. 如果审核模板与运行差异之间存在任何差异，则该差异将显示为超链接。单击超链接可查看差异（如果有）。除了配置差异之外，还会显示纠正配置。您还可以将所有纠正命令导出到本地文件夹并纠正配置。

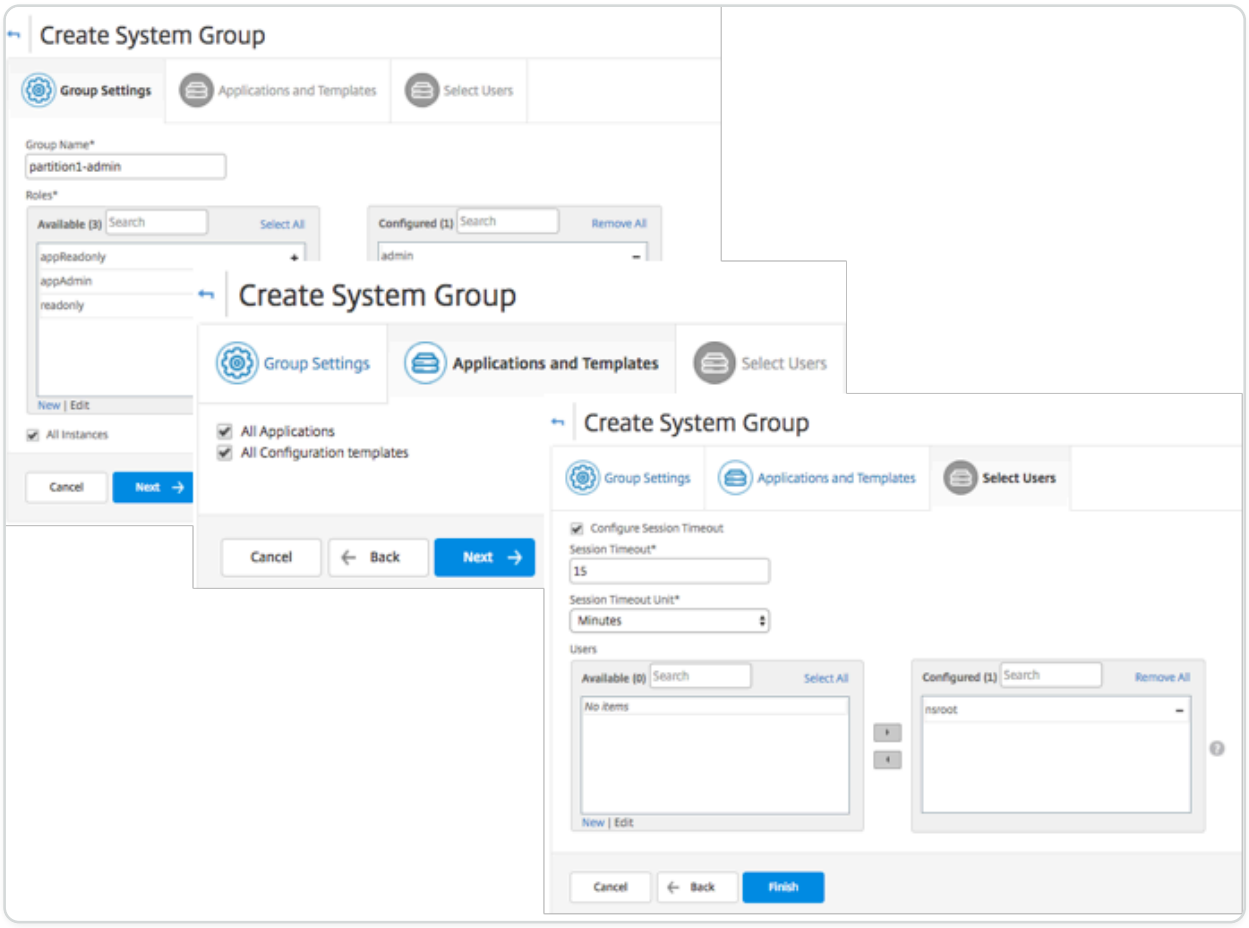
创建组：

1. 导航到**设置 > 用户管理 > 组**，然后单击**添加**。
2. 在**创建系统用户**页面上，指定以下内容：
   - **组设置**选项卡：输入组名称和角色权限。要允许访问特定实例，请清除**所有实例**复选框，然后在**选择实例**页面上选择您的实例。
   - **应用程序和模板**选项卡：您可以选择在所有应用程序和配置模板中使用此组。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **选择用户**选项卡：选择您要添加到此组的用户。您可以单击“**可用**”表中的“**新建**”链接来创建新用户。（可选）配置会话超时，您可以在其中配置用户保持活动状态的时间段。

3. 单击“**完成**”。



创建用户：

1. 导航到“**设置 > 用户管理 > 用户**”，然后单击“**添加**”。
2. 在“**创建系统用户**”页面上，指定用户名和密码。（可选）您可以启用外部身份验证并配置会话超时。
3. 通过将“**可用**”列表中的组名添加到“**已配置**”列表，将用户分配给组。
4. 单击“**创建**”。

现在注销并使用 user-p1 凭据登录。您只能查看和管理分配给您进行管理和监控的管理员分区。

创建 NetScaler 高可用性对

NetScaler 高可用性 (HA) 对可在停机或网络故障期间提供不间断运行。您可以使用 NetScaler Console 创建 NetScaler 实例的 HA 对。有关详细信息，请参阅 NetScaler 高可用性。

请执行以下步骤在 NetScaler Console 中创建 NetScaler 实例的 HA 对：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 导航到 **基础架构 > 实例 > NetScaler**。
2. 从列表中选择要创建 HA 对的 NetScaler 实例。

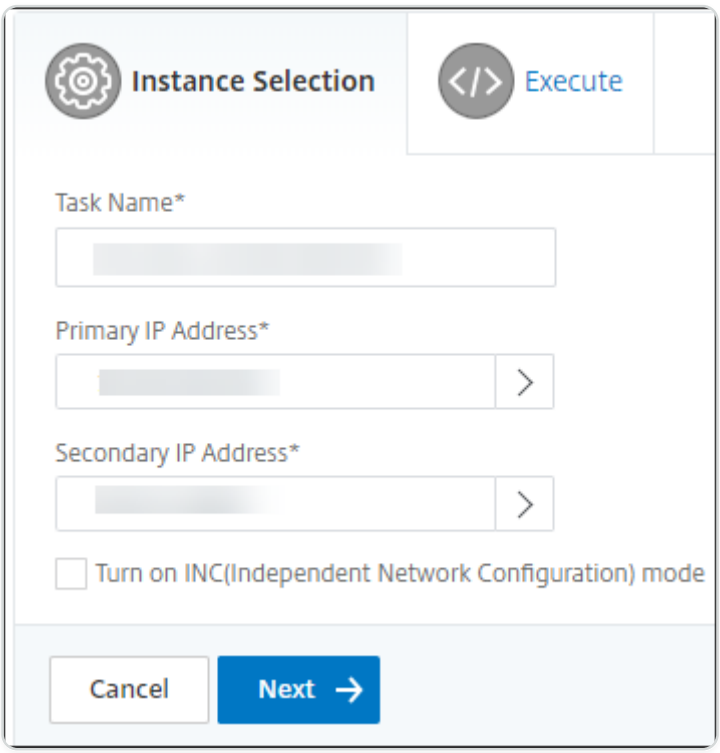
   所选实例将成为 HA 对中的主实例。
3. 单击选择 **操作 > 创建 HA 对**。
4. 在 **实例选择** 中，执行以下步骤：

   a. 在 **辅助 IP 地址** 中，单击以选择辅助实例。

   b. 选择要配置为 HA 对中辅助实例的 NetScaler 实例。

   c. 可选：如果 HA 对实例位于两个子网中，请选择 **启用 INC（独立网络配置）模式**。

   d. 单击 **下一步**。



5. 在 **执行** 中，您可以决定立即或稍后创建 HA 对。

   a. 在 **执行模式** 中，选择以下执行模式之一：

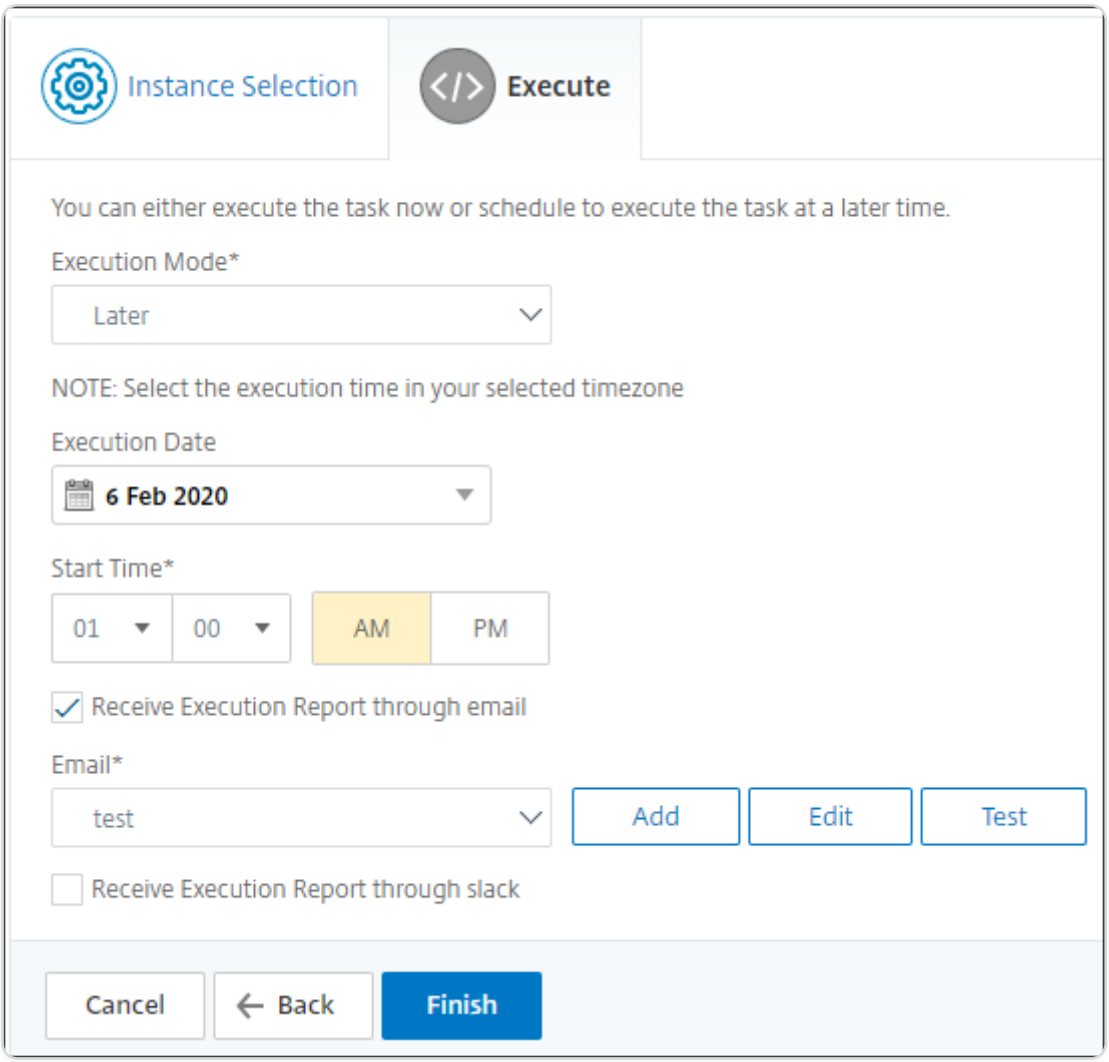
      - **立即** - 选择此选项可立即创建 HA 对。
      - **稍后** - 选择此选项可在特定日期和时间创建 HA 对。

   b. 如果您在“**执行模式**”列表中选择了“**稍后**”，请选择您要运行此任务的“**执行日期**”和“**开始时间**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

执行时间以 NetScaler Console 中设置的时区显示。

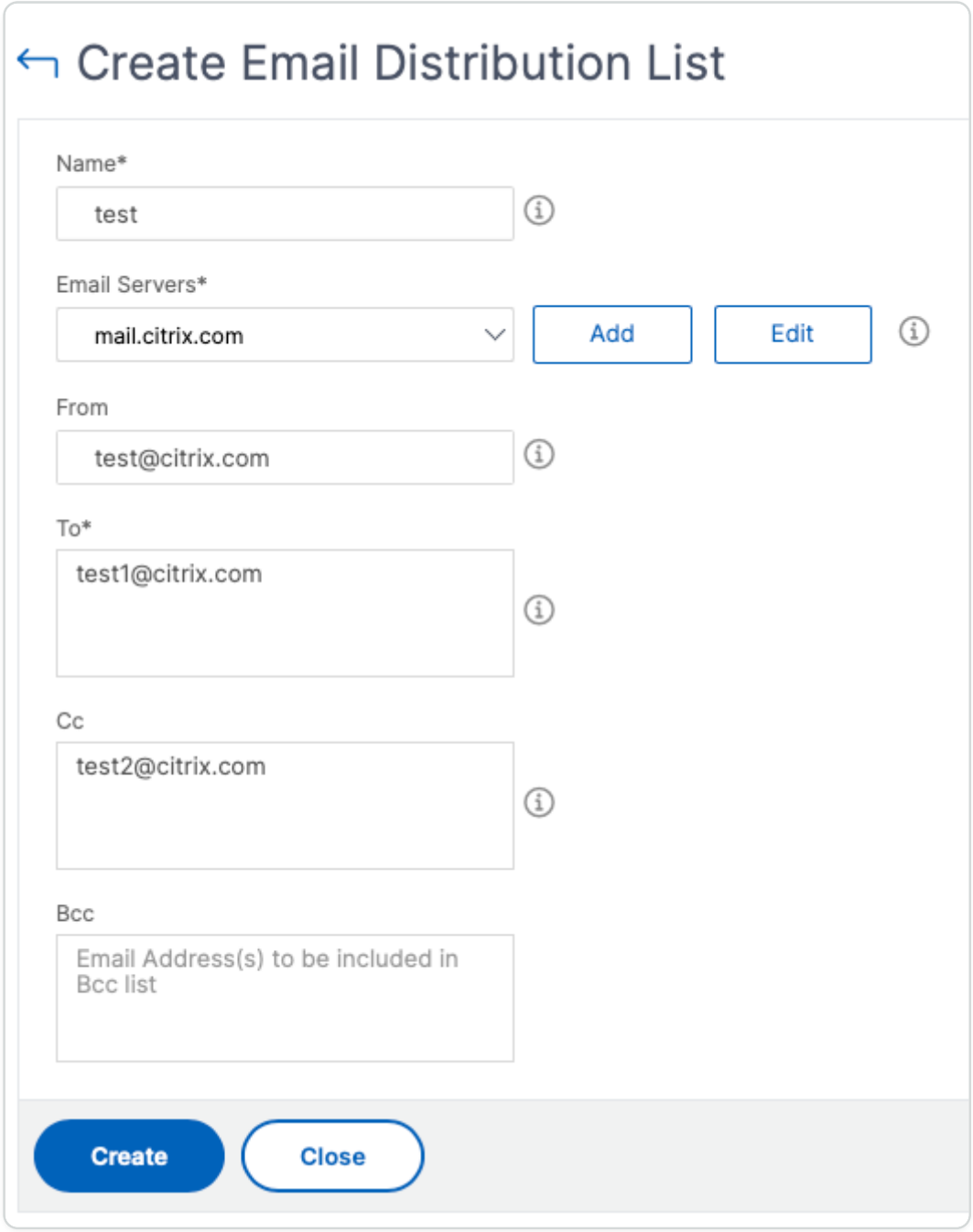


您可以通过以下方式接收此任务的执行报告：

- **电子邮件** - 从列表中选择电子邮件分发。

  要添加分发列表，请单击“**添加**”。指定添加分发列表所需的参数，然后单击“**创建**”。

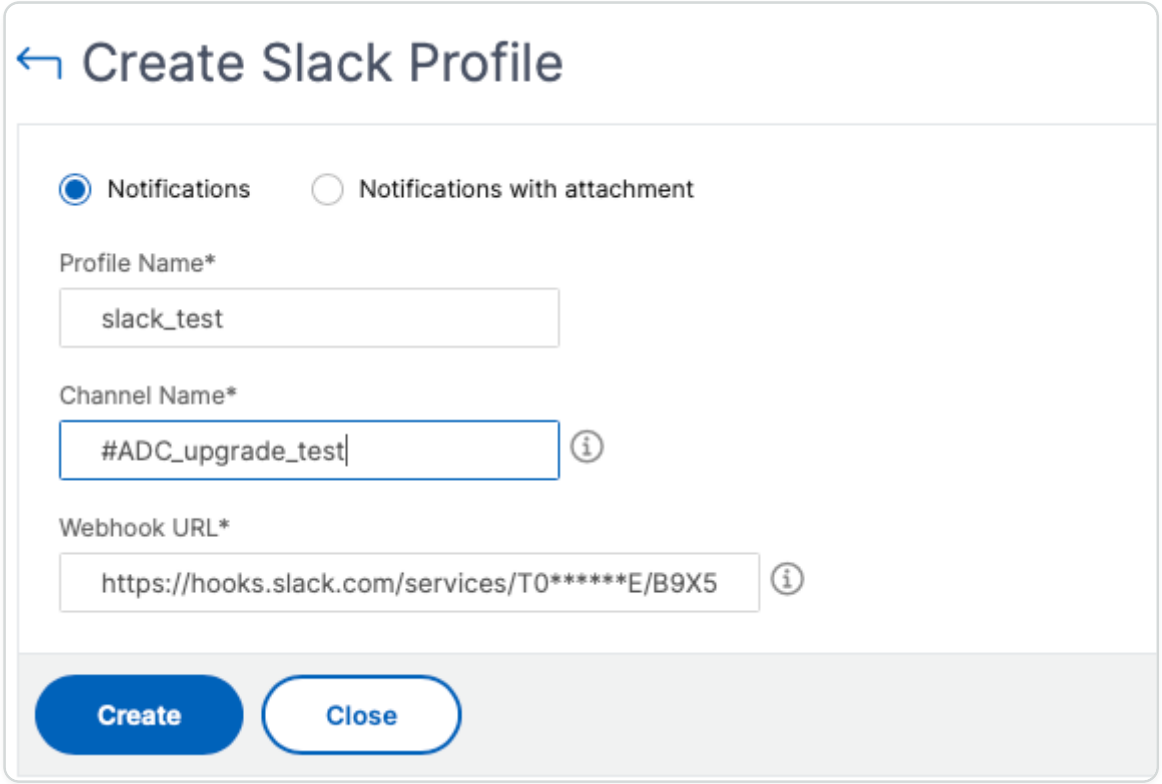
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Slack** - 从列表中选择 Slack 配置文件。

  要添加 Slack 配置文件，请单击“**添加**”。指定“**配置文件名称**”、“**频道名称**”和“**令牌**”，然后单击“**创建**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



备份和恢复 NetScaler 实例

您可以备份 NetScaler 实例的当前状态，然后使用备份文件将其恢复到相同状态。在升级实例之前或出于预防原因，请务必备份实例。稳定系统的备份使您能够在系统变得不稳定时将其恢复到稳定点。

有多种方法可以在 NetScaler 实例上执行备份和恢复。您可以使用 GUI 和 CLI 手动备份和恢复 NetScaler 配置。您还可以使用 NetScaler Console 执行自动备份和手动恢复。

NetScaler Console 使用 NITRO 调用以及安全外壳 (SSH) 和安全复制 (SCP) 协议备份您所管理的 NetScaler 实例的当前状态。

NetScaler Console 创建完整备份并恢复以下 NetScaler 实例类型：

- NetScaler SDX
- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

- 确保 NetScaler Console 配置文件具有备份和恢复 NetScaler 实例的管理员访问权限。
- 在 NetScaler Console 中，您无法对 NetScaler 群集执行备份和恢复操作。
- 您不能使用从一个实例获取的备份文件来恢复另一个实例。

备份文件以压缩的 TAR 文件形式存储在以下目录中：

```
/var/mps/tenants/root/device_backup/
```

为避免因磁盘空间不足而导致的问题，您可以在此目录中为每个 NetScaler 实例最多保存 50 个备份文件。

要备份和恢复 NetScaler 实例，您必须首先在 NetScaler Console 上配置备份设置。配置设置后，您可以选择单个 NetScaler 实例或多个实例，并创建这些实例中配置文件的备份。如有必要，您还可以使用这些备份文件恢复 NetScaler 实例。

配置实例备份设置

“**实例备份设置**”页面允许您在 NetScaler Console 上配置设置，以备份选定的 NetScaler 实例或多个实例：

1. 在 NetScaler Console 中，导航到“**设置**”>“**管理**”。
2. 在“**备份**”中，选择“**配置系统和实例备份**”。
3. 选择“**实例**”并指定以下内容：
   - **启用实例备份**：默认情况下，NetScaler Console 已启用 NetScaler 实例的备份功能。如果您不想为实例创建备份文件，请清除此选项。
   - **密码保护文件**：（可选）选择密码保护选项以加密备份文件。加密备份文件可确保备份文件中的所有敏感信息安全。

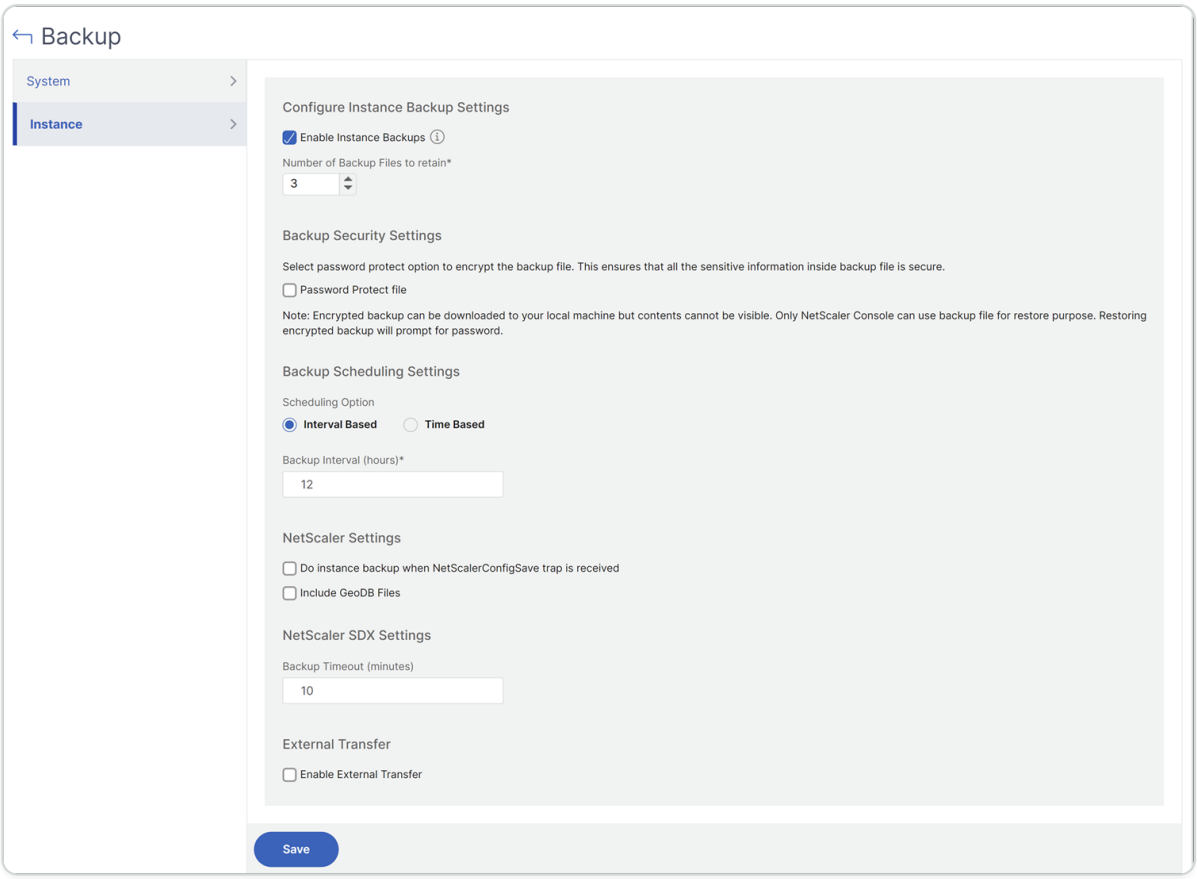
     注意：

     您可以将加密的备份文件下载到本地计算机，但无法使用 NetScaler Console GUI 或任何文本编辑器打开该文件。恢复加密备份文件时，系统会提示您提供密码。但是，您可以在系统上打开未加密的备份文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **要保留的备份文件数**：指定要在 NetScaler Console 中保留的备份文件数。每个 NetScaler 实例最多可以保留 50 个备份文件。默认值为三个备份文件。

> **注意：**
>
> 每个备份文件都需要一定的存储空间。建议您根据需要，在 NetScaler Console 上存储最佳数量的 NetScaler 备份文件。

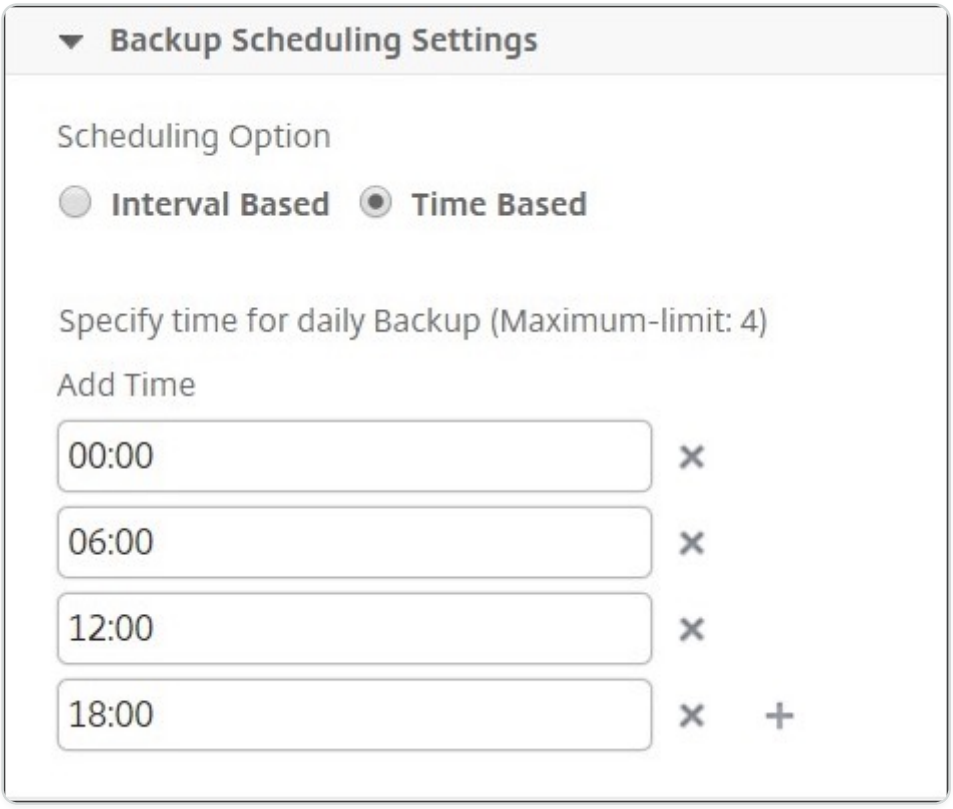


- **备份计划设置**：（可选）有两个用于创建备份文件的选项可用，但一次只能使用一个选项：

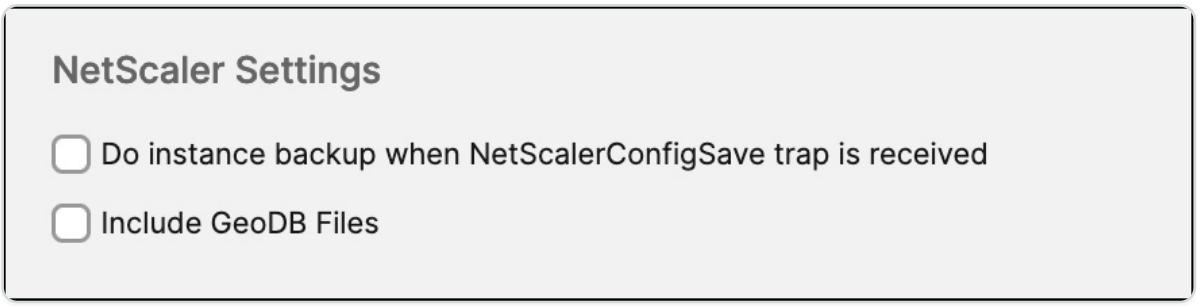
  a. 默认的备份计划选项是“基于间隔”。在指定间隔过去后，NetScaler Console 中会创建一个备份文件。默认备份间隔为 12 小时。

  b. 您还可以将计划备份的类型更改为“基于时间”。在此选项中，以 `hours:minutes` 格式指定时间，以便在指定时间备份实例。NetScaler Console 允许实例每天最多进行四次备份。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

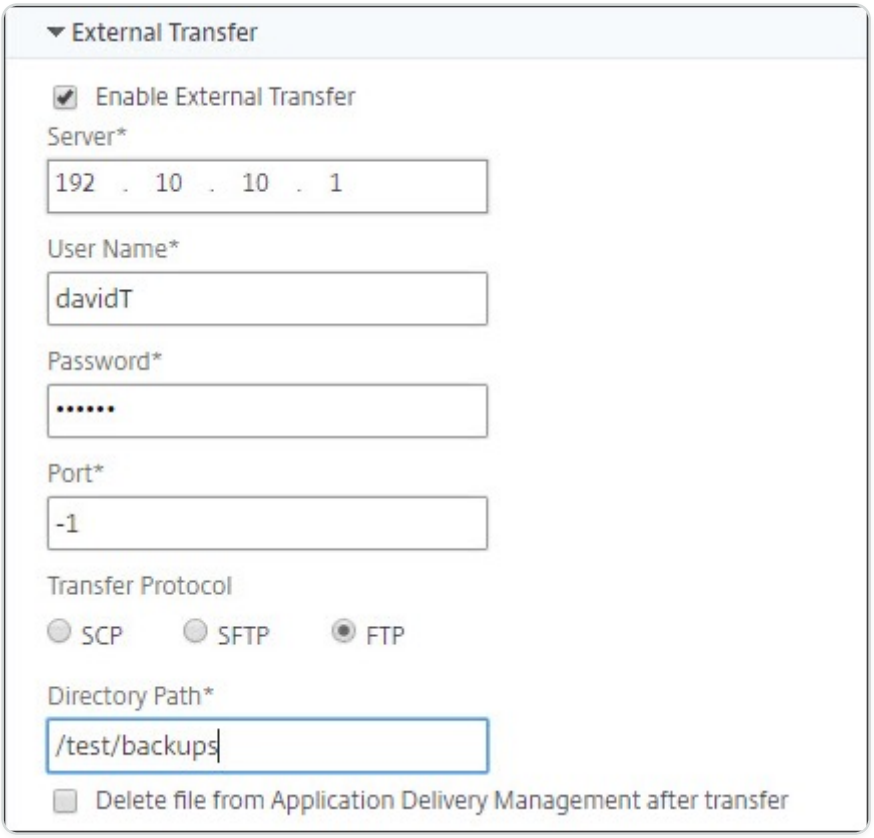


- **NetScaler 设置：**（可选）默认情况下，当 NetScaler Console 收到“NetScalerConfigSave”陷阱时，它不会创建备份文件。但是，您可以启用该选项，以便每当 NetScaler 实例向 NetScaler Console 发送“NetScalerConfigSave”陷阱时，都创建一个备份文件。每当实例上的配置保存时，NetScaler 实例都会发送“NetScalerConfigSave”。
- **地理数据库文件：**（可选）默认情况下，NetScaler Console 不备份地理数据库文件。您也可以启用该选项来创建这些文件的备份。



- **外部传输：**（可选）NetScaler Console 允许您将 NetScaler 实例备份文件传输到外部位置：
  a. 指定位置的 IP 地址。
  b. 指定您要将备份文件传输到的外部服务器的用户名和密码。
  c. 指定传输协议和端口号。
  d. 您可以指定文件必须存储的目录路径。
  e. 可选，您也可以在将备份文件传输到外部服务器后，从 NetScaler Console 中删除该文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

当任何选定的 NetScaler 实例备份失败时，NetScaler Console 会向自身发送 SNMP 陷阱或 Syslog 通知。

使用 NetScaler Console 为选定的 NetScaler 实例创建备份

如果要备份选定的 NetScaler 实例或多个实例，请执行此任务：

1. 在 NetScaler Console 中，导航到 **Infrastructure > Instances**。在 **Instances** 下，选择要在屏幕上显示的实例类型（例如，NetScaler VPX）。
2. 选择要备份的实例。
   - 对于 MPX、VPX 和 BLX 实例，从 **Select Action** 列表中选择 **Backup/Restore**。
   - 对于 SDX 实例，单击 **Backup/Restore**。
3. 在 **Backup Files** 页面上，单击 **Back Up**。
4. 您可以指定是否加密备份文件以提高安全性。您可以输入密码，也可以使用之前在 Instance Backup Settings 页面上指定的全局密码。
5. 单击 **Continue**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 NetScaler Console 还原 NetScaler 实例

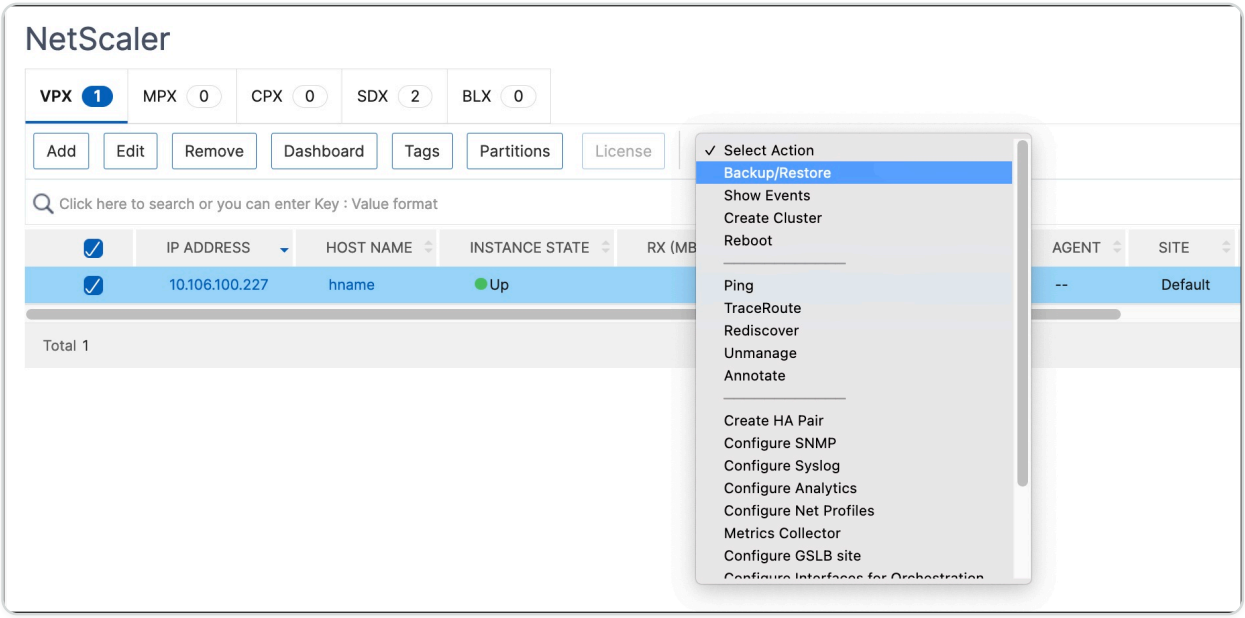
注意：

如果您的 NetScaler 实例处于 HA 对中，则需要注意以下事项：

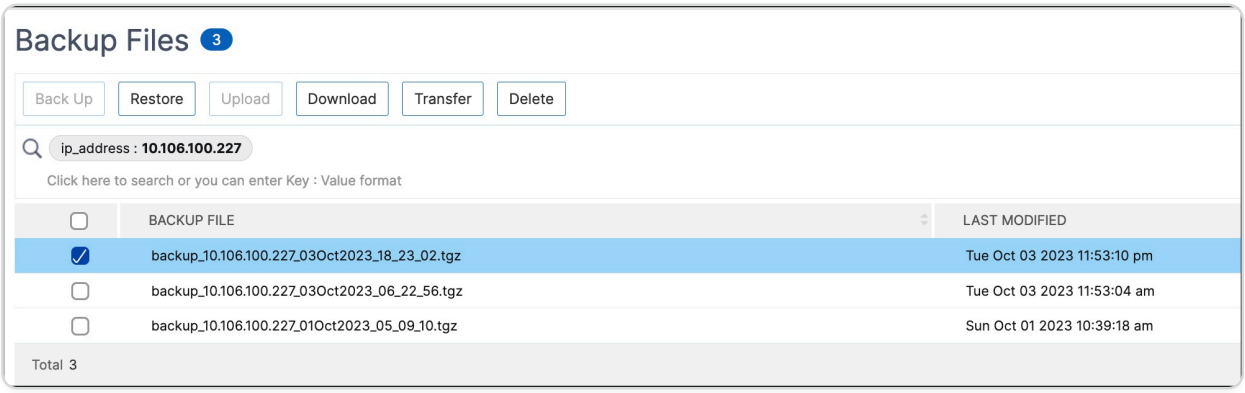
- 从创建备份文件的同一实例还原。例如，假设备份是从 HA 对的主实例中获取的。在还原过程中，请确保还原的是同一实例，即使它不再是主实例。
- 当您在主 NetScaler 实例上启动还原过程时，您无法访问主实例，并且辅助实例将更改为 **STAYSECONDARY**。一旦主实例上的还原过程完成，辅助 NetScaler 实例将从 **STAYSECONDARY** 更改为 **ENABLED** 模式，并再次成为 HA 对的一部分。在还原过程完成之前，主实例可能会出现停机。

执行此任务以使用您之前创建的备份文件还原 NetScaler 实例：

1. 导航到**基础架构 > 实例**，选择要恢复的实例，然后单击**选择操作 > 备份/恢复**。



2. 在**备份文件**页面上，选择包含要恢复的设置的备份文件，然后单击**恢复**。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 NetScaler Console 恢复 NetScaler SDX 设备

在 NetScaler Console 中，NetScaler SDX 设备的备份包括以下内容：

- 托管在设备上的 NetScaler 实例
- SVM SSL 证书和密钥
- 实例修剪设置（采用 XML 格式）
- 实例备份设置（采用 XML 格式）
- SSL 证书轮询设置（采用 XML 格式）
- SVM 数据库文件
- SDX 上存在的设备的 NetScaler 配置文件
- NetScaler 构建映像
- NetScaler XVA 映像，这些映像存储在以下位置： `/var/mps/sdx_images/`
- SDX 单一捆绑包映像 (SVM+XS)
- 第三方实例映像（如果已预配）

将您的 NetScaler SDX 设备恢复到备份文件中可用的配置。在设备恢复期间，整个当前配置将被删除。

如果您正在使用不同 NetScaler SDX 设备的备份来恢复 NetScaler SDX 设备，请确保在开始恢复过程之前，添加许可证并配置新设备的管理服务网络设置，使其与备份文件中的设置匹配。也就是说，新设备必须获得许可并满足备份文件的最低许可要求。例如，如果备份包含五个总计 5 GB 的 VPX 实例，则新设备也必须能够支持这些要求。或者，如果备份设备具有白金许可证，则新设备必须具有相同或更高的许可证。必须在新设备上正确配置网络设置，例如 IP 地址、子网掩码、网关、XenServer IP 地址和 DNS 服务器。

在恢复 SDX 设备之前，请确保备份的 SDX 设备平台变体与设备相同。您无法从不同的平台变体进行恢复。

注意：

在恢复 SDX RMA 设备之前，请确保备份版本与 RMA 版本相同或更高。

要从备份文件恢复 SDX 设备：

1. 在 NetScaler Console GUI 中，导航到 **Infrastructure > Instances > NetScaler > SDX**。选择一个实例。
2. 单击 **备份/恢复**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 选择您要恢复的同一实例的备份文件。
4. 单击 **重新打包备份**。

   备份 SDX 设备时，XVA 文件和映像会单独存储，以节省网络带宽和磁盘空间。因此，在恢复 SDX 设备之前，您必须重新打包备份文件。

   重新打包备份文件时，它会包含所有备份文件，以便恢复 SDX 设备。重新打包的备份文件可确保成功恢复 SDX 设备。
5. 选择已重新打包的备份文件，然后单击 **恢复**。

强制故障转移到辅助 NetScaler 实例

例如，如果您需要更换或升级主 Citrix NetScaler 实例，您可能需要强制进行故障转移。您可以从主实例或辅助实例强制进行故障转移。当您在主实例上强制进行故障转移时，主实例将变为辅助实例，辅助实例将变为主实例。只有当主实例能够确定辅助实例处于 UP 状态时，才能进行强制故障转移。

强制故障转移不会传播或同步。要查看强制故障转移后的同步状态，您可以查看实例的状态。

在以下任何情况下，强制故障转移都会失败：

- 您在独立系统上强制进行故障转移。
- 辅助实例已禁用或处于非活动状态。如果辅助实例处于非活动状态，您必须等待其状态变为 UP 才能强制进行故障转移。
- 辅助实例配置为保持辅助状态。

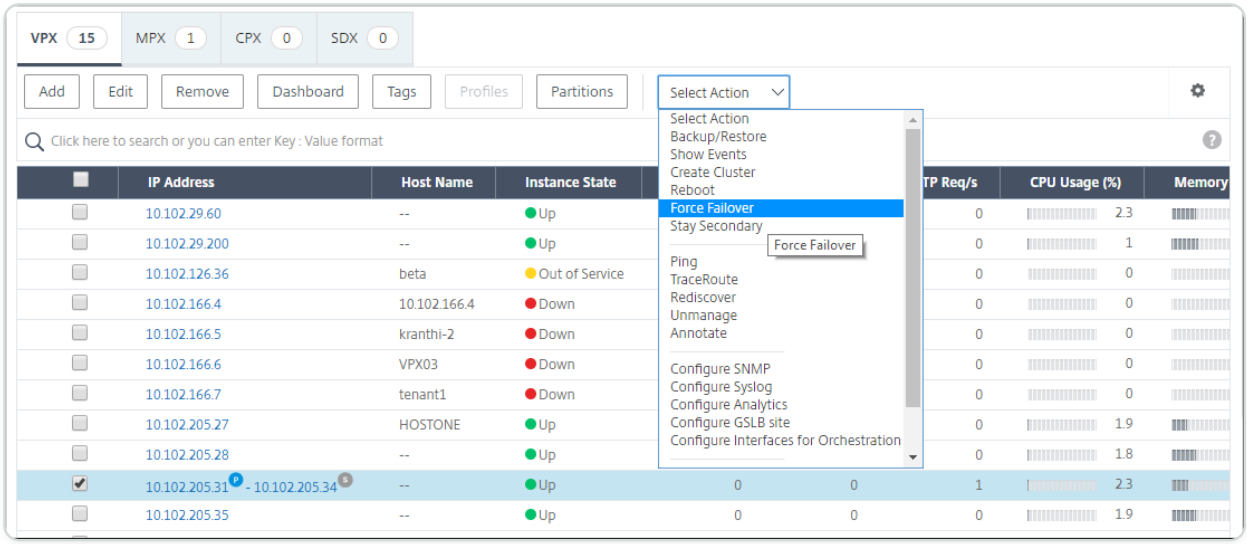
当您运行强制故障转移命令时，如果 NetScaler 实例检测到潜在问题，它会显示警告消息。该消息包含触发警告的信息，并在继续之前请求确认。

您可以在主实例或辅助实例上强制进行故障转移。

要使用 NetScaler Console 强制故障转移到辅助 NetScaler 实例：

1. 在 NetScaler Console 中，导航到 **基础架构 > 实例 > NetScaler > VPX** 选项卡，然后选择一个实例。
2. 从所选实例类型下列出的实例中，选择 HA 设置中的实例。
3. 从**操作**菜单中，选择**强制故障转移**。
4. 单击**是**以确认强制故障转移操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



强制辅助 NetScaler 实例保持辅助状态

在 HA 设置中，可以强制辅助节点保持辅助状态，无论主节点的状态如何。

例如，假设主节点需要升级，并且该过程需要几秒钟。在升级期间，主节点可能会停机几秒钟，但您不希望辅助节点接管。即使它检测到主节点发生故障，您也希望它保持辅助节点。

当您强制辅助节点保持辅助状态时，即使主节点停机，它也会保持辅助状态。此外，当您强制 HA 对中节点的状体保持辅助状态时，它不参与 HA 状态机转换。该节点的状态显示为 STAYSECONDARY。

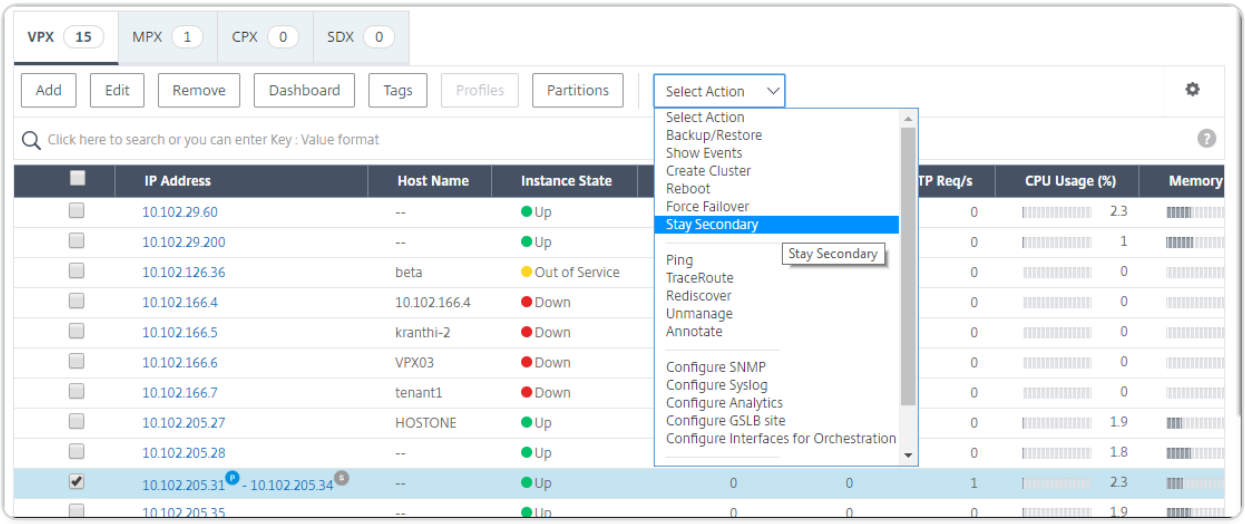
注意

当您强制系统保持辅助状态时，强制过程不会传播或同步。它仅影响您运行命令的节点。

使用 NetScaler Console 配置辅助 NetScaler 实例以保持辅助状态：

1. 在 NetScaler Console 中，导航到 **Infrastructure > Instances** > **NetScaler** > **VPX** 选项卡，然后选择一个实例。
2. 从所选实例类型下方的实例列表中选择 HA 设置中的实例。
3. 从 **Action** 菜单中，选择 **Stay Secondary**。
4. 单击 **Yes** 确认执行“Stay Secondary”操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



创建实例组

要创建实例组，您必须首先将所有 NetScaler 实例添加到 NetScaler Console。成功添加实例后，根据其实例系列创建实例组。创建实例组有助于您一次性对分组实例进行升级、备份或还原。

“**实例视图**”允许您查看所有托管实例及其关联组，从而轻松识别未映射的实例。您可以将未映射的实例分配给一个组。

使用 NetScaler Console 创建实例组

1. 在 NetScaler Console 中，导航到 **Infrastructure > Instances > Instance Groups**，然后单击 **Add**。
2. 为您的实例组指定一个名称，然后从 **Instance Family** 列表中选择 **NetScaler**。
3. 在 **Category** 中，选择 **Default** 选项。
4. 单击 **Select Instances**。在 **Select Instances** 页面上，选择要分组的实例，然后单击 **Select**。

   该表列出了所选实例及其详细信息。如果要从组中删除任何实例，请从表中选择该实例，然后单击 **Delete**。
5. 单击 **Create**。

创建实例组(/en-us/netscaler-application-delivery-management-software/media/024_instancegroups.png)

识别未映射的实例并将其添加到组中

1. 导航到 **基础架构 > 实例 > 实例组 > 实例视图**。
2. 选择一个或多个未映射的实例。
3. 单击 **添加实例组**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 从列表中选择所需的**实例组**。界面还会显示：
   - 可用的实例组。
   - 已映射到每个组的实例，有助于防止重复或不正确的分配。
5. 单击**保存**。所选实例将分配给所选组。

使用 NetScaler Console 在 SDX 上预配 NetScaler VPX 实例

您可以使用 NetScaler Console 在 SDX 设备上预配一个或多个 NetScaler VPX 实例。您可以部署的实例数量取决于您购买的许可证。如果添加的实例数量等于许可证中指定的数量，NetScaler Console 将限制您预配更多 NetScaler 实例。

在开始之前，请确保在 NetScaler Console 中添加要预配 VPX 实例的 SDX 实例。

要预配 VPX 实例，请执行以下操作：

1. 导航到 **基础架构 > 实例 > NetScaler**。
2. 在 **SDX** 选项卡中，选择要预配 VPX 实例的 SDX 实例。
3. 在 **选择操作** 中，选择 **预配 VPX**。

步骤 1 - 添加 VPX 实例

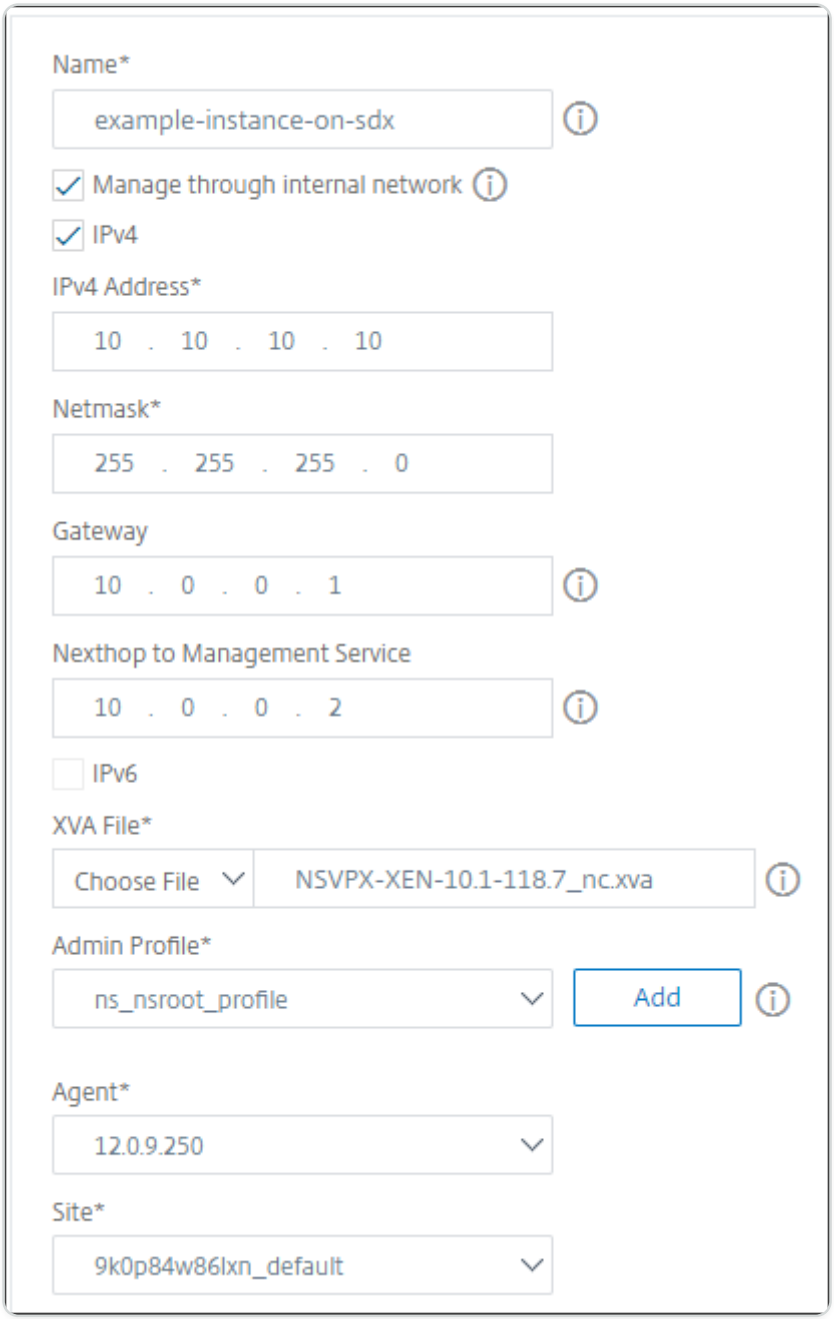
NetScaler Console 使用以下信息在 SDX 设备中配置 VPX 实例：

- **名称** - 为 NetScaler 实例指定一个名称。
- 在 SDX 和 VPX 之间建立通信网络。为此，请从列表中选择所需选项：
  - **通过内部网络管理** - 此选项为 NetScaler Console 和 VPX 实例之间的通信建立内部网络。
  - **IP 地址** - 您可以选择 **IPv4** 或 **IPv6** 地址或两者来管理 NetScaler VPX 实例。一个 VPX 实例只能有一个管理 IP（也称为 NetScaler IP）。您不能删除 NetScaler IP 地址。

    对于所选选项，为 IP 地址向 NetScaler Console 服务器分配子网掩码、默认网关和下一跳。
- **XVA 文件** - 选择要从中预配 VPX 实例的 XVA 文件。使用以下选项之一选择 XVA 文件。
  - **本地** - 从本地计算机选择 XVA 文件。
  - **设备** - 从控制台文件浏览器中选择 XVA 文件。
- **管理员配置文件** - 此配置文件提供对预配 VPX 实例的访问权限。使用此配置文件，NetScaler Console 从实例中检索配置数据。如果需要添加配置文件，请单击“**添加**”。
- **代理** - 选择要与实例关联的代理

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **站点** - 选择要添加实例的站点。



步骤 2 - 分配许可证

在“**许可证分配**”部分中，指定 VPX 许可证。您可以使用 Standard、Advanced 和 Premium 许可证。

- **分配模式** - 您可以为带宽池选择“**固定**”或“**突发**”模式。

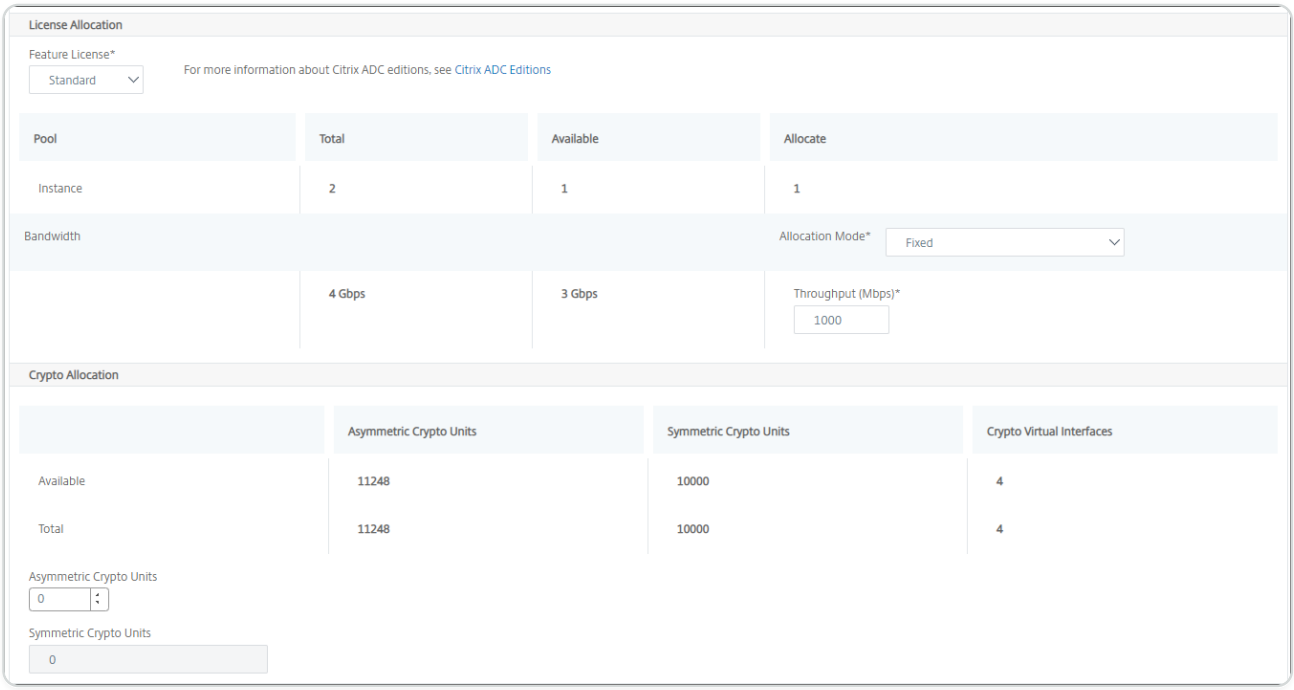
  如果选择“**突发**”模式，当达到固定带宽时，可以使用额外的带宽。

- **吞吐量** - 将总吞吐量（以 Mbps 为单位）分配给实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

为 SDX 设备上的 Citrix Secure Web Gateway™ (SWG) 实例购买单独的许可证（适用于 Secure Web Gateway 的 SDX 2 实例附加包）。此实例包不同于 SDX 平台许可证或 SDX 实例包。



从 SDX 12.0 57.19 版本开始，管理加密容量的界面已更改。

步骤 3 - 分配资源

在**资源分配**部分，为 VPX 实例分配资源以维持流量。

- **总内存 (MB)** - 为实例分配总内存。最小值为 `2048` MB。
- **每秒数据包数** - 指定每秒传输的数据包数量。
- **CPU** - 为实例指定 CPU 核心数量。您可以使用共享或专用 CPU 核心。

  当您为实例选择共享核心时，其他实例可以在资源短缺时使用该共享核心。

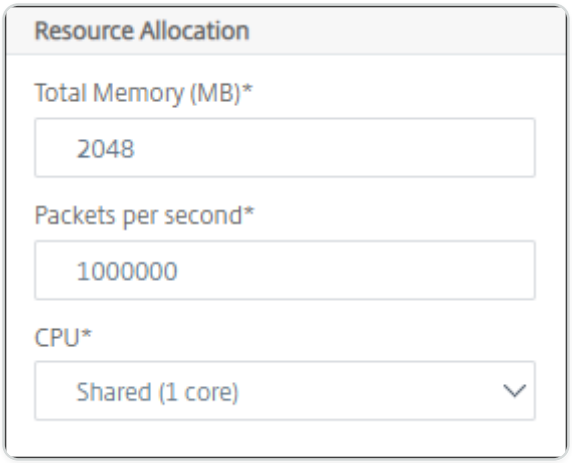
  重新启动已重新分配 CPU 核心的实例，以避免任何性能下降。

  如果您使用的是 SDX 25000xx 平台，则最多可以为实例分配 16 个核心。此外，如果您使用的是 SDX 2500xxx 平台，则最多可以为实例分配 11 个核心。

  注意

  对于一个实例，您可以配置的最大吞吐量为 180 Gbps。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



下表列出了支持的 VPX、单一捆绑映像版本以及您可以分配给实例的核心数量：

平台名称	总核心数	可用于 VPX 预配的总核心数	可分配给单个实例的最大核心数
SDX 8015、SDX 8400 和 SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500、SDX 13500、SDX 14500、SDX 16500、SDX 18500 和 SDX 20500	12	10	5
SDX 11515、SDX 11520、SDX 11530、SDX 11540 和 SDX 11542	12	10	5
SDX 17500、SDX 19500 和 SDX 21500	12	10	5
SDX 17550、SDX 19550、SDX 20550 和 SDX 21550	12	10	5
SDX 14020、SDX 14030、SDX 14040、SDX 14060、SDX 14080 和 SDX 14100	12	10	5

© 1997–2026 Citrix Systems, Inc. All rights reserved.

平台名称	总核心数	可用于 VPX 预配的总核心数	可分配给单个实例的最大核心数
SDX 22040、SDX 22060、SDX 22080、SDX 22100 和 SDX 22120	16	14	7
SDX 24100 和 SDX 24150	16	14	7
SDX 14020 40G、SDX 14030 40G、SDX 14040 40G、SDX 14060 40G、SDX 14080 40G 和 SDX 14100 40G	12	10	10
SDX 14020 FIPS、SDX 14030 FIPS、SDX 14040 FIPS、SDX 14060 FIPS、SDX 14080 FIPS 和 SDX 14100. FIPS	12	10	5
SDX 14040 40S、SDX 14060 40S、SDX 14080 40S 和 SDX 14100 40S	12	10	5
SDX 25100A、25160A、25200A	20	18	9
SDX 25100-40G、25160-40G、25200-40G	20	18	16（如果版本为 11.1-51.x 或更高）；9（如果版本为 11.1-50.x 或更低；所有 11.0 和 10.5 版本）
SDX 26100、26160、26200、26250	28	26	13

© 1997–2026 Citrix Systems, Inc. All rights reserved.

平台名称	总核心数	可用于 VPX 预配的总核心数	可分配给单个实例的最大核心数
15000-50G	16	14	7
SDX 16000	32	30	16
SDX 9100	10	9	9

注意

在 SDX 26xxx 平台上，最多可将 26 个 CPU 核心分配给 VPX 实例。如果将加密单元分配给实例，则最大核心数取决于加密单元和数据接口的数量。

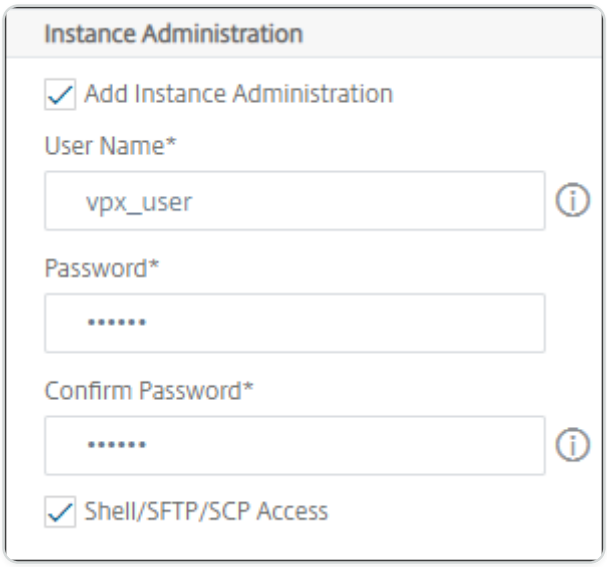
例如，如果您为实例分配 24000 个加密单元，则可以为该实例分配 24 个 CPU 核心和最多两个数据接口。SDX 设备将数据接口和加密单元视为 PCI 设备。对于 26000 个加密单元，VPX 实例预配将失败，因为没有空间添加数据接口。

步骤 4 - 添加实例管理

您可以为 VPX 实例创建管理员用户。为此，请在“**实例管理**”部分中选择“**添加实例管理**”。

指定以下详细信息：

- **用户名**：NetScaler 实例管理员的用户名。此用户具有超级用户访问权限，但无权访问用于配置 VLAN 和接口的网络命令。
- **密码**：指定用户名的密码。
- **Shell/Sftp/Scp 访问**：允许 NetScaler 实例管理员的访问权限。此选项默认处于选中状态。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

步骤 5 - 指定网络设置

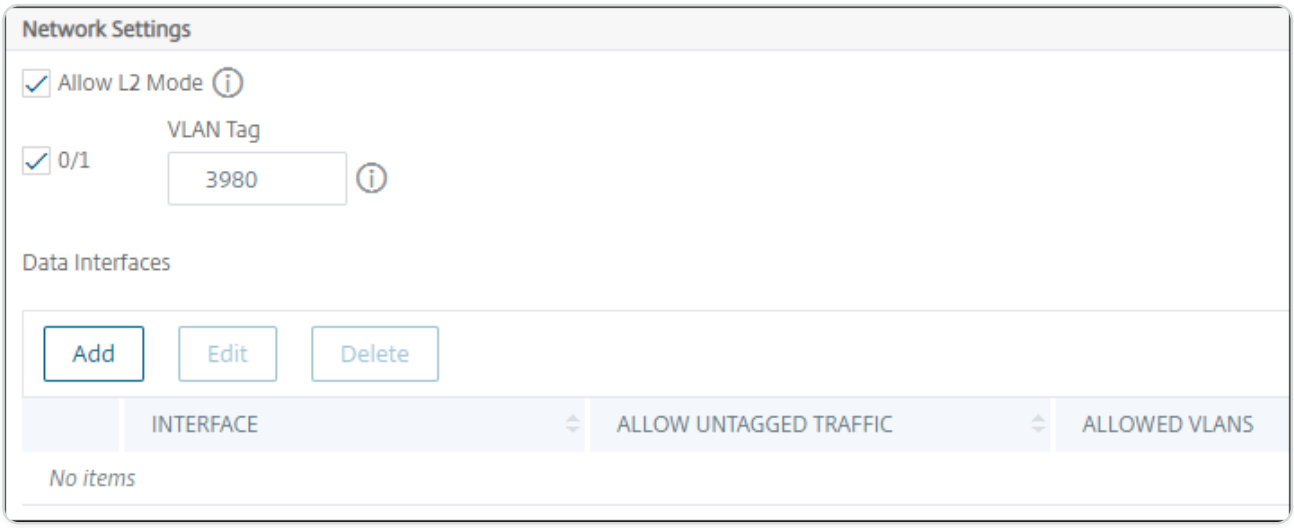
为实例选择所需的网络设置：

- **在网络设置下允许 L2 模式** - 您可以在 NetScaler 实例上允许 L2 模式。在网络设置下选择“允许 L2 模式”。在此之前，请登录实例并启用 L2 模式。

  > **注意**
  >
  > 如果禁用实例的 L2 模式，则必须登录该实例并从该实例禁用 L2 模式。否则，在重新启动实例后，可能会导致所有其他 NetScaler 模式被禁用。

- **0/1** - 在“**VLAN 标签**”中，为管理接口指定一个 VLAN ID。
- **0/2** - 在“**VLAN 标签**”中，为管理接口指定一个 VLAN ID。

默认情况下，接口 **0/1** 和 **0/2** 已选中。



在 **数据接口** 中，单击 **添加** 以添加数据接口并指定以下内容：

- **接口** - 从列表中选择接口。

  > **注意**
  >
  > 您添加到实例的接口 ID 不一定与 SDX 设备上的物理接口编号相对应。

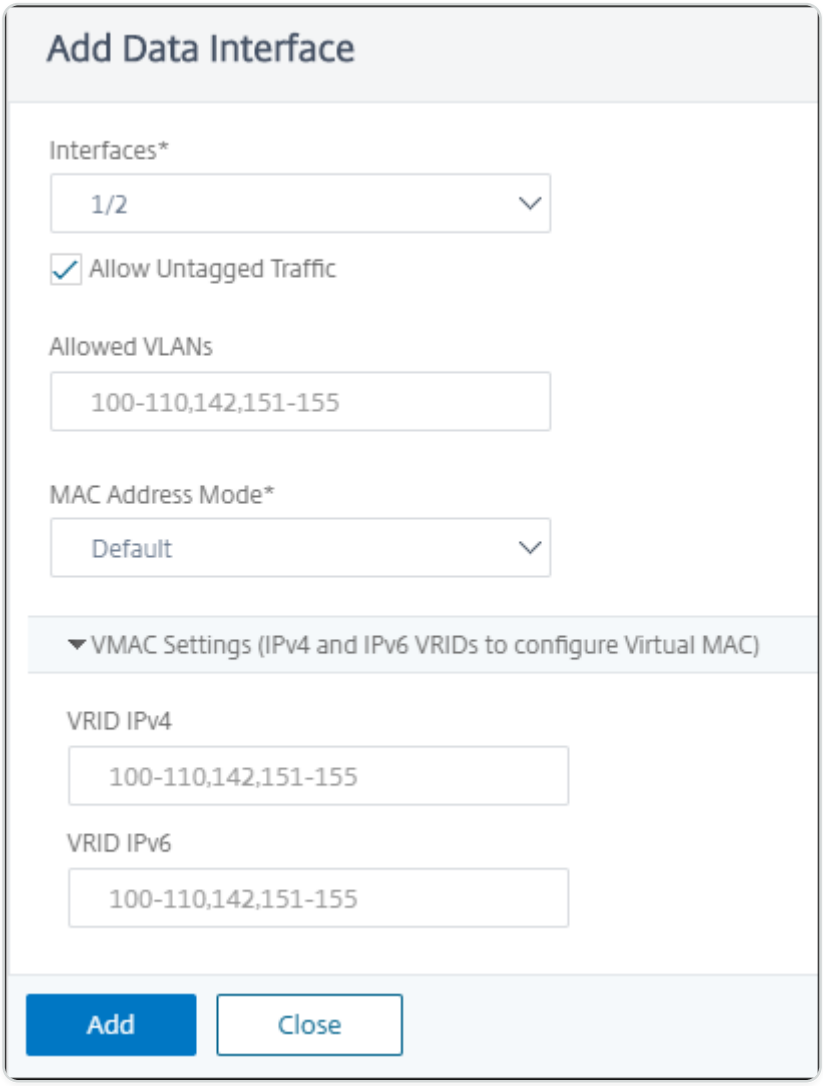
  例如，您与 instance-1 关联的第一个接口是 SDX 接口 1/4，当您在该实例中查看接口设置时，它显示为接口 1/1。此接口表示它是您与 instance-1 关联的第一个接口。

- **允许的 VLAN** - 指定可与 NetScaler 实例关联的 VLAN ID 列表。
- **MAC 地址模式** - 为实例分配 MAC 地址。从以下选项中选择：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **默认** - Citrix Workspace 分配 MAC 地址。
- **自定义** - 选择此模式以指定覆盖生成的 MAC 地址的 MAC 地址。
- **生成** - 使用之前设置的基本 MAC 地址生成 MAC 地址。

- **VMAC 设置（用于配置虚拟 MAC 的 IPv4 和 IPv6 VRID）**
  - **VRID IPV4** - 标识 VMAC 的 IPv4 VRID。可能的值：1–255。有关详细信息，请参阅 在接口上配置 VMAC。
  - VRID IPV6 - 标识 VMAC 的 IPv6 VRID。可能的值：1–255。有关详细信息，请参阅 在接口上配置 VMAC。



点击 **添加**。

步骤 6 - 指定管理 VLAN 设置

管理服务和 VPX 实例的管理地址 (NSIP) 位于同一子网中，并且通信通过管理接口进行。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

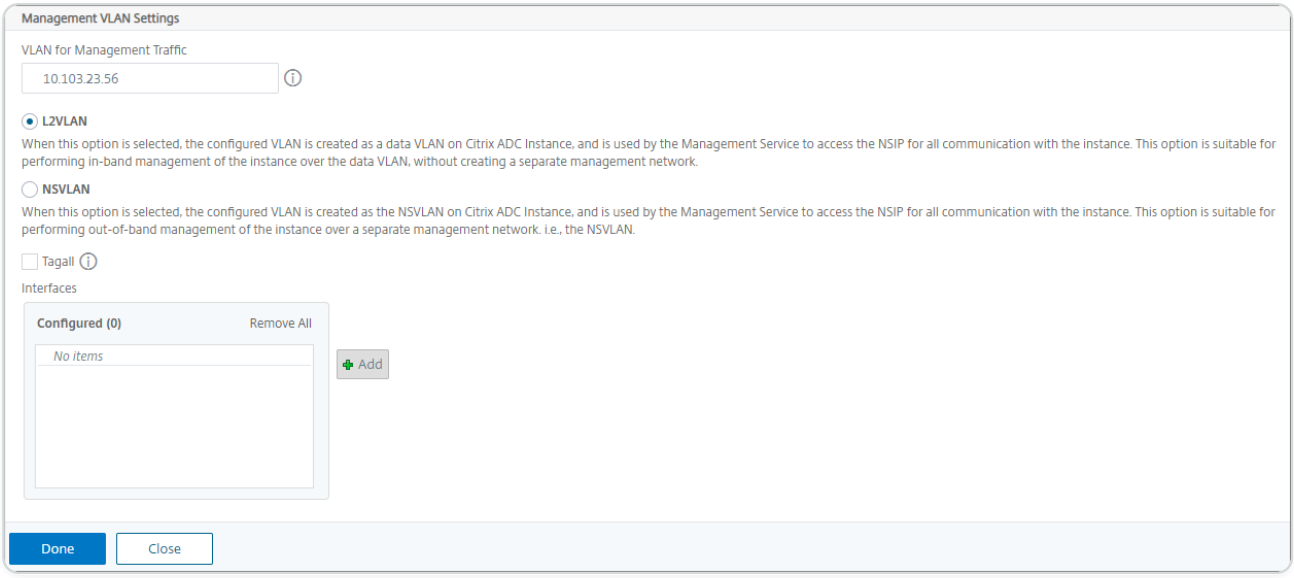
如果管理服务和实例位于不同的子网中，请在预置 VPX 实例时指定一个 VLAN ID。因此，当实例处于活动状态时，可以通过网络访问它。

如果您的部署要求在预置 VPX 实例时 NSIP 只能通过选定的接口访问，请选择 **NSVLAN**。并且，NSIP 将无法通过其他接口访问。

- HA 心跳仅在属于 NSVLAN 的接口上发送。
- 您只能从 VPX XVA 版本 `9.3-53.4` 及更高版本配置 NSVLAN。

重要

- 预置 VPX 实例后，您无法更改此设置。
- 如果未选择 **NSVLAN**，VPX 实例上的 `clear config full` 命令会删除 VLAN 配置。



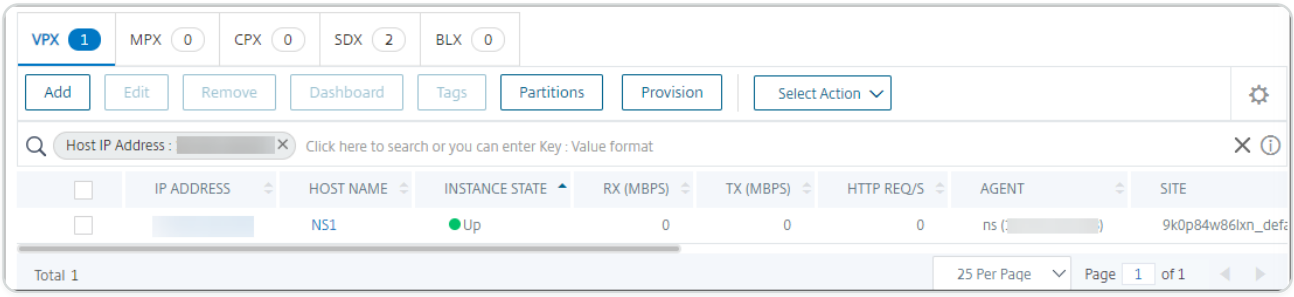
点击 **完成** 以预置 VPX 实例。

查看已预置的 VPX 实例

要查看新预置的实例，请执行以下操作：

1. 导航到 **基础架构 > 实例 > NetScaler**。
2. 在 **VPX** 选项卡中，通过 **主机 IP 地址** 属性搜索实例，并为其指定 SDX 实例 IP。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在 VMware ESX 上预配 NetScaler VPX 实例

您可以使用 NetScaler Console 在 VMware ESX 中自动化 NetScaler VPX 实例的部署和管理。当您使用 NetScaler Console 在 VMware ESX 上预配 NetScaler VPX 实例时，该实例可在 NetScaler Console GUI 中立即进行管理。

NetScaler Console 使用已部署实例的 NetScaler 模板在 VMware ESX 中预配新实例。它存储 VMware vCenter 的数据中心，其中所需的 VMware ESX 服务器详细信息位于一个站点中。此外，它还使用云访问配置文件来访问 VMware vCenter 并在 VMware ESX 上部署 VPX。

先决条件

在 VMware ESX 中预配 NetScaler VPX 实例之前，请确保完成以下操作：

1. 安装受支持的 VMware ESXi 版本（6.0、6.5 和 6.7）。
2. 在满足最低系统要求的管理工作站上安装 VMware Client。
3. 下载 NetScaler VPX 安装文件。
4. 将 NetScaler VPX 文件转换为 ESX 中的模板。
5. 为 NetScaler Console 创建访问 VMware vCenter 的权限。
6. 在 NetScaler Console 中创建站点。

将 NetScaler VPX 文件转换为模板

NetScaler Console 使用由 NetScaler VPX 文件转换而来的 ESX 中的 NetScaler 模板。执行以下步骤将 VPX 文件转换为模板。

1. 使用 NetScaler 安装文件在 VMware 上部署 NetScaler VPX 实例。

   首次部署 VPX 实例时，请使用 NetScaler 安装文件。有关详细信息，请参阅 在 VMware 上安装 NetScaler VPX 实例。

2. 右键单击已部署的 VM，然后选择 **模板**。
3. 单击 **转换为模板**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

将 VPX 安装文件转换为模板(/en-us/netscaler-application-delivery-management-software/media/convert-to-template.png)

为 NetScaler Console 访问 VMware vCenter 创建权限

要在 VMware vCenter 中启用 NetScaler Console 进行预配和管理，请按照以下步骤操作：

1. 创建具有特权的自定义角色
   a. 登录 VMware vCenter 并导航到 **角色** 部分。
   b. 为 NetScaler Console 创建一个定制的自定义角色。
   c. 分配以下特权：

```
Datastore.AllocateSpace

Resource.AssignVMToPool

VirtualMachine.Config.AdvancedConfig

VirtualMachine.Inventory.CreateFromExisting

VirtualMachine.Inventory.Delete

VirtualMachine.Interact.PowerOff

VirtualMachine.Interact.PowerOn

VirtualMachine.Provisioning.DeployTemplate
```

2. 创建用户
   a. 定义角色后，导航到 **用户和组** 部分。
   b. 为 NetScaler Console 创建一个用户以访问 VMware vCenter。
   c. 为新创建的用户提供密码。
3. 将角色与用户关联
   a. 导航到 **全局权限** 部分并将自定义角色与用户关联。
   b. 此关联为 NetScaler Console 提供在 VMware vCenter 上执行必要操作的权限。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

列出的权限是 NetScaler Console 访问 VMware vCenter 的最低要求。创建具有有限权限的用户是可选的。如果任何用户拥有的权限包含指定权限的超集，则该用户可以提供这些凭据。

有关在 VMware vCenter 中配置具有权限的用户角色的更多信息，请参阅配置用户访问。

在 NetScaler Console 中创建站点

在 NetScaler Console 中创建站点并添加 VMware ESX 详细信息。

1. 在 NetScaler Console 中，导航到 **基础架构 > 实例 > 站点**。
2. 单击**添加**。
3. 在**选择云**窗格中，
   a. 选择**数据中心**作为**站点**类型。
   b. 从**类型**列表中选择 **VMware vCenter**。
   c. 单击**下一步**。
4. 在**选择区域**窗格中，
   a. 在**云访问配置文件**窗格中，选择为您的 VMware ESX 创建的配置文件。如果没有配置文件，请创建一个。
   b. 要创建云访问配置文件，请单击**添加**并指定以下内容：
      - **名称** – 指定一个名称，用于在 NetScaler Console 中标识您的云访问配置文件。
      - **IP 地址** – 指定要预置 VPX 实例的 VMware vCenter 服务器的 IP 地址。
      - **用户名** – 指定用于访问 VMware vCenter 服务器的用户名。
      - **密码** – 指定用于访问 VMware vCenter 服务器的密码并确认密码。

      创建云访问配置文件(/en-us/netscaler-application-delivery-management-software/media/cap-vmware.png)
   c. 在**网络 (数据中心)**中，选择您拥有 NetScaler 模板的数据中心。
   d. 指定**站点名称**。
   e. 指定**区域**、**纬度**和**经度**，以标识数据中心的地理位置。
   f. 单击**完成**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 VMware 中创建用于实例预置的站点(/en-us/netscaler-application-delivery-management-software/media/create-site.png)

在 VMware ESX 上预置实例

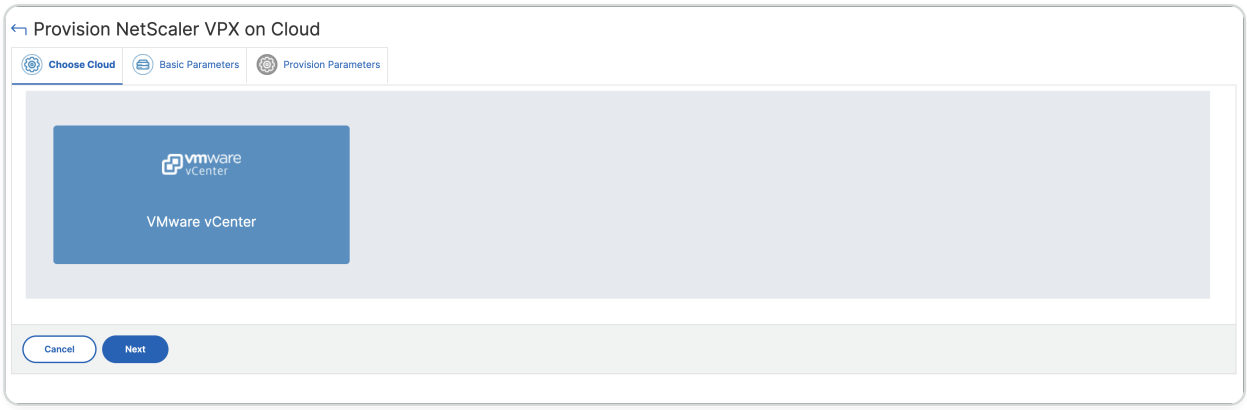
使用与您的 VMware ESX 关联的站点来预置 NetScaler VPX 实例。

注意：

目前，NetScaler Console 仅支持预置独立 NetScaler 实例。

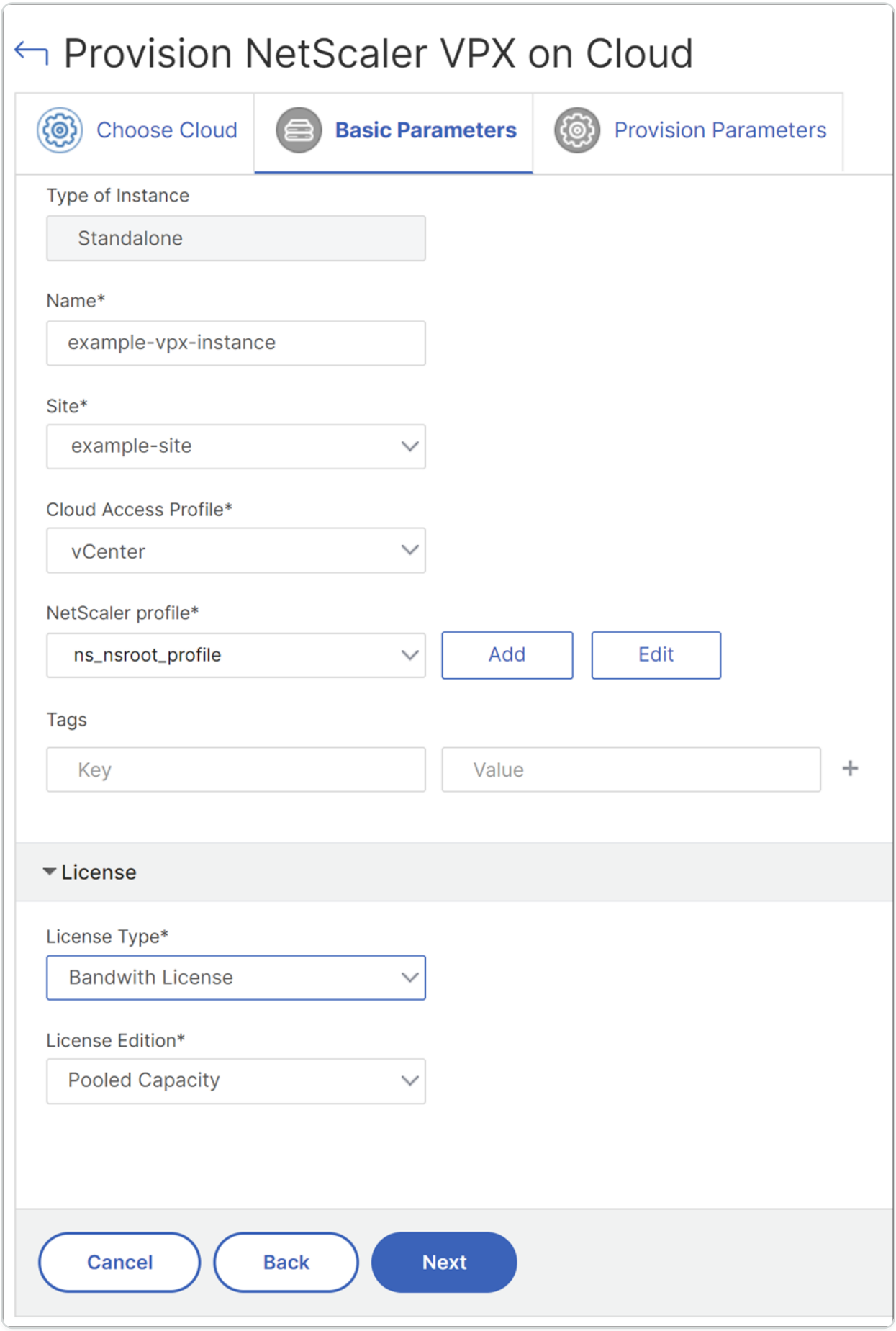
1. 在 NetScaler Console 中，导航到**基础结构 > 实例 > NetScaler**。
2. 在 **VPX** 选项卡中，单击 **Provision**。

   此选项将显示 **在云中预配 NetScaler VPX** 页面。
3. 选择 **VMware vCenter**，然后单击 **Next**。



4. 在 **基本参数** 中，指定以下内容：
   - **名称** – 指定实例的名称。
   - **站点** – 选择您之前创建的站点。
   - **云访问配置文件** – 选择在站点创建期间创建的云访问配置文件。
   - **NetScaler 配置文件** – 选择用于提供身份验证的 NetScaler 配置文件。
   - **许可证** – 使用池化容量许可将许可证应用于实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



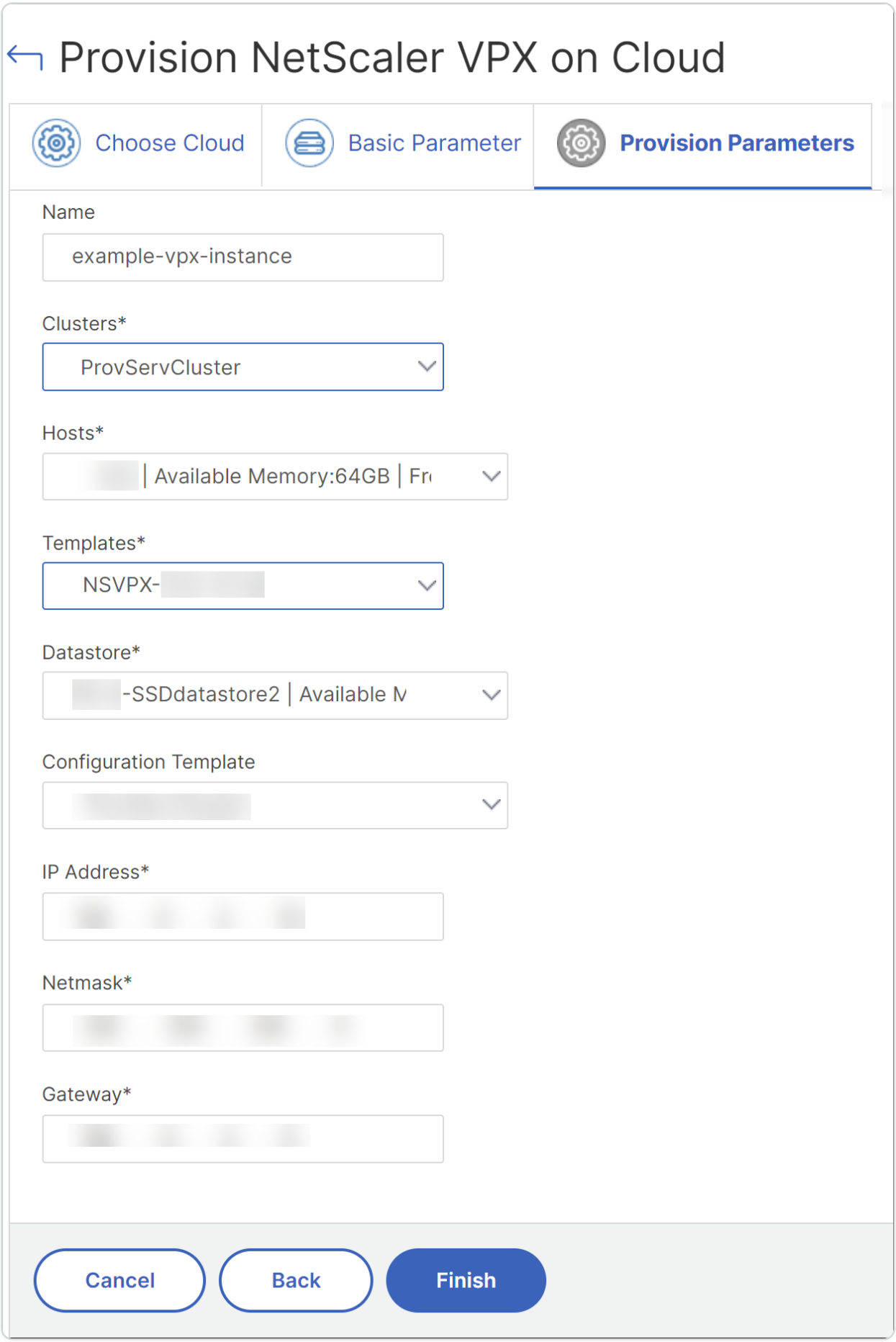
5. 单击 **Next**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. 在 **预配参数** 中，指定以下详细信息：

   - **群集** – 选择要预配实例的群集。
   - **主机** – 从列表中选择所需的主机。
   - **模板** – 从列表中选择要应用于实例的模板。
   - **数据存储** – 从列表中选择数据存储。
   - **IP 地址** – 为实例指定一个 IP 地址。
   - **网络掩码** – 为实例指定一个网络掩码。
   - **网关** – 为实例指定一个网关。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. 单击**完成**以预配 VPX 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重新发现多个 NetScaler VPX 实例

您可以在 NetScaler Console 设置中重新发现多个 NetScaler VPX 实例。此外，当您想要查看这些实例的最新状态和配置时，也可以重新发现多个 NetScaler VPX 实例。NetScaler Console 服务器会重新发现所有 NetScaler VPX 实例，并检查 Citrix NetScaler 实例是否可访问。

重新发现多个 NetScaler VPX 实例：

1. 在 Web 浏览器中，键入 NetScaler Console 服务器的 IP 地址（例如，`<http://192.168.100.1>`）。
2. 在“**用户名**”和“**密码**”字段中，输入管理员凭据。默认管理员凭据为 `nsroot` 和 `nsroot`。
3. 导航到 **Infrastructure（基础结构）> Instances（实例）> NetScaler** > **VPX** 选项卡，然后选择要重新发现的实例。
4. 在“**选择操作**”菜单中，单击“**重新发现**”。
5. 当出现运行“重新发现”实用程序的确认消息时，单击“**是**”。

   屏幕会报告每个 NetScaler VPX 实例的重新发现进度。

取消管理实例

如果您想停止 NetScaler Console 与网络中实例之间的信息交换，可以取消管理这些实例。

取消管理 NetScaler 实例会使该 NetScaler 实例处于未管理状态或从 NetScaler Console 注销。NetScaler Console 将无法再联系或与该 NetScaler 实例通信以执行任何基于 NetScaler Console 的功能。

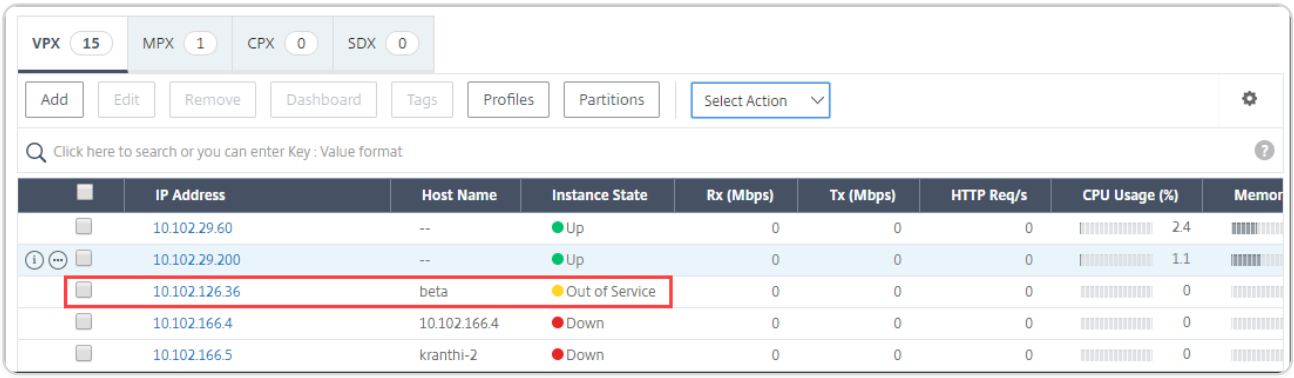
对于基于 LAS 的许可，取消管理 NetScaler 实例会使该 NetScaler 实例失去其基于 LAS 的许可。

取消管理实例：

导航到 **Infrastructure > Instances > NetScaler** \> **VPX** 选项卡。在实例列表中，右键单击一个实例并选择 **Unmanage**，或者选择该实例并从 **Select Action** 列表中选择 **Unmanage**。

所选实例的状态将变为 **Out of Service**，如下图所示。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



跟踪到实例的路由

通过跟踪从 NetScaler Console 到实例的数据包路由，您可以找到诸如到达实例所需的跳数等信息。Traceroute 跟踪数据包从源到目标的路径。它显示网络跳数列表以及路由中每个实体的 IP 地址和主机名。

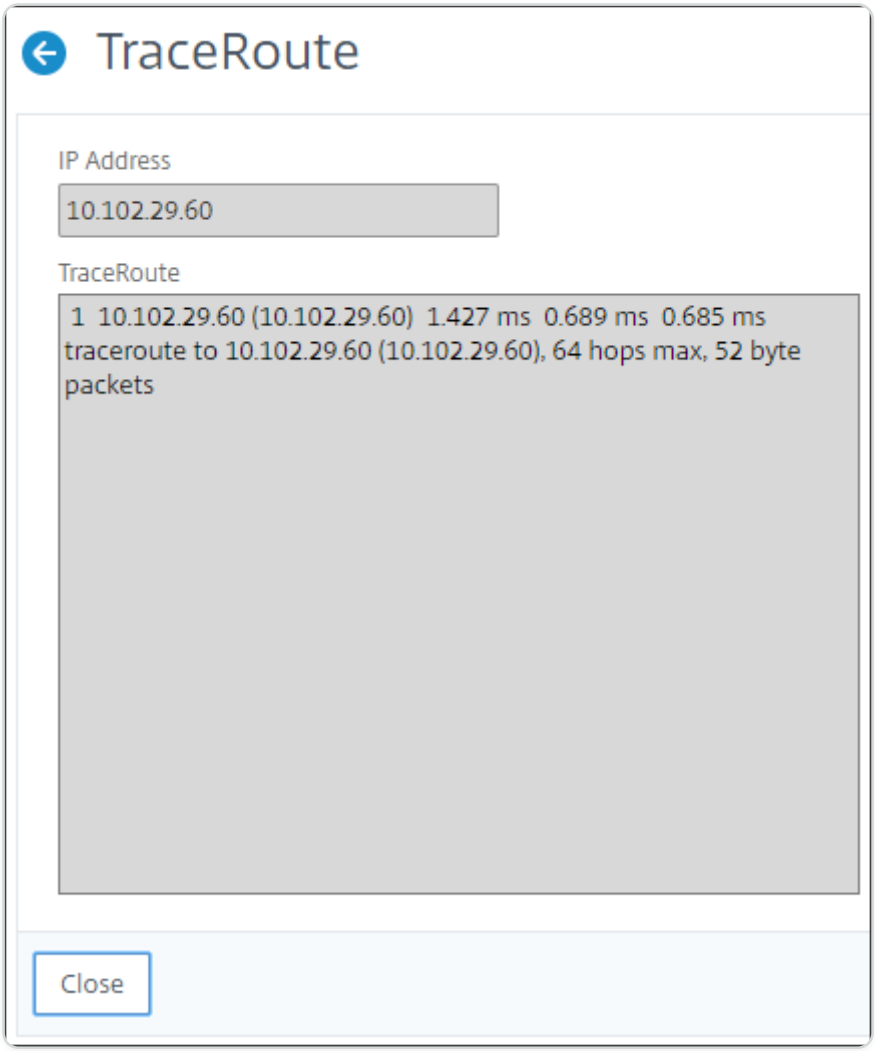
Traceroute 还会记录数据包从一个跳到另一个跳所需的时间。如果数据包传输中断，traceroute 会显示问题所在。

要跟踪实例的路由：

1. 在 NetScaler Console 中，导航到 **基础架构 > 实例 > NetScaler** > **VPX** 选项卡。
2. 在实例列表中，右键单击一个实例，然后选择 **TraceRoute**，或者选择该实例，然后从 **选择操作** 菜单中单击 **TraceRoute**。

TraceRoute 消息框显示到实例的路由以及每个跳所消耗的时间（以毫秒为单位）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



查看 NetScaler 拥有的 IP 地址

您可以直接从 NetScaler Console GUI 查看在 NetScaler 实例上配置的 IP 地址。您只能在 NetScaler 实例上执行配置更改和其他操作。

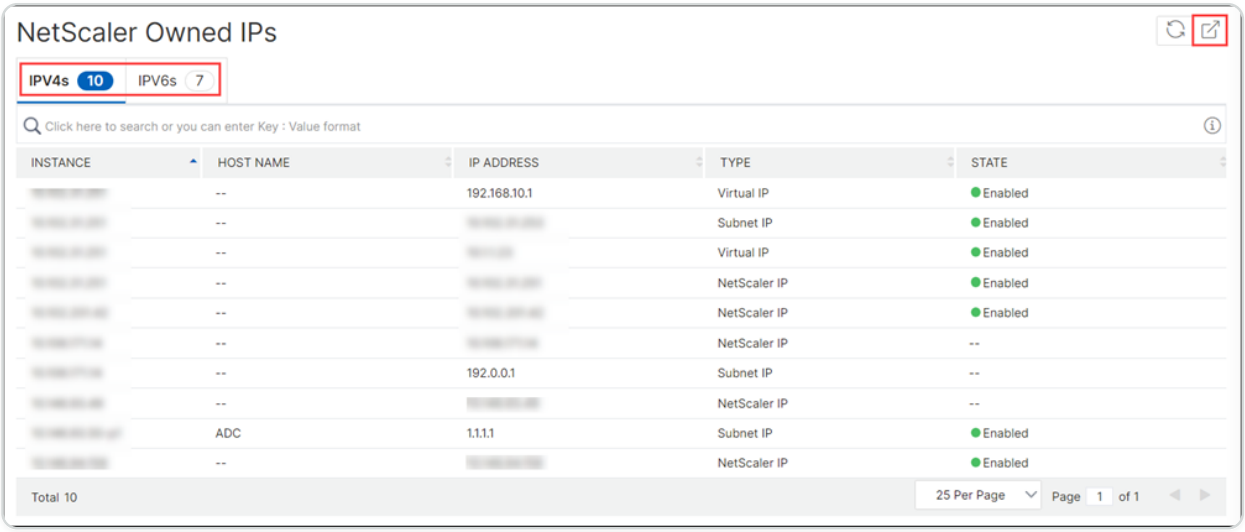
要查看 NetScaler 拥有的 IP 地址，请导航到 **Infrastructure > Instances > NetScaler Owned IPs** 。

此功能显示在 NetScaler 实例上配置的 IPv4 和 IPv6 地址。IP 地址类型包括：

- NetScaler IP 地址
- 子网 IP 地址
- 虚拟 IP 地址
- ADNS 服务 IP 地址
- GSLB IP 地址
- 群集 IP 地址

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 映射的 IP 地址



导出 NetScaler 拥有的 IP 地址

要导出 NetScaler 拥有的 IP 地址：

1. 导航到 **基础架构 > 实例 > NetScaler 所属 IP**。
2. 在“**NetScaler 拥有的 IP**”页面上，单击右上角的导出图标。
3. 在“**导出报告**”页面上，单击“**立即导出**”。
4. 在“**立即导出**”页面上，选择导出选项：

   对于“**快照**”导出：

   a. 选择导出文件格式：PDF、JPG 或 PNG。

      快照导出(/en-us/netscaler-application-delivery-management-software/media/export-now-snapshot.png)

   对于“**表格**”导出：

   a. 选择导出文件格式：PDF 或 CSV。
   b. 从列表中选择要导出的数据记录数。

      表格导出(/en-us/netscaler-application-delivery-management-software/media/export-now-tabular.png)

5. 单击“**导出**”。

安排导出 NetScaler 拥有的 IP 地址

要安排导出 NetScaler 拥有的 IP 地址：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 导航到“**基础架构 > 实例 > NetScaler 拥有的 IP**”。
2. 在“**NetScaler 拥有的 IP**”页面上，单击右上角的导出图标。
3. 在“**导出报告**”页面上，单击“**计划导出**”。
4. 在“**计划导出**”页面上，输入以下详细信息：
   a. 输入主题和描述。
   b. 选择导出类型。

      对于“**快照**”导出类型：

      - 选择导出文件格式：PDF、JPG 或 PNG。

      对于“**表格**”导出类型：

      - 选择导出文件格式：PDF 或 CSV。
      - 从列表中选择要导出的数据记录数。

   c. 选择重复频率：每日、每周或每月。
   d. 选择导出时间。
   e. 选择如何发送导出的 IP 地址：电子邮件、Slack 或两者。

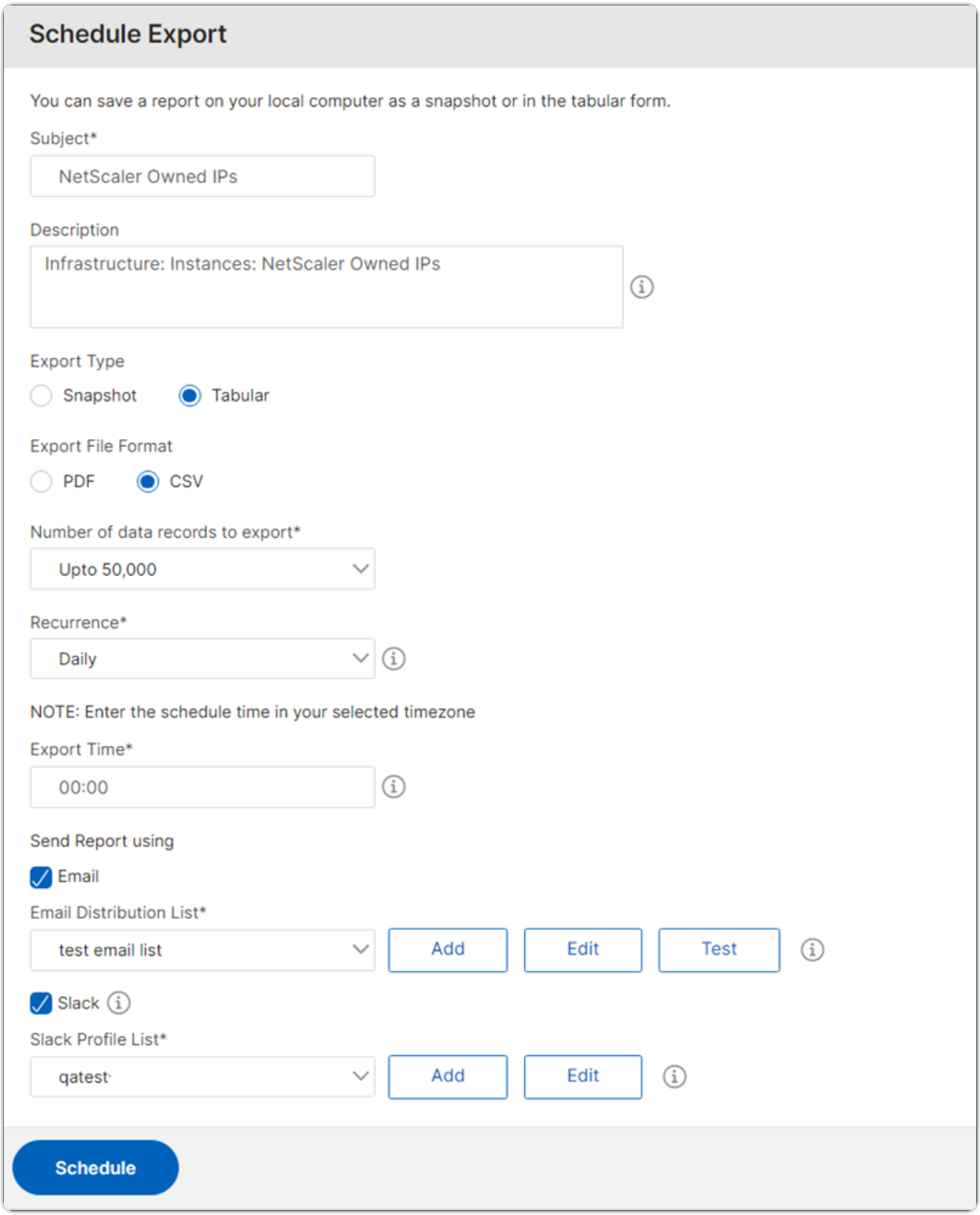
      对于电子邮件：

      - 选择“**电子邮件**”并选择电子邮件分发列表以发送 NetScaler 拥有的 IP 地址列表。
        - 要添加电子邮件分发列表，请单击“**添加**”并指定电子邮件服务器详细信息。
        - 要编辑电子邮件分发列表，请单击“**编辑**”。
        - 要验证电子邮件分发列表是否正常工作，请单击“**测试**”。这将向选定的电子邮件分发列表发送一封测试电子邮件。

      对于 Slack：

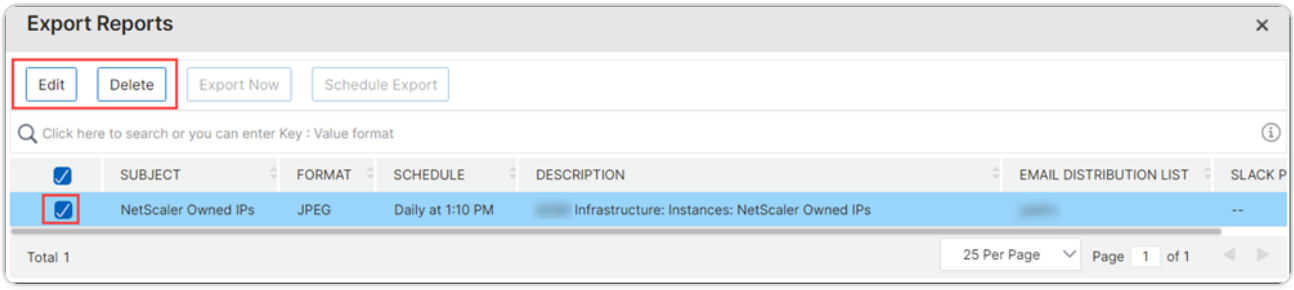
      - 选择“**Slack**”并选择 Slack 配置文件列表以发送 NetScaler 拥有的 IP 地址列表。
        - 要添加 Slack 配置文件，请单击“**添加**”并指定 Slack 频道的“**配置文件名称**”、“**频道名称**”和“**令牌**”。
        - 要编辑现有 Slack 频道，请单击“**编辑**”。
5. 单击“**计划**”以计划导出。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



计划后，您的导出计划将显示在“**导出报告**”页面上，您可以选择该计划以执行编辑或删除操作。编辑选定的计划后，单击“**保存**”以保存编辑的更改。“**删除**”将删除该计划。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

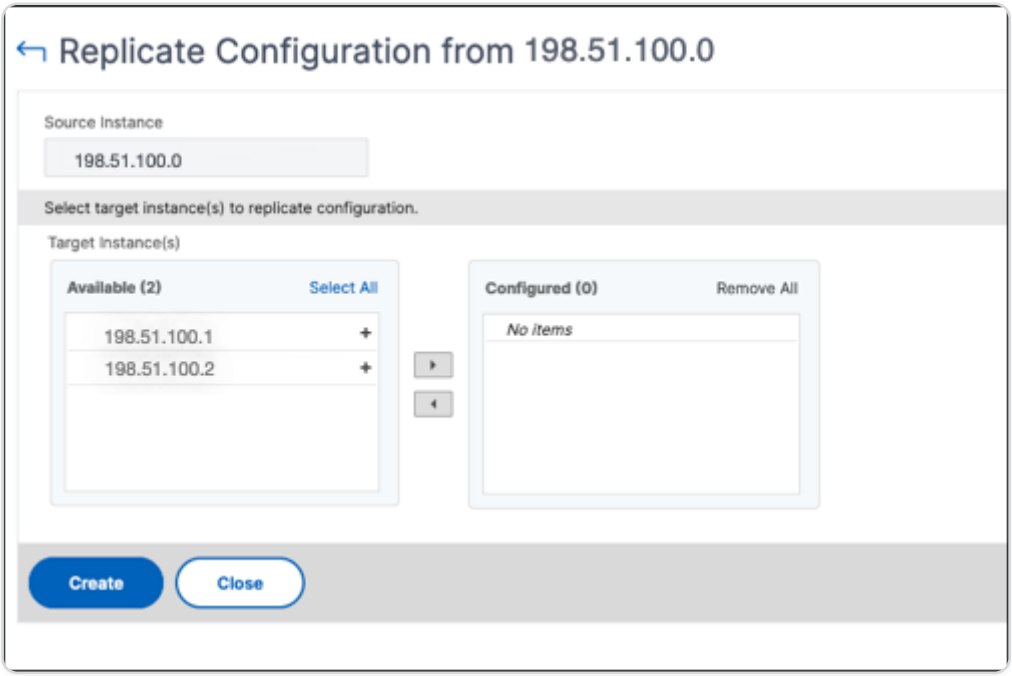


将配置从一个 NetScaler 实例复制到另一个实例

您可以使用 NetScaler Console 的复制配置功能，将配置从一个 NetScaler 实例复制到一个或多个实例上。

将配置从一个实例复制到其他 NetScaler 实例

1. 导航到 **Infrastructure > Instances > NetScaler**。选择要将其配置复制到其他实例的源实例，然后从 **Select Action** 列表中单击 **Replicate Configuration**。
2. 在 **Replicate Configuration** 中，选择要应用源实例配置的目标实例。您可以将配置从单个源实例复制到一个或多个目标实例。



3. 单击 **Create**。

复制的配置将添加到 NetScaler® 实例列表中。要查看复制实例的状态，请单击刷新图标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

在复制过程中，源实例的所有网络 IP 都将复制到目标实例。如果目标实例与源实例位于不同的网络中，则目标实例中的 IP 可能无法访问。当 IP 无法访问时，目标实例中实体的状态将显示为“关闭”。

要查看在托管 NetScaler 实例上配置的实体的状态，请导航到 **Infrastructure > Network Functions**。

SSL 证书管理

任何需要处理机密或敏感信息的组织或个人网站都必须拥有 SSL 证书。Web 服务器上的 SSL 证书有助于向连接客户端保证 Web 服务器的真实性。它不仅可以验证网站的身份，还有助于生成会话密钥，该密钥稍后用于加密整个会话。

安全套接字层 (SSL) 证书是任何 SSL 事务的一部分，是一种数字数据形式 (X509)，用于识别公司（域）或个人。该证书具有一个公钥组件，任何希望与服务器启动安全事务的客户端都可以看到该组件。相应的私钥安全地驻留在 Citrix NetScaler 设备上，用于完成非对称密钥（或公钥）加密和解密。

NetScaler Console 为您提供了一个统一控制台，可自动执行 SSL 证书的安装、更新、删除、链接和下载。它有助于维护网站的声誉和客户信任。NetScaler Console 现在为您简化了证书管理的各个方面。通过统一控制台，您可以配置自动化策略，以根据组织 IT 策略确保推荐的颁发者、密钥强度、协议和算法。这样，您可以密切关注未使用或即将过期的证书。

您可以通过以下任一方式获取 SSL 证书和密钥：

- 从授权的证书颁发机构 (CA) 获取，例如 Verisign
- 通过在 NetScaler 设备上生成新的 SSL 证书和密钥

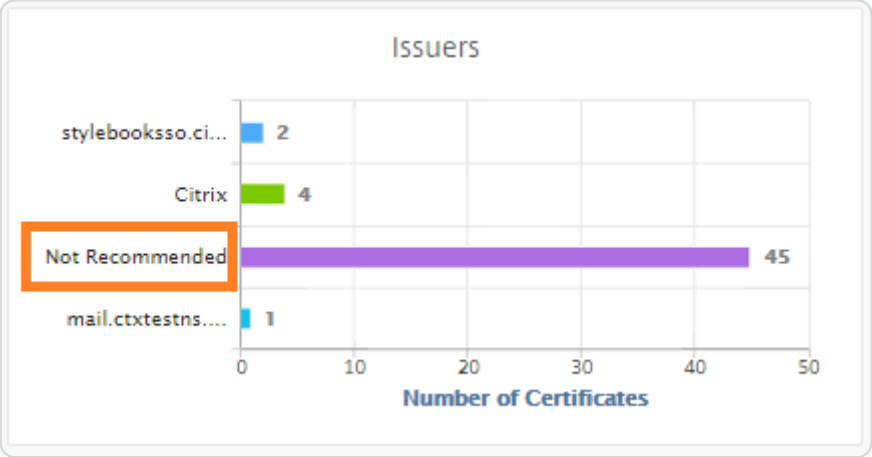
企业 SSL 策略设置

每个企业都有自己的 SSL 策略，并定义了所有 SSL 证书必须遵守的要求。安全一直是所有企业用户的首要任务之一，因此 SSL 设置发挥着重要作用。

例如，ABC 公司规定所有证书的最小密钥强度必须为 2,048 位及以上。证书必须由受信任的 CA 或颁发者授权。管理员必须检查所有此类 SSL 参数，以确保证书符合公司策略。手动验证每个证书是一项繁琐的工作。为了克服这种情况，NetScaler Console 帮助您配置企业 SSL 策略设置，并显示带有“不推荐”标签的任何不合规证书。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以在 SSL 控制面板上查看不合规（不推荐）证书的摘要。



注意

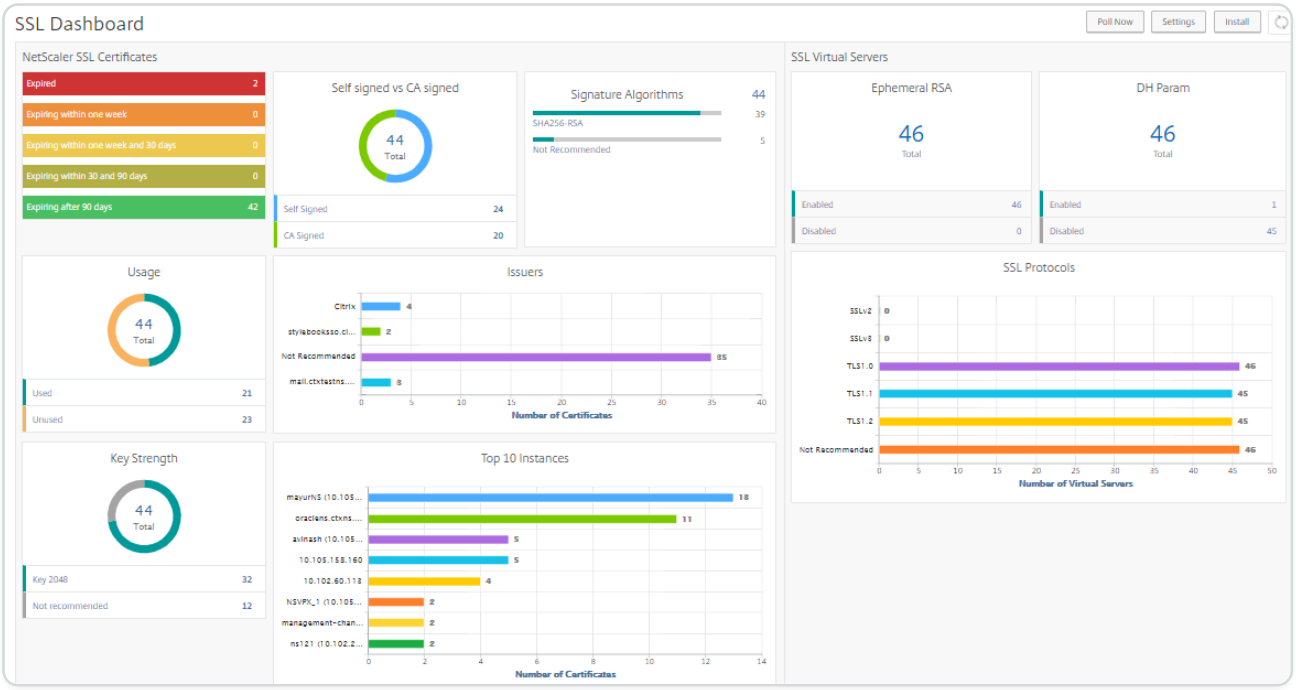
“不推荐”证书根据不同的参数进行分类，您可以在相关组件中查看它们。

NetScaler Console 证书的工作原理

SSL 控制面板为您提供所有安装在不同 NetScaler 实例上的 SSL 证书的可视化呈现。SSL 控制面板包含每个安装在 NetScaler 实例上的证书的以下信息。它根据以下内容进行分类：

- **自签名与 CA 签名。** “自签名与 CA 签名”部分可帮助您将证书分为自签名证书和 CA 签名证书。
- **签名算法。** 此部分根据用于加密的签名算法对 SSL 证书进行分类。
- **使用情况。** 此部分根据已使用和未使用证书对您的 SSL 证书进行分类。未使用的证书需要特别关注，因为它们可能未绑定到虚拟服务器。
- **颁发者。** 此部分根据证书的颁发者对 SSL 证书进行分类。
- **密钥强度。** 此部分根据私钥的密钥强度对 SSL 证书进行分类。
- **前 10 个实例。** 此部分根据安装的 SSL 证书数量，提供前 10 个 NetScaler 实例的详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



SSL 证书管理用例

以下用例描述了如何使用 SSL 证书来管理和监控跨多个 NetScaler 实例的证书。

安装 SSL 证书

想象一下，您拥有大量 NetScaler 实例，您必须在这些实例上部署所需的 SSL 证书。NetScaler Console 为您提供了一个统一的控制台，可以一次性在多个 NetScaler 实例上部署 SSL 证书。

例如，您可能希望在一个或多个 NetScaler 实例上安装一些 SSL 证书。通过这种方法，您可以最大限度地减少在每个 NetScaler 实例上手动安装 SSL 证书的干预。您可以在一个或多个 NetScaler 实例上批量安装 SSL 证书。

要获取 SSL 证书的摘要，请登录到 **NetScaler Console**，然后导航到 **基础架构 > SSL 控制面板**。

证书过期通知设置

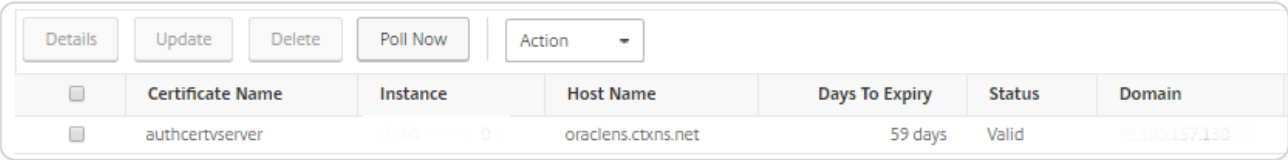
在此用例中，您可能在多个 NetScaler 实例中拥有许多证书，跟踪每个证书的到期成为一项负担。手动跟踪每个证书并在其到期前更新是一项繁琐的工作。为避免此类情况，您可以配置 NetScaler Console 以将通知或警报发送到配置的电子邮件、寻呼机、Slack 或 ServiceNow 配置文件。通过这种方式，您可以及时了解证书到期日期，并在到期日期之前续订证书。

例如，您可能忘记跟踪即将到期的证书。证书过期会导致服务中断，这可能会影响用户的众多应用程序。借助 NetScaler Console 证书到期通知设置，您可以避免此类意外情况。

您可以在 **SSL 仪表板**上查看摘要并跟踪即将到期的证书。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要查看任何持续时间内到期证书的报告，您可以单击磁贴以获取在该窗口中到期的所有此类证书的详细信息。



证书续订

您现在可以从 NetScaler Console 续订证书。您可以续订现有证书或根据以下内容创建证书：

更新现有证书

在此用例中，您必须在从证书颁发机构 (CA) 收到续订的证书后更新现有证书。您现在可以从 NetScaler Console 更新现有证书，而无需登录 NetScaler 实例。

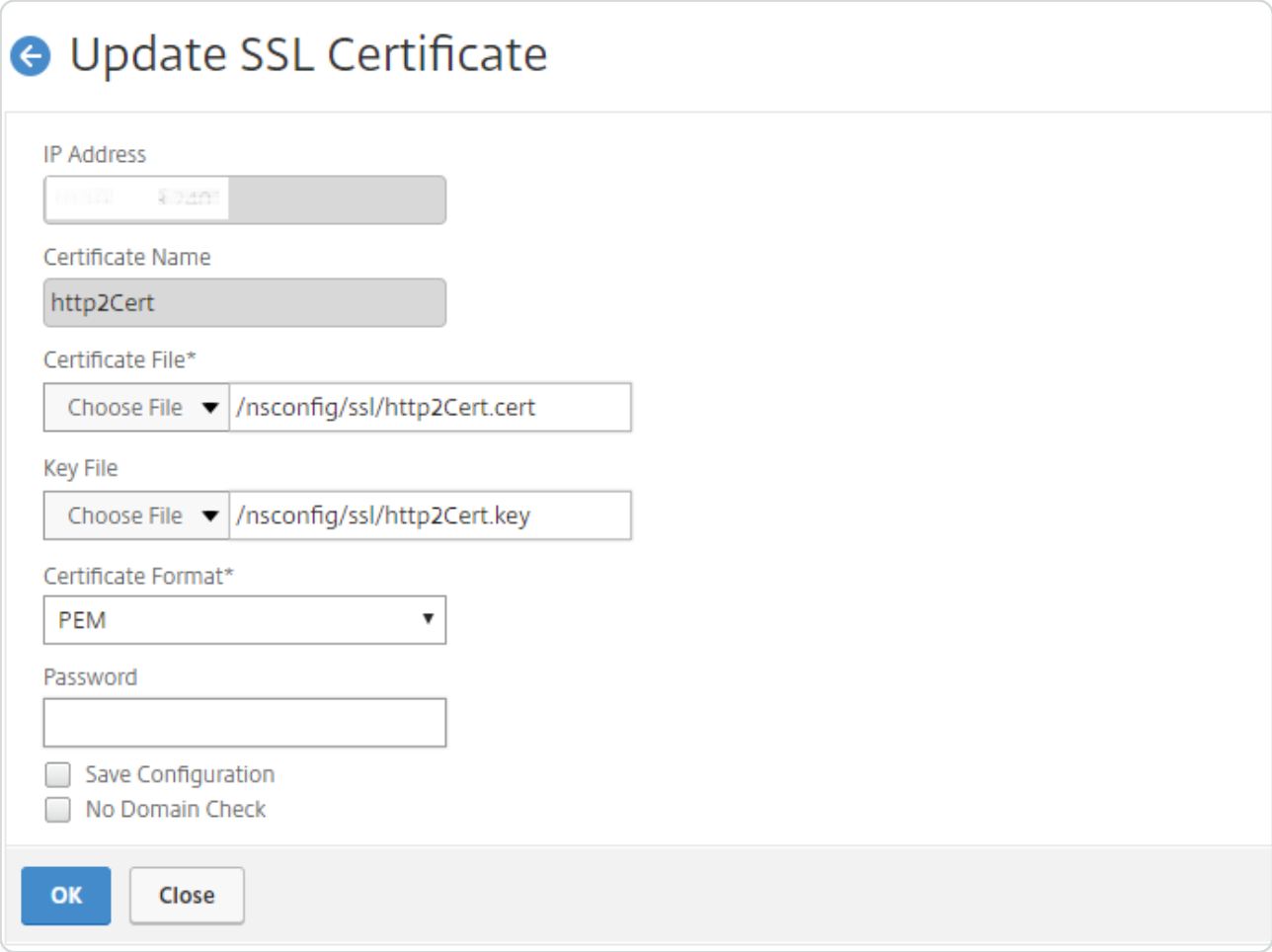
例如，现有证书可能存在一些更改或修改。CA 颁发续订的证书。现在，您无需前往 NetScaler 设备，即可从 NetScaler Console 更新 SSL 证书。

要更新任何证书，请登录 NetScaler Console，然后导航到 **Infrastructure > SSL Dashboard**。

选择要更新的证书，然后单击 **Update**。

您可以选择从 NetScaler Console 更新所选证书的相关字段。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



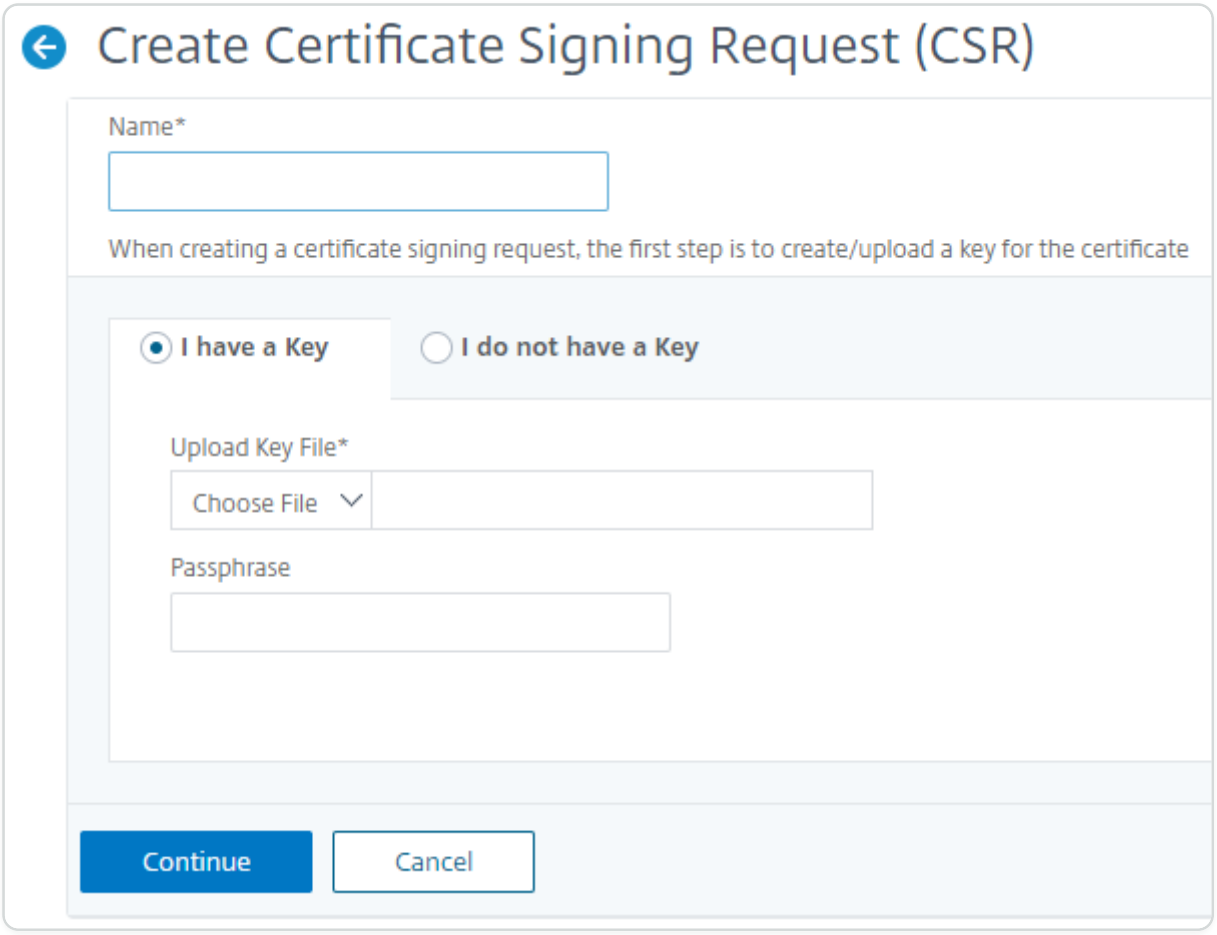
创建证书签名请求

设想一个用例，其中一个 SSL 证书不符合组织策略。您希望从证书颁发机构获取新证书。您现在可以从 NetScaler Console 生成证书签名请求 (CSR)。CSR 和公钥可以发送给 CA 以获取 SSL 证书。

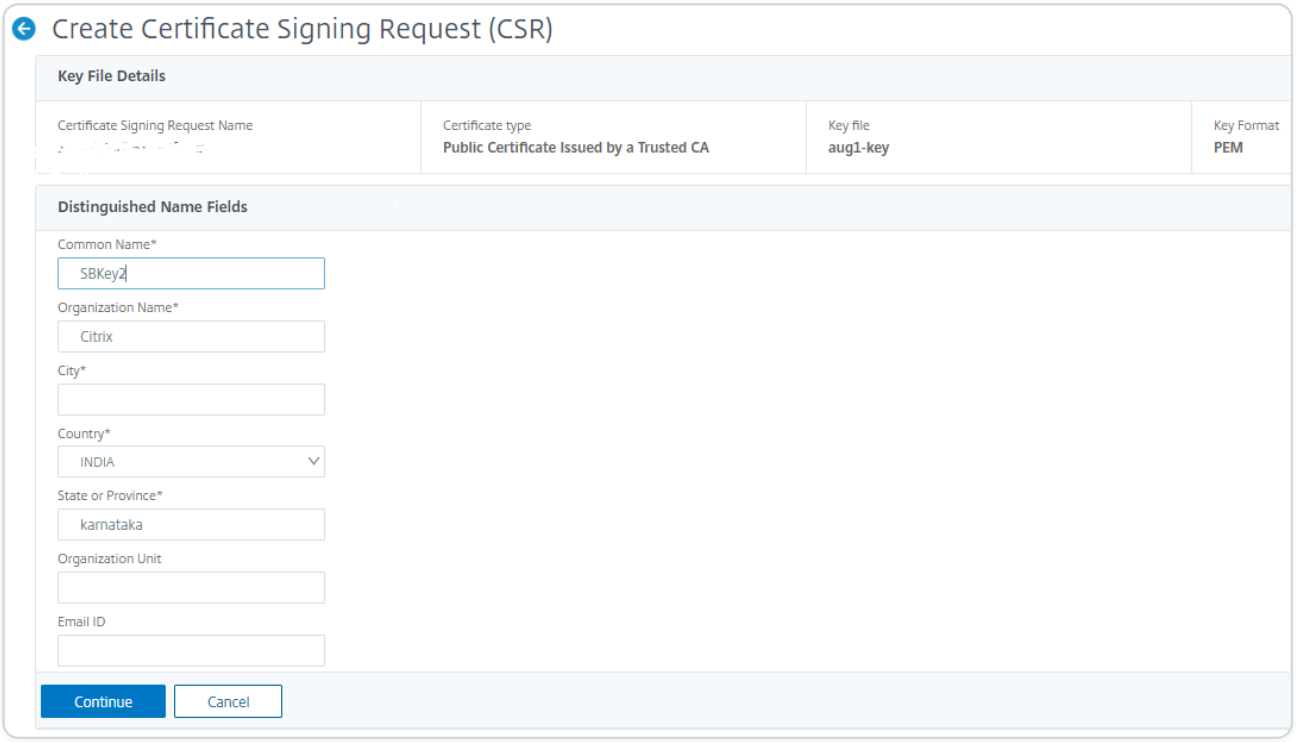
要确定并创建 CSR，请选择所需的证书，然后单击**创建 CSR**。

您需要有一个公钥或私钥值对。要上传密钥，请单击**选择文件**并从列表中选择。要创建密钥，请选择**我没有密钥选项**并指定相关参数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



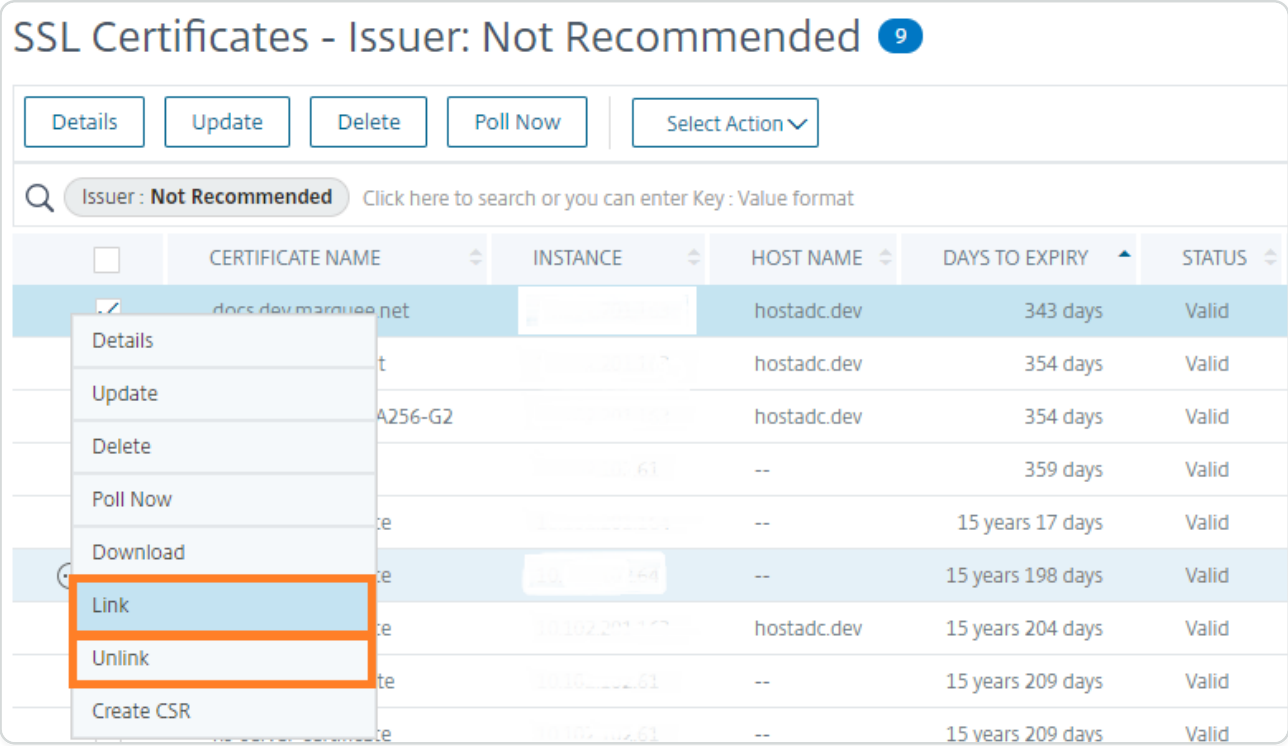
提供所选密钥的更多详细信息，例如常用名、组织名称、城市、国家/地区、省/州、组织单位和电子邮件 ID，以创建 CSR。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

链接和取消链接 SSL 证书

您可以将多个 SSL 证书相互绑定以创建证书捆绑包。要将一个证书链接到另一个证书，第一个证书的颁发者必须与第二个证书的域匹配。

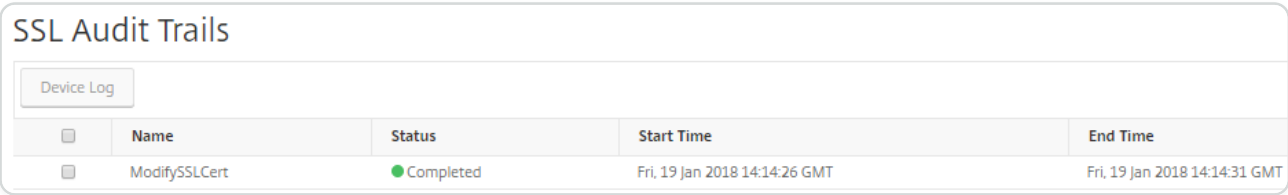


审计日志

审计日志是 NetScaler Console 生成的文本日志文件集合。它显示了使用 NetScaler Console 添加、修改和更改到特定 NetScaler 设备的 SSL 证书的历史记录。审计日志还显示 NetScaler 设备的 IP 地址、状态、开始时间和特定操作的结束时间。

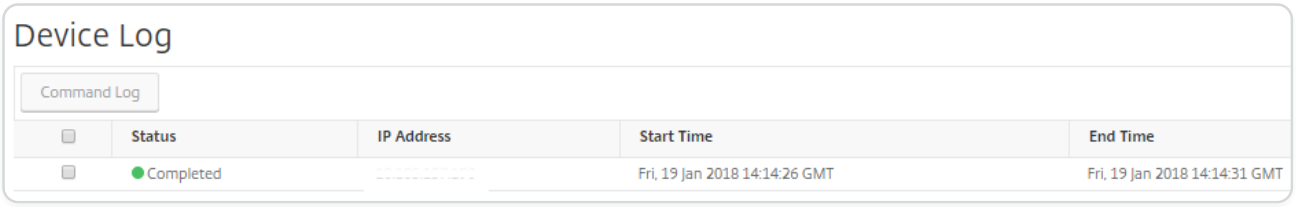
在此示例中，您可能希望验证特定证书在一段时间内发生的更改。您可以选择通过设备日志和命令日志查看证书的更改历史记录。

要确定 SSL 证书的信息，请在**SSL 仪表板**上单击**审计日志**。应用程序摘要包括 SSL 证书状态以及开始时间和结束时间。

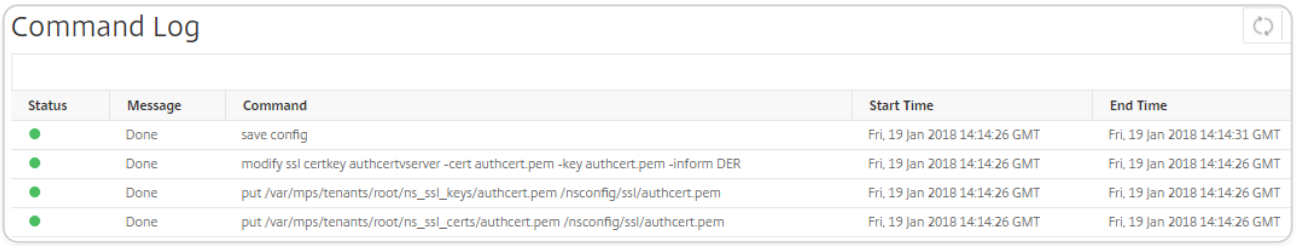


要确定特定 SSL 证书的 NetScaler 设备信息，请选择您选择的相关证书复选框。单击**设备日志**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



要查看命令类型和消息的信息，请单击**命令日志**。



使用 ACME 协议进行自动化证书续订

NetScaler Console 支持自动化证书管理环境 (ACME)，这是一种旨在自动化 SSL/TLS 证书续订的开放协议。

以前，网络管理员必须经历劳动密集型、多阶段的手动证书续订过程。ACME 支持通过提供一个强大的自动化证书续订框架来缓解这些挑战，以执行以下操作：

- 从受信任的证书颁发机构 (CA) 请求新证书。
- 使用自动化方法验证域所有权（例如，DNS-01 质询）。
- 在到期前自动续订证书。

NetScaler® Console 中的 ACME 支持

NetScaler Console 使用 `acme.sh` 客户端并支持以下证书颁发机构：

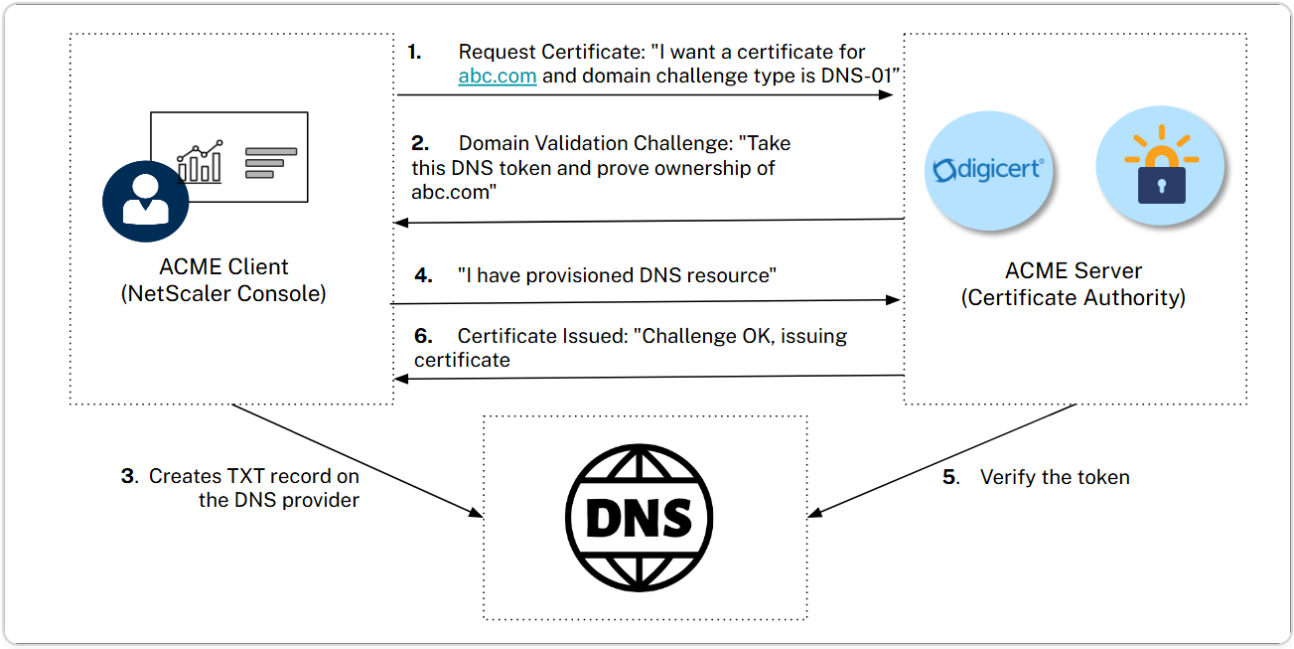
- 让我们加密
- DigiCert Inc
- 赛迪高有限公司
- 安信公司
- GlobalSign
- GoDaddy.com, Inc
- ZeroSSL
- 谷歌信任服务
- 谷歌公共CA
- BuyPass Go SSL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 阿克塔利斯
- SSL.com
- 哈希公司 Vault
- 斯莫尔斯泰普
- 佩布尔
- HARICA
- EJBCA

以下步骤说明了 NetScaler Console 中如何进行自动化证书续订：

1. 当 NetScaler Console 使用 `acme.sh` 客户端为域发起证书请求时，该客户端会连接到所选的证书颁发机构（例如，Let's Encrypt 或 DigiCert）。
2. CA 会发出一个挑战以证明域所有权，在这种情况下，这是一个 DNS-01 挑战。
3. NetScaler Console 使用预配置的凭据，自动使用 CA 提供的值更新域的 DNS TXT 记录。
4. CA 验证 TXT 记录，确认域所有权。
5. 成功验证后，CA 会将 SSL/TLS 证书颁发给 NetScaler Console。
6. NetScaler Console 将证书存储在相应的存储区（证书存储区/零接触存储区）中。
7. 根据您提供的续订窗口，NetScaler Console 会在证书过期日期之前自动重复此续订过程。



借助 NetScaler Console 中的 ACME 支持，您可以执行以下操作：

- 在证书过期前自动续订
- 在续订期间从一个 CA 切换到另一个 CA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 生成或上传 CSR 并请求新证书

以下是主要优势：

- 全自动生命周期，无需手动干预证书颁发或续订。
- 可自定义的续订计划，以满足组织需求（例如，设置为在到期前 7 天续订）。
- 消除因证书过期导致的停机时间。
- 通过自动化过期跟踪和续订来降低运营开销。
- 借助始终有效且符合 CA 最佳实践的证书，提高安全态势。

ACME 集成配置步骤

集成 ACME 是一次性过程，包括以下步骤：

- 步骤 1：配置证书颁发机构 (CA)。
- 步骤 2：选择要续订的证书。
- 步骤 3：添加 DNS 提供商并映射相应的域。

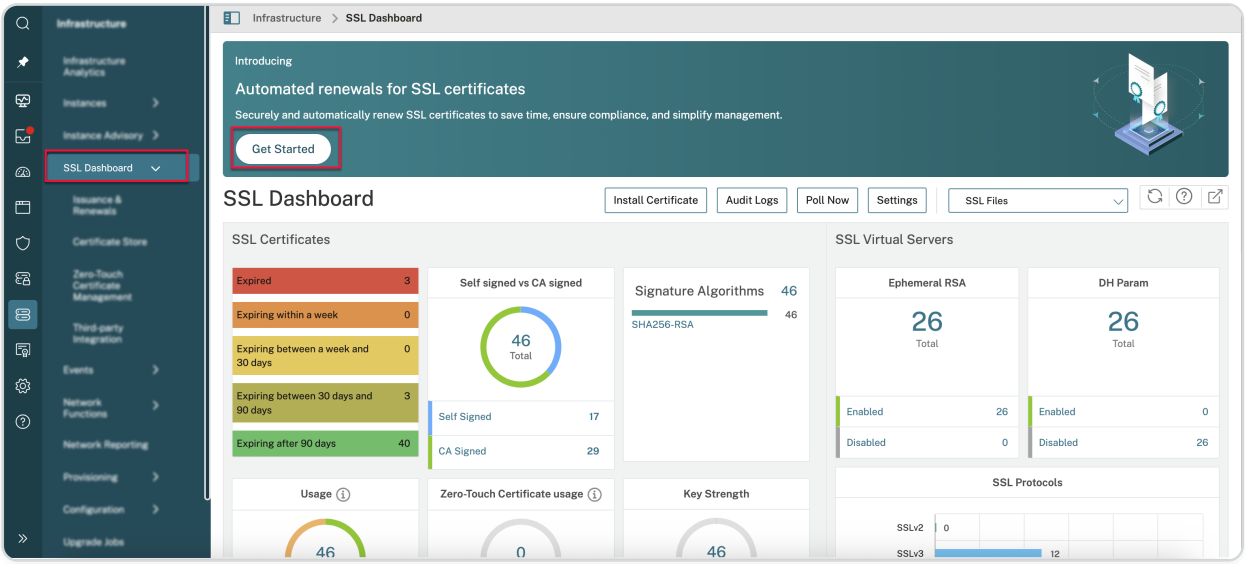
先决条件

- 确保您必须拥有证书颁发机构 (CA) 的有效帐户以及相应的许可证。
- 确保您拥有 DNS 提供商访问凭据。

步骤 1：配置证书颁发机构 (CA)

执行以下步骤以注册用于续订的证书颁发机构 (CA)：

1. 导航到 **Infrastructure > SSL Dashboard**。如果您是首次配置 ACME，则会看到一个横幅，上面显示“SSL 证书的自动续订”。单击 **Get Started**。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

或

导航到 **基础架构 > SSL 控制板 > 第三方集成 > CA 供应商**，然后单击 **添加**。

2. 输入名称并选择 CA 供应商。目前，仅支持 **Let's Encrypt** 和 **DigiCert Inc**。
3. 提供其他详细信息，例如电子邮件地址、ACME 目录 URL。
4. 输入 NetScaler Console 必须自动续订证书的天数。
5. 单击 **保存并继续**。NetScaler Console 尝试连接到 CA。如果连接失败，请查看提供的详细信息，更正配置详细信息，然后重试。

   ACME 配置 CA 供应商(/en-us/netscaler-application-delivery-management-software/media/acme-configure-ca-vendor.png)

步骤 2：选择要续订的证书

添加 CA 详细信息后，NetScaler Console 会自动扫描所有证书（来自证书存储和零接触存储），并单独列出由配置的 CA 颁发的证书。查看列出的证书。

1. 选择要自动续订的证书。例如，如果您将 Let’s Encrypt 配置为 CA，并且有 2 个来自 Let’s Encrypt 的证书和 2 个来自其他供应商的证书，则仪表板会显示：`Let’s Encrypt: 2 and Other CA: 2`。

   ACME 支持高级架构(/en-us/netscaler-application-delivery-management-software/media/acme-select-certificates.png)

2. 您可以单击 **添加** 以添加由不同 CA 颁发的证书，或单击 **删除** 以删除您不想自动续订的证书。如果您选择来自不同供应商的证书，系统会提示您确认供应商更改。确认后，当这些证书的续订窗口到达时，它们将通过新配置的 CA 进行续订。

   > **注意：**
   >
   > 确保证书存储和零接触证书存储中没有重复的证书。如果存在重复证书，则每个存储的续订过程将发生两次。

   ACME 支持高级架构(/en-us/netscaler-application-delivery-management-software/media/acme-vendor-change-prompt.png)

3. 单击 **保存并继续**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

续订后，证书仍保留在其各自的存储中。例如，如果证书存储在证书存储中，则其续订版本也放置在证书存储中。如果证书存储在零接触存储中，则其续订版本也放置在零接触存储中。

证书部署行为取决于存储类型。

- 如果证书存储在证书存储中，则必须手动部署到 NetScaler。
- 如果证书存储在零接触存储中，则证书会自动部署到 NetScaler，无需管理员干预。 我们建议您使用零接触证书管理，以实现续订证书的无缝、全自动部署。有关更多信息，请参阅零接触证书管理。

步骤 3：添加 DNS 提供商并映射域

1. 在“**DNS 提供商和域映射**”页面上，单击“**添加**”。
2. 从“**选择 DNS 提供商**”下拉列表中选择 DNS 提供商。 `acme.sh` 支持的 DNS 提供商列在下拉列表中。如果您在列表中没有看到您的 DNS 提供商，则表示它不受支持。
3. 输入提供商详细信息，例如访问密钥 ID、秘密访问密钥，然后单击“**保存**”以保存配置。
4. 在“**域映射**”下，单击“**添加域**”。
5. 选择由配置的 DNS 提供商服务的域。

重要提示：

确保每个域都链接到正确的 DNS 提供商。NetScaler Console 使用这些映射自动执行 DNS-01 质询。在颁发或续订期间，NetScaler Console 会在映射的 DNS 提供商中创建所需的 TXT 记录。验证成功后，CA 会颁发或续订证书。仅当所有关联域都正确映射到其 DNS 提供商时，证书才会续订。

例如，如果您的组织使用 Amazon Route53 作为 DNS 提供商。首先，在 DNS 提供商详细信息下添加 Amazon Route53 凭据（访问密钥 ID 和秘密密钥）。然后，映射由 Amazon Route53 管理的域（例如：example.com、app.example.com）。当这些域的证书颁发或续订时，NetScaler Console 会自动在 Amazon Route53 中创建所需的 TXT 记录。验证成功后，CA 会颁发或续订证书。
支持以下公共 DNS 提供商：

- 1984.托管
- ACME DNS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- AcmeProxy 服务器 API
- Active24
- Akamai.com 边缘 DNS
- 阿里云
- All-inkl Kas 服务器
- Alviy.com
- 亚马逊 Route53
- Anexia.com CloudDNS
- ArtFiles.de
- ArvanCloud.ir
- autoDNS-InternetX
- 阿祖尔 DNS
- Azion.om
- Beget.com
- BookMyName.com
- Bunny.net
- CloudFlare
- ClouDNS.net
- ConoHa
- Constellix.com
- 核心网络
- cPanel 服务器 API
- Curanet.dk
- cyon.ch
- DDNSS.de
- deSEC.io
- DigitalOcean
- DirectAdmin
- DNS 服务
- DNSExit.com

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- dns.la
- DNSMadeEasy
- 迪恩西普尔
- dnsHome.de
- DNSPod.cn
- DNSPod.com
- 多曼-奥芬西夫 do.de
- DomeneShop.no
- DreamHost
- DuckDNS.org
- durabledns.com
- Dyn.com
- DynDnsFree.de
- Dynu.com
- DynV6.com
- easyDNS.net
- edgecenter DNS 接口
- EUserv.com
- 艾克索斯凯尔
- Fornex.com
- FreeDNS
- FreeMyIP.com
- Gandi 实时DNS
- Gcore.com
- GeoScaling.com
- GoDaddy.com
- 谷歌云 DNS
- Google 域名
- Hetzner.com
- Hexonet.com

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- hosting.de
- HuaweiCloud.com
- 飓风电气
- 飓风电气 HE.net DDNS
- 英孚博克斯
- Infomaniak.com
- INWX
- IONOS 云 DNS
- IONOS.de
- InternetBS.net
- ISPConfig 3.1 管理面板
- jdcloud.com
- Joker.com
- kapper.net
- King.host
- 诺特 DNS
- Leaseweb.com
- 莱克西肯 DNS 客户端
- 利马城.de
- 莱诺德
- Linode.com-Old
- 卢皮亚
- LuaDNS
- MailinaBox
- MaraDNS
- mijn.host
- Misaka.io
- MyDNS.JP
- 神话野兽.com
- Name.com

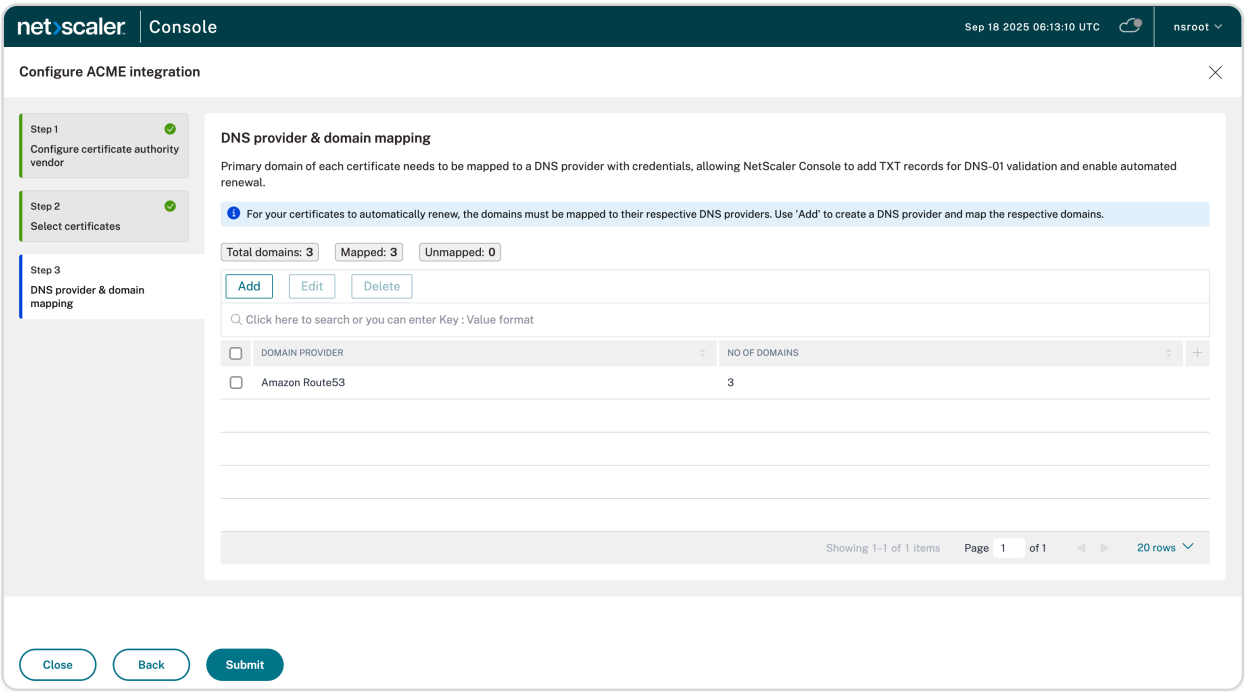
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 纳姆奇普
- NameMaster.de
- 纳姆西洛
- Nanelo.com
- NederHost.nl
- Neodigit.net
- 内特卡普
- Netlify.com
- nic.ru
- 尼亚拉
- NLnetLabs NSD
- NS1.com
- 内克塞斯
- one.com
- Online.net
- omg.lol
- OpenProvider
- OpenStack Designate 应用程序接口
- 欧朋森
- Oracle 云基础设施-OCI
- OVH.com
- 普莱斯克 XML
- PointHQ
- Porkbun.com
- PowerDNS
- RackCorp.com
- RackSpace.com
- rage4.com
- RcodeZero
- reg.ru

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ScaleWay.com
- 施伦德科技
- 赛莱特
- SelfHost.de
- ServerCow.de
- Simply.com
- 泰克尼蒂姆 DNS 服务器
- tele3.cz
- Tencent.com
- Timeweb.Cloud
- TransIP.nl
- UltraDNS
- 联合域名转售
- unoeuro.com
- variomedia.de
- Vercel.com
- veesp.com
- versio.nl AuroraDNS
- VSCALE
- vshosting.cz CloudDNS
- 沃特
- Websupport.sk
- West.cn
- World4You.com
- 扬德克斯 360 商业版 DNS API。
- 扬德克斯云 DNS
- 泽洛尔
- Zone.eu
- ZoneEdit.com
- 佐诺米

© 1997–2026 Citrix Systems, Inc. All rights reserved.



完成所有三个步骤后，NetScaler Console 会配置 ACME CA 服务器。所选证书将针对映射的域进行续订。 NetScaler Console 会定期检查证书的有效性，并在证书过期前（根据配置的续订窗口）续订它们。无需手动干预，证书始终保持有效和最新。

颁发和续订

导航到 **Infrastructure > SSL Dashboard > Issuance & Renewals** 以检查所有续订活动以及证书颁发产生的新请求。

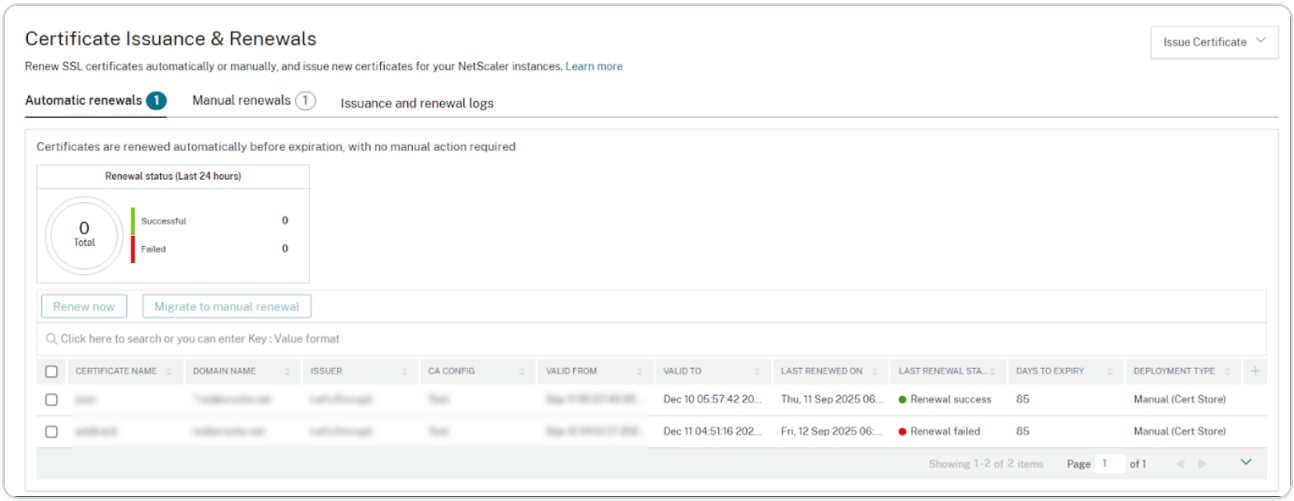
自动续订

自动续订选项卡列出了已注册自动续订的证书。当达到配置的续订窗口时，NetScaler Console 会自动续订它们。

您还可以在计划的续订窗口之前触发按需续订。要进行按需续订，请选择所需的证书，然后单击**立即续订**。

如果您不希望某些证书自动续订，可以将其移至手动续订。要将证书从自动续订转移到手动续订，请选择所需的证书，然后单击**迁移到手动续订**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



手动续订

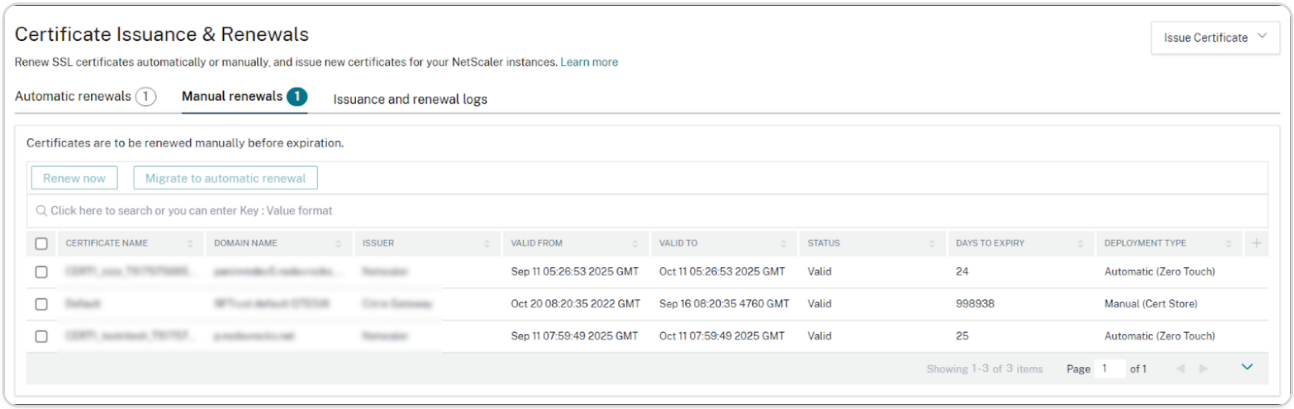
手动续订选项卡列出了所有必须手动续订的证书。这些证书必须手动更新，方法是离线续订证书并将其上传到相应的存储，或者使用**立即续订**选项。

要续订证书，请选择一个证书并单击**立即续订**。如果证书由注册的 CA 颁发，并且其域的 DNS 提供商已配置，则您可以使用 ACME 按需续订它，而无需将其移至自动续订。

您还可以将证书移至自动续订。要将证书从手动续订转移到自动续订，请选择所需的证书，然后单击**迁移到自动续订**。

注意：

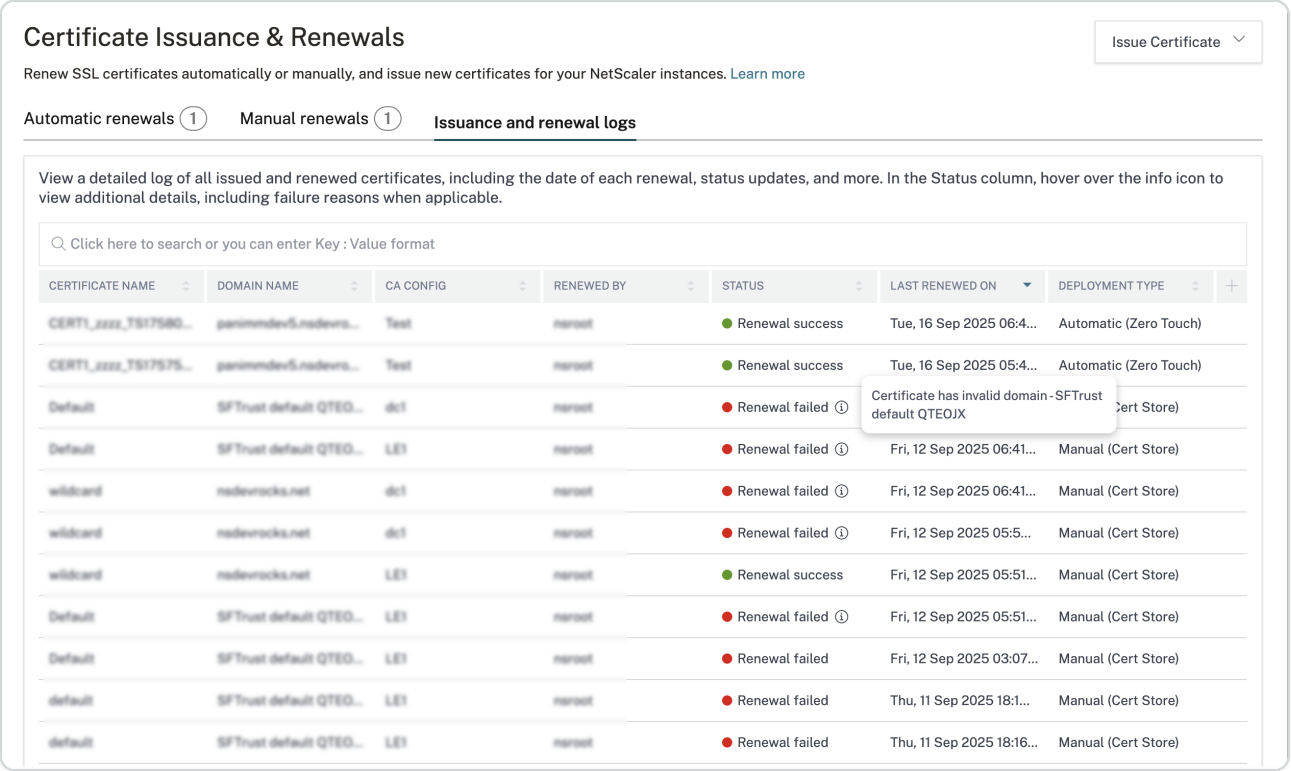
您一次只能续订或迁移一个证书。



颁发和续订日志

“**颁发和续订日志**”选项卡提供了使用 ACME 的证书请求列表，包括颁发和续订。对于失败的事件，您可以单击信息图标以查看详细的错误信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



颁发证书

NetScaler Console 中的 ACME 集成支持直接使用 ACME 协议请求新证书。您可以在 NetScaler Console 中创建 CSR，也可以上传现有 CSR 来请求新证书。

导航到 **Infrastructure > SSL dashboard > Issuances & Renewal**，然后单击**颁发证书**，并根据您的场景选择以下选项之一：

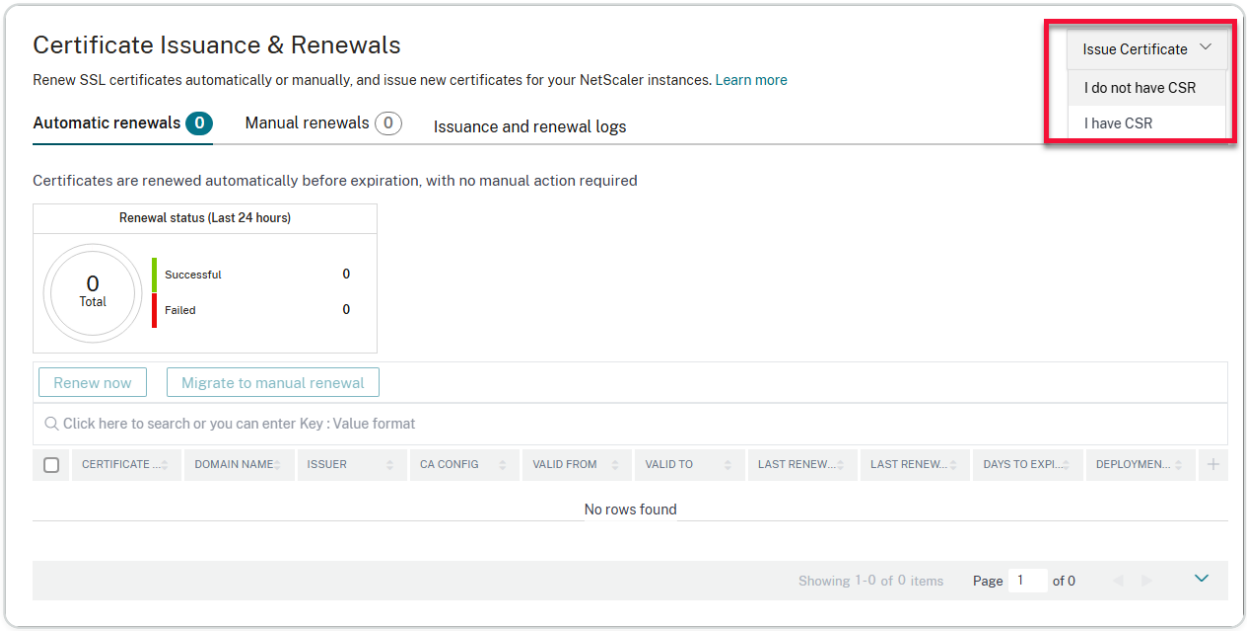
- **我没有 CSR**：如果您还没有 CSR，NetScaler Console 允许您生成一个并颁发新证书。
- **我有 CSR**：如果您已经有离线生成的 CSR，则可以上传它来颁发证书。

不使用 CSR 颁发证书

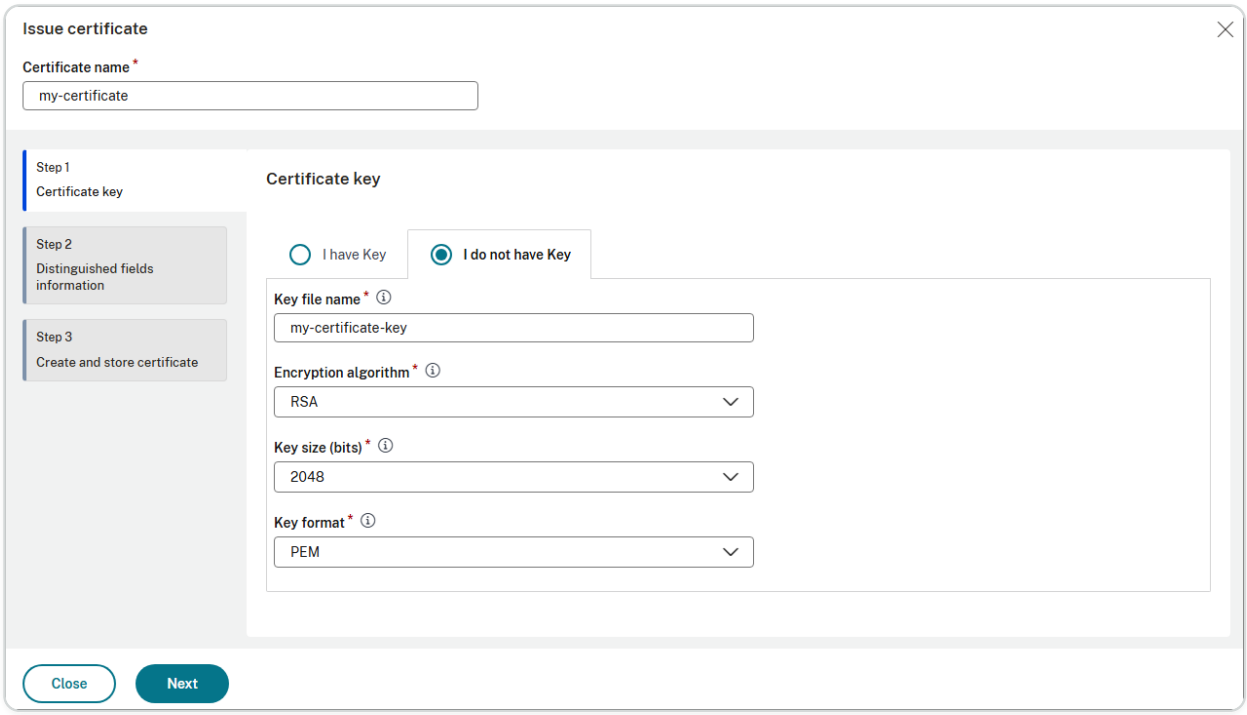
执行以下步骤以生成 CSR 并颁发新证书：

1. 导航到 **Infrastructure > SSL dashboard > Issuances & Renewal**，然后单击**颁发证书**并选择**我没有 CSR**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

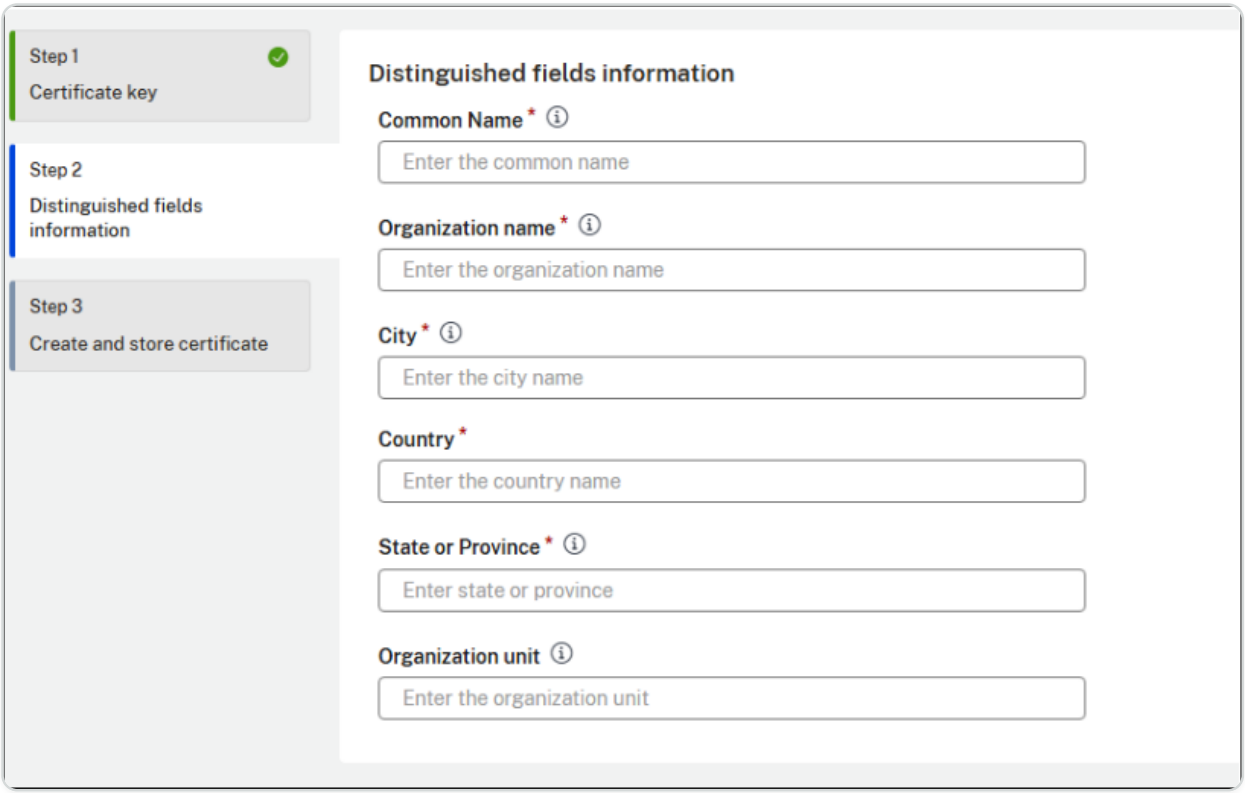


2. 在“**证书密钥**”页面上，通过选择**我有一个密钥**来上传现有密钥，或通过选择**我没有密钥**来生成新密钥。

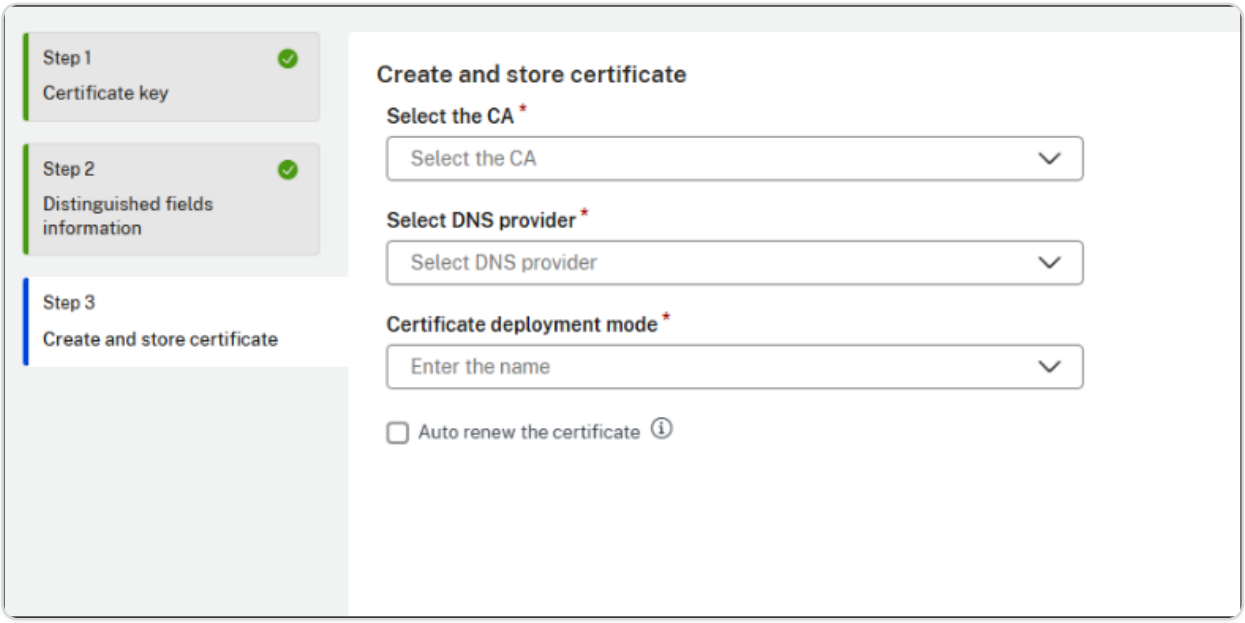


3. 输入所需的 CSR 信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 为 ACME 请求选择 CA、DNS 提供程序和证书部署模式。对于手动部署，请选择 **Cert Store**；对于 NetScaler 上的自动部署，请选择 **Zero Touch Store**。
5. 如果您希望证书将来自动续订，请选择 **Auto renew the certificate**。



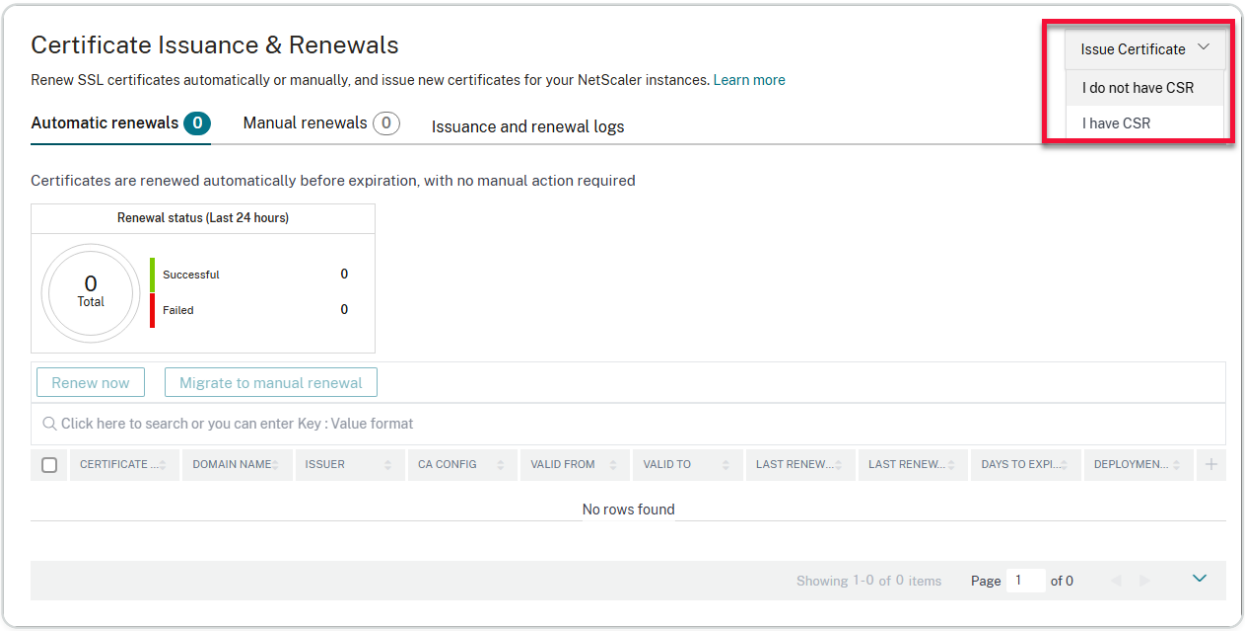
6. 单击 **Save**。

使用 CSR 颁发证书

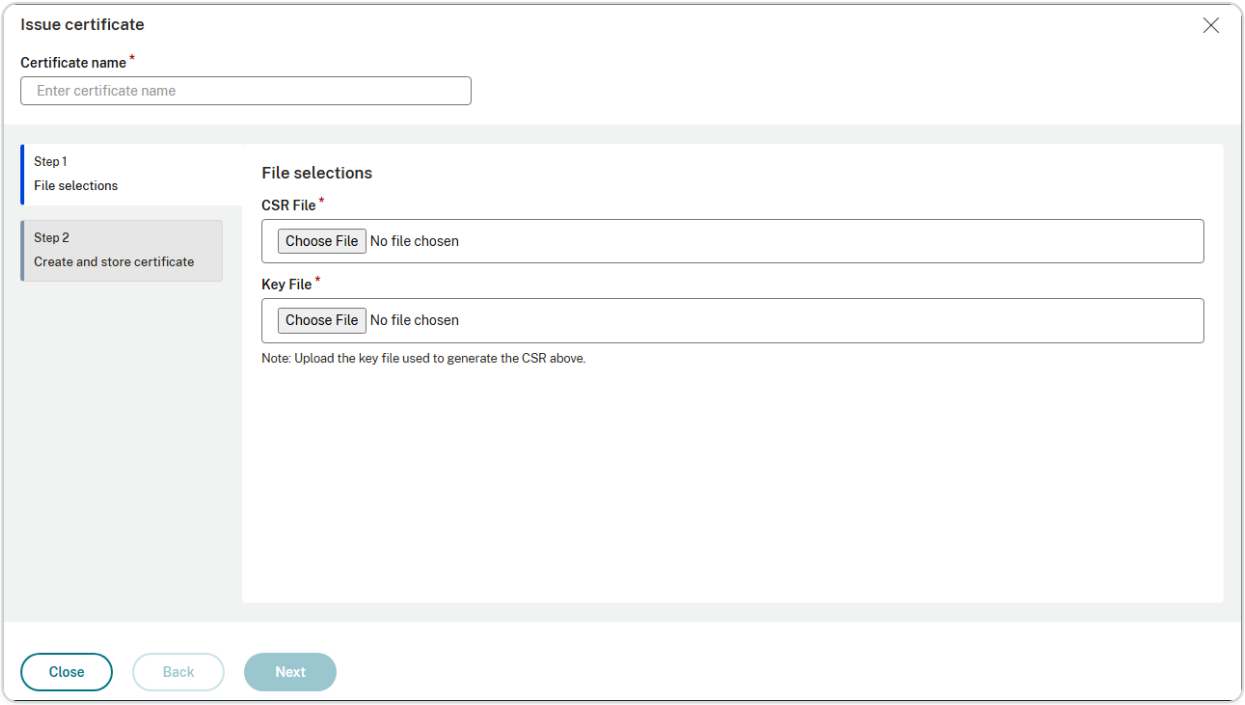
如果您已经离线生成了 CSR 并希望上传它以颁发证书，请执行以下步骤：

1. 导航到 **基础设施 > SSL 控制面板 > 颁发与续订**，然后单击 **颁发证书** 并选择 **我有 CSR**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

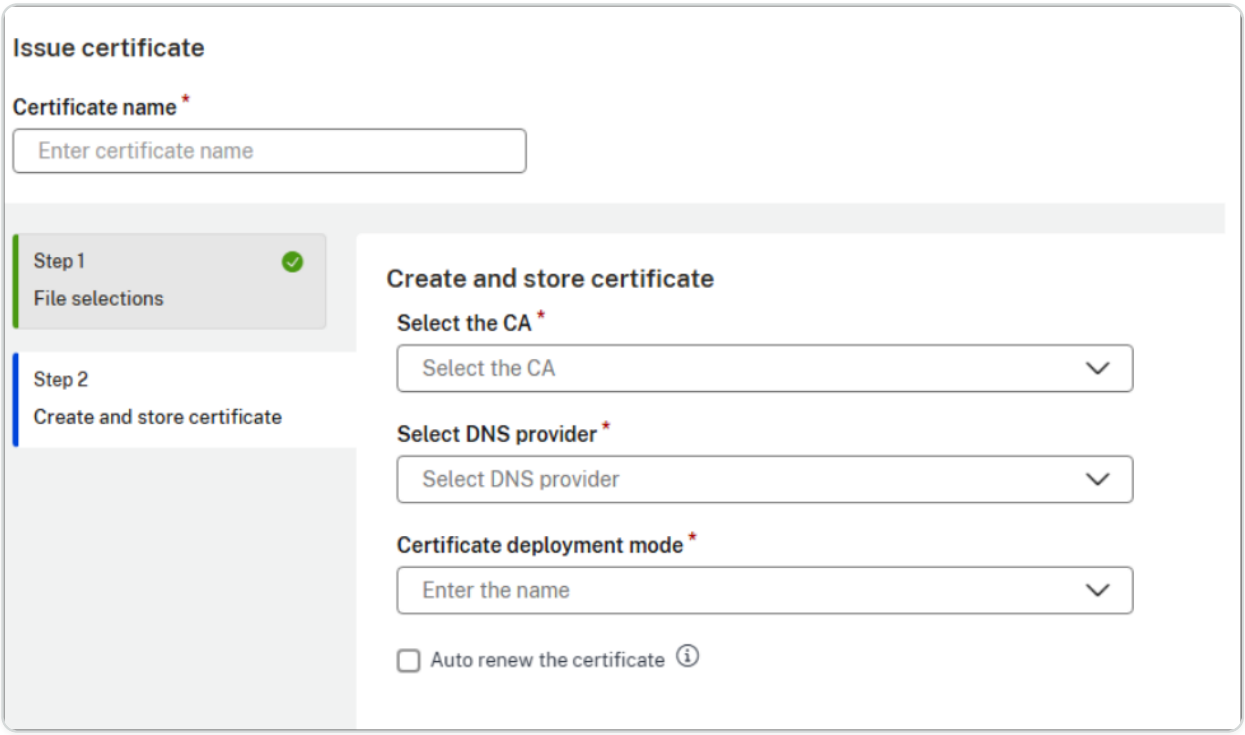


2. 从本地系统选择 CSR 文件和关联的密钥文件。



3. 为 ACME 请求选择 CA、DNS 提供程序和证书部署模式。对于手动部署，请选择 **Cert Store**；对于 NetScaler 上的自动部署，请选择 **Zero Touch Store**。
4. 如果您希望证书将来自动续订，请选择 **Auto renew the certificate**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 点击**保存**。

第三方集成

您可以添加和管理多个 CA 供应商和 DNS 提供商。

您可以从**第三方集成**页面执行以下操作：

- 添加或编辑 CA 供应商
- 更改自动续订设置
- 添加或编辑来自现有已配置 CA 的证书
- 添加或编辑 DNS 提供商
- 更改域映射

添加或编辑 CA 供应商

您可以注册多个 CA 供应商，以管理由不同供应商颁发的证书。您还可以编辑现有 CA 供应商的详细信息。

1. 导航到 **SSL 控制板 > 第三方集成 > ACME > CA 供应商**。点击**添加**。
2. 要添加 CA 供应商，请提供 CA 供应商的名称并选择 CA。
3. 要编辑现有 CA 供应商的详细信息，请选择 CA 供应商并点击**编辑**。
4. 添加或更新所需详细信息。
5. 点击 **保存**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

更改自动续订设置

要更改自动续订设置，请执行以下步骤：

1. 导航到 **SSL 控制板 > 第三方集成 > ACME > CA 供应商**。
2. 选择一个 CA 供应商，然后点击 **编辑**
3. 在 **配置证书颁发机构供应商** 中，根据您的要求在 **自动续订设置** 部分更改天数。
4. 点击 **保存并继续**。
5. 完成工作流程。

从现有已配置的 CA 添加或编辑证书

要从现有已配置的 CA 添加或编辑证书，请执行以下步骤

1. 导航到 **SSL 控制板 > 第三方集成 > ACME > CA 供应商**。
2. 选择一个 CA 供应商，然后点击 **编辑**。
3. 导航到 **步骤 2 选择证书**，然后添加或删除所需的证书。
4. 点击 **保存并继续**。
5. 完成工作流程。

注意：

如果证书尚未从原始 CA 解除映射，则它不会出现在新 CA 的选择列表中。

添加或编辑 DNS 提供程序

要添加新的 DNS 提供程序或编辑现有 DNS 提供程序的现有域映射，请执行以下步骤：

1. 导航到 **SSL 仪表板 > 第三方集成 > ACME > DNS 提供商.**
2. 要添加 DNS 提供程序，请单击“**添加**”。选择 DNS 提供程序，然后单击“**保存**”。
3. 要编辑现有 DNS 提供程序，请选择 DNS 提供程序，然后单击“**编辑**”。
4. 添加或更新所需详细信息。
5. 单击“**保存**”。

更改域映射

要编辑现有 DNS 提供程序的域映射，请执行以下步骤：

1. 导航到 **SSL 仪表板 > 第三方集成 > ACME > DNS 提供商.**
2. 选择 DNS 提供程序，然后单击“**编辑**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 导航到“**域映射**”，并根据需要添加或删除域。
4. 单击“**保存**”。

重要：

如果域未映射，其证书续订将停止。请务必将域重新映射到有效的 DNS 提供程序，以确保续订继续进行。

限制

- 证书续订仅适用于 `acme.sh` 支持的 DNS 提供程序。

排查与自动证书续订相关的问题

本节列出了一些可能出现的常见错误消息及其相关的根本原因：

- 当证书中的域名不符合 ACME 要求时，会报告“**证书具有无效域 - ADCD**”错误。
- 当请求的域名缺少点（例如“example”而不是“example.com”）时，会报告“**请求的标识符无效 :: 无法为“testdomain”颁发：域名需要至少一个点**”错误。
- 当 ACME 客户端无法从 CA 获取随机数时（通常是由于网络或服务器问题），会报告“**无法从 CA 服务器获取随机数。请检查 CA 服务器配置。**”错误。
- 当 ACME 客户端无法初始化与 CA 服务器的通信时（可能是由于配置错误），会报告“**无法初始化 CA 服务器的 API。请检查 CA 服务器配置。**”错误。
- 当域名格式无效或 ACME 协议不允许时，会报告“**提供的域名无效。请检查域名并重试。**”错误。
- 当证书请求未更改域列表且证书已存在时，会报告“**域未更改。具有相同配置的证书已存在。**”错误。
- 当 ACME 客户端无法为域验证添加所需的 DNS TXT 记录时，会报告“**添加域验证 TXT 记录时出错。请检查 DNS 配置并重试。**”错误。
- 当存在签名不匹配时（通常是由于客户端和服务器之间的时间同步问题），会报告“**签名不匹配。请检查服务器时间，因为它可能未同步。**”错误。
- 当未为基于 DNS 的域验证指定 DNS 提供程序时，会报告“**证书缺少 DNS 提供程序名称。**”错误。
- **由于未配置活动 DNS 提供程序，续订已跳过。** 在尝试证书续订但未配置活动 DNS 提供程序时报告此消息。
- **验证联系人时出错 :: 无法解析电子邮件地址** 在提供的联系人电子邮件地址无效或无法解析时报告此消息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **无法处理最终订单请求。（对于无效的 ACME 目录 URL）** 当 ACME 客户端无法完成订单时报告此消息，这通常是由于 ACME 目录 URL 无效或无法访问造成的。
- **DNS 提供程序 - TestDNS 不存在或未激活。** 在系统中找不到或未激活指定的 DNS 提供程序时报告此消息。
- **配置 CA ID 为空/不存在。** 在 CA 配置 ID 缺失或与任何现有配置不匹配时报告此消息。

零接触证书管理

在 NetScaler Console 中，您可以在运行版本 **14.1-34.x** 及更高版本的托管 NetScaler 实例上配置零接触证书管理。借助零接触证书管理，您可以消除手动干预，并构建一个内存中的零接触证书存储，以服务应用程序请求。导航到 **Infrastructure > SSL Dashboard > Zero-Touch Certificate Management**，在 NetScaler Console 上上传所有证书和密钥，并在托管 NetScaler 实例上启用它。NetScaler 会定期轮询证书存储库，并根据需要提供必要的证书。

借助零接触证书管理，NetScaler® 会自动完成以下过程：

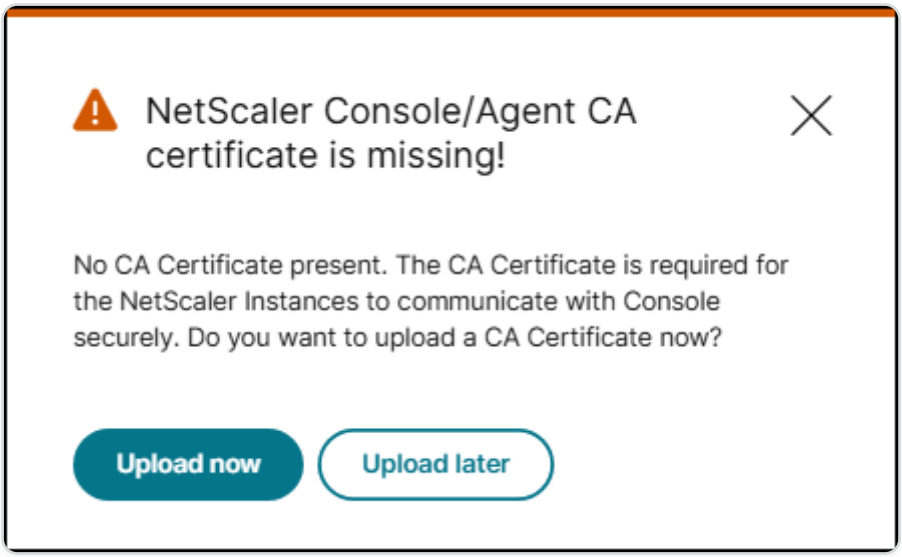
- 添加、绑定和链接证书
- 按特定顺序或一起提供证书和密钥
- 根据请求安装和使用合适的证书
- 在定期轮询周期内删除过期证书

有关零接触证书如何在 NetScaler 实例上工作的更多信息，请参阅 NetScaler 零接触证书管理。

作为管理员，您必须在 NetScaler Console 中确保以下事项：

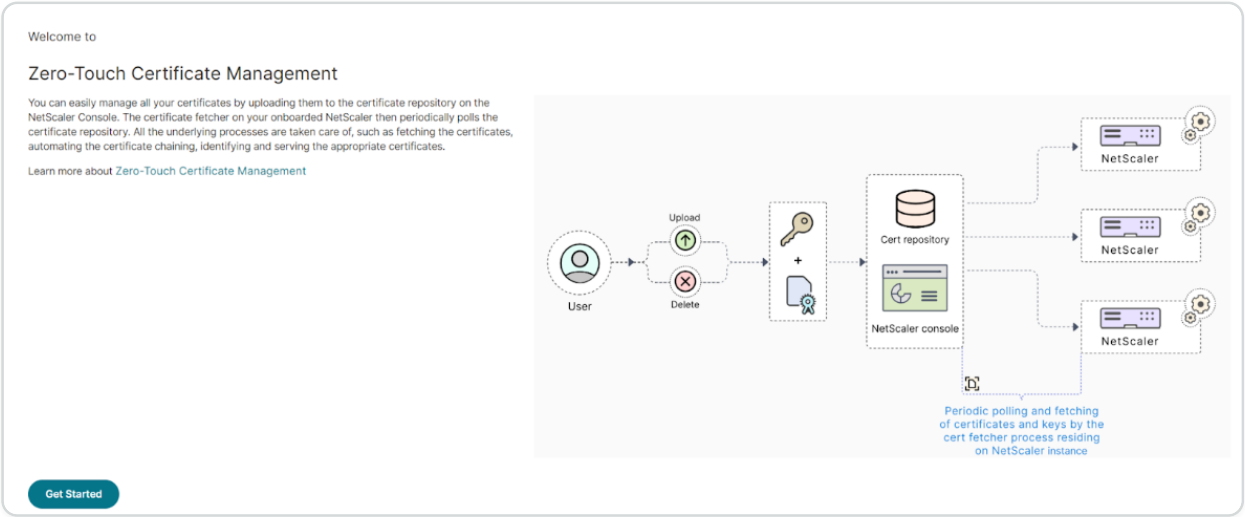
- NetScaler 实例正在运行版本 14.1-34.x 或更高版本，并且它们在 NetScaler Console 中进行管理。
- 上传证书（任何格式）和密钥。然后，在托管 NetScaler 实例上启用零接触。
- 确保 NetScaler Console 上存在有效的 CA 证书。如果您有更新的 Console CA 证书，请在托管 NetScaler 实例上启用零接触之前上传该证书。如果 NetScaler Console 上没有 CA 证书，则会显示以下错误消息：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



上传证书

1. 导航到 **基础架构 > SSL 仪表板 > 零接触证书管理**。
2. 点击**开始使用**。



3. 列出了运行版本 14.1-34.x 或更高版本的 NetScaler 实例。您可以点击**配置零接触**以启用零接触，或者点击**跳过**以继续下一步。
4. 点击**上传**以上传所有证书（可以是任何格式，例如 .pem、.cer 和 .crt）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

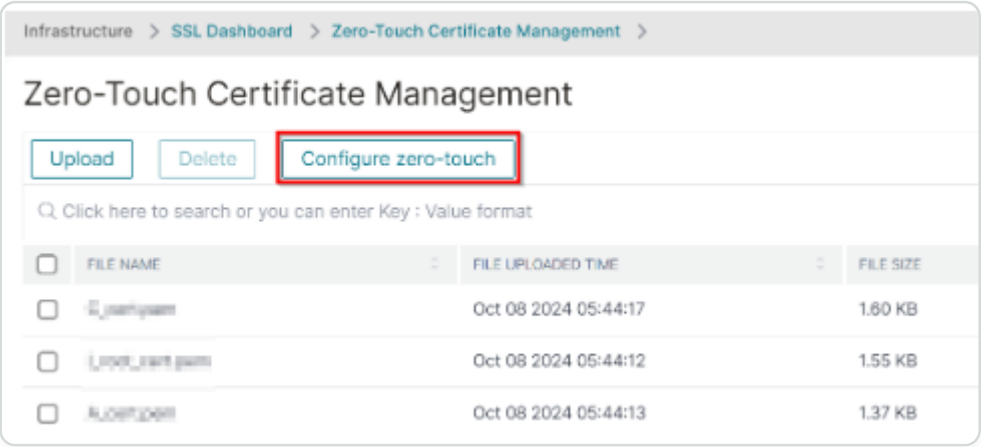
注意：

- 证书或密钥文件必须小于 8192 字节。
- 如果您正在上传多个证书或密钥文件，最大支持大小为 50000 字节。
- 如果证书或密钥文件受密码保护，请确保提供密码。如果未提供密码，则不会上传证书或密钥文件。

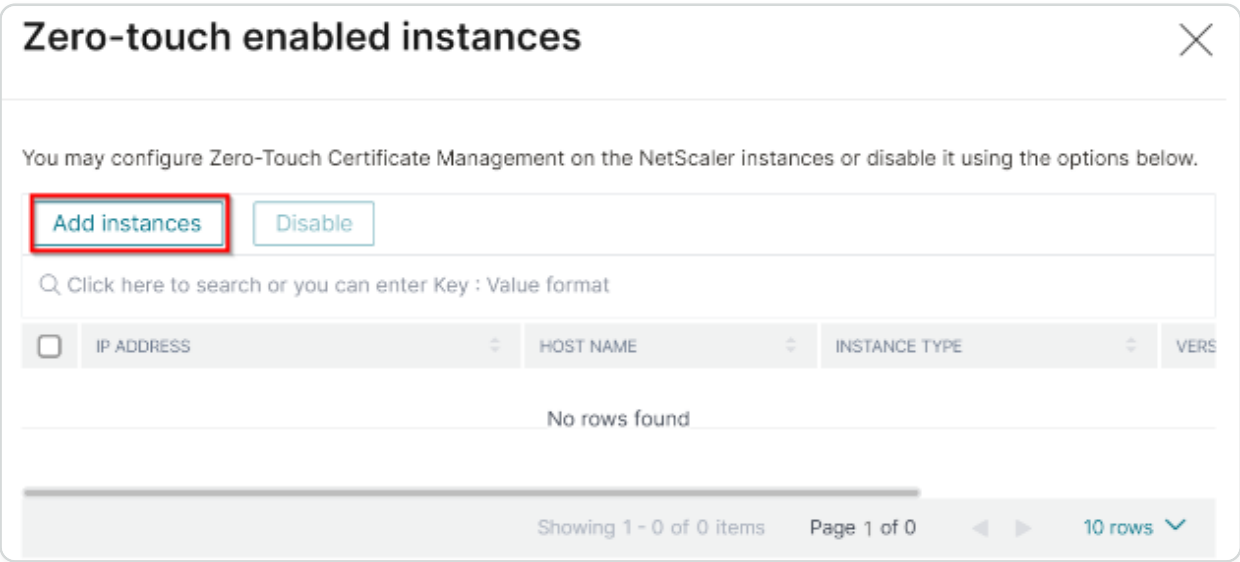
启用零接触证书管理

上传证书后，您必须在托管的 NetScaler 实例上启用零接触。

1. 在**零接触证书管理**页面上，点击**配置零接触**。



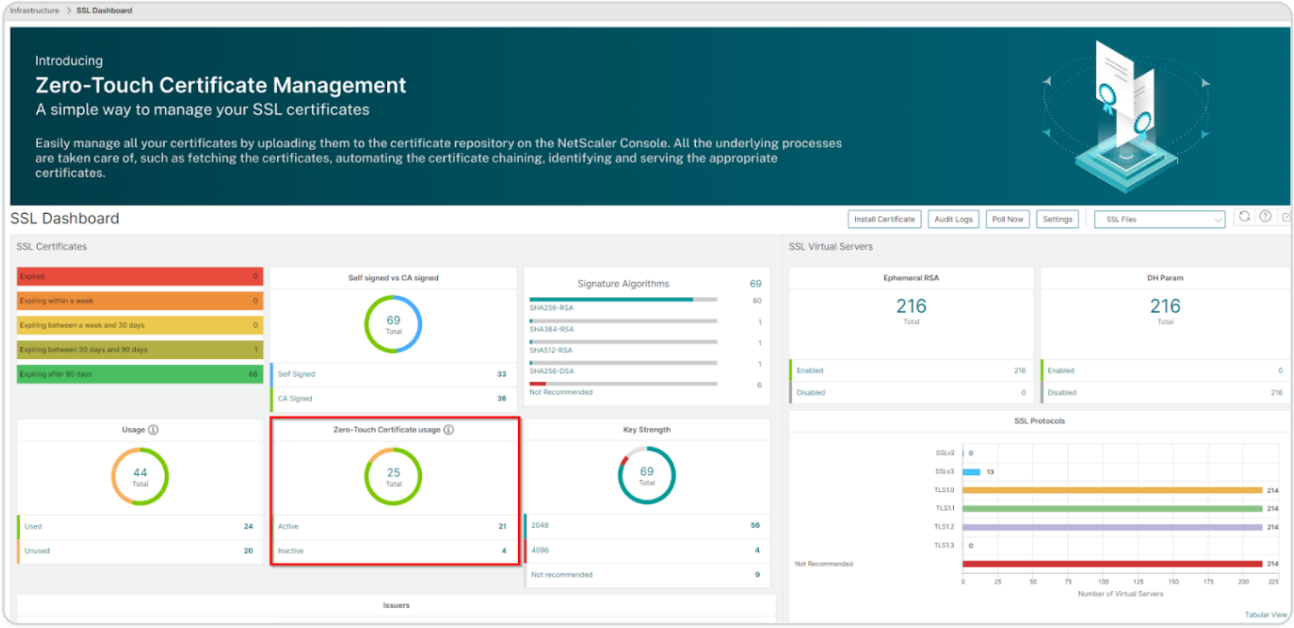
2. 点击**添加实例**，选择实例，然后点击**启用**。



NetScaler Console 使用默认轮询间隔从 NetScaler 实例轮询所有证书。您可以使用**立即轮询**选项立即进行轮询。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 **SSL 控制面板**中，您还可以查看零接触证书使用情况，其中显示了活动和非活动证书的详细信息。



SSL 过滤模式支持

NetScaler 实例会获取特定 SSL 证书和私钥的元数据。这种最小权限方法可确保实例仅访问其所需的资产，从而防止一个实例上的泄露暴露您的整个证书基础架构。此功能对于具有多个管理员管理一组 NetScaler 实例以实现不同目的的环境特别有用。

部分优势包括：

- **安全分段** - 在每个 NetScaler 级别限制元数据访问，以最大限度地减少攻击面并遵守组织安全策略。
- **简化的管理体验** - 通过仅向管理员显示与其 NetScaler 实例组相关的资产，降低了多租户或部门部署的复杂性。
- **优化资源利用率** - 通过仅获取所需 SSL 证书和私钥的元数据，防止系统内存膨胀。

过滤模式配置定义了 NetScaler 实例和 SSL 文件如何通过特定的同步类型进行交互。您可以通过 NetScaler Console 管理这些设置，以确保每个实例仅获取必要的元数据。

组件	同步类型	描述
NetScaler 实例	自定义同步	此模式下的 NetScaler 实例仅获取专门映射到该实例的证书和密钥的元数据。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

组件	同步类型	描述
NetScaler 实例	全局同步	此模式下的 NetScaler 实例会获取所有已上传证书和私钥的元数据。
SSL 文件	自定义文件	这些文件专门映射到自定义同步模式下的 NetScaler 实例。
SSL 文件	全局文件	全局同步模式下的所有 NetScaler 实例都会获取这些文件的元数据。

配置筛选模式设置

要配置筛选模式，请为您的实例和文件定义同步类型。这可确保敏感元数据的安全优化分发。

您可以通过使用 SSL 仪表板的“**证书文件**”和“**NetScaler 实例**”部分中的上传按钮直接上传证书和私钥。

要使用 GUI 进行配置：

1. **上传新文件（零日）** - 导航到“**证书文件和 NetScaler 实例 > 上传**”以添加新资产。

   选择以下同步类型之一：

   - **全局** - 选择使用全局同步模式并完成上传。
   - **自定义** - 选择使用自定义同步模式，选择要映射的特定实例，然后上传文件。

2. **移动现有文件（第 N 天）** - 要将证书和密钥从全局同步模式切换到自定义同步模式，请选择目标 NetScaler 实例，然后单击“**添加现有文件**”。
3. **选择域** - 选择实例后，选择相关域以触发切换。NetScaler Console 会自动检测并将相应的证书和私钥文件切换到自定义同步模式。
4. **查看资产** - 导航到登录页面，查看自定义同步模式下映射到每个 NetScaler 实例的所有证书和私钥文件。
5. **切换同步模式** - 要将实例返回到全局同步模式，请在登录页面上单击“**切换到全局同步**”。

使用 SSL 仪表板

您可以使用 NetScaler Console 中的 SSL 证书仪表板查看图表，这些图表可帮助您跟踪证书颁发者、密钥强度和签名算法。SSL 证书仪表板还显示指示以下内容的图表：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

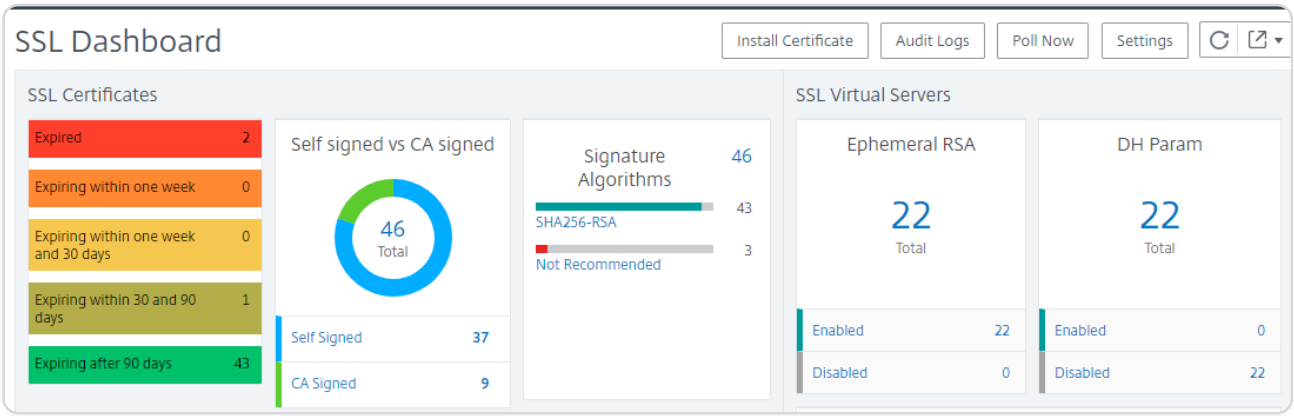
- 证书过期后的天数
- 已使用和未使用证书的数量
- 自签名和 CA 签名证书的数量
- 颁发者数量
- 签名算法
- SSL 协议
- 按使用中证书数量排名前 10 的实例

监控 SSL 证书

如果您的公司有 SSL 策略，并且您已定义了某些 SSL 证书要求，例如所有证书必须具有至少 2048 位的密钥强度，并且必须由受信任的 CA 机构授权，那么您可以使用 NetScaler Console 上的 SSL 仪表板来监控您的证书。

再举一个例子，您可能已上传了一个新证书，但忘记将其绑定到虚拟服务器。SSL 仪表板会突出显示正在使用或未使用的 SSL 证书。在“**使用情况**”部分中，您可以看到已安装的证书数量和正在使用的证书数量。您可以进一步单击图表，查看证书名称、正在使用它的实例、其有效期、其签名算法等。

要在 NetScaler Console 中监控 SSL 证书，请导航到“**基础结构 > SSL 仪表板**”。



NetScaler Console 允许您轮询 SSL 证书，并立即将实例的所有 SSL 证书添加到 NetScaler Console。为此，

1. 导航到 **Infrastructure（基础架构）> SSL Dashboard（SSL 控制板）**。
2. 单击 **Poll Now（立即轮询）**。

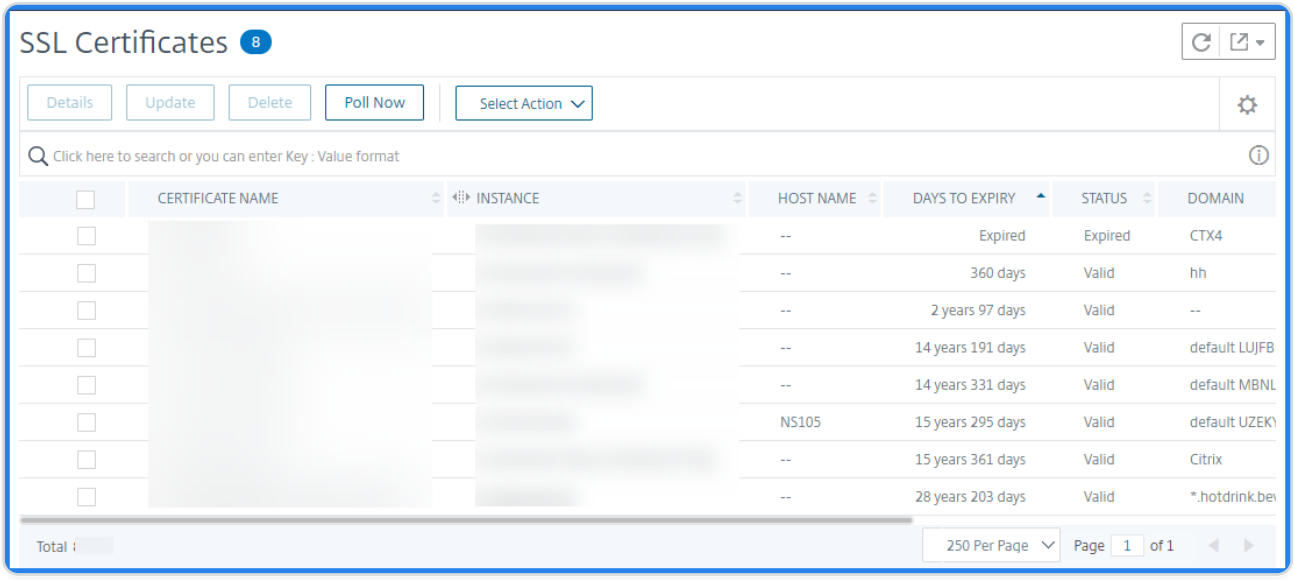
   在 **Poll Now（立即轮询）** 页面上，您可以轮询所有托管的 NetScaler 实例或选择特定实例。
3. 单击 **Start Polling（开始轮询）**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 **SSL Dashboard（SSL 控制板）** 中，您可以监控 NetScaler SSL 证书、SSL 虚拟服务器和 SSL 协议。

您可以单击控制板上的指标以查看与 SSL 证书、SSL 虚拟服务器或 SSL 协议相关的详细信息。

例如，当您单击控制板上 **Self signed vs CA signed（自签名与 CA 签名）** 下的数字时，NetScaler Console GUI 会显示 NetScaler 实例上的所有 SSL 证书。



NetScaler Console SSL 控制板还显示在您的虚拟服务器上运行的 SSL 协议的分布。作为管理员，您可以通过 SSL 策略指定要监控的协议，有关更多信息，请参阅 配置 SSL 策略。支持的协议有 SSLv2、SSLv3、TLS 1.0、TLS 1.1、TLS 1.2 和 TLS 1.3。虚拟服务器上使用的 SSL 协议以条形图格式显示。单击特定协议会显示使用该协议的虚拟服务器列表。

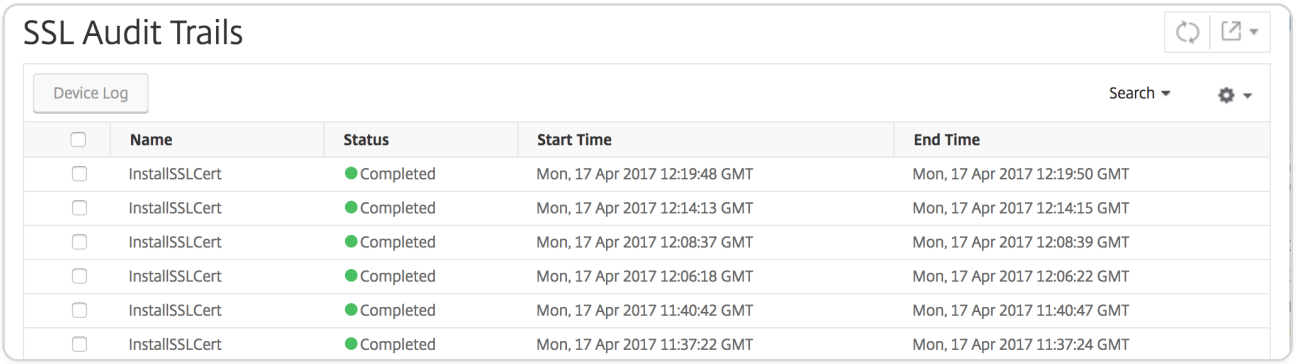
在 SSL 控制板上启用或禁用 Diffie-Hellman (DH) 或临时 RSA 密钥后，将显示一个环形图。即使服务器证书不支持导出客户端（例如 1024 位证书），这些密钥也能实现与导出客户端的安全通信。单击相应的图表会显示已启用 DH 或临时 RSA 密钥的虚拟服务器列表。

查看 SSL 证书的审计跟踪

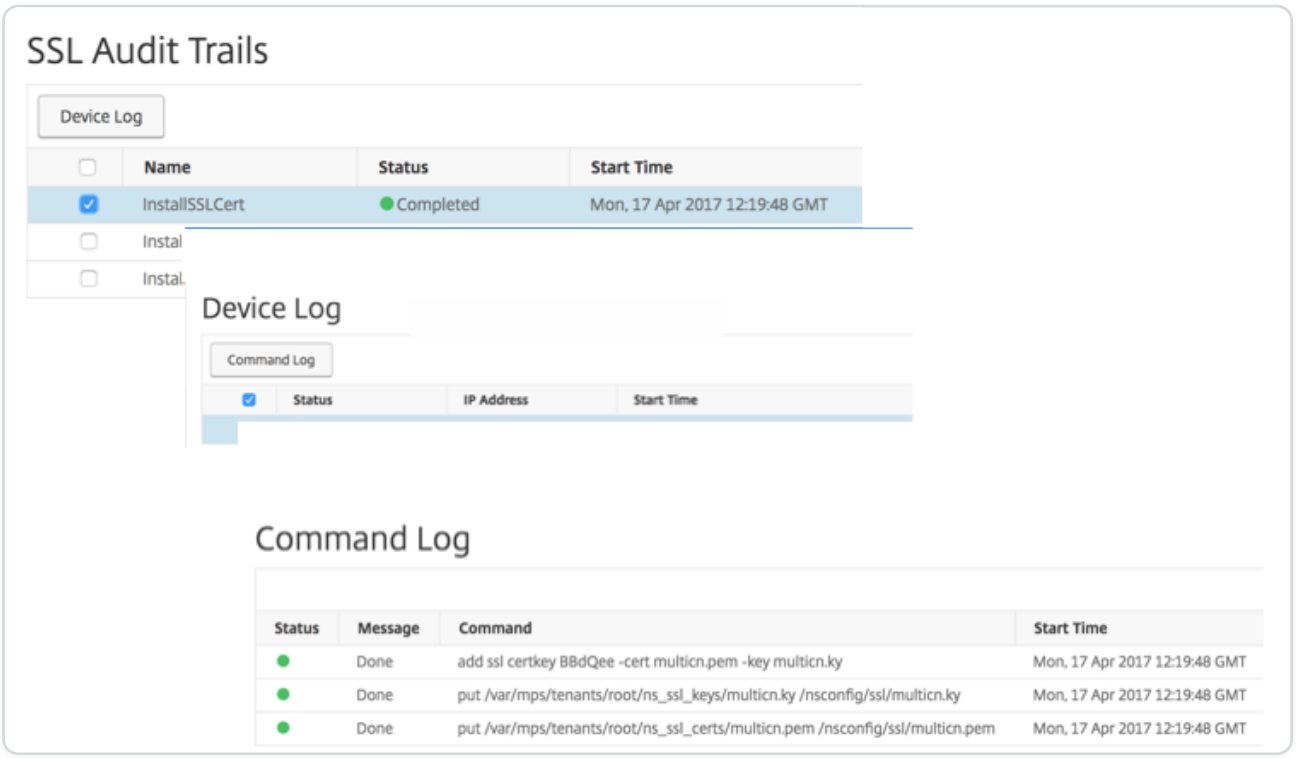
您现在可以在 NetScaler Console 上查看 SSL 证书的日志详细信息。日志详细信息显示在 NetScaler Console 上使用 SSL 证书执行的操作，例如：安装 SSL 证书、链接和取消链接 SSL 证书、更新 SSL 证书以及删除 SSL 证书。审计跟踪信息在监控具有多个所有者的应用程序上进行的 SSL 证书更改时非常有用。

要查看在 NetScaler Console 上使用 SSL 证书执行的特定操作的审计日志，请导航到 **Infrastructure（基础架构）> SSL Dashboard（SSL 控制板）** \>，然后单击 **Audit Logs（审计日志）**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



对于使用 SSL 证书执行的特定操作，您可以查看其状态、开始时间和结束时间。此外，您还可以查看执行操作的实例以及在该实例上运行的命令。

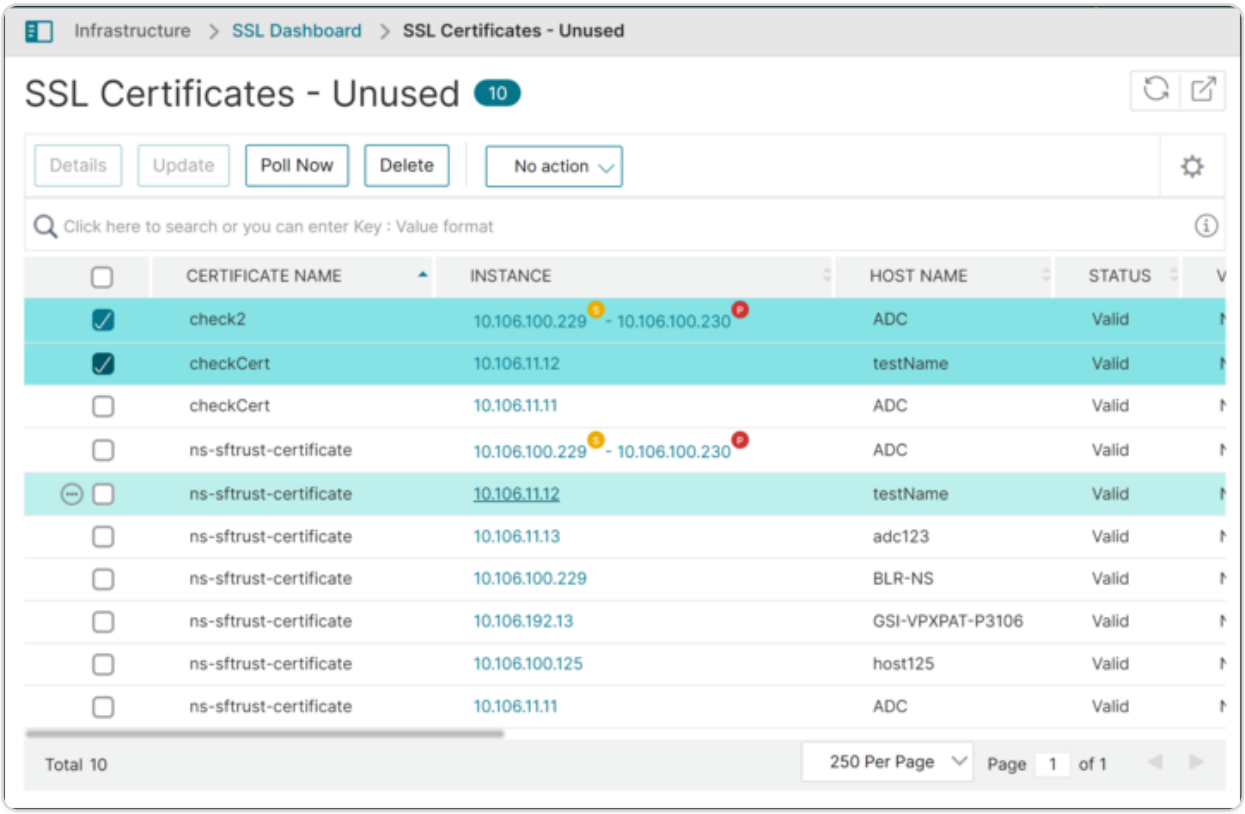


在 SSL 控制面板上删除 SSL 证书

NetScaler 14.1-38.x 及更高版本提供了一个选项，可以在删除所选 SSL 证书配置的同时，从 NetScaler 中删除关联的 SSL 证书文件。要删除 SSL 证书，请执行以下操作：

1. 导航到 **基础架构 > SSL 控制面板**。
2. 在显示 SSL 证书详细信息的 **SSL 证书** 部分中，单击 **未使用** 标签上的链接。
3. 将显示一个包含未使用证书列表的页面。
4. 选择一个或多个要删除的未使用证书。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 单击 **删除**。
6. 将出现一个 **确认** 对话框，提供以下选项，用于从 NetScaler® 中删除证书文件：
   - **不删除**：跳过从 NetScaler 中删除证书文件。
   - **删除**：从 NetScaler 中删除过期和未过期证书的证书文件。
   - **如果过期则删除**：仅从 NetScaler 中删除过期证书的证书文件。

> **注意：**
>
> 对于早于 14.1-38.x 的 NetScaler 版本，所有这三个选项都将跳过证书文件的删除。 随配置一起删除证书文件的选项仅适用于 NetScaler 14.1-38.x 及更高版本。

7. 根据您的需求选择相应的选项。
8. 单击“**是**”删除证书，或单击“**否**”退出工作流而不进行任何更改。

SSL 审计跟踪(/en-us/netscaler-application-delivery-management-software/media/delete-certificate.png)

在 SSL 控制板上排除默认 NetScaler 证书

NetScaler Console 允许您根据偏好显示或隐藏 SSL 控制板图表上显示的默认 NetScaler 证书。默认情况下，所有证书（包括默认证书）都会显示在 SSL 控制板上。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要在 SSL 控制板上显示或隐藏默认证书：

1. 在 NetScaler Console GUI 中，导航到“**基础结构 > SSL 控制板**”。
2. 在“**SSL 控制板**”页面上，单击“**设置**”。
3. 在“**设置**”页面上，选择“**常规**”。
4. 键入证书过期天数，以接收有关证书过期的通知。
5. 选择通知方法并创建相应的配置文件。
6. 在“**证书筛选器**”部分中，清除“**显示默认证书**”复选框，然后单击“**保存并退出**”。

   排除默认证书(/en-us/netscaler-application-delivery-management-software/media/nmas-ssl-dashboard-3.png)

查看、上传和下载 SSL 文件

要在 NetScaler Console 上查看 SSL 文件，请导航到“**基础结构 > SSL 控制板 > NetScaler Console 上的 SSL 文件**”。

您可以在 NetScaler Console 上查看、上传和下载以下文件：

- SSL 证书
- SSL 密钥
- SSL CSR

要在 NetScaler 实例上查看和下载 SSL 文件，请导航到 **Infrastructure > SSL Dashboard > SSL Files on NetScaler**。

只有在 NetScaler 实例已手动或通过计划备份过程进行备份后，您才能访问 SSL 文件。

重要提示：

要启用从 NetScaler 实例下载 SSL 文件，请启用 **Instance SSL certificates** 功能。有关更多信息，请参阅 启用或禁用 NetScaler Console 功能。

查看 SSL 证书链

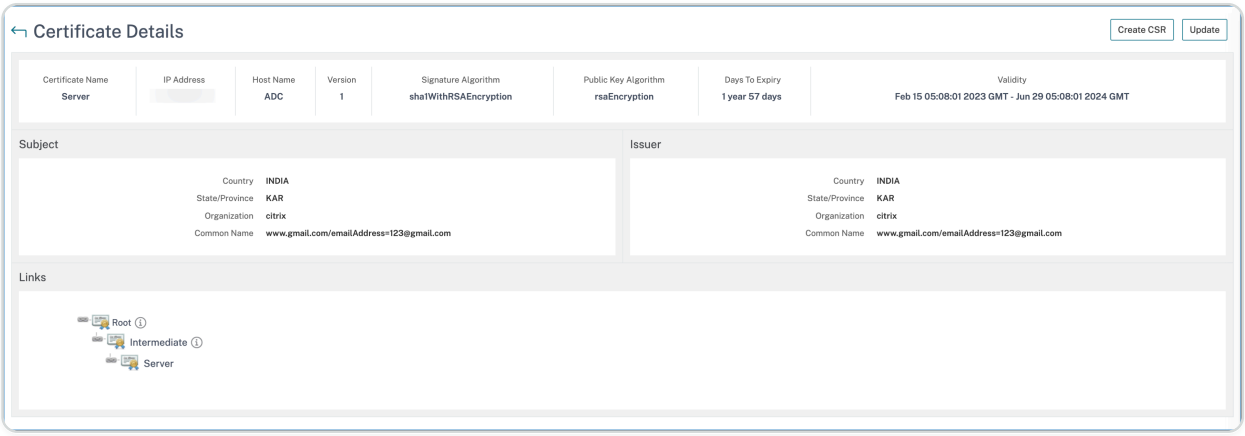
您可以查看从中间证书到根 CA 证书的完整证书链。

要查看证书链：

1. 导航到 **Infrastructure > SSL Dashboard**，然后单击任意磁贴中的 SSL 证书。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 在 **SSL Certificates** 页面中，选择一个证书并单击 **Details**。证书链显示在 **Links** 下。



设置 SSL 证书过期通知

作为安全管理员，您可以设置通知，以便在证书即将过期时通知您，并包含有关哪些 Citrix NetScaler 实例使用这些证书的信息。通过启用通知，您可以及时续订 SSL 证书。

例如，您可以设置电子邮件通知，使其在证书到期前 30 天发送到电子邮件分发列表。

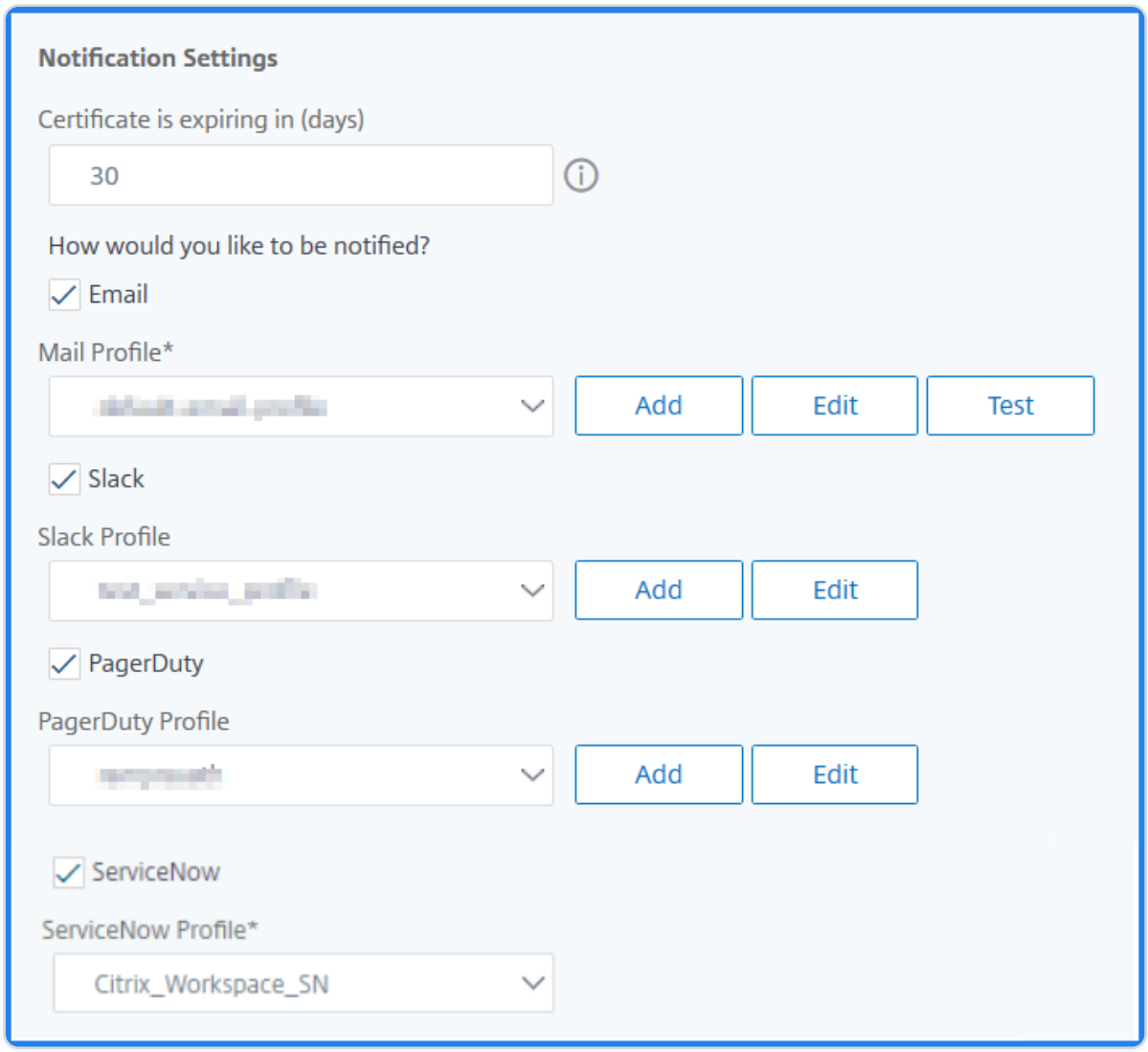
从 NetScaler Console 设置通知：

1. 在 NetScaler Console 中，导航到 **基础设施 > SSL 仪表板**。
2. 在 **SSL Dashboard** 页面上，单击 **Settings**。
3. 在 **SSL Settings** 页面上，单击 **Edit** 图标。
4. 在 **Notification Settings** 部分中，指定您希望在到期日期前多少天发送通知。
5. 选择您要发送的通知类型。从下拉菜单中选择通知类型和分发列表。通知类型如下：
   - **电子邮件** – 指定邮件服务器和配置文件详细信息。当您的证书即将过期时，将触发一封电子邮件。
   - **短信** – 指定短消息服务 (SMS) 服务器和配置文件详细信息。当您的证书即将过期时，将触发一条短信。
   - **Slack** - 指定 Slack 配置文件详细信息。
   - **PagerDuty 警报** - 指定 PagerDuty 配置文件。根据您在 PagerDuty 门户中配置的通知设置，当您的证书即将过期时，将发送通知。
   - **ServiceNow** - 当您的证书即将过期时，通知将发送到默认的 ServiceNow 配置文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要

确保 Citrix Cloud ITSM Adapter 已为 ServiceNow 配置并与 NetScaler Console 集成。有关更多信息，请参阅将 NetScaler Console 与 ServiceNow 实例集成。



6. 单击 **保存并退出**。

当您的 SSL 证书即将过期时，NetScaler Console 现在会将 SSL 证书过期陷阱发送到外部陷阱目标服务器。当满足以下两个条件时，NetScaler Console 会发送陷阱：

- 您已在 SSL 仪表板设置页面中配置了证书过期天数。
- 您已添加陷阱目标。

您可以通过导航到 **设置 > SNMP > 陷阱目标** 来设置陷阱目标。输入发送陷阱的目标 SNMP 服务器的 IP 地址。输入端口号，并将“public”（不带引号）作为社区字符串。

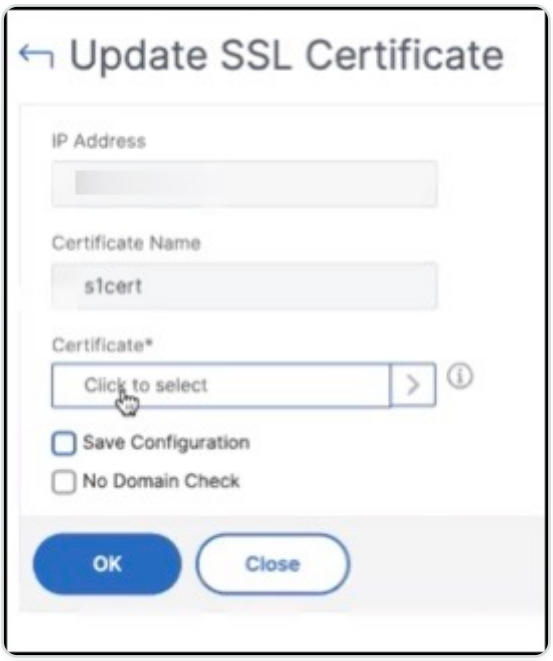
© 1997–2026 Citrix Systems, Inc. All rights reserved.

更新已安装的证书

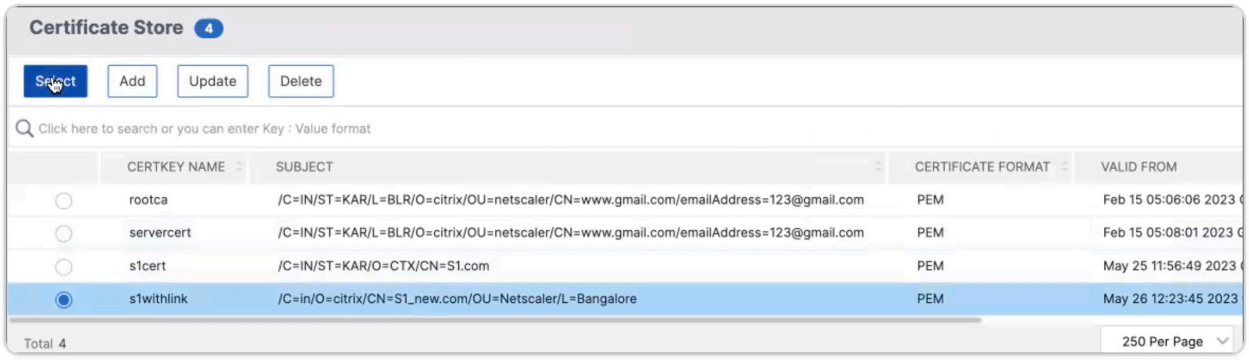
从证书颁发机构 (CA) 收到续订证书后，您无需登录到各个 NetScaler 实例来更新证书。您可以使用证书存储中的证书在 NetScaler Console 中更新现有证书。

要从 NetScaler Console 更新 SSL 证书：

1. 在 NetScaler Console 中，导航到 **基础架构 > SSL 控制面板**。
2. 单击任意图表以查看 SSL 证书列表。
3. 在 **SSL Certificates** 页面中，选择一个证书并单击 **Update**。或者，单击 SSL 证书以查看其详细信息，然后单击 **SSL Certificate** 页面右上角的 **Update**。
4. 在 **Update SSL Certificate** 页面中，选择 **Certificate** 以查看 **Certificate Store** 页面。

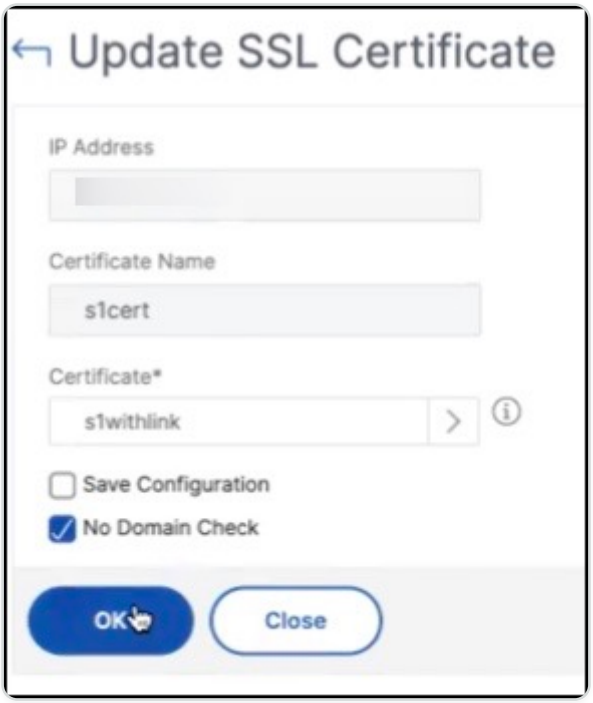


5. 在 **Certificate Store** 页面中，选择要添加的证书文件。单击 **Select**。



6. 如果新证书的域名与旧证书不匹配，并且您希望服务器托管新域，请选择 **No Domain Check**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



单击 **OK**。绑定到此证书的所有 SSL 虚拟服务器都将自动更新。

> **注意：**
>
> 当您使用证书存储中的证书链更新现有 SSL 证书时，现有证书将与链接的证书一起更新。选择证书并单击 **Details** 以查看证书链。

在 NetScaler 实例上安装 SSL 证书

在 Citrix NetScaler 实例上安装 SSL 证书之前，请确保证书由受信任的 CA 颁发。此外，请确保证书密钥的密钥强度为 2048 位或更高，并且密钥使用安全的签名算法进行签名。

从另一个 NetScaler 实例安装 SSL 证书：

您还可以从选定的 NetScaler 实例导入证书，并通过 NetScaler Console GUI 将其应用于其他目标 NetScaler 实例。

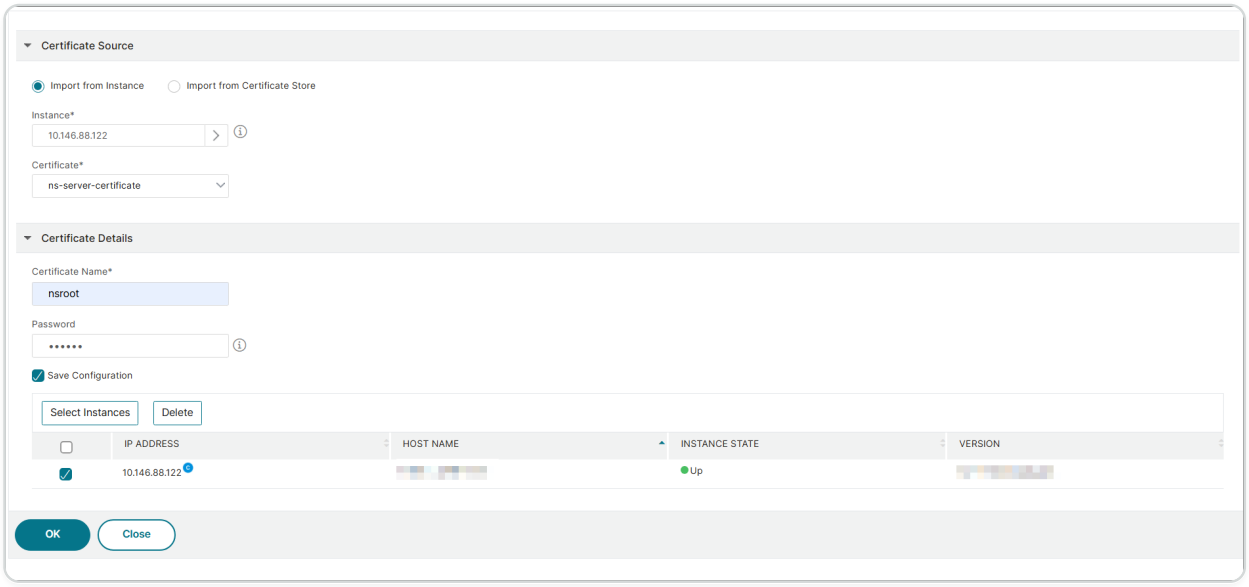
1. 导航到 **基础架构 > SSL 控制板**。
2. 单击**安装证书**。
3. 在**在 NetScaler 实例上安装 SSL 证书**页面上，指定以下参数：
   a. **证书源** 选择**从实例导入**选项。
      - 选择要导入证书的**实例**。
      - 从实例上的所有 SSL 证书文件列表中选择**证书**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **证书详细信息**

- **证书名称**。指定证书密钥的名称。
- **密码**。用于加密私钥的密码。您可以使用此选项上传加密的私钥。

4. 单击**选择实例**以选择要在其上安装证书的 NetScaler 实例。
5. 要保存配置以供将来使用，请选中**保存配置**复选框。
6. 单击 **确定**。



从 NetScaler Console 安装 SSL 证书：

1. 在 NetScaler Console 中，导航到 **基础架构 > SSL 仪表板**。
2. 单击 **安装证书**。
3. 在 **在 NetScaler 实例上安装 SSL 证书** 页面上，指定以下参数：

   a. **证书源** 选择 **从证书存储导入** 选项。

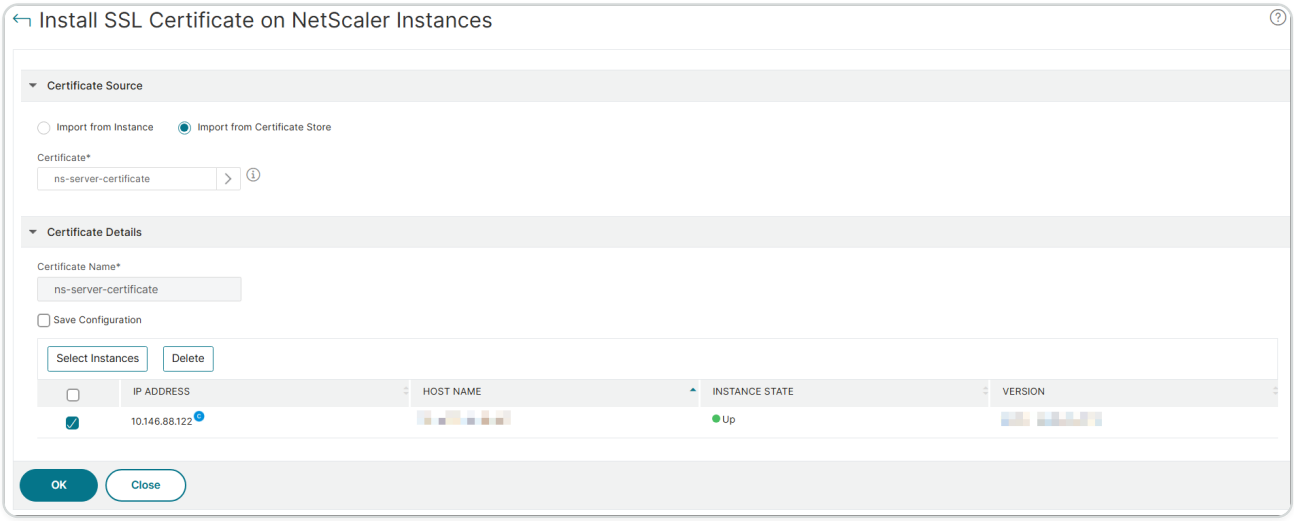
   - **证书文件** - 通过选择 **本地**（您的本地计算机）或 **设备**（证书文件必须存在于 NetScaler Console 虚拟实例上）来上传 SSL 证书文件。

   b. **证书详细信息**

   - **证书名称** – 指定证书密钥的名称。

4. 单击 **选择实例** 以选择您要在其上安装证书的 NetScaler Console 实例。
5. 要保存配置以备将来使用，请选中 **保存配置** 复选框。
6. 单击 **确定**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



创建证书签名请求 (CSR)

证书签名请求 (CSR) 是一个加密文本块，在将使用证书的服务器上生成。它包含将包含在证书中的信息，例如您的组织名称、常用名称（域名）、地区和国家/地区。

使用 NetScaler Console 创建 CSR：

1. 在 NetScaler Console 中，导航到 **基础架构 > SSL 控制板**。
2. 单击任意图表以查看已安装的 SSL 证书列表，然后选择要为其创建 CSR 的证书，并从 **选择操作** 列表中选择 **创建 CSR**。
3. 在 **创建证书签名请求 (CSR)** 页面上，为 CSR 指定名称。
4. 执行以下操作之一：
   - **上传密钥** - 选择 **我有密钥** 选项。要上传密钥文件，请选择 **本地**（您的本地计算机）或 **设备**（密钥文件必须存在于 NetScaler Console 虚拟实例上）。
   - **创建密钥** - 选择“我没有密钥”选项，然后指定以下参数：

加密算法	密钥类型。例如，RSA。
密钥文件名	存储 RSA 密钥的文件的名称。
密钥大小	以位为单位的密钥大小。
公共指数值	从提供的下拉列表中选择 **3** 或 **F4**。此值是创建 RSA 密钥所需的密码算法的一部分。
密钥格式	默认选择 PEM。PEM 是 SSL 证书推荐的密钥格式。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PEM 编码算法	在下拉列表中，选择要用于加密生成的 RSA 密钥的算法（**DES** 或 **DES3**）。如果选择此算法，则需要提供 PEM 密码。
PEM 密码	如果您选择了 PEM 编码算法，请输入密码。
确认 PEM 密码	确认您的 PEM 密码。

5. 单击**继续**。
6. 在下一页上，提供更多详细信息。

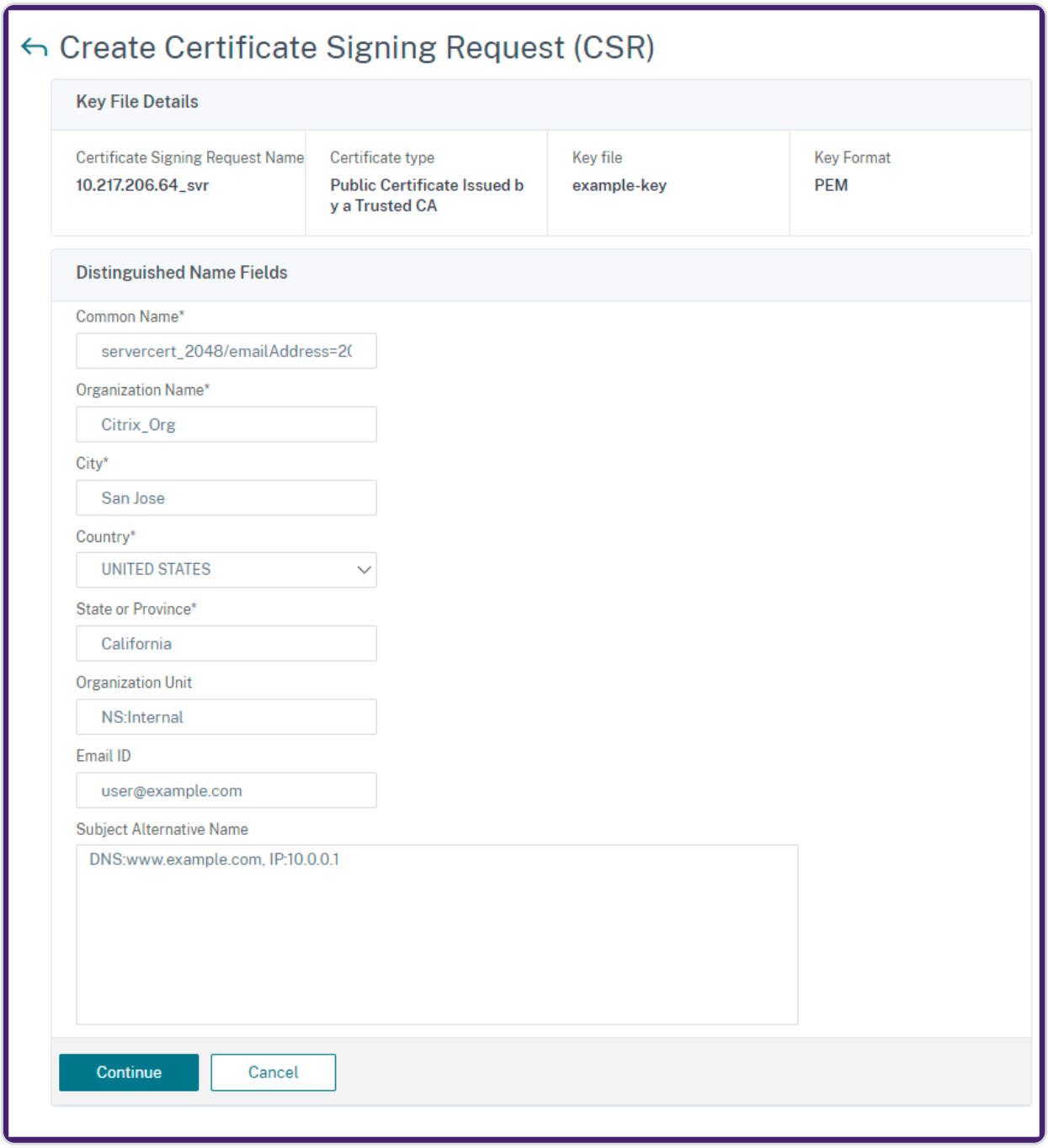
   大多数字段都具有从所选证书主题中提取的默认值。主题包含通用名称、组织名称、省/市/自治区和国家/地区等详细信息。

   在**主题备用名称**字段中，您可以指定多个值，例如使用单个证书的域名和 IP 地址。主题备用名称可帮助您使用单个证书保护多个域。

   以以下格式指定域名和 IP 地址：

```
DNS:<Domain name>, IP:<IP address>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在此示例中，它保护 `10.0.0.1` 和 `www.example.com`。

查看字段并单击“**继续**”。

注意

大多数 CA 接受通过电子邮件提交证书。CA 会将有效证书返回到您提交 CSR 的电子邮件地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

链接和取消链接 SSL 证书

通过将多个证书链接在一起，您可以创建一个证书捆绑包。要将一个证书链接到另一个证书，第一个证书的颁发者必须与第二个证书的域匹配。例如，如果您想将证书 A 链接到证书 B，则证书 A 的“颁发者”必须与证书 B 的“域”匹配。

使用 NetScaler Console 将一个 SSL 证书链接到另一个证书：

1. 在 NetScaler Console 中，导航到 **基础架构 > SSL 控制板**。
2. 单击任意图表以查看 SSL 证书列表。
3. 选择要链接的证书，然后从**操作**下拉列表中选择**链接**。
4. 从匹配的证书列表中，选择要链接到的证书，然后单击**确定**。

> **注意**
>
> 如果未找到匹配的证书，将显示以下消息：未找到可链接的证书。

使用 NetScaler Console 取消链接 SSL 证书：

1. 在 NetScaler Console 中，导航到 **基础架构 > SSL 控制板**。
2. 单击任意图表以查看 SSL 证书列表。
3. 选择任意一个已链接的证书，然后从**操作**下拉列表中选择**取消链接**。
4. 单击**确定**。

> **注意**
>
> 如果所选证书未链接到其他证书，将显示以下消息：证书没有任何 CA 链接。

配置企业策略

您可以在 NetScaler Console 中配置企业策略，并添加所有受信任的 CA、安全的签名算法，以及为您的证书密钥选择推荐的密钥强度。如果安装在您的 Citrix NetScaler 实例上的任何证书尚未添加到企业策略中，SSL 证书仪表板会将这些证书的颁发者显示为“**不推荐**”。

此外，如果证书密钥强度与企业策略中推荐的密钥强度不匹配，SSL 证书仪表板会将这些密钥的强度显示为“**不推荐**”。

在 NetScaler Console 上配置企业策略：

1. 在 NetScaler Console 中，导航到 **基础结构** \> **SSL 仪表板**，然后单击 **设置**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 在“SSL 设置”页面上，单击“**编辑**”图标以添加所有受信任的 CA、安全的签名算法，并为您的证书和密钥选择推荐的密钥强度。支持的密钥强度为 512、1024、2048、3072 和 4096 位。
   - “**推荐的密钥强度**” - 表示算法安全性和密钥中的位数。
   - “**推荐的签名算法**” - 表示为应用程序颁发的签名令牌。
   - “**推荐的受信任 CA**” - 表示颁发数字证书的受信任实体。单击“**+**”图标可添加更多实体。
   - “**推荐的 SSL 协议**” - 表示 TLS/SSL 版本。
3. 单击“**保存**”以保存您的企业策略。

> **注意**
>
> SSL 仪表板仅显示通过“**设置**”选项选择的“**签名算法**”，其他则显示为“**不推荐**”。

从 NetScaler 实例轮询 SSL 证书

NetScaler Console 每 24 小时自动轮询一次 SSL 证书，方法是使用 NITRO 调用和安全复制 (SCP) 协议。您也可以手动轮询 SSL 证书，以发现 Citrix NetScaler 实例上新添加的 SSL 证书。轮询所有 NetScaler 实例的 SSL 证书会给网络带来沉重负担。

您无需轮询所有 NetScaler 实例的 SSL 证书，只需手动轮询选定实例的 SSL 证书即可。

在 NetScaler 实例上轮询 SSL 证书：

1. 在 NetScaler Console 中，导航到 **基础架构 > SSL 控制板**。
2. 在“**SSL 控制板**”页面上，在右上角，单击“**立即轮询**”。

   轮询 SSL 证书(/en-us/netscaler-application-delivery-management-software/media/nmas-ssl-dashboard-1.png)
3. 此时会弹出“**立即轮询**”页面，您可以选择轮询网络中的所有 NetScaler 实例或轮询选定的实例。
   a. 要轮询所有 NetScaler 实例的 SSL 证书，请选择“**所有实例**”选项卡，然后单击“**开始轮询**”。

      开始轮询(/en-us/netscaler-application-delivery-management-software/media/config-audit-poll-now-1.png)
   b. 要轮询特定实例，请选择**选择 实例**选项卡，从列表中选择实例，然后单击**立即轮询**。

      轮询特定实例(/en-us/netscaler-application-delivery-management-software/media/config-audit-poll-now-2.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 NetScaler Console 证书存储来管理 SSL 证书

NetScaler Console 证书存储可帮助您在一个位置存储和管理 SSL 证书。您以后可以使用存储的证书来配置 NetScaler 设置。

证书存储允许您添加、更新和删除 SSL 证书。您还可以使用证书存储从 NetScaler 实例导入证书并将其应用于其他目标 NetScaler 实例。

将 SSL 证书添加到证书存储

1. 导航到 **Infrastructure > SSL Dashboard**，然后从列表中选择 **Manage Certificate Store**。

   证书存储(/en-us/netscaler-application-delivery-management-software/media/certstore-list.png)

2. 单击 **Add**。
3. 在 **Add Certificate** 页面上，输入以下详细信息：

   - **证书密钥名称** - 输入证书的名称。名称只能包含 ASCII 字母数字、下划线和连字符，且必须少于 30 个字符。证书创建后，您无法更改名称。
   - **证书文件** - 浏览到本地驱动器并上传证书文件。
   - **密钥文件** - 从本地计算机上传密钥文件。
   - **密码** - 如果您有 PEM 格式的加密私钥，请键入用于加密私钥的密码。
   - **添加证书链** - 选择此选项可在证书链中添加证书。
   - **证书链** - 浏览到本地驱动器并上传证书文件。
   - 单击 **Create**。

更新证书存储中的 SSL 证书

1. 导航到 **Infrastructure > SSL Dashboard**，然后从列表中选择 **Manage Certificate Store**。
2. 选择要更新的证书，然后单击 **Update**。
3. 在 **Update Certificate** 页面上，输入以下详细信息：

   - **证书密钥名称** - 显示您选择更新的证书的名称。
   - **证书文件** - 要更新证书文件，请上传一个证书文件。
   - **密钥文件** - 要更新密钥文件，请从本地计算机上传一个密钥文件。
   - **密码** - 如果您有 PEM 格式的加密私钥，请键入用于加密私钥的密码短语。
   - **添加证书链** - 选择此选项可在证书链中添加证书。
   - **证书链** - 浏览到本地驱动器并上传证书文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 单击 **OK**。

从证书存储中删除 SSL 证书

1. 导航到 **Infrastructure > SSL Dashboard**，然后从列表中选择 **Manage Certificate Store**。
2. 选择证书，然后单击 **Delete**。
3. 出现提示时，单击 **Yes** 删除证书。

在 NetScaler® 实例上安装 SSL 证书

1. 导航到 **Infrastructure > SSL Dashboard**，然后从列表中选择 **Manage Certificate Store**。
2. 选择证书，然后单击 **Install**。
3. 在 **Install SSL Certificate on NetScaler Instances** 页面中，输入以下详细信息：

   a. **证书源**

   - **证书** - 显示您选择的证书名称。

   b. **证书详细信息**

   - **证书名称** - 显示证书的名称。
   - **保存配置** - 选择此选项以保存 NetScaler 配置。证书安装后，NetScaler 配置将保存。

4. 单击 **Select Instances** 以选择要安装证书的 NetScaler 实例。

单击 **OK**。

从 NetScaler 实例导入证书

1. 导航到 **Infrastructure > SSL Dashboard**，然后从列表中选择 **Manage Certificate Store**。
2. 单击 **导入 NetScaler 证书**。
3. 在 **Import NetScaler Certificates** 页面中，您可以选择以下选项卡之一：

   - **导入 NetScaler 证书** - 单击 **开始轮询** 以轮询所有 NetScaler 实例上的所有 SSL 证书。
   - **选择实例** - 选择一个 NetScaler 实例，然后单击 **导入 NetScaler 证书** 以仅轮询所选 NetScaler 实例上的 SSL 证书。

   轮询后，SSL 证书和密钥文件将被下载并添加到证书存储中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

如果存储中存在相同的证书名称，则证书导入操作将失败。但是，导入操作会继续轮询剩余的证书，并将可用的 NetScaler 证书添加到存储中。

更新服务器证书无需中间上传

您可以续订证书，而无需重复上传中间证书的任务。此增强功能减少了手动工作量，并最大限度地降低了配置错误的风险。

轻松续订

NetScaler Console 默认在更新期间保留现有证书链。这可确保您的链保持完整和有效，即使您只上传新的服务器级证书。

主要改进

- **降低复杂性** - 消除了标准服务器证书更新期间强制性的中间上传。
- **安全第一** - 自动链保留可防止“链断裂”，这是 SSL 握手错误的常见原因。

更新服务器证书无需中间上传

1. 导航到 **基础架构 > SSL 控制板 > 证书存储**。
2. 选择要更新的证书，然后单击 **更新**。
3. **覆盖现有证书链** - 如果您的续订需要更改中间链，请选择此选项：
   - **使用捆绑包** - 用新上传的捆绑包替换现有链。
   - **不使用捆绑包** - 完全移除当前证书链。
4. **添加证书链** - 如果您的主服务器证书文件中未包含中间证书，请选择此选项以手动上传并附加中间证书。

示例

最终证书结构取决于您现有的证书链状态以及您在更新期间选择的选项。

场景 A：现有证书没有链

更新操作	结果
新上传的证书不包含链	服务器证书已更新。未添加中间链。
新上传的证书包含链	服务器证书已更新，并附加了新的中间链。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

场景 B：现有证书包含链

更新操作	结果
新上传的证书包含链（“覆盖现有证书链”已启用）	服务器证书已更新，现有中间链已替换为新链。
新上传的证书不包含链（“覆盖现有证书链”已启用）	服务器证书已更新，现有中间链已明确删除。

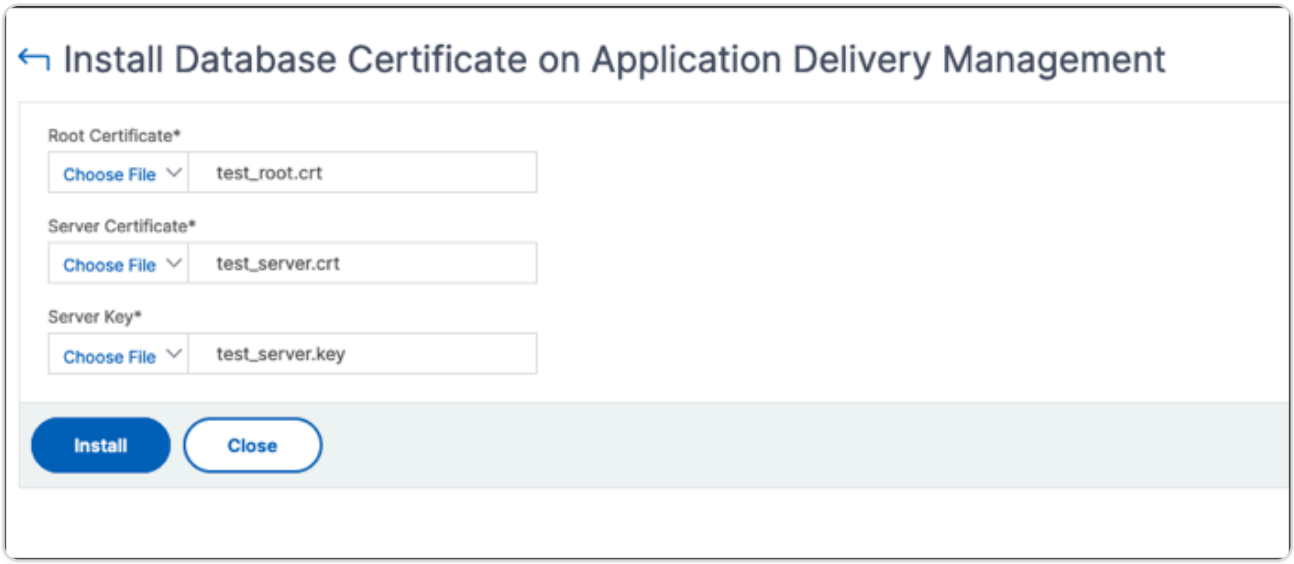
在高可用性部署中管理数据库自定义证书和密码

NetScaler Console 允许您使用来自受信任证书颁发机构的自有证书替换默认内置数据库证书。您还可以在 NetScaler Console 数据库中配置自己的密码套件。此功能为您的证书管理需求提供了更大的灵活性和安全性，并使用受信任的 SSL 证书保护 HA 节点之间的所有通信。

在 NetScaler Console 上安装数据库证书

要在 HA 设置中安装证书，请执行以下操作：

1. 导航到 **设置 > HA 部署**，然后单击 **数据库证书**。
2. 单击 **Installed Certificate** 选项卡，然后单击 **Install New Certificate**。
3. 在 **Install Database Certificate on Application Delivery Management** 页面中，上传根证书、服务器证书和服务器密钥。您可以执行以下操作之一：
   - 选择 **Choose File > Local** 从本地计算机上传证书或密钥文件。
   - 选择 **Choose File > Appliance** 上传 NetScaler Console 上存在的证书或密钥文件。
4. 单击 **Install**。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

如果存在多个链式证书，则必须将它们合并到一个文件中。请确保连接顺序正确，即中间证书在前，根证书在后。此顺序对于正确识别证书链至关重要。

例如，以下命令将每个证书文件（intermediate_certificate1.crt、intermediate_certificate2.crt 和 root_certificate.crt）的内容附加到名为 combined_certs.crt 的文件中：

```
cat intermediate_certificate1.crt >> combined_certs.crt
cat intermediate_certificate2.crt >> combined_certs.crt
cat root_certificate.crt >> combined_certs.crt
```

管理您已安装的数据库证书

要查看、下载和删除已安装的证书，请执行以下操作：

1. 导航到 **设置 > HA 部署**，然后单击 **数据库证书**。
2. 单击 **Certificate Files** 选项卡，然后选择 **Root Certificates**、**Server Certificates** 或 **Server Keys** 以查看相应文件。
3. 要将文件下载到本地计算机，请单击 **Download**。
4. 要删除证书文件，请选择该文件并单击 **Delete**。在出现的确认对话框中，单击 **OK**。

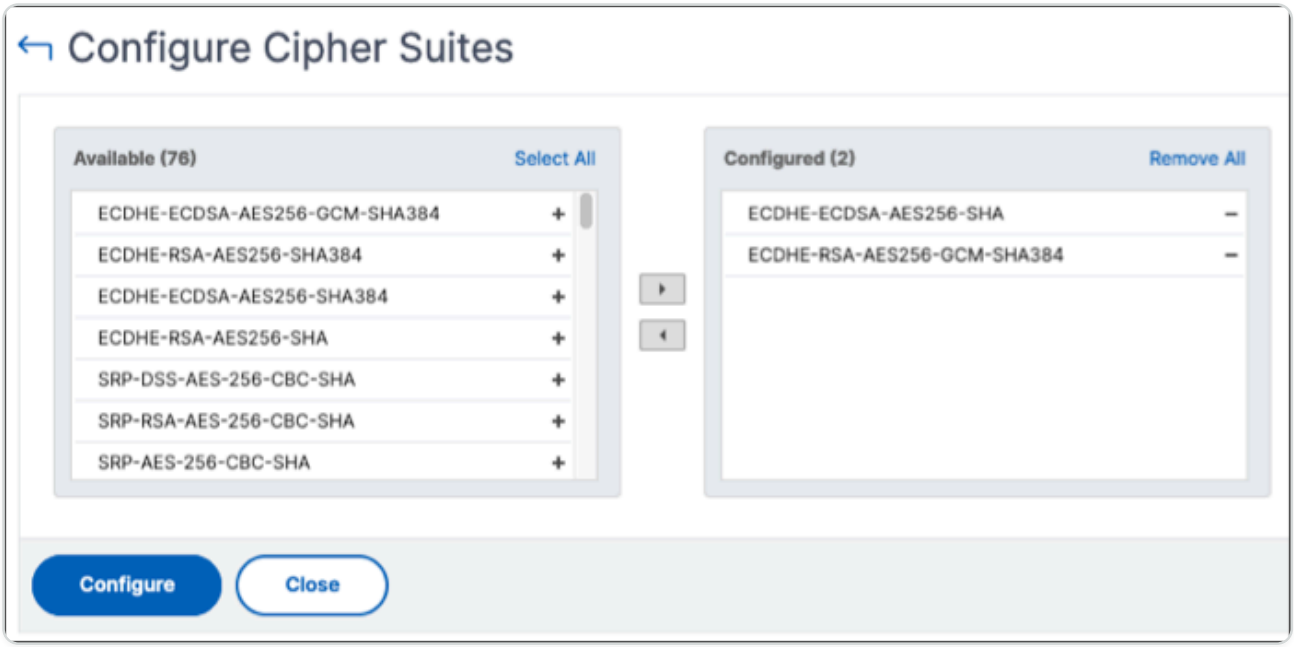
(/en-us/netscaler-application-delivery-management-software/media/ha-manage-db-certs.png)

配置数据库密码套件

要为 HA 部署配置密码套件，请执行以下操作：

1. 导航到 **设置 > HA 部署**，然后单击 **数据库证书**。
2. 单击 **Ciphers** 选项卡，然后单击 **Configure Cipher**。
3. 在 **Configure Cipher Suites** 页面中，从可用密码列表中选择一个或多个密码。
4. 单击 **Configure**。在出现的确认对话框中，单击 **Yes** 以更改密码设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

更改密码设置会重新启动 NetScaler Console 辅助节点和灾难恢复节点。

事件

当 Citrix NetScaler 实例的 IP 地址添加到 NetScaler Console 时，NetScaler Console 会发送一个 NITRO 调用，并隐式地将自身添加为实例的陷阱目标，以接收其陷阱或事件。

事件表示托管 NetScaler 实例上发生的事件或错误。例如，当发生系统故障或配置更改时，会在 NetScaler Console 服务器上生成并记录一个事件。NetScaler Console 中收到的事件显示在“事件摘要”页面（**基础架构 > 事件**）上，所有活动事件都显示在“事件消息”页面（**基础架构 > 事件 > 事件消息**）中。

NetScaler Console 还会检查实例上生成的事件，以形成不同严重级别的警报。这些警报随后会显示为消息，其中一些可能需要立即关注。例如，系统故障可归类为“严重”事件严重性，需要立即处理。

您可以配置规则来监视特定事件。规则使监视在您的 NetScaler 基础架构中生成的众多事件变得更加容易。

您可以通过配置具有特定条件并为规则分配操作的规则来筛选一组事件。当生成的事件符合规则中的筛选条件时，将运行与该规则关联的操作。您可以创建筛选器的条件包括：严重性、NetScaler 实例、类别、故障对象、配置命令和消息。

您还可以确保在事件清除之前，在特定时间间隔内为某个事件触发多个通知。作为一项额外措施，您可以使用特定的主题行和用户消息自定义电子邮件，并上传附件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

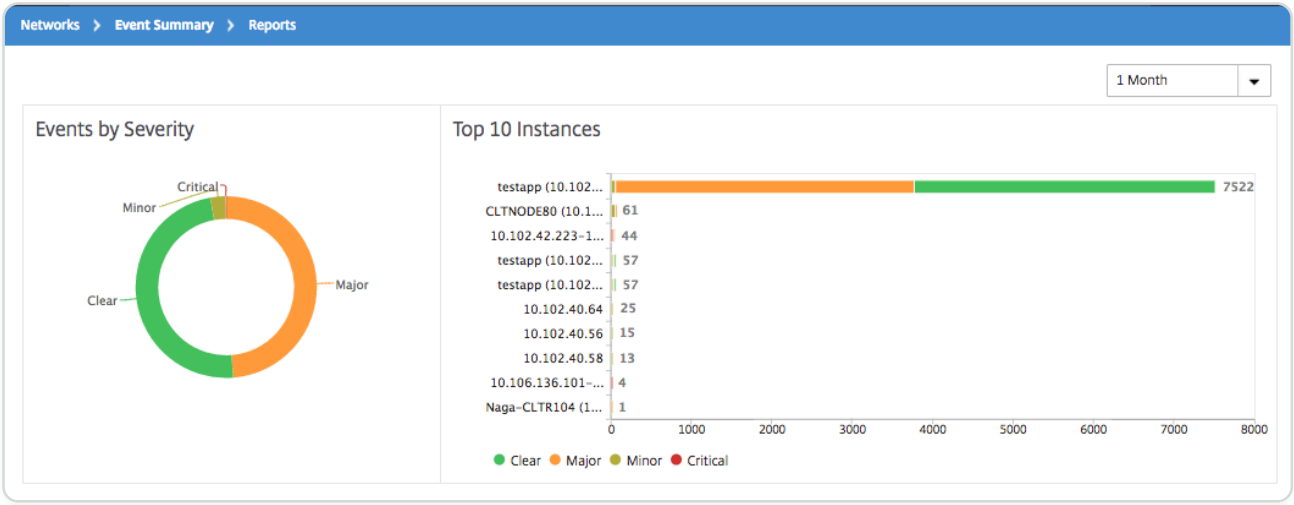
使用事件仪表板

作为网络管理员，您可以查看 NetScaler 实例上的配置更改、登录条件、硬件故障、阈值违规和实体状态更改等详细信息，以及特定实例上的事件及其严重性。您可以使用 NetScaler Console 的事件仪表板查看为所有 NetScaler 实例上的关键事件严重性详细信息生成的报告。

查看事件仪表板上的详细信息：

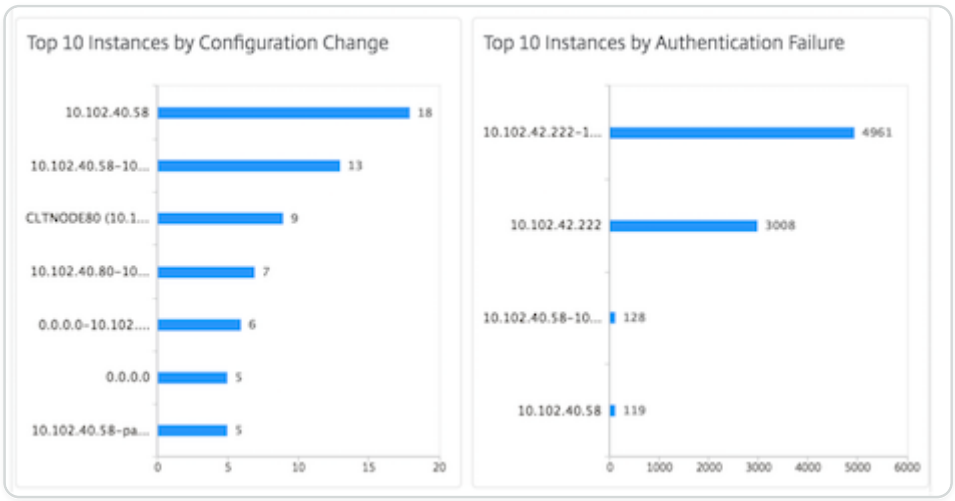
导航到 **基础架构 > 事件 > 报告**。

仪表板上的“前 10 个设备”图表显示了按生成的事件数量排名前 10 的实例的报告。您可以单击图表上的实例以查看事件严重性的更多详细信息。



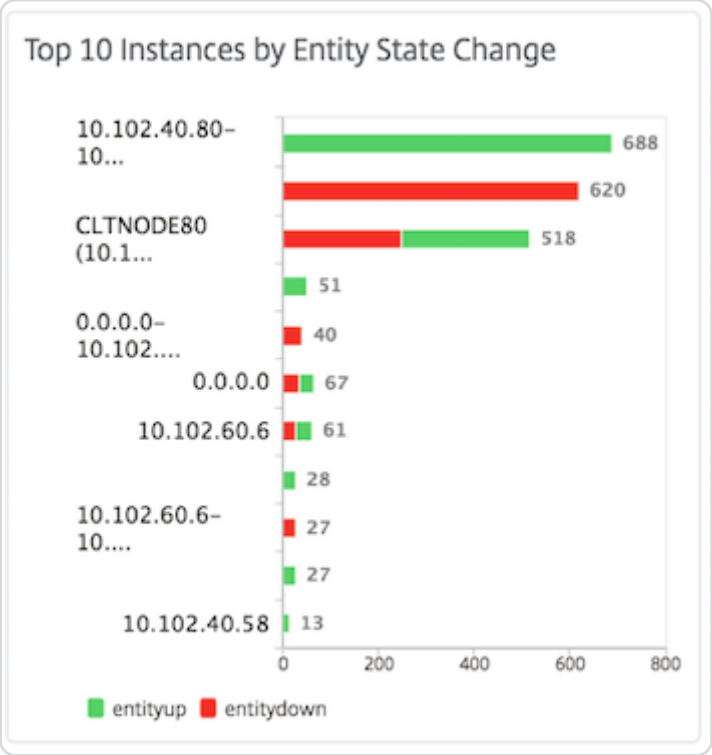
您可以通过导航到 NetScaler 实例类型（**Infrastructure > Events > Reports** \> **NetScaler/ NetScaler SDX**）来查看更多详细信息，包括：

- 按硬件故障排名前 10 的设备
- 按配置更改排名前 10 的设备
- 按身份验证失败排名前 10 的设备

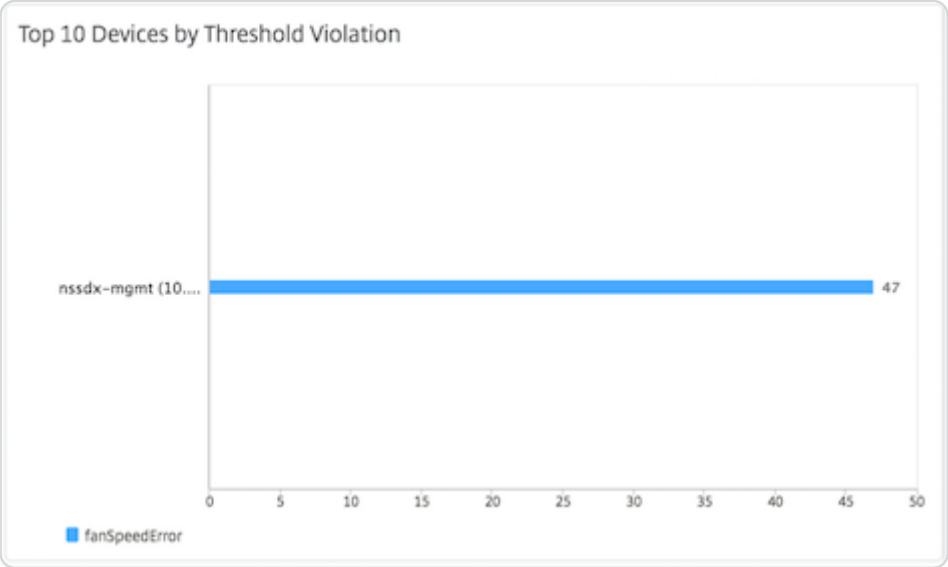


© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 按实体状态更改排名前 10 的设备



- 按阈值违规排名前 10 的设备



为事件设置事件时效

您可以设置事件时效选项以指定时间间隔（以秒为单位）。NetScaler Console 会监控设备，直到达到设定的持续时间，并且仅当事件时效超过设定的持续时间时才生成事件。

注意：

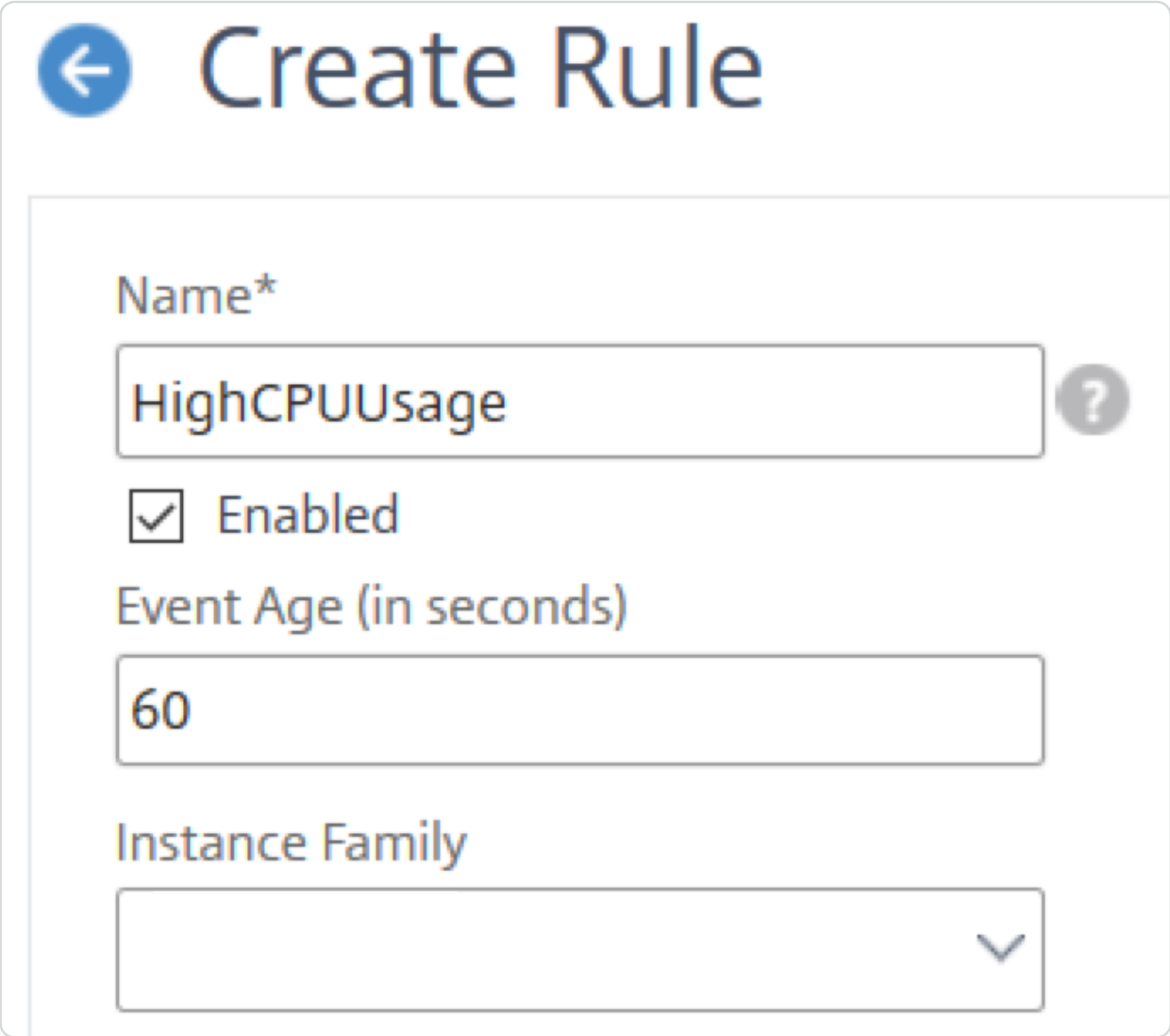
> 事件时效的最小值为 60 秒。如果将**事件时效**字段留空，则事件发生后会立即应用事件规则。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

例如，假设您要管理各种 NetScaler 设备，并在任何虚拟服务器停机 60 秒或更长时间时通过电子邮件收到通知。您可以创建包含必要筛选器的事件规则，并将该规则的事件时效设置为 60 秒。然后，只要虚拟服务器停机 60 秒或更长时间，您就会收到一封电子邮件通知，其中包含实体名称、状态更改和时间等详细信息。

在 NetScaler Console 中设置事件时效：

1. 在 NetScaler Console 中，导航到**基础结构 > 事件 > 规则**，然后单击**添加**。
2. 在**创建规则**页面上，设置规则参数。
3. 以秒为单位指定事件时效。



设置事件时效时，请确保在**类别**部分中设置所有相关陷阱，并在**严重性**部分中设置相应的严重性。在前面的示例中，选择 `entityup`、`entitydown` 和 `entityofs` 陷阱。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

计划事件过滤器

创建规则过滤器后，如果您不希望 NetScaler Console 服务器在每次生成的事件满足过滤器条件时都发送通知，则可以安排过滤器仅在特定的时间间隔（例如每天、每周或每月）触发。

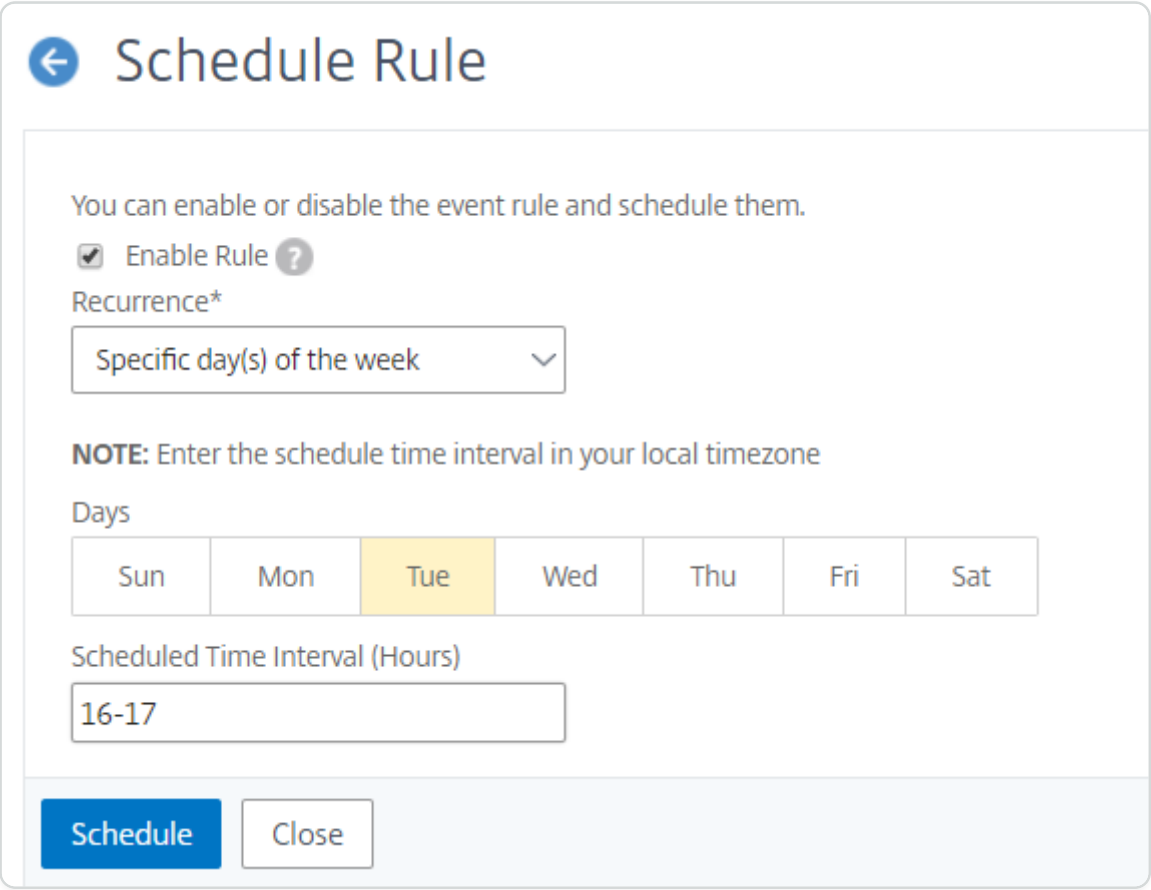
例如，如果您已为实例上不同应用程序在不同时间安排了系统维护活动，则实例可能会生成多个警报。

如果您已为这些警报配置了过滤器并为这些过滤器启用了电子邮件通知，则当 NetScaler Console 收到这些陷阱时，服务器会发送大量电子邮件通知。如果您希望服务器仅在特定时间段内发送这些电子邮件通知，则可以通过安排过滤器来实现。

使用 NetScaler Console 安排过滤器：

1. 在 NetScaler Console 中，导航到 **基础架构 > 事件 > 规则**。
2. 选择要为其安排过滤器的规则，然后单击 **View Schedule**。
3. 在 **Scheduled Rule** 页面上，单击 **Schedule** 并指定以下参数：
   - **启用规则** – 选中此复选框以启用计划的事件规则。
   - **重复** - 安排规则的间隔。选择一周中的特定某天或一个月中的特定日期。
   - **天数**：选择运行规则的星期几。您可以选择多天。
   - **日期**：输入日期。您可以输入多个日期，用逗号分隔。
   - **计划时间间隔（小时）** – 安排规则的小时数（使用 24 小时制）。
4. 单击 **Schedule**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



设置事件的重复电子邮件通知

为确保所有关键事件都得到处理，并且不会错过任何重要的电子邮件通知，您可以选择为符合所选条件的事件规则发送重复的电子邮件通知。例如，如果您为涉及磁盘故障的实例创建了事件规则，并且希望在问题解决之前一直收到通知，则可以选择接收有关这些事件的重复电子邮件通知。

这些电子邮件通知会以预定义的间隔重复发送，直到收件人确认已看到通知或事件规则被清除。

注意

只有在您的 NetScaler 实例设置并发送了等效的“清除”陷阱时，事件才能自动清除。

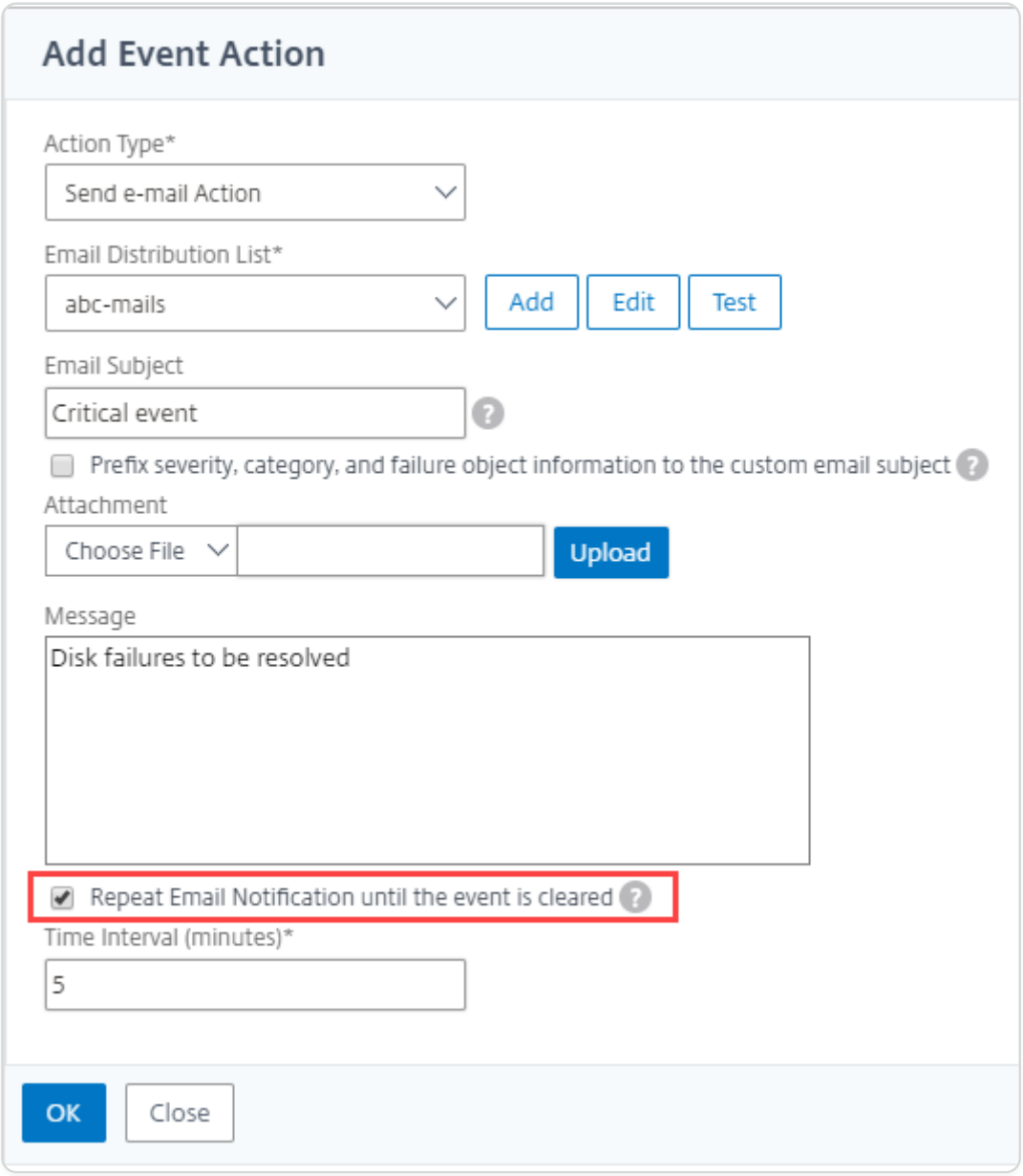
要手动清除事件，您可以执行以下操作：

- 导航到 **Infrastructure（基础架构）> Events（事件）> Event Summary（事件摘要）**，选择一个 **Category（类别）**，然后选择该类别中的一个事件，然后单击 **Clear（清除）**。
- 或者，导航到 **Infrastructure（基础架构）> Events（事件）> Event Messages（事件消息）**。选择一个实例类型，然后从下面的网格中选择一个事件，然后单击 **Clear（清除）**。

要从 NetScaler Console 设置重复电子邮件通知：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 在 NetScaler Console 中，导航到 **Infrastructure（基础架构）> Events（事件）> Rules（规则）**，然后单击 **Add（添加）** 以创建规则。
2. 在 **Create Rule（创建规则）** 页面上，设置规则参数。
3. 在 **Event Rule Actions（事件规则操作）** 下，单击 **Add Action（添加操作）**。然后，从 **Action Type（操作类型）** 下拉列表中选择 **Send e-mail Action（发送电子邮件操作）**，并选择一个 **Email Distribution List（电子邮件分发列表）**。
4. 当传入事件与配置的规则匹配时，您还可以添加自定义主题行和用户消息，并将附件上传到您的电子邮件中。
5. 选中 **Repeat Email Notification until the event is cleared（重复电子邮件通知，直到事件被清除）** 复选框。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

抑制事件

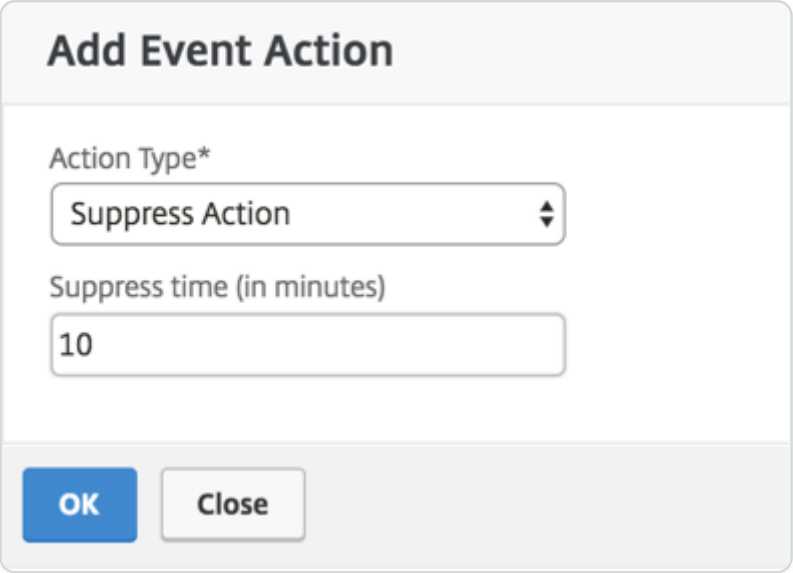
当您选择“**抑制操作**”事件操作时，您可以配置一个时间段（以分钟为单位），在此期间事件将被抑制或丢弃。您可以将事件抑制至少 1 分钟。

注意:

> 您还可以将抑制时间配置为 0 分钟，这意味着无限时间。如果您未指定任何时间持续时间，则 NetScaler Console 会将抑制时间视为零，并且它永不失效。

使用 NetScaler Console 抑制事件：

1. 在 NetScaler Console 中，导航到“**基础结构 > 事件 > 规则**”。单击“**添加**”。
2. 指定创建规则所需的所有参数。
3. 在“**事件规则操作**”下，单击“**添加操作**”以分配事件的通知操作。
4. 在“**添加事件操作**”页面上，从“**操作类型**”下拉列表中选择“**抑制操作**”，并指定事件必须被抑制的时间段（以分钟为单位）。
5. 单击“**确定**”。



创建事件规则

您可以配置规则来监控特定事件。规则使监控整个基础架构中生成的大量事件变得更加容易。

您可以通过配置具有特定条件的规则并为规则分配操作来筛选一组事件。当生成的事件符合规则中的筛选条件时，将运行与该规则关联的操作。您可以创建筛选器的条件包括：严重性、Citrix 应用交付控制器 (NetScaler) 实例、类别、故障对象、配置命令和消息。

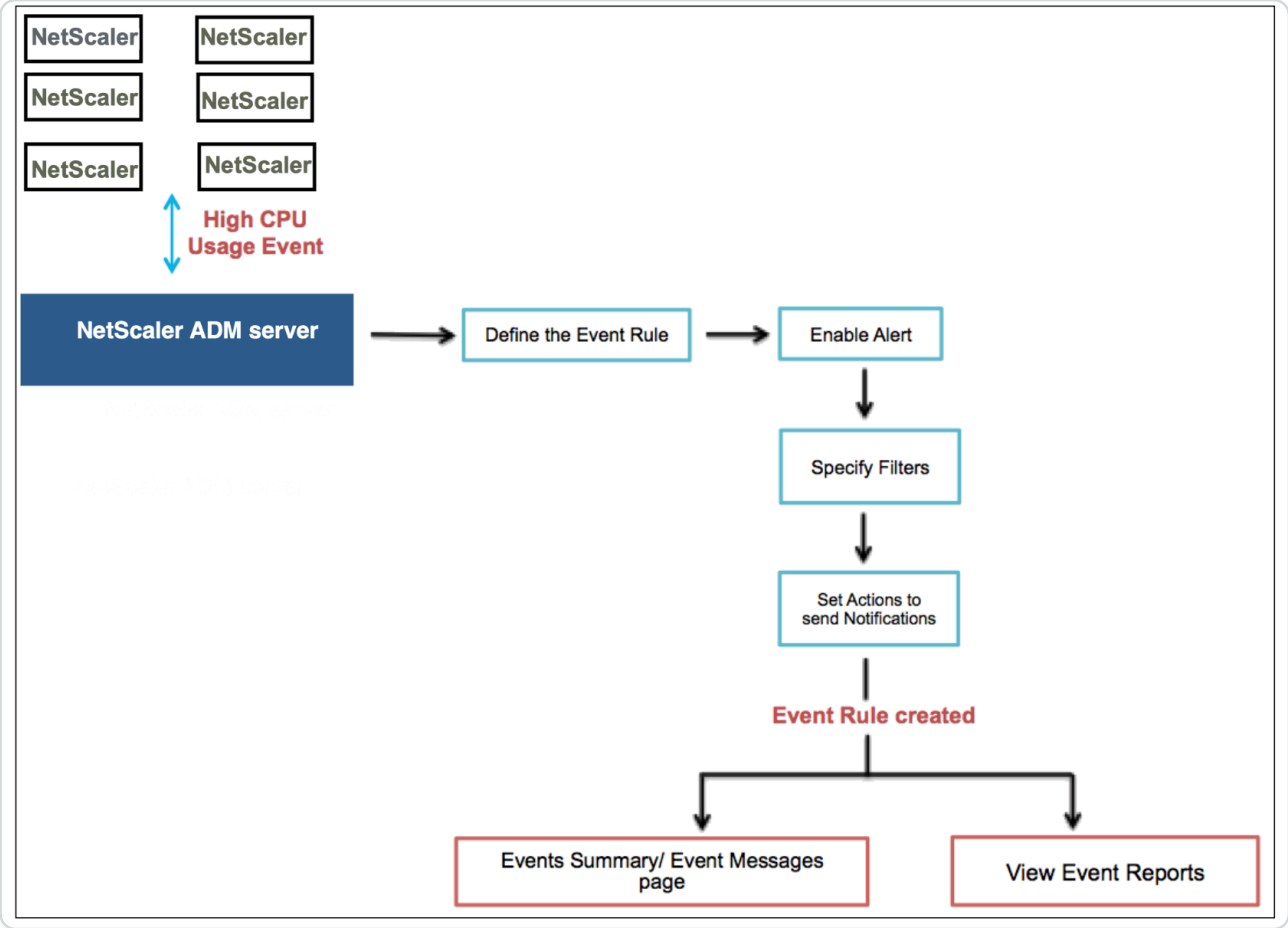
您可以为事件分配以下操作：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **发送电子邮件操作**：针对符合筛选条件的事件发送电子邮件。
- **发送陷阱操作**：将 SNMP 陷阱发送或转发到外部陷阱目标
- **运行命令操作**：当传入事件符合配置的规则时运行命令。
- **执行作业操作**：针对符合您指定筛选条件的事件运行作业。
- **抑制操作**：在特定时间段内抑制或丢弃事件。
- **发送 Slack 通知**：针对符合筛选条件的事件，在配置的 Slack 频道上发送通知。
- **发送 PagerDuty 通知**：根据 PagerDuty 配置，针对符合筛选条件的事件发送事件通知。
- **发送 ServiceNow 通知**：针对符合筛选条件的事件自动生成 ServiceNow 事件。

有关详细信息，请参阅 添加事件规则操作

您还可以设置在指定的时间间隔内重新发送通知，直到事件被清除。您还可以使用特定的主题行、用户消息和附件来自定义电子邮件。



例如，作为管理员，您可能希望监控特定 NetScaler 实例的“高 CPU 使用率”事件，因为这些事件可能导致您的 NetScaler 实例中断。您可以：

- 创建一个规则来监控这些实例，并指定一个操作，以便在发生“高 CPU 使用率”类别的事件时向您发送电子邮件通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 将规则安排在特定时间运行，例如上午 11 点到晚上 11 点之间，这样您就不会在每次生成事件时都收到通知。

配置事件规则涉及以下任务：

1. 定义规则
2. 选择规则检测到的事件的严重性
3. 指定事件类别
4. 指定规则适用的 NetScaler 实例
5. 选择故障对象
6. 指定高级筛选器
7. 指定规则检测到事件时要采取的操作

步骤 1 - 定义事件规则

导航到 **Infrastructure > Events > Rules**，然后单击 **Add**。如果要启用规则，请选中 **Enable Rule** 复选框。

您可以设置 **Event Age** 选项来指定 NetScaler Console 刷新事件规则的时间间隔（以秒为单位）。

注意：

> 事件持续时间的最小值为 60 秒。如果将**事件持续时间**字段留空，则事件规则会在事件发生后立即应用。

根据上述示例，您可能希望每当您的 NetScaler 实例发生持续 60 秒或更长时间的“CPU 使用率高”事件时，都能通过电子邮件收到通知。您可以将事件持续时间设置为 60 秒，这样，每当您的 NetScaler 实例发生持续 60 秒或更长时间的“CPU 使用率高”事件时，您都会收到一封包含事件详细信息的电子邮件通知。

创建事件规则(/en-us/netscaler-application-delivery-management-software/media/create-event-rule.png)

您还可以按**实例系列**筛选事件规则，以跟踪 NetScaler Console 从哪个 NetScaler 实例接收到事件。

如果您想包含除星号 (*) 模式匹配之外的正则表达式，请选择**启用带正则表达式匹配的高级筛选器**。

步骤 2 - 选择事件的严重性

您可以创建使用默认严重性设置的事件规则。严重性指定了您要添加事件规则的事件的当前严重性。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以定义以下严重性级别：严重、主要、次要、警告、清除和信息。

定义严重性级别(/en-us/netscaler-application-delivery-management-software/media/createer2.png)

注意

您可以为通用事件和高级特定事件配置严重性。要修改 NetScaler Console 上管理的 NetScaler 实例的事件严重性，请导航到**基础架构 > 事件 > 事件设置**。选择要配置事件严重性的**类别**，然后单击**配置严重性**。分配新的严重性级别，然后单击**确定**。

步骤 3 - 指定事件类别

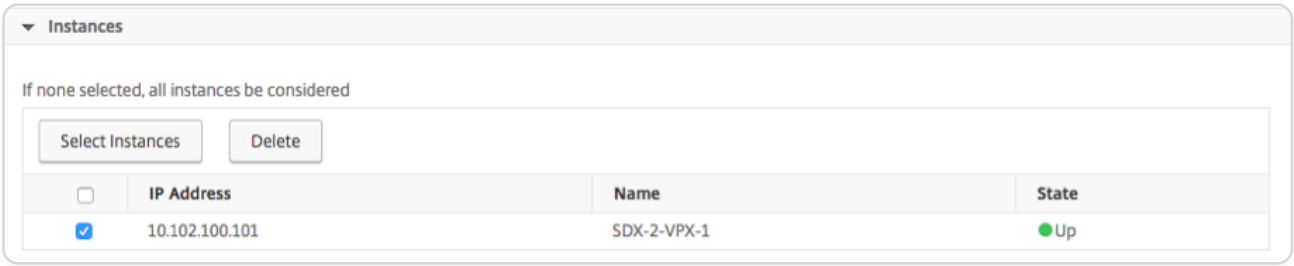
您可以指定 NetScaler 实例生成的事件类别。所有类别都在 NetScaler 实例上创建。然后，这些类别会映射到 NetScaler Console，可用于定义事件规则。选择要考虑的类别，并将其从**可用**表移动到**已配置**表。

在上述示例中，您必须从显示的表中选择“cpuUsageHigh”作为事件类别。

定义事件类别(/en-us/netscaler-application-delivery-management-software/media/createer3.png)

步骤 4 - 指定 NetScaler 实例

选择要为其定义事件规则的 NetScaler 实例的 IP 地址。在“**实例**”部分中，单击“**选择实例**”。在“**选择实例**”页面中，选择您的实例，然后单击“**选择**”。



步骤 5 - 选择故障对象

您可以从提供的列表中选择故障对象，也可以添加已生成事件的故障对象。您还可以指定正则表达式来添加故障对象。根据指定的正则表达式，故障对象会自动添加到列表中。故障对象是已生成事件的实体实例或计数器。

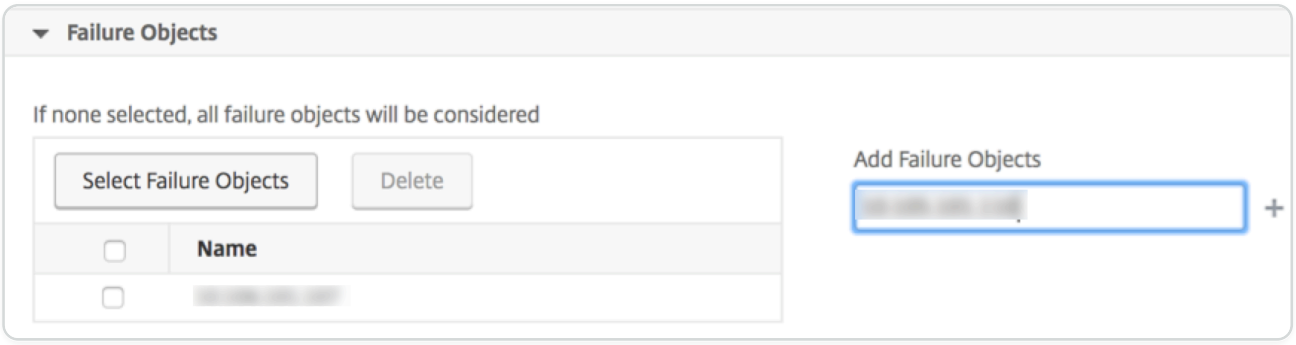
重要

要使用正则表达式列出故障对象，请在步骤 1中选择“**启用带正则表达式匹配的高级筛选器**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

故障对象会影响事件的处理方式，并确保其反映所通知的确切问题。使用此筛选器，您可以快速跟踪故障对象上的问题并确定问题的原因。例如，如果用户存在登录问题，则此处的故障对象是用户名或密码，例如 `nsroot`。

此列表可以包含所有阈值相关事件的计数器名称、所有实体相关事件的实体名称、所有证书相关事件的证书名称等。

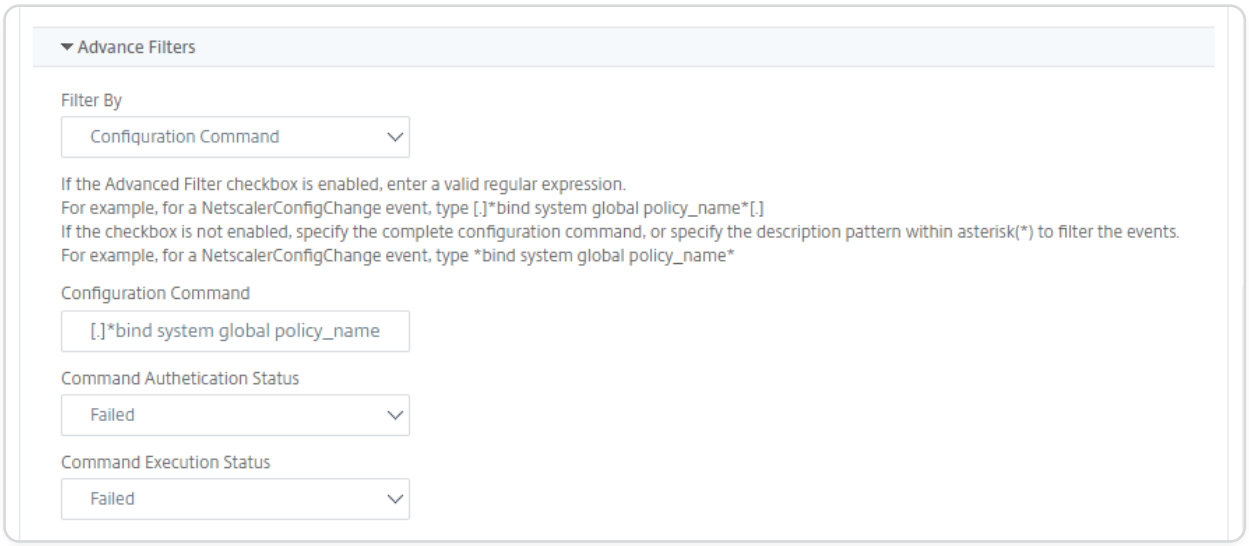


步骤 6 - 指定高级筛选器

您可以通过以下方式进一步筛选事件规则：

- **配置命令** - 您可以指定完整的配置命令，或指定正则表达式来筛选事件。

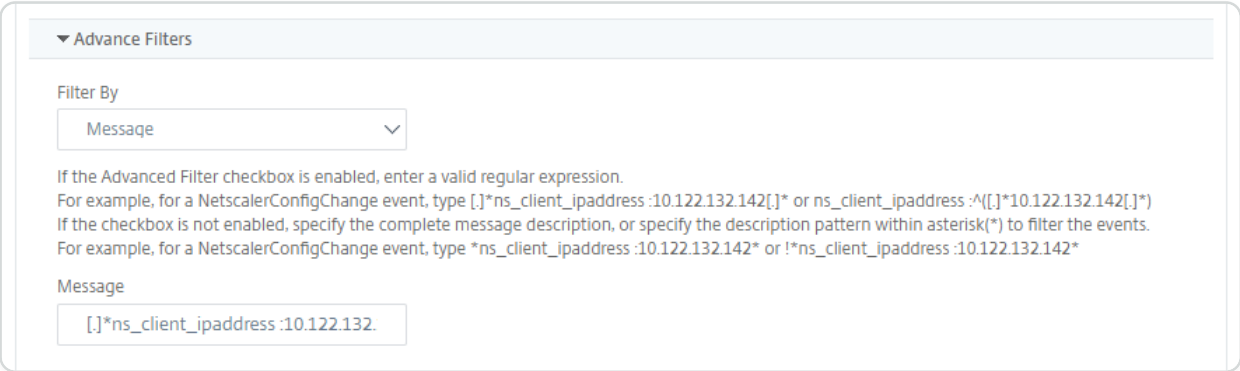
  您可以根据命令的身份验证状态和/或其执行状态进一步筛选事件规则。例如，对于 `NetscalerConfigChange event`，键入 `[.]*bind system global policy_name[.]*`。



- **消息** - 您可以指定完整的消息描述，或指定正则表达式来筛选事件。

  例如，对于 `NetscalerConfigChange` 事件，键入 `[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :\^([.]*10.122.132.142[.]*)`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



步骤 7 - 添加事件规则操作

您可以添加事件规则操作来为事件分配通知操作。当事件满足您在上方设置的已定义筛选条件时，将发送或执行这些通知。您可以添加以下事件操作：

- 发送电子邮件操作
- 发送陷阱操作
- 运行命令操作
- 运行作业操作
- 抑制操作
- 发送 Slack 通知
- 发送 PagerDuty 通知
- 发送 ServiceNow 通知

设置电子邮件事件规则操作

当您选择“发送电子邮件操作”事件操作类型时，当事件满足定义的筛选条件时，将触发一封电子邮件。您必须通过提供邮件服务器或邮件配置文件详细信息来创建电子邮件分发列表，或者您可以选择之前创建的电子邮件分发列表。

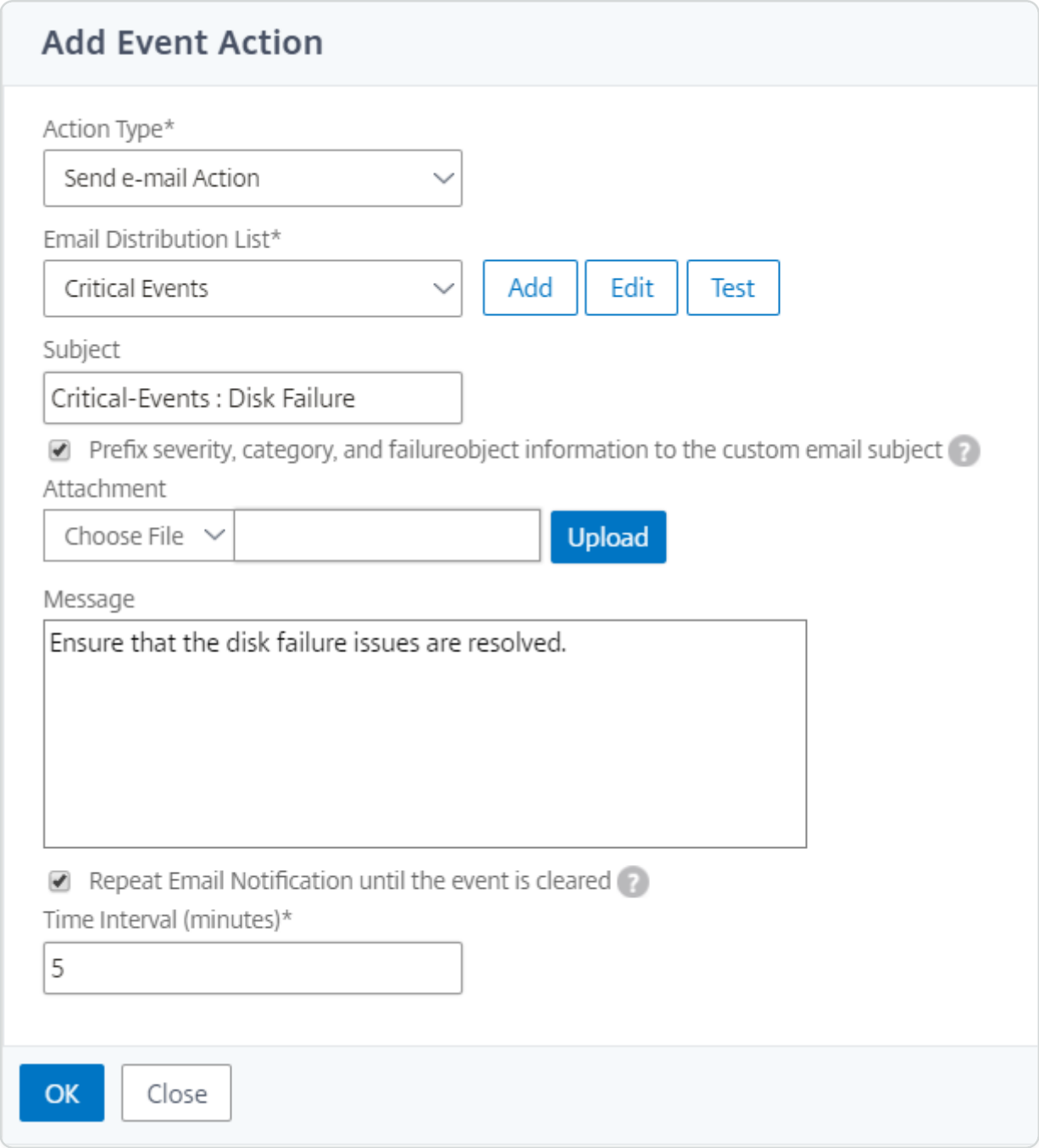
由于在 NetScaler Console 中配置了大量虚拟服务器，您每天可能会收到大量电子邮件。电子邮件具有默认主题行，其中提供有关事件严重性、事件类别和故障对象的信息。但主题行不包含有关这些事件源自的虚拟服务器名称的任何信息。您现在可以选择包含一些附加信息，例如受影响实体的名称、故障对象的名称。

当传入事件与配置的规则匹配时，您还可以添加自定义主题行和用户消息，并上传附件到您的电子邮件中。

在发送事件通知电子邮件时，您可能希望发送一封测试电子邮件来测试配置的设置。现在，在配置电子邮件服务器、关联的分布式列表和其他设置后，“测试”按钮允许您发送测试电子邮件。此功能可确保设置正常工作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您还可以通过选择**重复电子邮件通知，直到事件清除**复选框，为符合您所选条件的事件规则发送重复电子邮件通知，从而确保所有关键事件都得到处理，并且不会错过任何重要的电子邮件通知。例如，如果您为涉及磁盘故障的实例创建了事件规则，并且希望在问题解决之前收到通知，则可以选择接收有关这些事件的重复电子邮件通知。



设置陷阱事件规则操作

当您选择**发送陷阱操作**事件操作类型时，SNMP 陷阱将发送或转发到外部陷阱目标。通过定义陷阱分发列表（或陷阱目标和陷阱配置文件详细信息），当事件符合定义的筛选条件时，陷阱消息将发送到特定的陷阱侦听器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

设置运行命令操作

当您选择**运行命令操作**事件操作时，您可以创建可在 NetScaler Console 上运行的命令或脚本，以处理与特定筛选条件匹配的事件。

您还可以为**运行命令操作**脚本设置以下参数：

参数	描述
$源	此参数对应于接收事件的源 IP 地址。
$类别	此参数对应于筛选器类别下定义的陷阱类型
$实体	此参数对应于已生成事件的实体实例或计数器。它可以包括所有阈值相关事件的计数器名称、所有实体相关事件的实体名称以及所有证书相关事件的证书名称。
$严重性	此参数对应于事件的严重性。
失败对象	故障对象会影响事件的处理方式，并确保故障对象反映所通知的确切问题。这可用于快速跟踪问题并确定故障原因，而不是简单地报告原始事件。

注意

在命令执行期间，这些参数将替换为实际值。

例如，假设您希望在负载平衡虚拟服务器状态为**“关闭”**时设置运行命令操作。作为管理员，您可能希望通过添加另一个虚拟服务器来提供快速解决方案。在 NetScaler Console 中，您可以执行以下操作：

- 编写脚本 (.sh) 文件。

  以下是示例脚本 (.sh) 文件：

```
#!/bin/sh

source=$1

failureobj=$2
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
payload='{"params":{"warning":"YES"},"lbvserver":
{"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","port":"
80","td":"","m":"IP","state":"ENABLED","rhistate":"PASSIVE","appflowlog
":"ENABLED","

bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":""}}'

url="http://$source/nitro/v1/config/lbvserver"

curl --insecure -basic -u nsroot:nsroot -H "Content-type: application/
json" -X POST -d $payload $url
```

- 将 .sh 文件保存在 NetScaler 代理上的任何持久位置。例如，`/var`。
- 在 NetScaler Console 中提供 .sh 文件位置，以便在满足规则条件时运行。

要设置**运行命令**操作以创建新的虚拟服务器，请执行以下操作：

1. 定义规则
2. 选择事件的严重性
3. 选择事件类别 **entitydown**
4. 选择已配置虚拟服务器的实例
5. 为虚拟服务器选择或创建故障对象
6. 在 **事件规则操作** 下，单击 **添加操作**，然后从 **操作类型** 列表中选择 **运行命令操作**。
7. 在 **命令执行列表** 下，单击 **添加**。

   将显示“创建命令分发列表”页面。

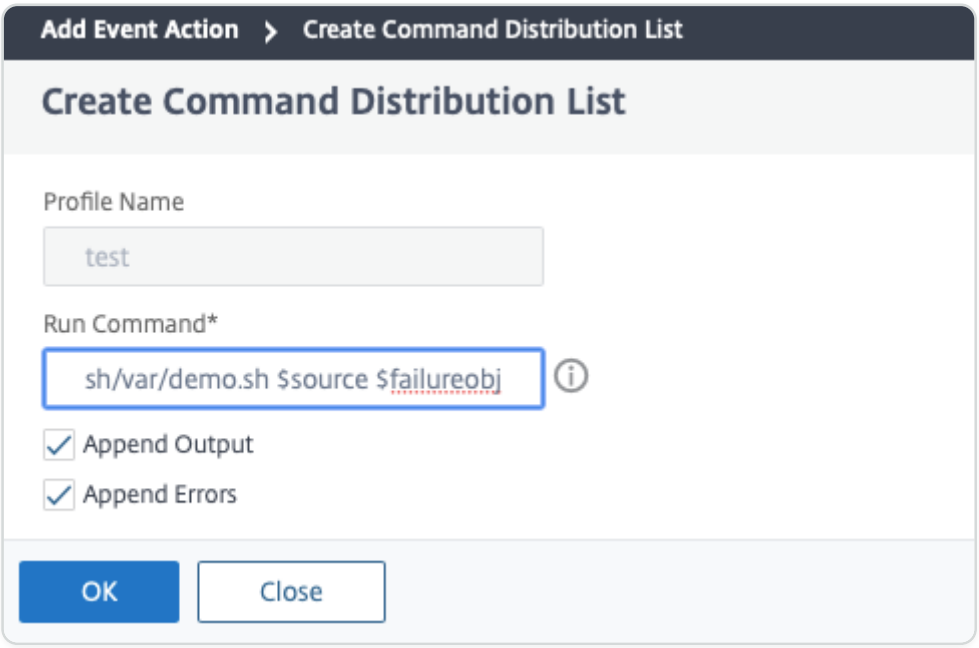
   a. 在 **配置文件名称** 中，指定您选择的名称
   b. 在 **运行命令** 中，指定必须运行脚本的 NetScaler 代理位置。例如：`/sh/var/demo.sh $source $failureobj`。
   c. 选择 **追加输出** 和 **追加错误**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注意**
>
> 如果您希望在 NetScaler Console 服务器日志文件中存储运行命令脚本时生成的输出和错误（如果有），则可以启用 **追加输出** 和 **追加错误** 选项。如果您不启用这些选项，NetScaler Console 将丢弃运行命令脚本时生成的所有输出和错误。

d. 单击 **创建**。

8. 在 **添加事件操作** 页面中，单击 **确定**。



> **注意**
>
> 如果您希望将运行命令脚本时生成的输出和错误（如果有）存储在 NetScaler Console 服务器日志文件中，可以启用 **Append Output** 和 **Append Errors** 选项。如果您不启用这些选项，NetScaler Console 将丢弃运行命令脚本时生成的所有输出和错误。

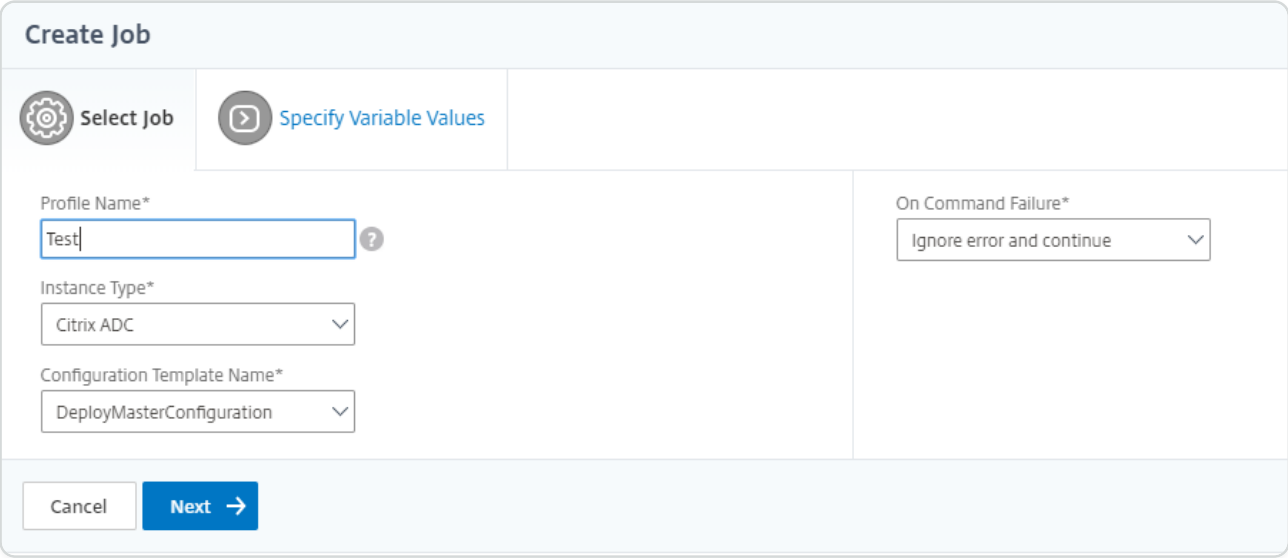
设置 `Execute` 作业操作

通过创建包含配置作业的配置文件，作业将作为内置作业或自定义作业运行，适用于 NetScaler 和 NetScaler SDX 实例，以响应与您指定的筛选条件匹配的事件和警报。

1. 在 **Event Rule Actions** 下，单击 **Add Action**，然后从 **Action Type** 下拉列表中选择 **Execute Job Action**。
2. 创建一个配置文件，其中包含您希望在事件满足定义的筛选条件时运行的作业。

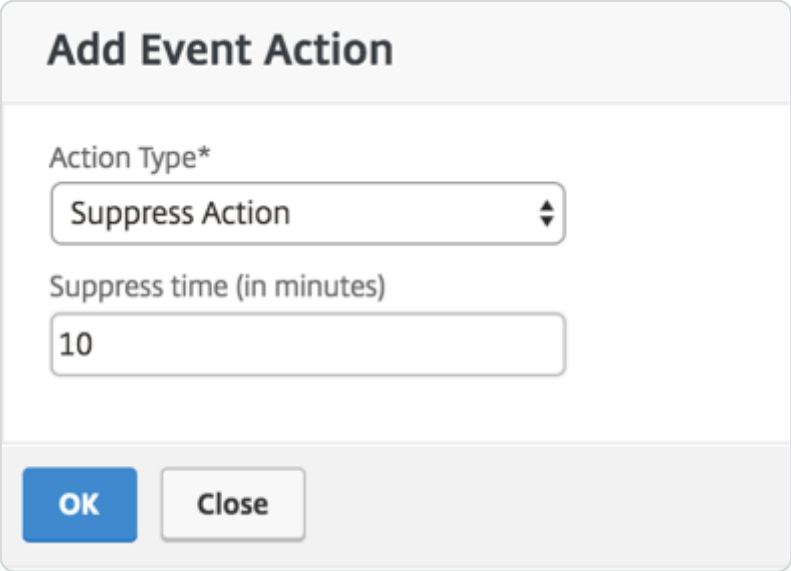
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 创建作业时，请指定配置文件名称、实例类型、配置模板以及如果作业上的命令失败您希望执行的操作。
4. 根据所选的实例类型和配置模板，指定您的变量值，然后单击 **Finish** 创建作业。



设置抑制操作

当您选择 **Suppress Action** 事件操作时，可以配置一个时间段（以分钟为单位），在此期间事件将被抑制或丢弃。您可以将事件抑制至少 1 分钟。



从 NetScaler Console 设置 Slack 通知

通过在 NetScaler Console GUI 中提供配置文件名称和 webhook URL 来配置所需的 Slack 频道。事件通知随后将发送到此频道。您可以配置多个 Slack 频道来接收这些通知。

1. 在 NetScaler Console 中，导航到 **Infrasturcture > Events > Rules**，然后单击 **Add** 创建规则。
2. 在 **创建规则** 页面上，设置规则参数，例如严重性和类别。选择必须监控的实例和故障对象。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在 **事件规则操作** 下，单击 **添加操作**。然后，从 **操作类型** 列表中选择 **发送 Slack 通知**，并选择 **Slack 配置文件列表**。
4. 您还可以通过单击 **Slack 配置文件列表** 字段旁边的 **添加** 来添加 Slack 配置文件列表。
5. 键入以下参数以创建配置文件列表：
   a. **配置文件名称**。键入要在 NetScaler Console 上配置的配置文件列表的名称
   b. **频道名称**。键入要发送事件通知的 Slack 频道的名称。
   c. **Webhook URL**。键入您之前输入的频道的 Webhook URL。传入 Webhook 是一种将外部源消息发布到 Slack 的简单方法。该 URL 在内部链接到频道名称，所有事件通知都将发送到此 URL，以便发布到指定的 Slack 频道。Webhook 示例如下：`<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`
6. 在 **添加事件操作** 窗口中，单击 **创建**，然后单击 **确定**。

注意：

您还可以通过导航到 **系统** \> **通知** \> **Slack 配置文件** 来添加 Slack 配置文件。单击 **添加** 并按照前面部分所述创建配置文件。

您可以查看已创建的 Slack 配置文件的状态。

您的事件规则现已创建，其中包含适当的过滤器和明确定义的事件规则操作。

从 NetScaler Console 设置 PagerDuty 通知

您可以在 NetScaler Console 中添加 PagerDuty 配置文件作为选项，以根据您的 PagerDuty 配置监控事件通知。PagerDuty 使您能够通过电子邮件、短信、推送通知和注册号码上的电话来配置通知。

在 NetScaler Console 中添加 PagerDuty 配置文件之前，请确保您已在 PagerDuty 中完成所需的配置。有关更多信息，请参阅 PagerDuty 文档。

您可以选择您的 PagerDuty 配置文件作为以下功能的通知选项之一：

- **事件** – 为 NetScaler 实例生成的事件列表。
- **许可证** – 当前处于活动状态、即将过期等的许可证列表。
- **SSL 证书** – 添加到 NetScaler 实例的 SSL 证书列表。

在 NetScaler Console 中添加 PagerDuty 配置文件：

1. 使用管理员凭据登录到 NetScaler Console。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 导航到 **设置 > 通知 > PagerDuty 配置文件**。
3. 单击“**添加**”以创建新配置文件。
4. 在“创建 PagerDuty 配置文件”页面中：
   a. 提供您选择的配置文件名称。
   b. 输入“**集成密钥**”。

      您可以从 PagerDuty 门户获取集成密钥。
   c. 单击“**创建**”。

   用例：

   考虑以下场景：

   - 希望将通知发送到您的 PagerDuty 配置文件。
   - 已在 PagerDuty 中将电话呼叫配置为接收通知的选项。
   - 希望接收 NetScaler 事件的电话呼叫警报。

   配置方法：

   a. 导航到 **事件** > **规则**
   b. 在 **创建规则** 页面上，配置所有其他参数以创建规则。
   c. 在 **创建规则操作** 下，单击 **添加操作**。

      显示 **添加事件操作** 页面。

      i. 在 **操作类型** 下，选择 **发送 PagerDuty 通知**。
      ii. 选择您的 PagerDuty 配置文件，然后单击 **确定**。

   配置完成后，每当为 NetScaler 实例生成新事件时，您都会收到电话呼叫。通过电话呼叫，您可以决定：

   - 确认事件
   - 将其标记为已解决
   - 上报给其他团队成员

从 NetScaler Console 自动生成 ServiceNow 事件

通过在 NetScaler Console GUI 上选择 ServiceNow 配置文件，您可以为 NetScaler Console 事件自动生成 ServiceNow 事件。您必须在 NetScaler Console 中选择 ServiceNow 配置文件才能配置事件规则。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在配置事件规则以自动生成 ServiceNow 事件之前，请将 NetScaler Console 与 ServiceNow 实例集成。有关详细信息，请参阅 为 ServiceNow 配置 ITSM 适配器。

要配置事件规则，请导航到 **事件** > **规则**。

1. 在“**创建规则**”页面上，配置所有其他参数以创建规则。
2. 在“**创建规则操作**”下，单击“**添加操作**”。

   将显示“**添加事件操作**”页面。

   a. 在“**操作类型**”中，选择“**发送 ServiceNow 通知**”。
   b. 在“**ServiceNow 配置文件**”中，从列表中选择“**Citrix_Workspace_SN**”配置文件。
   c. 单击“**确定**”。

修改 NetScaler 实例上发生的事件的报告严重性

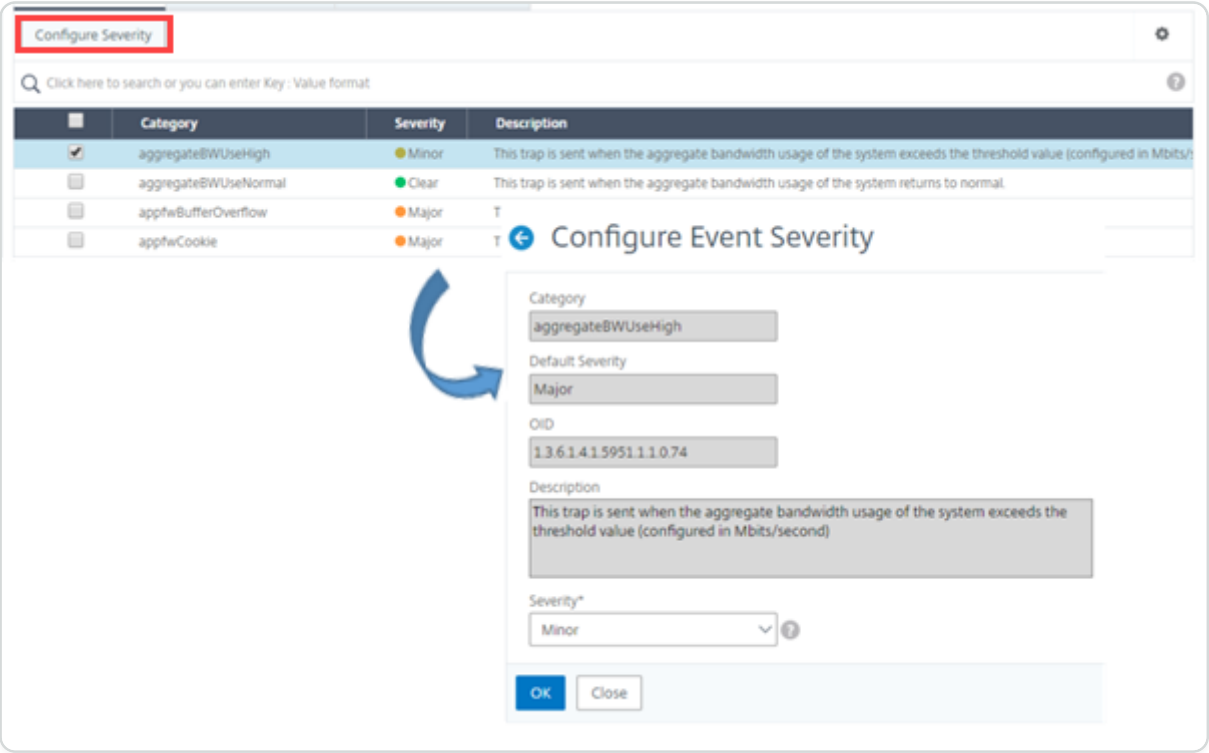
您可以管理所有设备上生成的事件报告，以便您可以查看特定实例上特定事件的事件详细信息，并根据事件严重性查看报告。您可以创建使用默认严重性设置的事件规则，并且可以更改严重性设置。您可以为通用事件和企业特定事件配置严重性。

您可以定义以下严重性级别：严重、主要、次要、警告和清除。

修改事件严重性：

1. 导航到 **基础结构 > 事件 > 事件设置**。
2. 单击要修改的 NetScaler 实例类型的选项卡。然后，从列表中选择类别，并单击 **配置严重性**。
3. 在 **配置事件严重性** 中，从下拉列表中选择严重性级别。
4. 单击 **确定**。

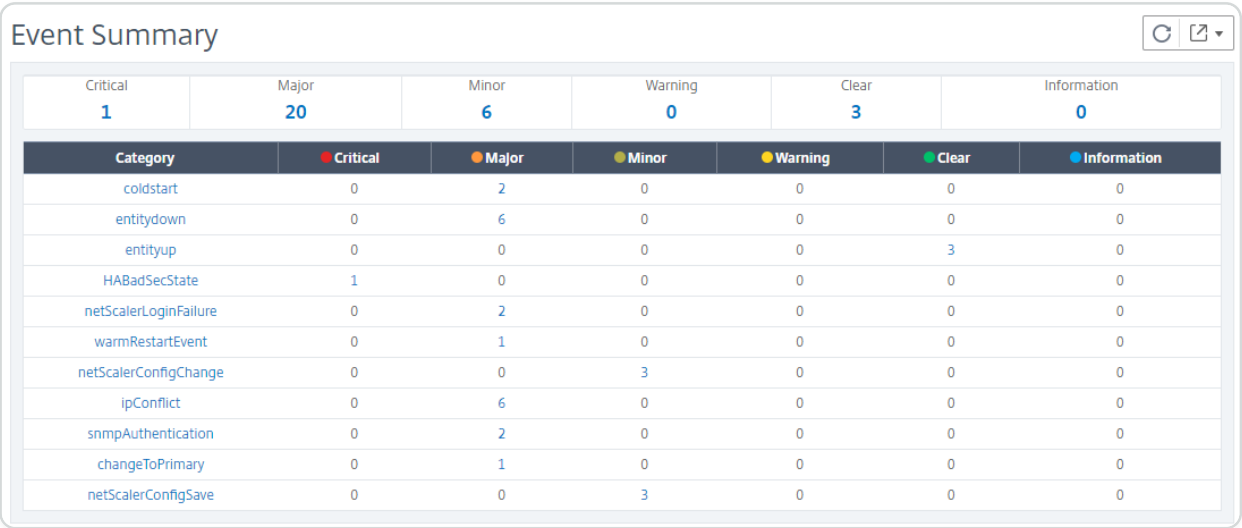
© 1997–2026 Citrix Systems, Inc. All rights reserved.



查看事件摘要

您现在可以查看“事件摘要”页面，以监控 NetScaler Console 服务器上接收到的事件和陷阱。导航到 **基础架构 > 事件**。“事件摘要”页面以表格形式显示以下信息：

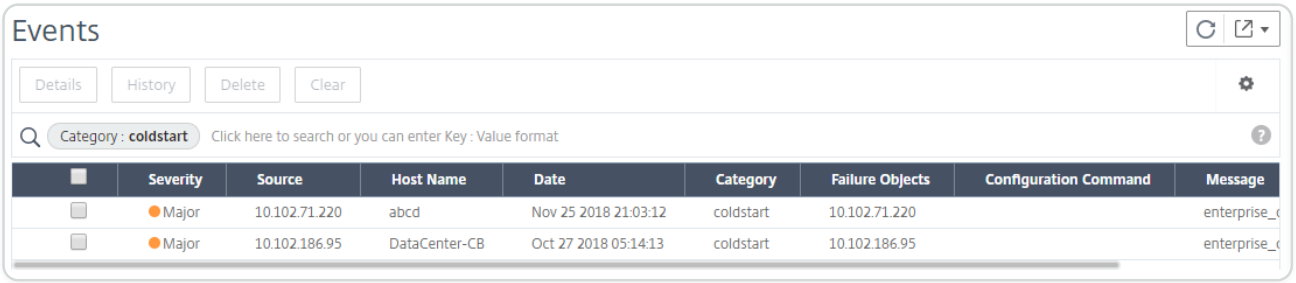
- **NetScaler Console 接收到的所有事件的摘要**。事件按类别列出，不同的严重性显示在不同的列中：严重、主要、次要、警告、清除和信息。例如，当 NetScaler 实例关闭并停止向 NetScaler Console 服务器发送信息时，会发生严重事件。事件发生期间，会向管理员发送通知，解释实例关闭的原因、关闭时长等。然后，该事件会记录在“事件摘要”页面上，您可以在该页面上查看摘要并访问事件的详细信息。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **每个类别接收到的陷阱数量**。按严重性分类的陷阱数量。默认情况下，从 NetScaler 实例发送到 NetScaler Console 的每个陷阱都具有分配的严重性，但作为网络管理员，您可以在 NetScaler Console GUI 中指定其严重性。

如果您单击类别类型或陷阱，您将被带到 **事件**页面，在该页面上，类别和严重性等筛选器已预选。此页面显示有关事件的更多信息，例如 NetScaler 实例的 IP 地址和主机名、接收陷阱的日期、类别、故障对象、运行的配置命令以及消息通知。



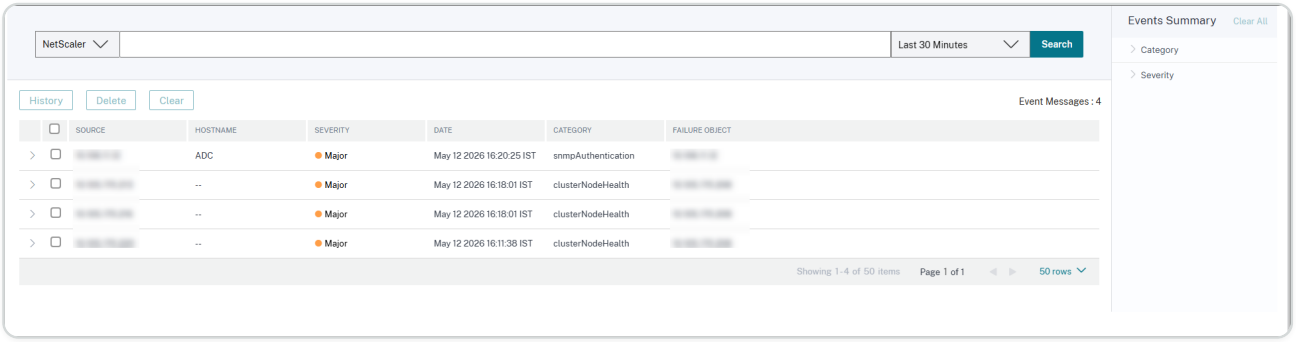
查看事件消息

NetScaler® Console 中收到的所有活动事件都显示在“**Infrastructure > Events > Event Messages**”页面中。

在“**Event Messages**”页面上，您可以查看实例列表和事件详细信息，例如严重性、类别、事件发生日期和故障对象。

您可以根据事件发生的时间（例如，最近 30 分钟、1 小时、1 天）筛选事件。您还可以根据自己的偏好选择自定义时间。

NetScaler Console 支持自定义 SNMP 陷阱，这些陷阱在“**Event Messages**”下标记为“**custom**”。“**custom**”标签可帮助您将它们与默认 SNMP 警报区分开来。



显示事件严重性和 SNMP 陷阱详细信息

在 NetScaler Console 中创建事件及其设置后，您可以立即在“事件摘要”页面上查看该事件。同样，您可以在“基础架构控制板”上详细查看和监控添加到 NetScaler Console 服务器的所有 Citrix NetScaler 实例的运行状况、正常运行时间、型号和版本。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在“基础架构控制板”上，您现在可以屏蔽不相关的值，以便更轻松地详细查看和监控 NetScaler 实例的事件严重性、运行状况、正常运行时间、型号和版本等信息。

例如，严重性级别为“**严重**”的事件可能很少发生。但是，当这些严重事件确实在您的网络中发生时，您可能希望进一步调查、故障排除和监控事件发生的位置和时间。如果选择除“严重”之外的所有严重性级别，则图表仅显示严重事件的发生情况。此外，通过单击图表，您将进入“**基于严重性的事件**”页面，在该页面上，您可以查看所选持续时间内发生严重事件的所有详细信息：实例源、日期、类别以及发生严重事件时发送的消息通知。

同样，您可以在控制板上查看 NetScaler VPX 实例的运行状况。您可以屏蔽实例正常运行的时间，只显示实例停止服务的时间。通过单击图表，您将进入该实例的页面，其中已应用*停止服务*筛选器，并查看主机名、每秒接收的 HTTP 请求数、CPU 使用率等详细信息。您还可以选择该实例并查看特定 Citrix 实例的控制板以获取更多详细信息。

在 NetScaler Console 中按严重性选择特定事件：

1. 使用管理员凭据登录 NetScaler Console。
2. 导航到“**基础架构 > 控制板**”。

   或者，

   导航到“**基础架构 > 事件 > 报告**”。
3. 从页面右上角的菜单中，选择要按严重性查看事件的持续时间。

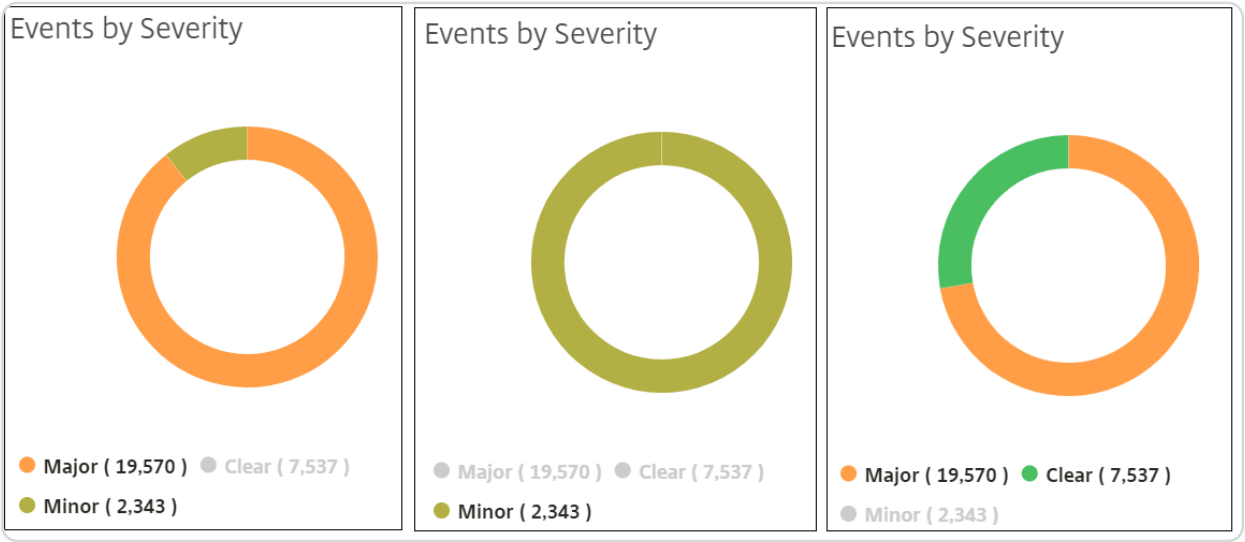
   事件严重性(/en-us/netscaler-application-delivery-management-software/media/masvc-events-report-severity-mask.png)
4. “**按严重性划分的事件**”圆环图以可视化方式显示所有事件的严重性。不同类型的事件以不同颜色的部分表示，每个部分的长度对应于该严重性类型事件的总数。
5. 您可以单击圆环图上的每个部分，以显示相应的“**基于严重性的事件**”页面，该页面显示所选持续时间内所选严重性的以下详细信息：

   - 实例源
   - 事件数据
   - NetScaler 实例生成的事件类别
   - 发送的消息通知

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

在圆环图下方，您可以看到图表中表示的严重性列表。默认情况下，圆环图显示所有严重性类型的所有事件，因此列表中的所有严重性类型都会突出显示。您可以切换严重性类型，以便更轻松地查看和监控您选择的严重性。



在 NetScaler Console 上查看 NetScaler SNMP 陷阱详细信息：

您现在可以在 NetScaler Console 服务器的“**事件设置**”页面上查看从其托管的 NetScaler 实例接收到的每个 SNMP 陷阱的详细信息。导航到“**基础架构 > 事件 > 事件设置**”。对于从您的实例接收到的特定陷阱，您可以表格形式查看以下详细信息：

- **类别** - 指定事件所属实例的类别。
- **严重性** - 事件的严重性由颜色及其严重性类型指示。
- **描述** - 指定与事件关联的消息。

例如，对于陷阱类别为 **monRespTimeoutBelowThresh** 的事件，陷阱的描述显示为“当监视器探测的响应超时恢复正常，低于设定的阈值时，将发送此陷阱。”

查看和导出 NetScaler syslog 消息

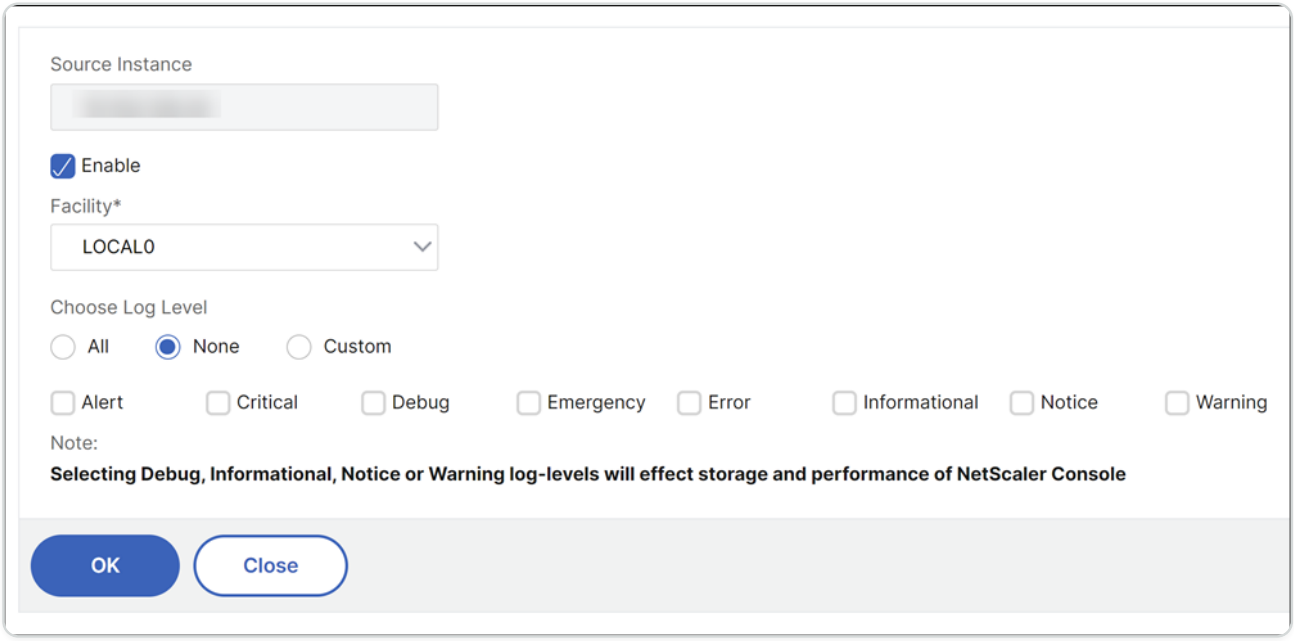
在您的 NetScaler Console 中，您可以监控在 Citrix NetScaler 实例上生成的 syslog 事件。为此，您必须将 NetScaler Console 配置为 NetScaler 实例的 syslog 服务器。配置 NetScaler Console 后，所有 syslog 消息都会从 NetScaler 实例重定向到 NetScaler Console。

将 NetScaler Console 配置为 syslog 服务器

请按照以下步骤将 NetScaler Console 配置为 syslog 服务器：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 在 NetScaler Console 图形用户界面中，导航到 **Infrastructure > Instances**。
2. 选择您希望从中收集 syslog 消息并在 NetScaler Console 中显示的 NetScaler 实例。
3. 在“**选择操作**”列表中，选择“**配置 Syslog**”。
4. 单击“**启用**”。
5. 在“**Facility**”下拉列表中，选择本地或用户级别设备。
6. 选择 syslog 消息所需的日志级别。
7. 单击“**确定**”。



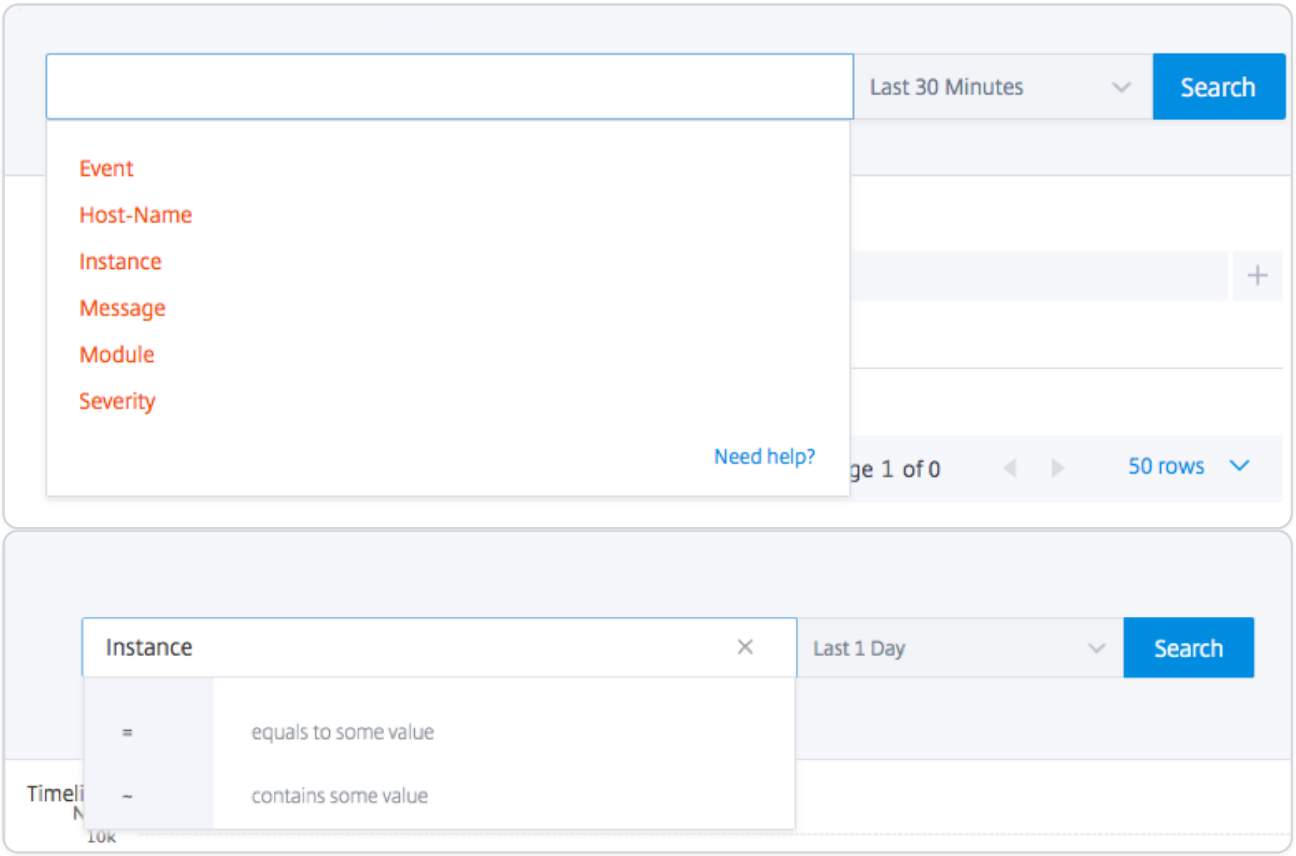
这些步骤配置了 NetScaler 实例中的所有 syslog 命令，NetScaler Console 开始接收 syslog 消息。

查看和搜索 syslog 消息

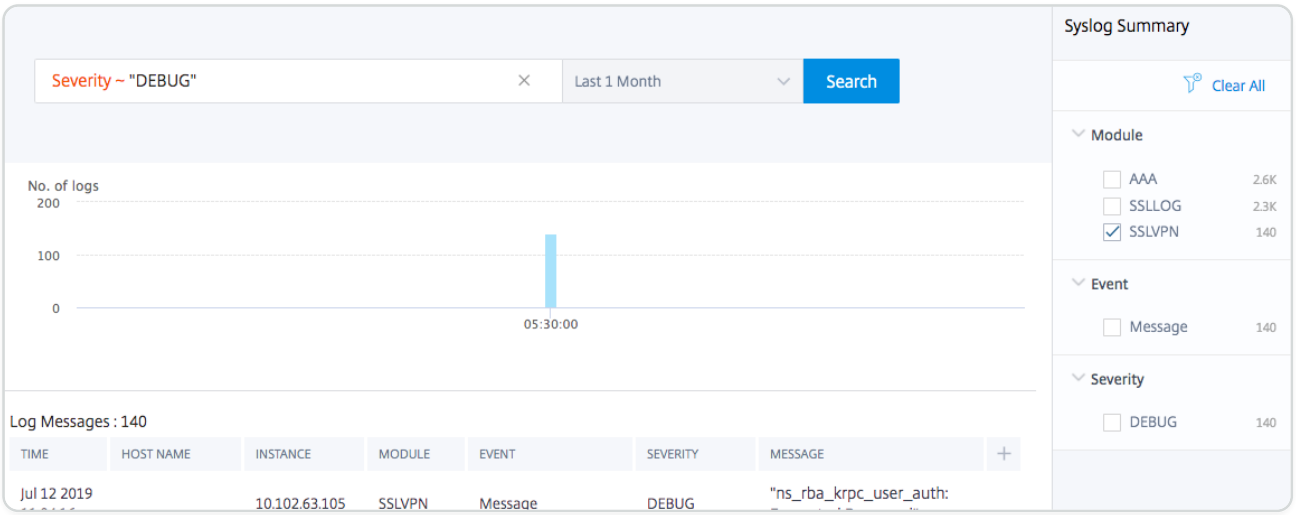
您可以查看在托管 NetScaler 实例上生成的所有 syslog 消息。syslog 消息集中存储在数据库中，可在“**Infrastructure > Events > Syslog Messages**”下用于审计目的。您可以结合此日志信息并从收集的数据中导出分析报告。

此外，您可以使用筛选器缩小 syslog 消息的搜索结果范围，并实时准确找到您要查找的内容。单击“**需要帮助？**”以打开内置搜索帮助。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



接下来，添加搜索词。对于某些类别，将显示预填充的搜索词列表。默认情况下，搜索时间为 1 天。您可以通过单击向下箭头来更改时间范围和日期范围。您可以通过从“**Syslog 摘要**”窗格中选择选项来进一步缩小搜索范围。

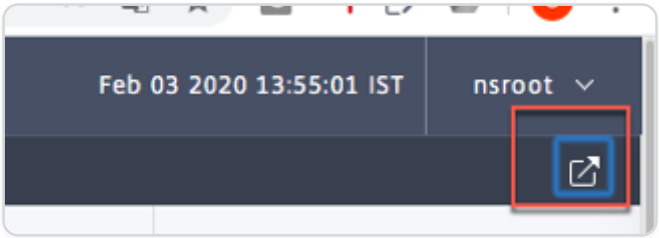


导出和计划 syslog 消息

您可以通过计划导出服务器上接收到的所有 syslog 消息，无需登录 NetScaler Console 即可查看 syslog 消息。您可以将 NetScaler 实例上生成的 syslog 消息导出为 PDF、CSV、PNG 和 JPEG 格式。您可以计划将这些报告导出到指定的电子邮件地址或 Slack 帐户，并可设置不同的时间间隔。

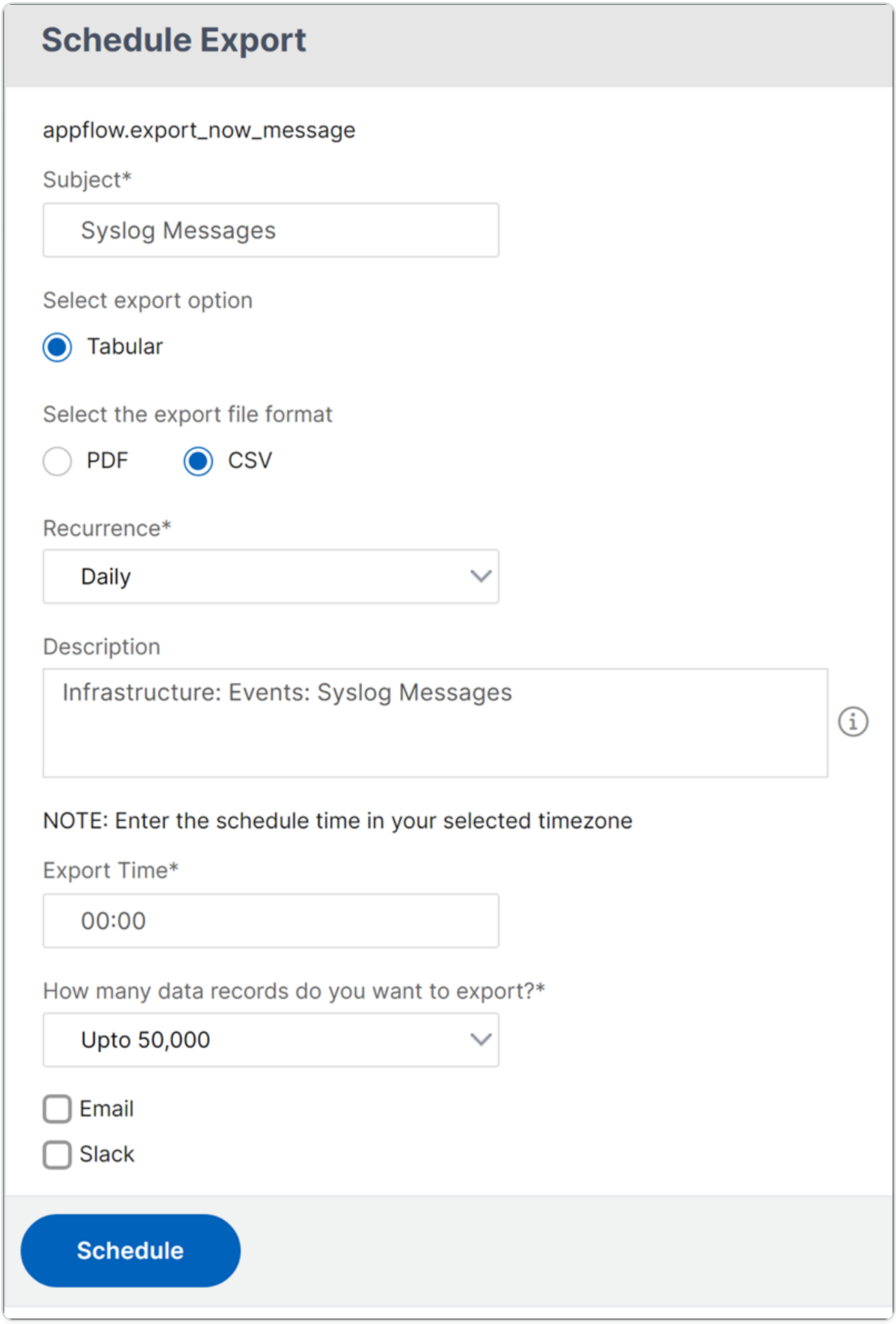
要导出和计划日志消息，请单击右上角的箭头图标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 要导出日志消息，请单击“**导出报告 > 立即导出**”，选择所需格式，然后单击“**导出**”。
- 要计划导出 syslog 消息，请单击“**导出报告 > 计划报告**”，并设置所需参数。您可以通过电子邮件或 Slack 接收报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

抑制 syslog 消息

当配置为 syslog 服务器时，NetScaler Console 会接收由配置的 NetScaler 实例发送给它的所有 syslog 消息。您可能不希望看到大量消息。例如，您可能对查看所有信息级别消息不感兴趣。现在，您可以丢弃一些您不感兴趣的 syslog 消息。您可以通过设置一些过滤器来抑制进入 NetScaler Console 的某些 syslog 消息。NetScaler Console 会丢弃所有符合条件的邮件。这些丢弃的消息不会出现在 NetScaler Console GUI 上，也不会存储在客户的 NetScaler Console 数据库中。

您可以通过设置一些过滤器来抑制进入 NetScaler Console 的某些已记录的 syslog 消息。可用于抑制 syslog 消息的两个过滤器是严重性和设施。您还可以抑制来自特定 NetScaler 实例或多个实例的消息。您还可以提供文本模式，供 NetScaler Console 搜索和抑制消息。NetScaler Console 会丢弃所有符合条件的邮件。这些丢弃的消息不会出现在 NetScaler Console GUI 上，也不会存储在客户数据库中。因此，存储服务器上节省了大量空间。

抑制 syslog 消息的一些用例如下：

- 如果您想忽略所有信息级别消息，请抑制级别 6（信息）
- 如果您只想记录防火墙错误情况，请抑制除级别 3（错误）之外的所有级别

通过创建过滤器抑制 syslog 消息

1. 在 NetScaler Console 中，导航到 **基础架构 > 事件 > Syslog 消息** \> **抑制过滤器**。
2. 在 **Create Suppress Filter** 页面上，更新以下信息：

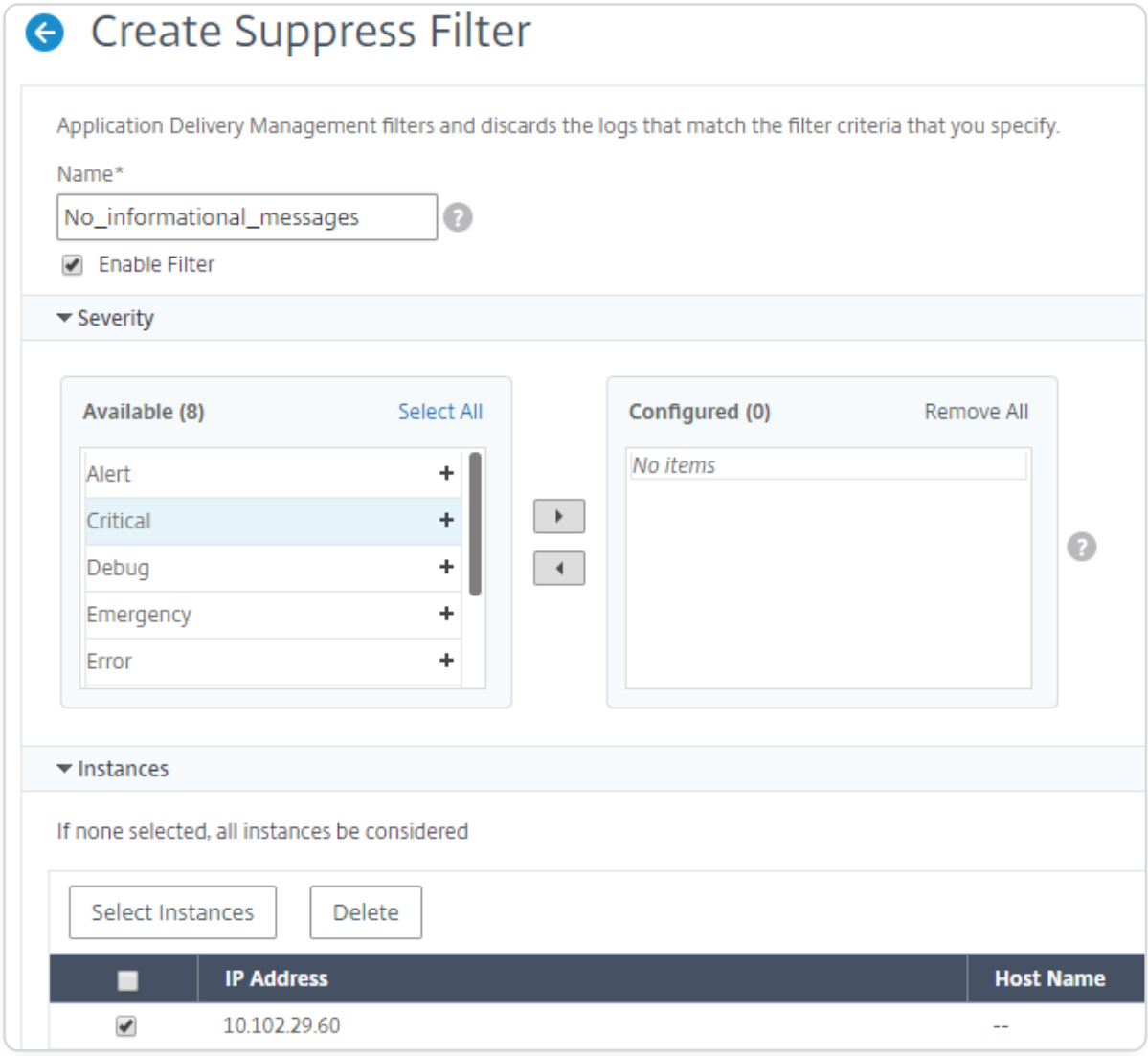
   a. **Name** - 键入过滤器的名称。

   > **注意**
   >
   > 如果不同用户对多个 NetScaler 实例具有不同的访问权限，则必须为不同实例创建不同的过滤器，因为用户只能看到他们有权访问所有实例的那些过滤器。

   b. **Severity** - 选择并添加必须抑制消息的日志级别。例如，如果您不想查看任何传入的信息性消息，可以选择“信息”来抑制这些消息。

   c. **Instances** - 选择已配置 syslog 消息的 NetScaler 实例。

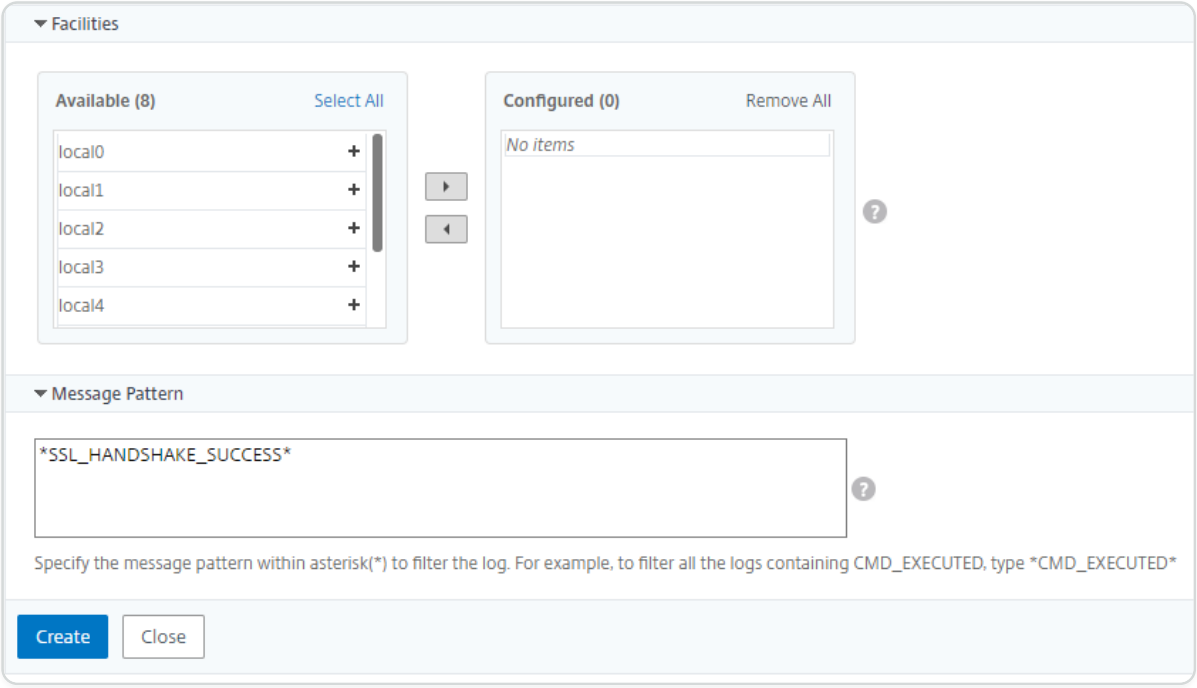
© 1997–2026 Citrix Systems, Inc. All rights reserved.



d. **设施** - 选择设施以根据生成消息的源来抑制消息。

e. **消息模式** - 您还可以键入由星号 (*) 括起来的文本模式来抑制消息。系统会搜索消息中的文本模式字符串，并抑制包含此模式的消息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



禁用筛选器

要允许在 NetScaler Console 上查看消息，您必须禁用筛选器。

1. 导航到 **基础结构 > 事件 > 系统日志消息** \> **抑制筛选器**，然后在“**抑制筛选器**”页面上，选择筛选器并单击“**编辑**”。
2. 在“**配置抑制筛选器**”页面上，清除“**启用筛选器**”复选框以禁用筛选器。

配置实例事件的清除设置

由您的 NetScaler Console 服务器管理的 Citrix NetScaler 实例持续发送事件消息数据，以存储在 NetScaler Console 上。您可以指定 NetScaler Console 保留网络报告数据、事件、审计日志和任务日志的时间间隔。默认情况下，此数据每 24 小时（00:00 时）清除一次。

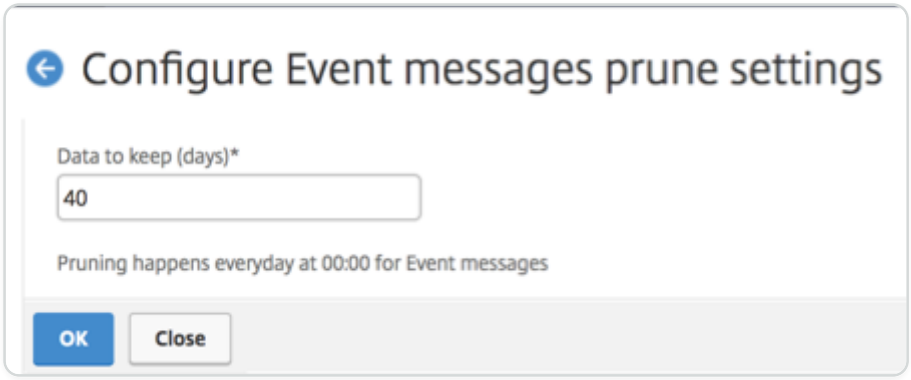
注意

您可以指定的值不能超过 40 天或少于 1 天。

要配置实例事件的清除设置：

1. 导航到 **系统** \> **系统管理**。
2. 在 **清除设置** 下，单击 **实例 事件清除设置**。
3. 输入您希望在 NetScaler Console 服务器上保留数据的时间间隔（天），然后单击 **确定**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



网络功能

使用网络功能特性，您可以监控在您管理的 Citrix NetScaler 实例上配置的实体的状态。您可以查看统计信息，例如事务详细信息、连接详细信息以及负载均衡虚拟服务器的吞吐量。您还可以在计划维护时启用或禁用这些实体。

网络功能仪表板为您提供以下图表：

- 客户端连接数最高的前 5 个虚拟服务器
- 服务器连接数最高的前 5 个虚拟服务器
- 吞吐量最大（MB/秒）的前 5 个虚拟服务器
- 吞吐量最低（MB/秒）的后 5 个虚拟服务器
- 虚拟服务器数量最多的前 5 个实例
- 虚拟服务器的状态
- 负载均衡虚拟服务器的运行状况
- 协议

为负载均衡实体生成报告

NetScaler Console 允许您查看所有级别的 Citrix NetScaler 实例实体的报告。您可以在 NetScaler Console \> Network Functions 中下载两种类型的报告：合并报告和单独报告。

合并报告：您可以下载并查看 NetScaler 实例上管理的所有实体的合并或汇总报告。

此报告可让您概览网络中 NetScaler 实例、分区和相应的负载均衡实体（虚拟服务器、服务组和服务）之间的映射关系。

下图显示了汇总报告的示例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:[redacted]
[redacted]	[redacted]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[redacted]	[redacted]		Load Balancing	334-lb#1.33.2.2:80			
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b1a9-26ca3			33f97d16-0413-4e6e-9f3d-8[redacted]
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8404-b5b6			33f97d16-0413-4e6e-9f3d-8[redacted]
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-99e1-6703			33f97d16-0413-4e6e-9f3d-8[redacted]
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing				

合并报告采用 CSV 格式。每列中的条目描述如下：

- **NetScaler IP 地址**：报告中显示 NetScaler 实例的 IP 地址
- **NetScaler® 主机名**：报告中显示主机名。
- **分区**：显示管理分区的 IP 地址
- **虚拟服务器**：\<name_of_the_virtual_server\>#virtual_IP_address:port_number
- **服务**：\<name_of_the_service\>#service-IP_address:port_number
- **服务组**：\<name_of_service_group\>#server_member1_IP_address:port,server_member2_IP_address:port,

注意

- 如果没有可用的主机名，则显示相应的 IP 地址。
- 空白列表示相应的实体未在该 NetScaler 实例上配置。

独立报告：您还可以下载并查看所有实例和实体的独立报告。例如，您可以仅下载负载平衡虚拟服务器、负载平衡服务或负载平衡服务组的报告。

NetScaler Console 允许您即时下载报告。您还可以安排报告每天、每周或每月在固定时间生成。

生成组合负载平衡报告

1. 在 NetScaler Console 中，导航到 **基础架构 > 网络功能 > 负载平衡**。
2. 在“**负载平衡**”页面上，单击

   。
3. 在打开的“**导出**”页面上，您有两个选项可查看报告：

   a. 选择“**立即导出**”选项卡，然后单击“**确定**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

合并报告将下载到您的系统。

b. 选择“**计划报告**”选项卡，以按固定间隔计划报告的生成和导出。指定报告生成重复设置，并创建用于导出报告的电子邮件配置文件。

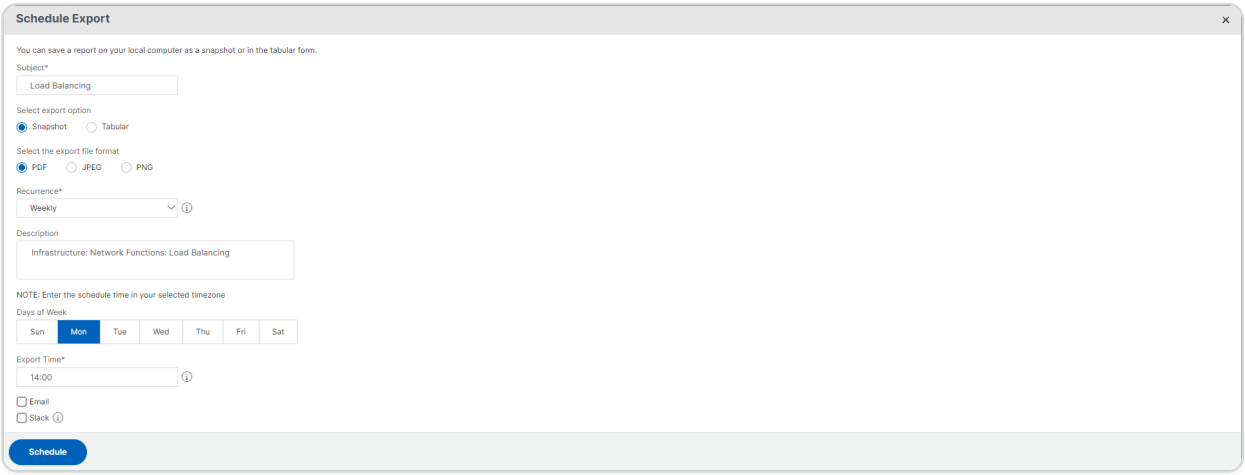
   i. **重复** - 从下拉列表中选择“**每日**”、“**每周**”或“**每月**”。

   ii. **重复时间** - 以 24 小时制输入时间（小时:分钟）。

   iii. **电子邮件配置文件** - 从下拉列表中选择一个配置文件，或单击“**+**”以创建电子邮件配置文件。

注意

如果您选择“**每周**”重复，请确保选择要安排报告的星期几。



注意

如果您选择**每月**重复，请确保输入所有您希望报告按计划生成的日期，并用逗号分隔。

生成单个负载均衡实体报告

您可以为与实例关联的特定类型实体生成并导出单个报告。例如，假设您想查看网络中所有负载均衡服务的列表。

1. 在 NetScaler Console 中，导航到 **基础架构 > 网络功能 > 负载均衡 > 服务。**
2. 在**服务**页面上，单击右上角的**导出**按钮。

   a. 如果您想立即生成并查看报告，请选择**立即导出**选项卡。

   b. 选择**计划导出**以按固定间隔计划生成和导出报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

您只能下载报告或将报告导出为邮件附件。您无法在 NetScaler Console GUI 上查看报告。

导出或计划导出网络功能报告

您可以在 NetScaler Console 中为选定的网络功能（例如负载平衡、内容切换、缓存重定向、全局服务器负载平衡 (GSLB)、身份验证和 NetScaler Gateway）生成综合报告。此报告可让您概览 NetScaler 实例、分区与网络中存在的相应绑定实体（虚拟服务器、服务组和服务）之间的映射。您可以将这些报告导出为 .csv 文件格式。

报告显示以下虚拟服务器数据：

- NetScaler® IP 地址
- 主机名
- 分区数据
- 虚拟服务器名称
- 虚拟服务器类型
- 虚拟服务器
- 目标 LB 虚拟服务器

注意

对于内容切换和缓存重定向虚拟服务器，“目标 LB 虚拟服务器”列出了所有 LB 服务器，即默认服务器和基于策略的服务器。

- 服务名称
- 服务组名称

您可以计划在不同时间间隔将这些报告导出到指定的电子邮件地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

- 对于 GSLB 虚拟服务器，网络功能报告仅显示 GSLB 虚拟服务器及其关联服务。
- 对于内容交换和缓存重定向虚拟服务器，报告仅显示与关联 LB 服务器的绑定。
- SSL 虚拟服务器未在此报告中列出，因为 NetScaler Console 上未维护单独的 SSL 虚拟服务器列表。
- 生成新报告时，旧报告将自动从您的帐户中清除。
- 您无法为 HAProxy 生成网络功能报告。

导出和计划网络功能报告：

1. 导航到 **基础架构 > 网络功能**。
2. 在“**网络功能**”页面上，在右侧窗格中，单击页面右上角的“**生成报告**”。
3. 在“**生成报告**”页面上，您有以下 2 个选项：

   a. 选择“**立即导出**”选项卡，然后单击“**确定**”。报告将下载到您的系统。

   下图显示了网络功能报告的示例。

NetScaler IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:8
[redacted]	[redacted]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[redacted]	[redacted]		Load Balancing	334-lb#1.33.2.2:80			
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b1a9-26ca3			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8404-b5b6			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-99e1-6703			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing				

   b. 选择“**计划报告**”选项卡，以定期计划报告的生成和导出。指定报告生成重复设置，并创建用于导出报告的电子邮件配置文件。

      i. **重复** - 从下拉列表框中选择“**每日**”、“**每周**”或“**每月**”。

      ii. **重复时间** - 以 24 小时制输入时间，格式为小时:分钟。

      iii. **电子邮件配置文件** - 从下拉列表框中选择一个配置文件，或单击 **+** 创建一个电子邮件配置文件。

单击 **启用计划** 以计划您的报告，然后单击 **确定**。通过选中 **启用计划** 复选框，您可以生成选定的报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

网络报告

您可以通过监控 NetScaler Application Delivery Management (NetScaler Console) 上的网络报告来优化资源使用。您可能有一个分布式部署，在多个位置部署了许多应用程序。为了确保应用程序的最佳性能，您还部署了多个 Citrix Application Delivery Controller (NetScaler) 实例来负载均衡、内容切换或压缩流量。网络性能会影响应用程序性能。为了持续维护应用程序的性能，您必须定期监控网络性能，并确保所有资源都得到最佳利用。

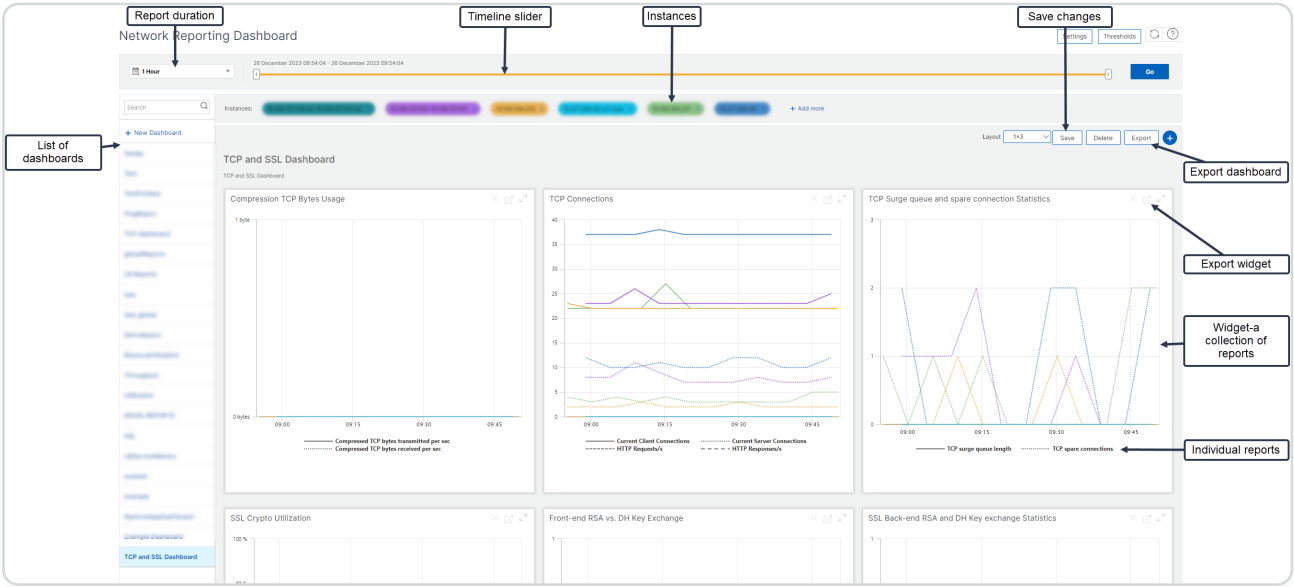
NetScaler Console 现在不仅允许您生成全局级别的实例报告，还可以生成虚拟服务器和网络接口等实体的报告。实例系列包括 NetScaler 实例。您可以为其生成报告的虚拟服务器如下：

- 负载均衡服务器、服务和服务组
- 内容切换服务器
- 缓存重定向服务器
- 全局服务负载均衡 (GSLB)
- 身份验证
- NetScaler 网关

NetScaler Console 中的网络报告仪表板具有高度可定制性。您现在可以为各种实例、虚拟服务器和其他实体创建多个仪表板。

网络报告仪表板

下图指出了仪表板中的各项功能：



- 左侧面板列出了在 NetScaler Console 中创建的所有自定义仪表板。您可以单击其中一个以查看仪表板包含的各种报告。例如，TCP 和 SSL 仪表板包含与 TCP 和 SSL 协议相关的各种报告。

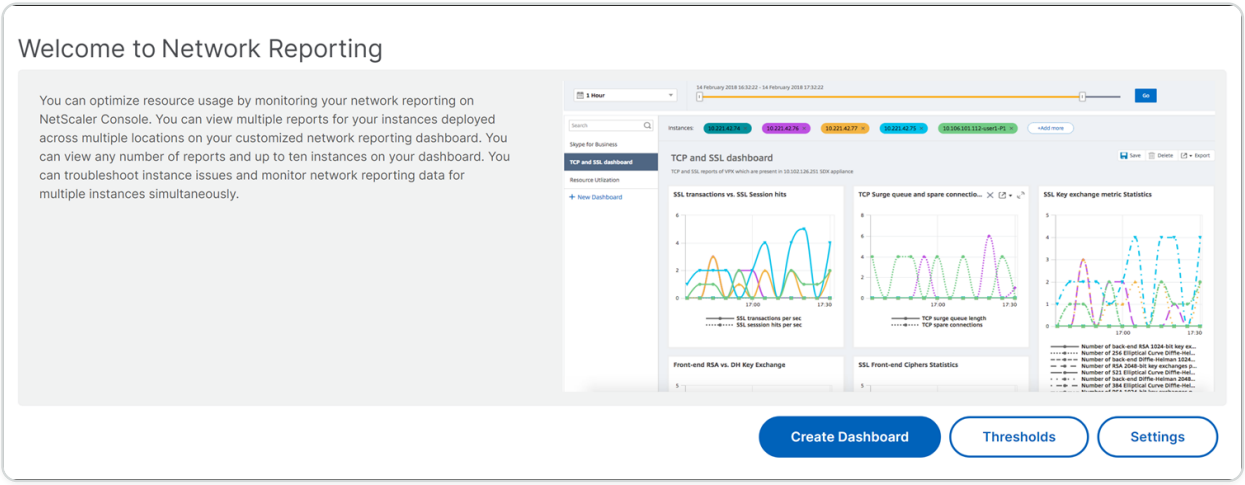
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 您可以使用多个小部件自定义每个仪表板以显示各种报告。小部件代表仪表板上的一个报告，即更多相关报告的集合。例如，压缩 TCP 字节使用情况报告包含每秒传输和接收的压缩 TCP 字节的报告。
- 您可以显示一小时、一天、一周或一个月的报告。此外，您现在可以使用时间轴滑块选项来自定义在 NetScaler Console 上生成的报告的持续时间。
- 您可以通过单击“X”来删除报告。您还可以将报告导出为 .pdf、.jpeg、.png 或 .csv 格式到您的系统。您还可以安排报告生成的时间和重复频率。您还可以配置一个电子邮件分发列表，报告将发送到该列表。
- 仪表板顶部的“实例”部分列出了生成报告的所有实例的 IP 地址。
- 您可以通过单击“X”删除实例，或向报告中添加更多实例。但是，目前 NetScaler Console 允许您查看 10 个实例的报告。
- 您还可以将整个仪表板导出为 .pdf、.jpeg、.png 或 .csv 格式到您的系统。对仪表板所做的任何更改都必须保存。单击“保存”以保存更改。

以下部分详细解释了创建仪表板、生成报告和导出报告的任务。

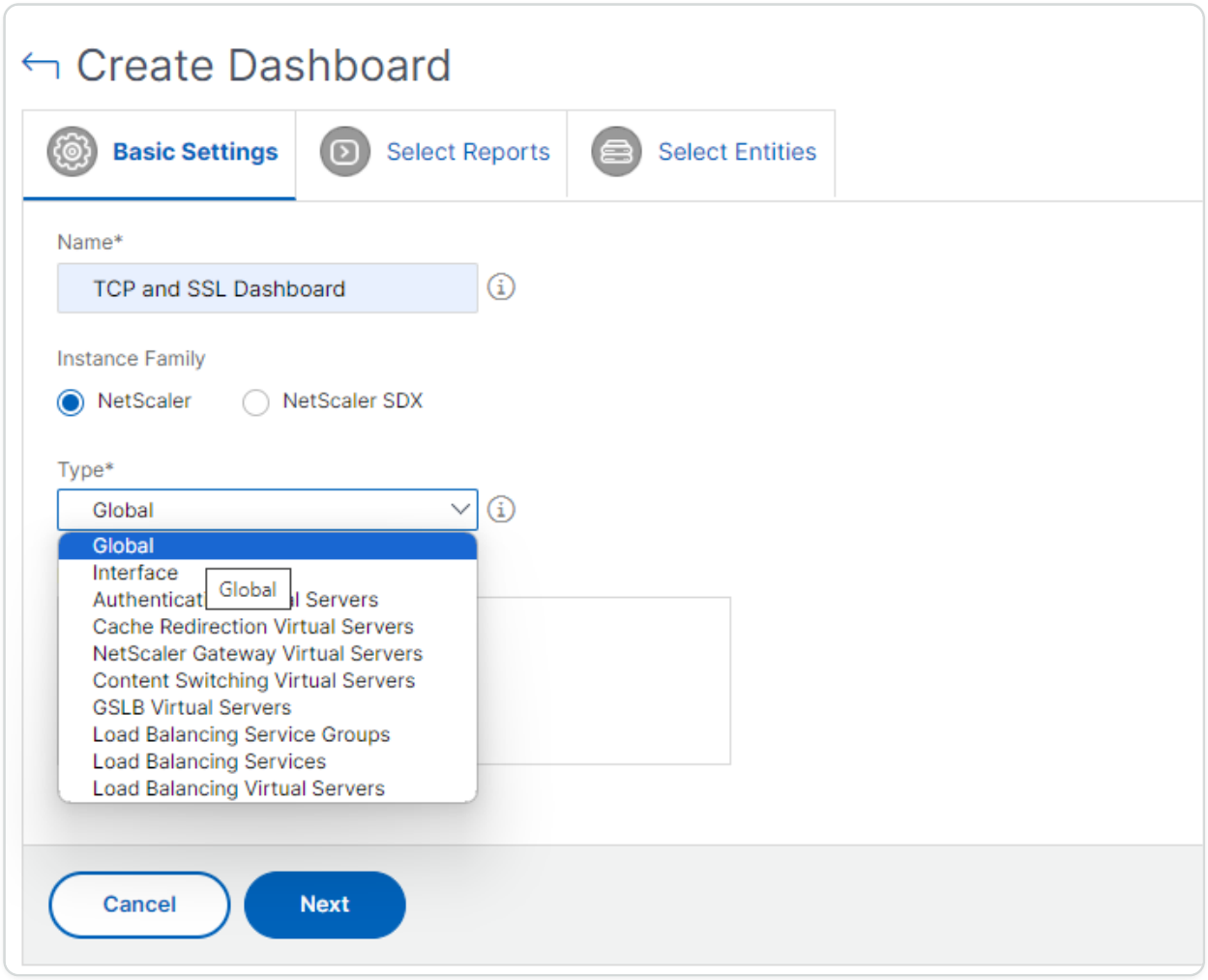
查看或创建仪表板：

1. 在 NetScaler Console 中，导航到 **基础架构 > 网络报告**。



2. 要查看现有仪表板，请单击“**查看仪表板**”。此时将打开“网络报告”**仪表板**页面，您可以在其中查看所有仪表板和报告小部件。
3. 要创建仪表板，请单击“**新建仪表板**”。此时将打开“创建仪表板”页面。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 在“基本设置”选项卡中，输入以下详细信息：

   a. **名称**。键入仪表板的名称。

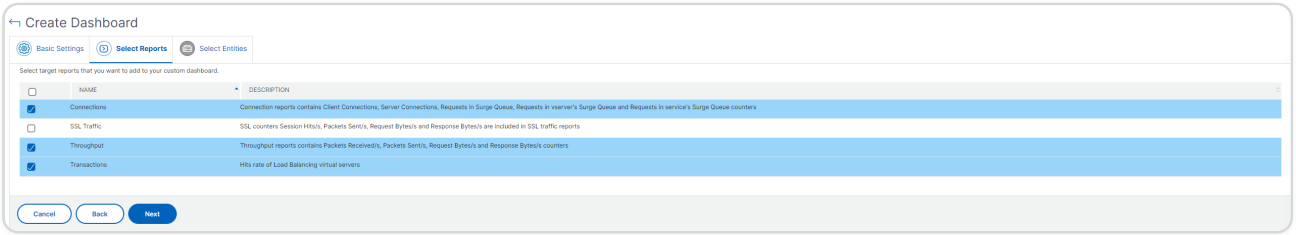
   b. **实例系列**。选择实例类型 - NetScaler 或 NetScaler SDX。

   c. **类型**。选择要为其生成报告的实体类型。在此示例中，选择负载平衡虚拟服务器。

   d. **描述**。为仪表板键入有意义的描述。

5. 单击**下一步**。将显示实例和特定实体支持的所有报告。

6. 在**选择报告**选项卡中，选择所需的报告。在此示例中，您可以选择事务、连接和吞吐量。单击**下一步**。

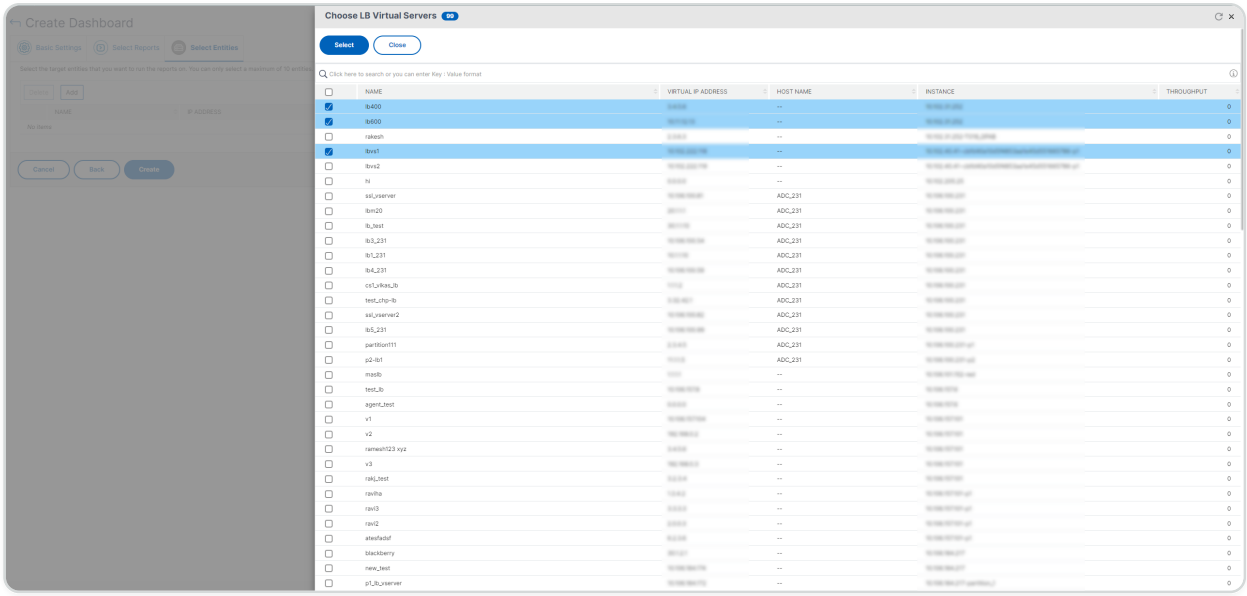


1. 在**选择实体**选项卡中，单击**添加**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

将出现一个窗口，其中包含实体列表，具体取决于**基本设置**选项卡中选择的实体类型。在此示例中，将出现**选择 LB 虚拟服务器**窗口。

2. 选择要监视的实体。



3. 单击**创建**。

仪表板已创建并显示您选择的所有报告。

注意

目前，您对图例或筛选器所做的任何更改都无法保存。

导出网络报告

虽然您可以将小组件报告导出为 .pdf、.png、.jpeg 或 .csv 格式，但只能将整个仪表板导出为 .pdf、.jpeg 或 .png 格式。

注意

如果您只有只读权限，则无法在 NetScaler Console 中导出报告。您需要编辑权限才能在 NetScaler Console 中创建文件并导出文件。

导出仪表板报告：

1. 导航到 **基础设施 > 网络报告**
2. 单击 **View Dashboards** 以查看您已创建的所有仪表板。
3. 在左侧窗格中，单击一个仪表板。在此示例中，单击 **Dashboard 1**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 单击页面右上角的导出按钮。
5. 在 **Export Now** 选项卡下，选择所需的格式，然后单击 **Export**。

   在 **Export** 页面上，您可以执行以下操作之一：

6. 选择 **Export Now** 选项卡。以 PDF、JPEG、PNG 或 CSV 格式查看和保存报告。
7. 选择 **Schedule Export** 选项卡。以每日、每周或每月的方式安排报告，并通过电子邮件或 Slack 消息发送报告。

   您可以定期安排导出 **Network Reporting** 仪表板页面。例如，您可以设置一个选项，在特定时间每周生成一次前一小时的仪表板报告。然后，报告将每周生成并显示仪表板的状态。如果用户设置了时间戳和日期戳，报告将覆盖它们。

注意

- 如果您选择每周重复，请确保选择您希望安排报告的周几。
- 如果您选择每月重复，请确保输入所有您希望安排报告的日期，并用逗号分隔。

在安排网络报告时，您可以通过在 **Subject** 字段中输入文本字符串来自定义报告的标题。在预定时间创建的报告将以此字符串作为其名称。

例如，对于源自特定虚拟服务器的网络报告，您可以将主题键入为“authentication-reports-10.106.118.120”，其中 10.106.118.120 是受监控虚拟服务器的 IP 地址。

注意

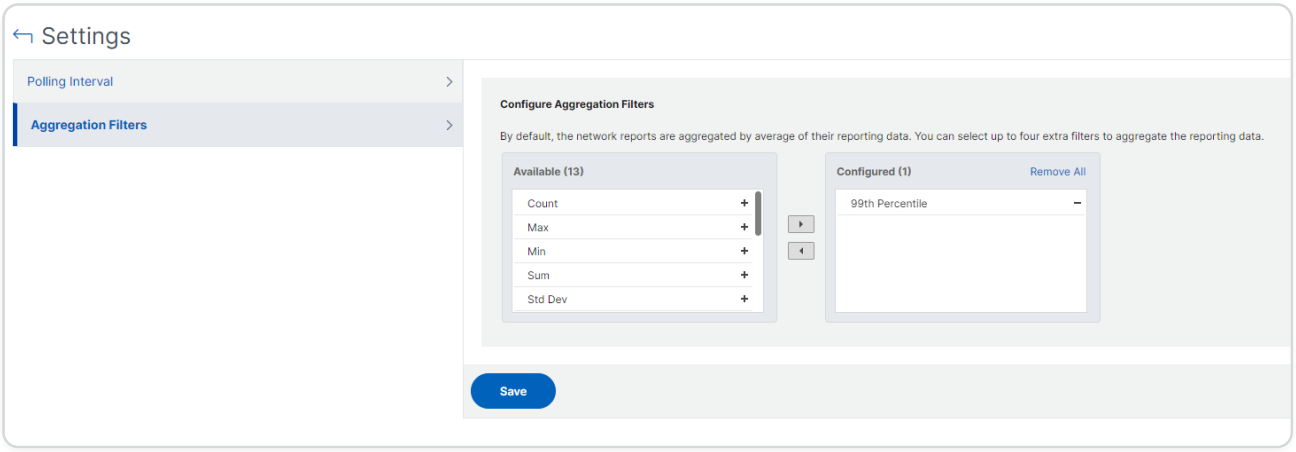
目前，此选项仅在您计划导出报告时可用。当您即时导出报告时，无法向报告添加标题。

通过应用聚合查看网络报告数据

您可以将聚合应用于网络性能数据，并在仪表板上查看应用程序性能。您还可以根据需要导出结果。通过对数据应用这些聚合，您可以分析并确保所有资源都得到最佳利用。导航到 **网络 > 网络报告**，并选择 1 天或更长时间段以获取 **查看方式** 选项。

在现有平均数据中，您可以通过从 **查看方式** 列表中选择选项来应用聚合。当您应用聚合时，仪表板中每个指标的数据都会更新。单击 **设置** 并选择 **聚合筛选器**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以添加的聚合如下：

- 计数
- 最大值
- 最小值
- 总和
- 标准差
- 方差
- 众数
- 中位数
- 第25百分位数
- 第75百分位数
- 第95百分位数
- 第99百分位数
- 第一个
- 最后一个

您最多可以将 4 个聚合选项添加到仪表板。添加聚合选项后，NetScaler Console 大约需要 1 小时才能为选定的聚合选项生成报告。

导出小部件报告：

1. 导航到 **基础设施 > 网络报告**。
2. 单击 **View Dashboards** 以查看您创建的所有仪表板。
3. 在左侧窗格中，单击一个仪表板。在此示例中，也单击 **Skype for Business**。
4. 选择一个小部件。例如，选择 **Load Balancing Virtual Server Transactions**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 单击页面右上角的导出按钮
6. 在 **Export Now** 选项卡下，选择所需的格式，然后单击 **Export**。

   导出小部件报告(/en-us/netscaler-application-delivery-management-software/media/nw-dash-widget-export.png)

如何在 NetScaler Console 上管理网络报告的阈值

为了监控 NetScaler 实例的状态，您可以在计数器上设置阈值，并在阈值超出时接收通知。在 NetScaler Console 上，您可以配置阈值，并查看、编辑和删除它们。

例如，当内容交换虚拟服务器的连接计数器达到指定值时，您可以收到电子邮件通知。您可以为特定实例类型定义阈值。您还可以选择要为所选实例中的特定计数器指标生成的报告。

当计数器值超出或低于（根据规则指定）阈值时，会生成指定严重性的事件，以表示性能相关问题。当计数器值恢复到您认为正常的值时，事件将被清除。可以通过导航到 **基础架构 > 事件 > 报告** 来查看这些事件。在“报告”页面上，您可以单击“**按严重性划分的事件**”圆环图以按严重性查看事件。

您还可以将操作与阈值关联，例如在阈值被突破时发送电子邮件或短信。

创建阈值：

1. 在 NetScaler Console 中，导航到 **基础架构 > 网络报告 > 阈值**。在 **阈值** 下，单击 **添加**。
2. 在 **创建阈值** 页面上，指定以下详细信息：
   - **名称**。阈值的名称。
   - **实例类型**。选择 NetScaler。
   - **报告名称**。提供有关此阈值信息的性能报告的名称。
3. 您还可以设置规则来指定何时生成或清除事件。您可以在 **配置规则** 部分下指定以下详细信息：
   - **指标**。选择要为其设置阈值的指标。
   - **比较器**。选择一个比较器来检查受监控值是大于等于还是小于等于阈值。
   - **阈值**。输入用于计算事件严重性的值。例如，如果“当前客户端连接数”的监控值达到 80%，您可能希望生成一个具有严重事件严重性的事件。在这种情况下，输入 80 作为阈值。您可以通过导航到“**基础架构 > 事件 > 报告**”来查看“严重”事件。在“报告”页面上，您可以单击“**按严重性划分的事件**”圆环图以按严重性查看事件。
   - **清除值**。输入指示何时清除该值的值。例如，当监控值达到 50% 时，您可能希望清除“当前客户端连接数”阈值。在这种情况下，输入 50 作为清除值。
   - **事件严重性**。选择要为阈值设置的安全级别。

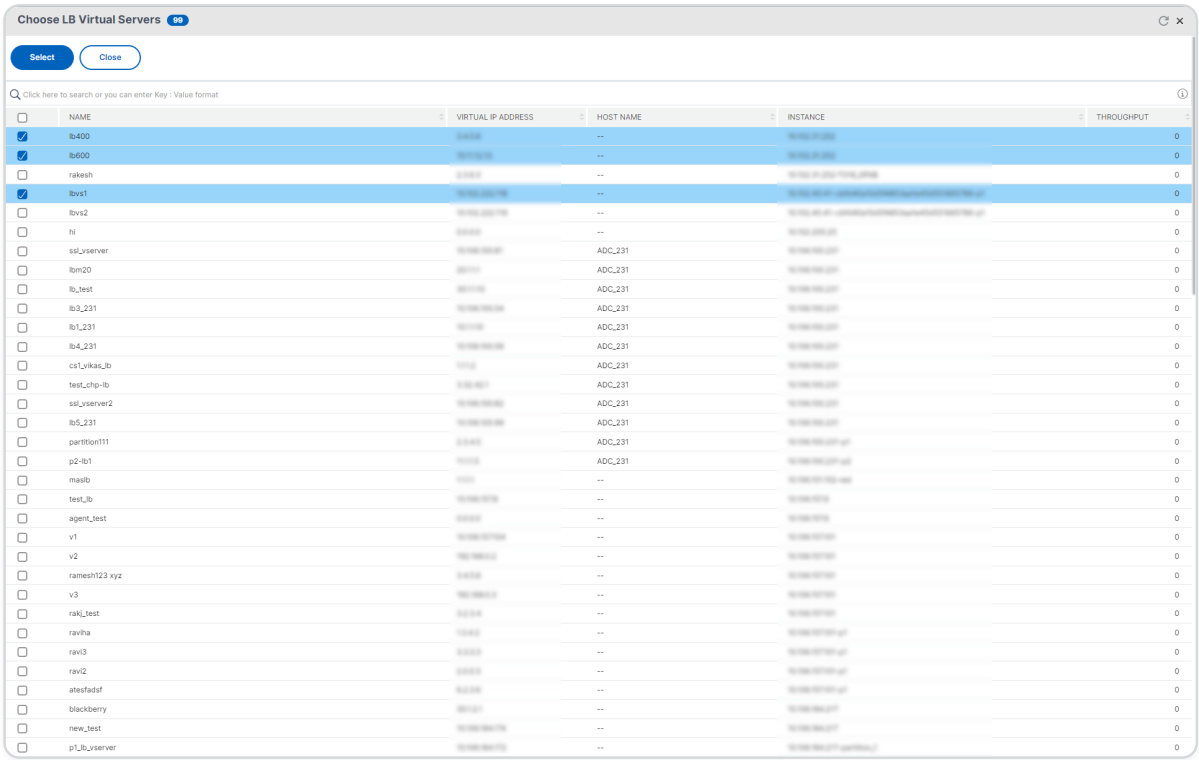
© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 您可以选择要设置阈值的实例和实体。在“**实例**”部分中，选择以下选项之一：

   - **所有实例**。为所有实例设置阈值。
   - **特定实例**。为特定实例设置阈值。使用右箭头将实例从“**可用**”列表移动到“**已配置**”列表。为“**已配置**”列表中的实例设置阈值。
   - **特定实体**。为特定实体设置阈值。

   单击“**添加**”以选择实体。

   将根据“**报告名称**”字段中选择的报告类型显示一个包含实体列表的窗口。在此示例中，将显示“**选择 LB 虚拟服务器**”窗口。



   选择要为其设置阈值的实体。单击“**选择**”。所选实体将显示在“**实例**”部分中。

   注意

   仅当您在“**报告名称**”中选择基于 vserver 的报告时，“**特定实体**”选项才会出现。例如，如果您选择“**LB 服务统计信息**”

5. 您还可以添加“**事件消息**”。输入当达到阈值时要显示的消息。NetScaler Console 会将监控值和阈值附加到此消息中。
6. 选择“**启用**”以启用阈值来生成警报。
7. 您可以选择配置**操作**，例如电子邮件通知、Slack 通知，或者同时配置电子邮件和 Slack 通知。

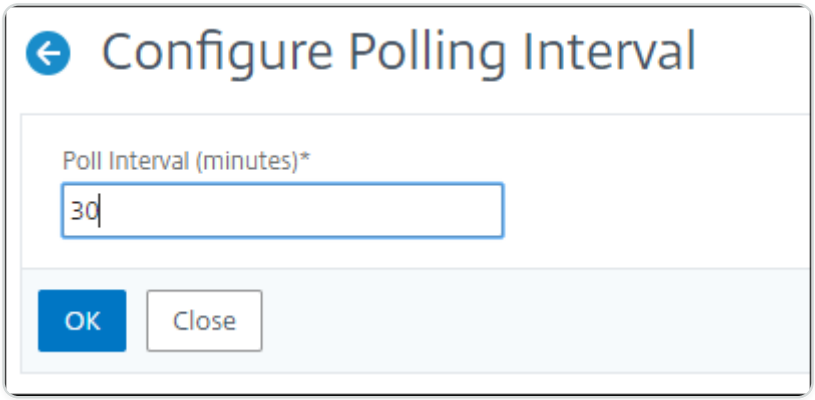
© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. 点击**创建**。

设置网络报告的性能轮询间隔

默认情况下，每 5 分钟，NITRO 调用会收集网络报告的性能数据。NetScaler Console 会检索实例统计信息（例如计数器信息），并根据每分钟、每小时、每天或每周对其进行聚合。您可以在预定义报告中查看这些聚合数据。

要设置性能轮询间隔，请导航到**基础架构 > 网络报告**，然后点击**配置轮询间隔**。您的轮询间隔不能少于 5 分钟或多于 60 分钟。



配置网络报告清除设置

您可以在 NetScaler Console 中配置网络报告数据的清除间隔。此设置限制了存储在 NetScaler Console 服务器数据库中的网络报告数据量。默认情况下，网络报告历史数据每 24 小时（01:00）清除一次。

注意

您可以指定的值不能超过 30 天或少于 1 天。

配置作业

NetScaler Application Delivery Management (NetScaler Console) 配置管理过程可确保在网络中的多个 Citrix NetScaler 实例之间正确复制配置更改、系统升级和其他维护活动。

NetScaler Console 允许您创建配置作业，帮助您轻松地在多个设备上以单个任务的形式执行所有这些活动。配置作业和模板将 NetScaler Console 上最重复的管理任务简化为单个任务。配置作业包含一组配置命令，您可以在一个或多个托管设备上运行这些命令。

配置作业可以使用 SSH 命令执行配置命令，也可以使用 SCP 从本地或复制文件到另一个设备，例如，我们可以安排 HA 故障转移或 HA 升级。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

尽管您可以选择任意数量的 NetScaler 实例进行升级，但 NetScaler Console 本地部署版最多支持 40 个并发升级线程。这意味着只能同时升级 40 个实例。

您可以使用 NetScaler Console 中的以下四个选项之一创建配置作业。使用其中一个选项创建可重用的命令和指令源，以便系统运行配置作业。

1. 配置模板
2. 实例
3. 文件
4. 录制和播放

配置模板

您可以在创建作业时创建配置模板，并将一组配置命令保存为模板。当您在“创建作业”页面上保存这些模板时，它们会自动显示在“创建模板”页面上。

注意 默认配置模板的“**重命名**”选项处于禁用状态。但是，您可以重命名自定义配置模板。

您可以使用以下模板之一：

配置编辑器：您可以使用配置编辑器键入 CLI 命令，将配置保存为模板，并使用它来配置作业。

内置模板：您可以从配置模板列表中进行选择。这些模板提供 CLI 命令的语法，并允许您为变量指定值。内置模板及其说明列在下表中。您可以使用内置模板选项来安排作业。作业是一组配置命令，您可以在一个或多个托管实例上运行这些命令。例如，您可以使用内置模板选项来安排作业以配置 syslog 服务器。您还可以选择立即运行作业或安排作业在以后运行。

实例

您可以对运行 NetScaler 11.0 及更高版本的 NetScaler SDX 实例执行单捆绑包升级。要执行单捆绑包升级，您可以使用 NetScaler Console 中的内置任务。您还可以通过提取正在运行的配置或已保存的配置，并在相同类型的另一个 NetScaler 实例上运行命令来升级 NetScaler 实例。这允许您将一个实例的配置复制到另一个实例上。

文件

您可以从本地计算机上传配置文件并创建作业。

使用文件的优势

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 您可以使用任何文本文件来创建可重用的配置命令源。
- 不需要任何格式。
- 文件可以保存在您的本地计算机上。

您可以创建并保存新文件，也可以导入现有文件并运行命令。

录制和播放

使用“创建作业”，您可以输入自己的 CLI 命令，也可以使用“录制和播放”按钮从 NetScaler 会话中获取命令。当您运行作业时，所选实例上 ns.conf 中的更改将被记录并复制到 NetScaler Console。

相关文章

- 如何在配置作业中使用 SCP (put) 命令
- 如何在配置作业中使用变量
- 如何从纠正命令创建配置作业
- 如何使用配置模板创建审计模板
- 如何使用录制和回放创建配置作业
- 如何在 NetScaler Console 上使用主配置模板

创建配置作业

作业是一组配置命令，您可以在一个或多个托管实例上创建和运行这些命令。您可以创建作业以跨实例进行配置更改，在网络上的多个实例上复制配置，以及使用 NetScaler Console GUI 记录和播放配置任务 并将其转换为 CLI 命令。

您可以使用 NetScaler Console 的配置作业功能来创建配置作业、发送电子邮件通知以及检查所创建作业的执行日志。

在 NetScaler Console 上创建配置作业：

1. 导航到 **Infrastructure（基础架构）> Configuration（配置）> Configuration Jobs（配置作业）**。
2. 单击 **Create Job（创建作业）**。
3. 在 **Create Job（创建作业）** 页面上，在 **Select Configuration（选择配置）** 选项卡下，指定作业名称并从列表中选择 **Instance Type（实例类型）**。
4. 在 **Configuration Source（配置源）** 列表中，选择要创建的配置作业模板。为所选模板添加命令。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 您可以输入命令，也可以从已保存的配置模板中导入现有命令。
- 在配置作业中创建作业时，您还可以在配置编辑器中添加不同类型的多个模板。
- 从 **Configuration Source（配置源）** 列表中，选择不同的模板，然后将模板拖到配置编辑器中。模板类型可以是 **Configuration Template（配置模板）**、**In built Template（内置模板）**、**Master Configuration（主配置）**、**Record and Play（录制和播放）**、**Instance（实例）** 和 **File（文件）**。

注意

如果首次添加 `Deploy Master Configuration Job` 模板，然后添加不同类型的模板，则整个作业模板将变为 `Master Configuration` 类型。

您还可以在配置编辑器中重新排列和重新排序命令。您可以通过拖放命令行将命令从一行移动到另一行。您还可以通过简单地更改文本框中的命令行号，将命令行从一行移动或重新排列到任何目标行。您还可以在编辑配置作业时重新排列和重新排序命令行。

您可以定义变量，使您能够为这些参数分配不同的值或跨多个实例运行作业。您可以在单个合并视图中查看在创建或编辑配置作业时定义的所有变量。单击 **Preview Variables（预览变量）** 选项卡，以在单个合并视图中预览您在创建或编辑配置作业时定义的变量。

您可以在配置编辑器上为每个命令自定义回滚命令。要指定自定义命令，请启用自定义回滚选项。

重要

要使自定义回滚生效，请完成“**创建作业**”向导。然后在“**执行**”选项卡中，从“**命令失败时**”列表中选择“**回滚成功命令**”选项。

5. 在“**选择实例**”选项卡中，选择要运行配置审核的实例。

   a. 在 NetScaler 高可用性对中，您可以在主节点或辅助节点本地运行配置作业。选择要在哪个节点上运行作业。

      - **在主节点上执行** - 选择此选项可在主节点上运行作业。
      - **在辅助节点上执行** - 选择此选项可在辅助节点上运行作业。

      您也可以选择主节点和辅助节点来运行相同的配置作业。如果您不选择主节点或辅助节点，配置作业将自动在主节点上运行。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. 在“**指定变量值**”选项卡中，您有两个选项：

   a. 下载输入文件以输入您在命令中定义的变量值，然后将文件上传到 NetScaler Console 服务器。

   b. 输入为所有实例定义的变量的通用值

   c. 单击“**下一步**”。

为作业发送电子邮件和 Slack 通知：

现在，每次运行或计划作业时都会发送电子邮件和 Slack 通知。通知包括作业成功或失败等详细信息以及相关详细信息。

1. 导航到“**基础架构 > 配置 > 配置作业**”。
2. 选择要启用电子邮件和 Slack 通知作业，然后单击 **编辑**。
3. 在 **执行** 选项卡中，转到 **通过以下方式接收执行报告** 窗格：

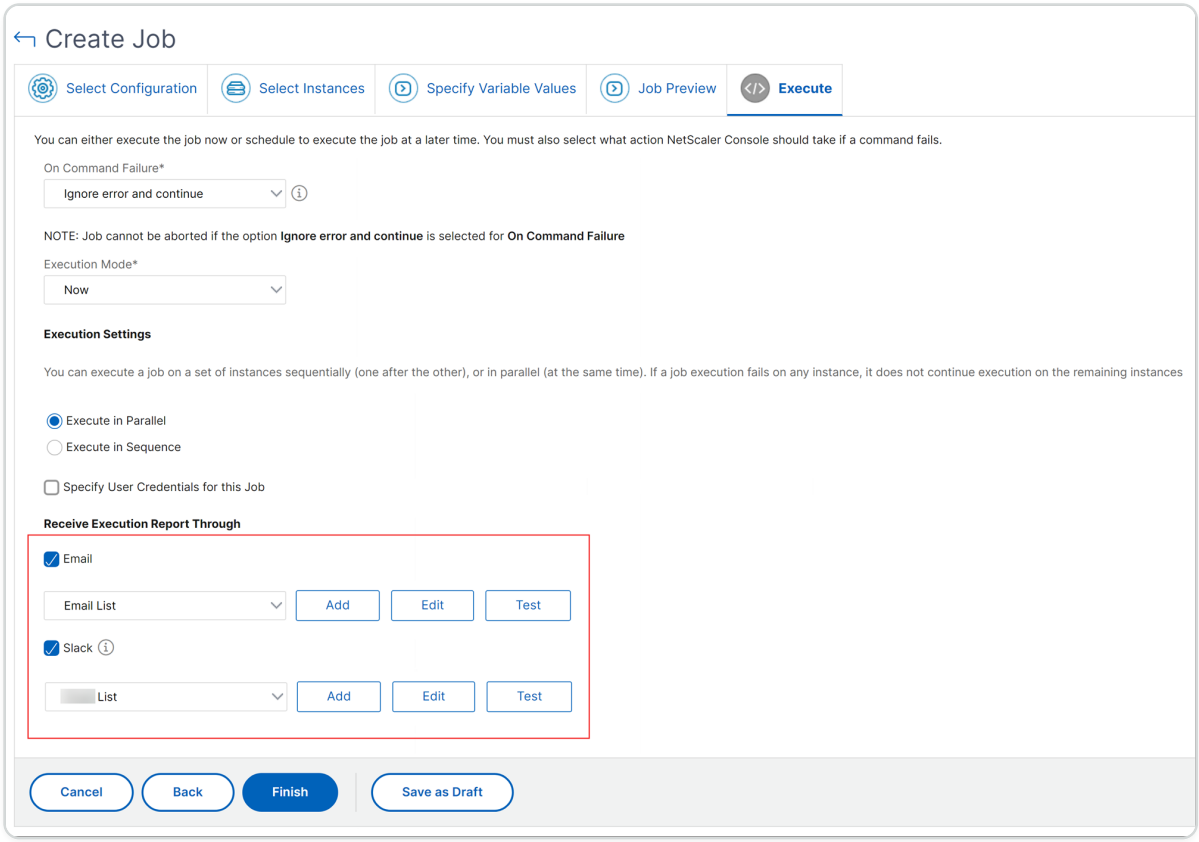
   - 选中 **电子邮件** 复选框，然后选择要发送执行报告的电子邮件分发列表。

     如果要添加电子邮件分发列表，请单击 **添加** 并指定电子邮件服务器详细信息。

   - 选中 **Slack** 复选框，然后选择要发送执行报告的 Slack 频道。

     如果要添加 Slack 配置文件，请单击 **添加** 并指定所需 Slack 频道的 **配置文件名称**、**频道名称** 和 **令牌**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 单击 **完成**。

为作业发送电子邮件和 Slack 通知：

现在，每次运行或计划作业时，都会发送电子邮件和 Slack 通知。通知包括作业成功或失败等详细信息以及相关详细信息。

1. 导航到 **基础架构 > 配置 > 配置作业**。
2. 选择要启用电子邮件和 Slack 通知作业，然后单击 **编辑**。
3. 在 **执行** 选项卡中，转到 **通过以下方式接收执行报告** 窗格：
   - 选中 **电子邮件** 复选框，然后选择要发送执行报告的电子邮件分发列表。

     如果要添加电子邮件分发列表，请单击 **添加** 并指定电子邮件服务器详细信息。
   - 选中 **Slack** 复选框，并选择要发送执行报告的 Slack 频道。

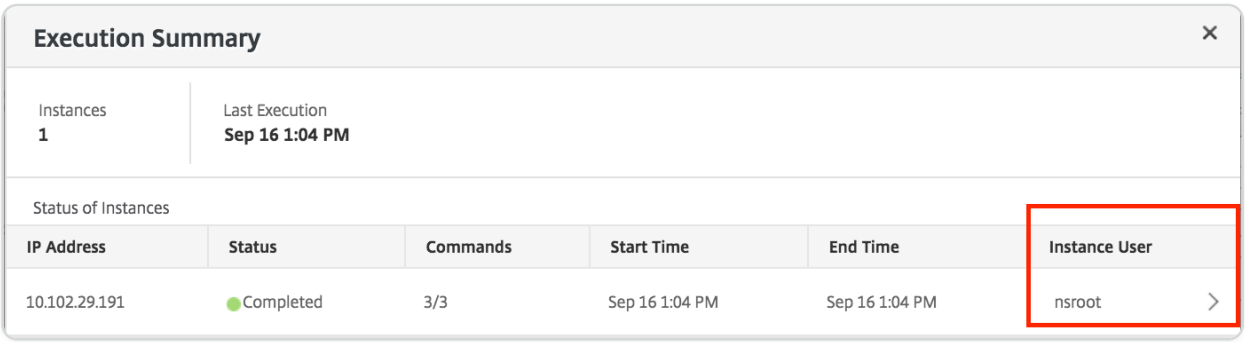
     如果要添加 Slack 配置文件，请单击 **添加**，并指定所需 Slack 频道的**配置文件名称**、**频道名称**和**令牌**。
4. 单击 **完成**。

查看执行摘要详细信息：

1. 导航到 **基础架构 > 配置 > 配置作业**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 选择要查看执行摘要的作业，然后单击 **详细信息**。
3. 单击 **执行摘要** 以查看：
   - 运行该作业的实例状态
   - 在作业上运行的命令
   - 作业的开始时间和结束时间，以及
   - 实例用户的名称



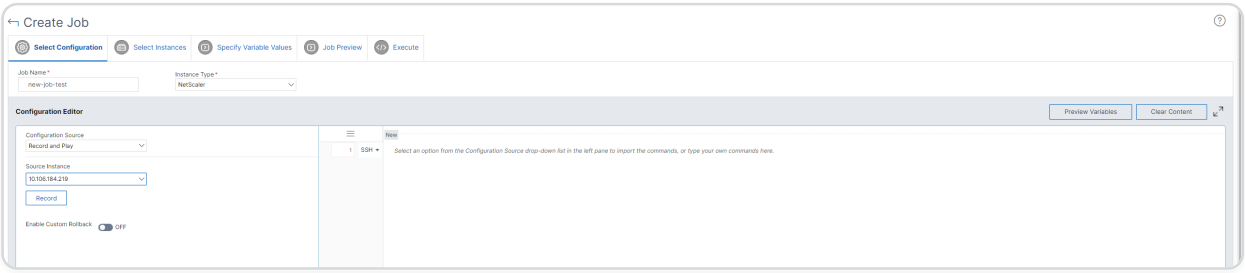
使用录制和回放创建配置作业

如果您习惯使用 NetScaler GUI 配置 NetScaler 实例，有时，您可能会发现很难回忆起确切的 CLI 命令来创建配置任务并在多个 NetScaler 实例上运行。

NetScaler Console 使您能够录制使用 NetScaler 实例的 GUI 执行的配置任务，并将其转换为 CLI 命令。然后，您可以从这些 CLI 命令创建配置任务，并在多个实例上运行此任务。

录制 GUI 配置并将其转换为配置任务

1. 导航到 **基础结构 > 配置作业**，然后单击 **创建作业**。
2. 指定作业名称和实例类型。
3. 从 **配置源** 列表中，选择 **录制和回放**，然后选择要录制配置的源实例。单击 **录制**。

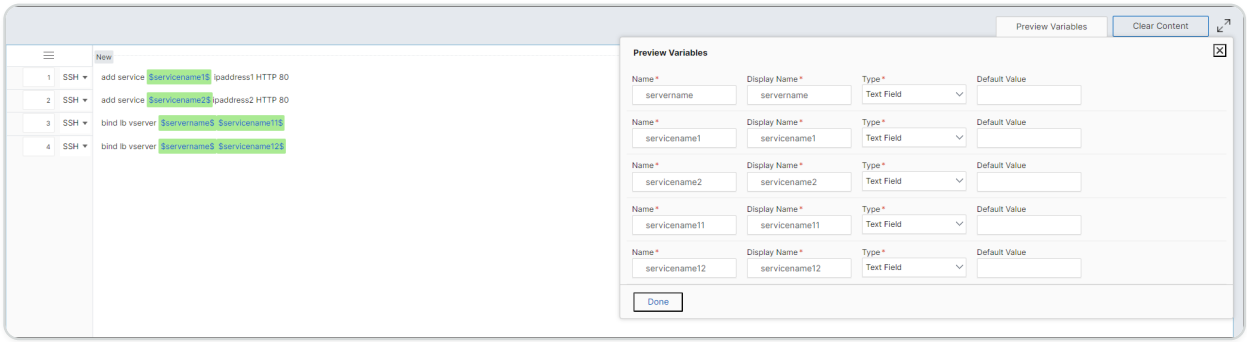


4. **NetScaler GUI** 将打开。配置您希望配置任务包含的功能和设置。然后，关闭 NetScaler GUI 窗口，并在 **配置编辑器** 中单击 **停止**。命令将作为链接显示在左侧窗格中。将命令拖动到右侧窗格，然后单击 **下一步**。

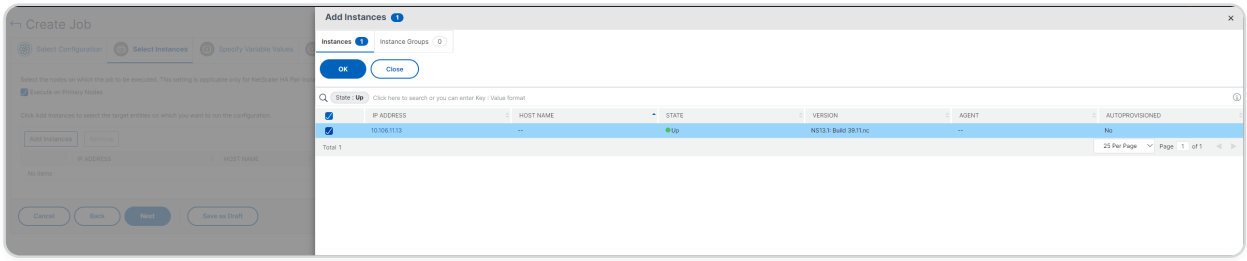
© 1997–2026 Citrix Systems, Inc. All rights reserved.

然后，您可以根据需要重新排列和重新排序配置编辑器中的命令。您可以通过拖放命令行将命令从一行移动到另一行。您还可以通过简单地更改文本框中的命令行号，将命令行从一行移动或重新排列到任何目标行。

5. 您可以在创建或编辑配置作业时，在一个统一视图中查看所有已定义的变量。
6. 执行以下操作之一，以在统一视图中查看所有变量：
   - 创建配置作业时，导航到 **基础结构 > 配置作业**，选择 **创建作业**。在 **创建作业** 页面上，您可以查看在创建配置作业时添加的所有变量。
   - 编辑配置作业时，导航到 **网络 \> 配置作业**，选择作业名称并单击 **编辑**。在 **配置作业** 页面上，您可以查看在创建配置作业时添加的所有变量。
7. 然后，您可以单击 **预览变量** 选项卡，以在统一视图中预览您在创建或编辑配置作业时定义的变量。
8. 出现一个新弹出窗口，以表格形式显示变量的所有参数，例如名称、显示名称、类型和默认值。您还可以编辑和修改这些参数。编辑或修改任何参数后，单击“**完成**”按钮。



9. 单击“**添加实例**”并选择要运行配置作业的实例。单击“**确定**”，然后单击“**下一步**”。



10. 如果您在命令中指定了变量，请在“**指定变量值**”选项卡上，选择以下选项之一来为您的实例指定变量：
    - “**上传变量值的输入文件：**”单击“**下载输入密钥文件**”以下载输入文件。在输入文件中，输入您在命令中定义的变量的值，然后将文件上传到 NetScaler Console 服务器。
    - “**所有实例的通用变量值**”：输入变量的值。变量因所选模板而异。

    包含变量值的输入文件会（以相同的文件名）持久保存在配置作业中。您可以查看和编辑在创建或编辑配置作业时之前使用和上传的这些输入文件。

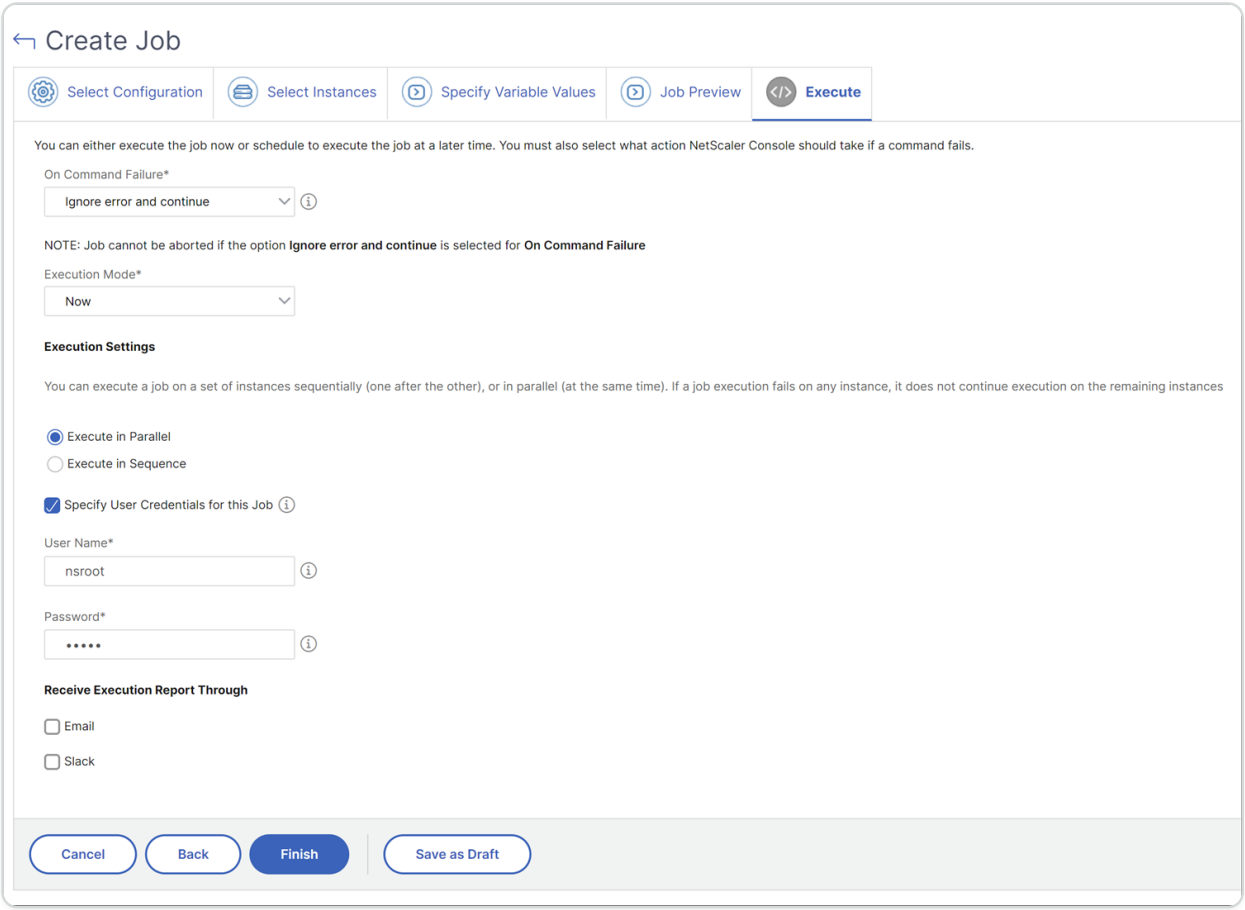
© 1997–2026 Citrix Systems, Inc. All rights reserved.

要在创建配置作业时查看运行配置作业，请导航到“**网络 \> 配置作业**”，然后单击“**创建作业**”。在“**创建作业**”页面中。在“**指定变量值**”选项卡上，选择“**所有实例的通用变量值**”选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑并上传文件（保持相同的文件名）。

要在编辑配置作业时查看已运行的配置作业，请导航到“**网络 \> 配置作业**”，选择作业名称，然后单击“**编辑**”。在“**配置作业**”页面中，在“**指定变量值**”选项卡上，选择“**所有实例的通用变量值**”选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑并上传文件（保持相同的文件名）。10. 在“**作业预览**”选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。

11. 在“**作业预览**”选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。
12. 在“**执行**”选项卡上，您可以选择立即运行作业或安排稍后运行。您还可以选择如果命令失败，NetScaler Console 必须采取什么操作。

    您还可以选择允许授权用户在您的托管实例上运行作业，并且您可以选择是否发送有关作业成功或失败的电子邮件通知以及其他详细信息。



13. 在“**作业**”页面上，您可以查看配置任务在所有实例上的执行进度。

使用配置作业将配置从一个实例复制到多个实例

您可以使用 NetScaler Console 的配置作业功能从 NetScaler 实例中提取特定配置，并将其复制到多个实例。

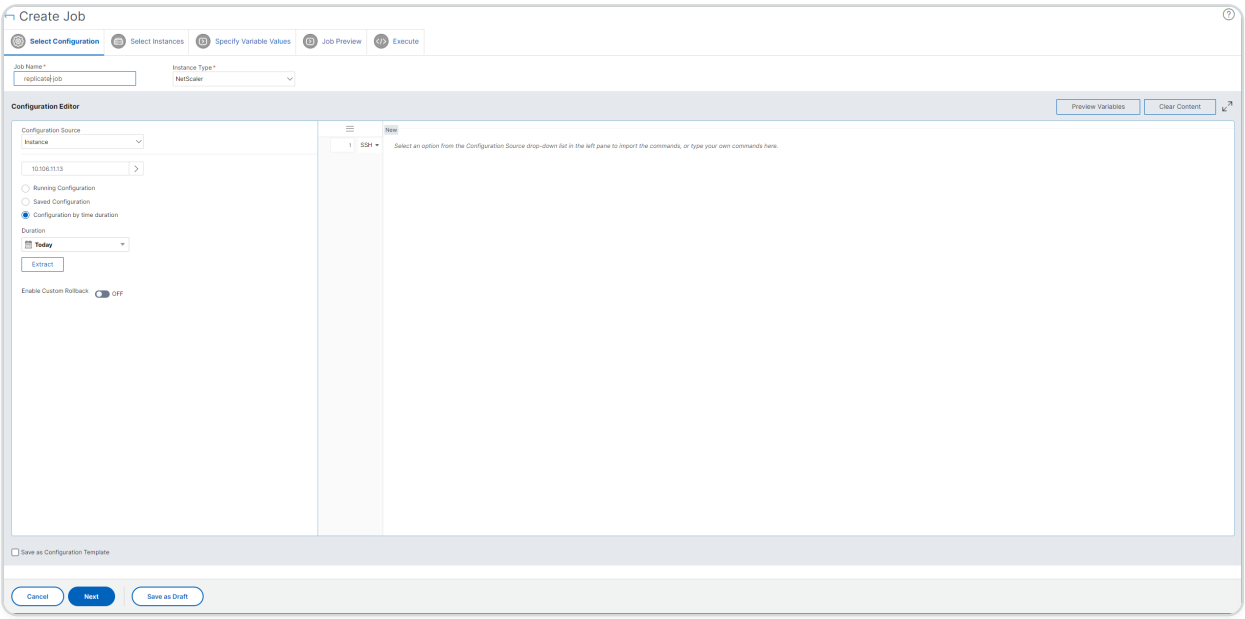
© 1997–2026 Citrix Systems, Inc. All rights reserved.

例如，您可能已在 NetScaler 实例上为您的部署配置了负载平衡和前端优化 (FEO)。但是，现在您只想将 FEO 配置复制到其他 NetScaler 实例。

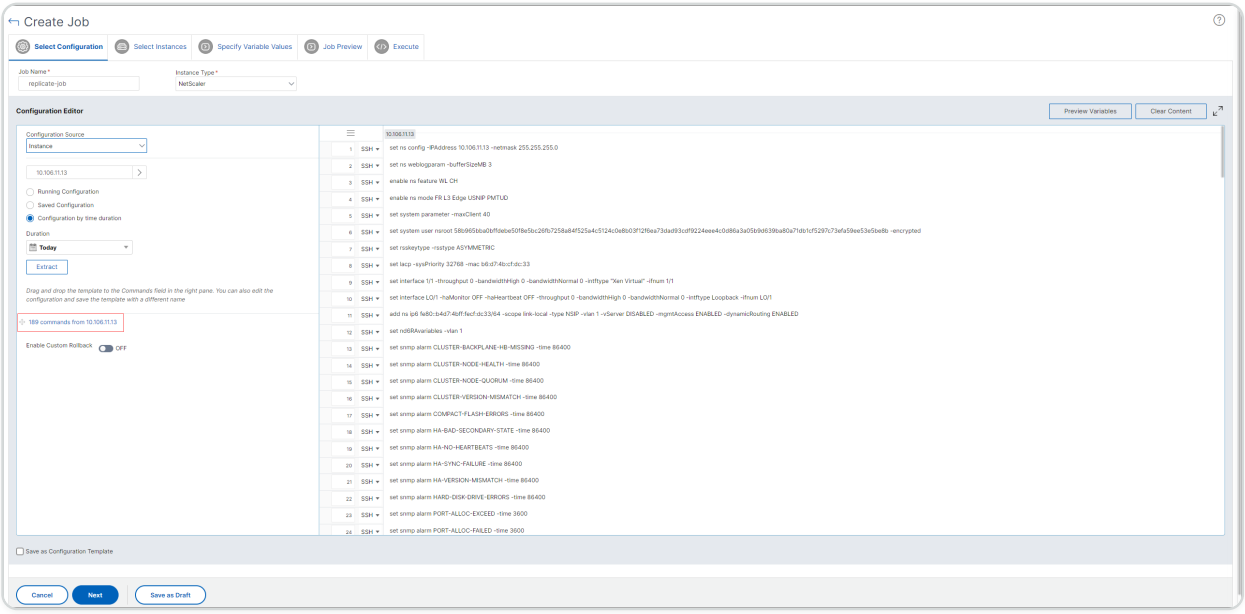
要从一个实例检索并将配置复制到其他 NetScaler 实例：

1. 导航到 **基础架构 > 配置作业**，然后单击 **创建作业**。
2. 指定作业名称和实例类型。
3. 选择 **Instance** 作为 **Configuration Source**，然后选择要复制其配置的源实例。选择要提取的配置类型。如果选择“按时间段配置”，请设置运行此配置的时间段，然后单击 **Extract**。

   在屏幕上显示您选择的时间段内在该实例上运行的命令数量，如以下图像中突出显示。



4. 将命令拖到右侧窗格中的 **Commands** 字段。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

仅保留与 FEO 相关的命令，并手动删除与负载平衡或任何其他配置相关的命令，然后单击 **Next**。

5. 单击 **Add Instances** 并添加要应用 FEO 配置的实例。单击 **OK**，然后单击 **Next**。
6. 如果您在命令中指定了变量，请在“指定变量值”选项卡上单击 **Download Input Key File**。在下载的文件中，为变量指定值，然后将文件上传到 NetScaler Console。
7. 在 **Job Preview** 选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。
8. 在“**执行**”选项卡上，单击“**完成**”以在选定的 NetScaler 实例上运行作业。

在配置作业中使用变量

配置作业是您可以在一个或多个托管实例上运行的一组配置命令。当您在多个实例上运行相同的配置时，您可能希望为配置中使用的参数使用不同的值。您可以定义变量，以便为这些参数分配不同的值或在多个实例上运行作业。

例如，考虑一个基本的负载平衡配置，您可以在其中添加一个负载平衡虚拟服务器，添加两个服务，并将服务绑定到虚拟服务器。现在，您可能希望在两个实例上使用相同的配置，但虚拟服务器和服务名称以及 IP 地址的值不同。您可以使用配置作业功能，通过使用变量定义虚拟服务器和服务的名称和 IP 地址来实现此目的。

在此示例中，使用了以下命令和变量：

`add lb vserver <servername> HTTP <ipaddress> <portnumber>`

`add service <servicename1> <ipaddress1> HTTP 80`

`add service <servicename2> <ipaddress2> HTTP 80`

`bind lb vserver <servername> <servicename1>`

`bind lb vserver <servername> <servicename2>`

在 NetScaler Console 中通过定义变量创建配置作业：

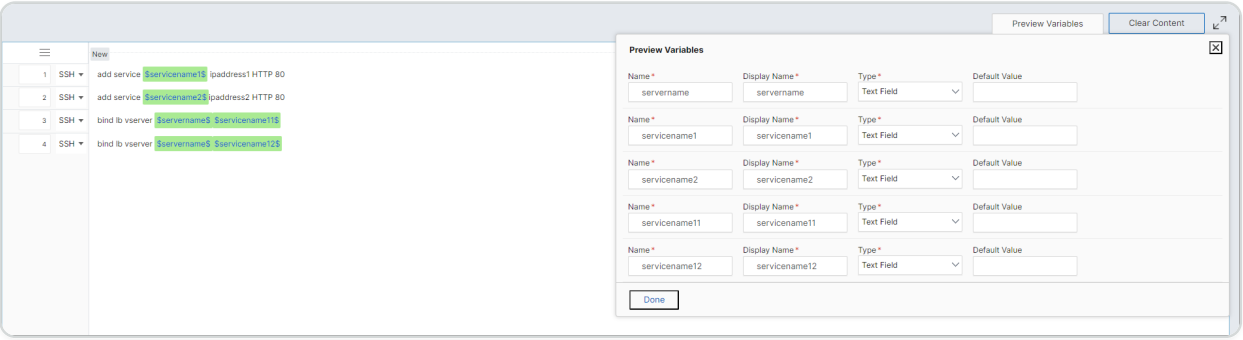
1. 导航到 **基础架构 > 配置作业**。
2. 单击 **创建作业**。
3. 在 **创建作业** 页面上，选择自定义作业参数，例如作业名称、实例类型和配置类型。
4. 在配置编辑器中，输入命令以添加负载平衡虚拟服务器、两个服务，并将服务绑定到虚拟服务器。双击选择要转换为变量的值，然后单击 **转换为变量**。例如，选择负载平衡服务器 `*ipaddress*` 的 IP 地址，然后单击 **转换为变量**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 当您看到美元符号包围变量的值时，单击该变量以进一步指定变量的详细信息，例如名称、显示名称和类型。如果您想进一步为变量指定默认值，还可以单击 **高级** 选项。单击 **保存**，然后单击 **下一步**。

   输入其余命令并定义所有变量。

6. 您可以在单个合并视图中查看在创建或编辑配置作业时定义的所有变量。
7. 执行以下操作之一，以在单个合并视图中查看所有变量：
   - 创建配置作业时，导航到 **Infrastructure > Configuration Jobs**，选择 **Create Job**。在 **Create Job** 页面上，您可以查看在创建配置作业时添加的所有变量。
   - 编辑配置作业时，导航到 **Network \> Configuration Jobs**，选择作业名称并单击 **Edit**。在 **Configure Job** 页面上，您可以查看在创建配置作业时添加的所有变量。
8. 然后，您可以单击 **Preview Variables** 选项卡，在单个合并视图中预览在创建或编辑配置作业时定义的变量。
9. 将出现一个新弹出窗口，以表格形式显示变量的所有参数，例如名称、显示名称、类型和默认值。您还可以编辑和修改这些参数。编辑或修改任何参数后，单击 **Done** 按钮。



10. 然后，您可以根据需要重新排列和重新排序配置编辑器中的命令。您可以通过拖放命令行将命令从一行移动到另一行。您还可以通过简单地更改文本框中的命令行号，将命令行从一行移动或重新排列到任何目标行。
11. 选择要运行配置作业的实例。
12. 在 **Specify Variable Values** 选项卡中，选择 **Upload input file for variable values** 选项，然后单击 **Download Input Key File**。在我们的示例中，您需要指定每个实例上的服务器名称、服务器和服务的 IP 地址、端口号以及服务名称。保存文件并上传。如果您的值未准确定义，系统可能会抛出错误。
13. 输入密钥文件将下载到您的本地系统，您可以通过为之前选择的每个 NetScaler 实例指定变量值来编辑它，然后单击 **Upload** 将输入密钥文件上传到 NetScaler Console。单击 **Next**。输入密钥文件将下载到您的本地系统，您可以通过为之前选择的每个 NetScaler 实例指定变量值来编辑它。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

在输入密钥文件中，变量在三个级别定义：

- 全局级别
- 实例组级别
- 实例级别

全局变量是应用于所有实例的变量值。实例组级别的变量值应用于组中定义的所有实例。实例级别的变量值仅应用于特定实例。

NetScaler Console 优先考虑实例级别的值。如果未向单个实例的变量提供任何值，NetScaler Console 将使用在组级别提供的值。如果未在组级别提供任何值，NetScaler Console 将使用在全局级别提供的变量值。如果您在所有三个级别为变量提供输入，NetScaler Console 将使用实例级别的值作为默认值。

14. 单击 **上传** 将输入密钥文件上传到 NetScaler Console。单击 **下一步**。

重要

当您从 Mac 上传 CSV 文件时，Mac 会将 CSV 文件存储为以分号而不是逗号分隔。这将导致您上传输入文件并运行作业时配置失败。如果您使用的是 Mac，请使用文本编辑器进行必要的更改，然后上传文件。

15. 您还可以为所有实例提供通用变量值，然后单击 **上传** 将输入密钥文件上传到 NetScaler Console。

    包含变量值的关键输入文件会（以相同的文件名）保留在配置作业中。您可以在创建或编辑配置作业时查看和编辑您之前使用和上传的这些输入文件。

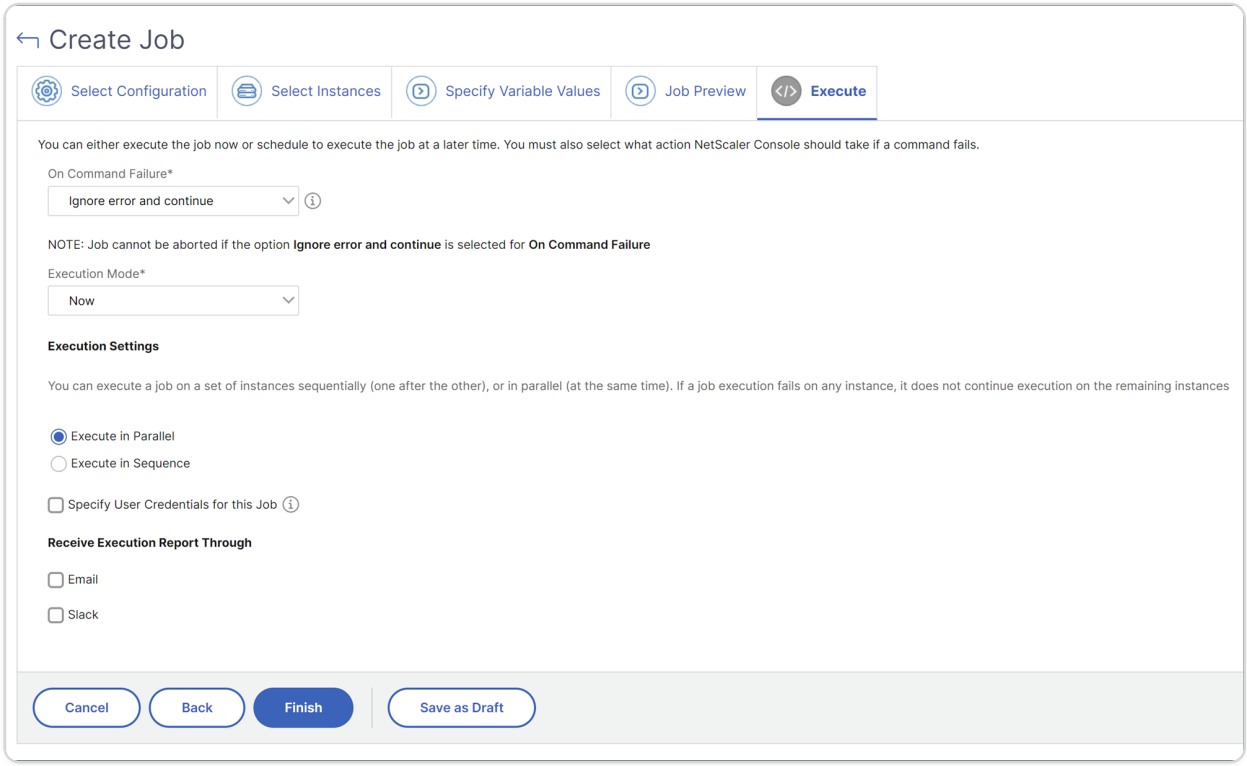
    要在创建配置作业时查看运行配置作业，请导航到 **网络 \> 配置作业**，然后单击 **创建作业**。在 **创建作业** 页面中。在 **指定变量值** 选项卡上，选择 **所有实例的通用变量值** 选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑并上传文件（保持相同的文件名）。

    要在编辑配置作业时查看已运行的配置作业，请导航到 **网络 \> 配置作业**，选择作业名称，然后单击 **编辑**。在 **配置作业** 页面中，在 **指定变量值** 选项卡上，选择 **所有实例的通用变量值** 选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑并上传文件（保持相同的文件名）。

16. 在 **作业预览** 选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

17. 在 **执行** 选项卡中，您可以选择立即运行作业或将其安排在以后运行。您还可以选择如果命令失败 NetScaler Console 必须采取的操作，以及是否希望发送有关作业成功或失败的电子邮件通知以及其他详细信息。



配置并运行作业后，您可以通过导航到 **基础架构 > 配置作业** 并选择您刚刚配置的作业来查看作业详细信息。单击 **详细信息**，然后单击 **变量详细信息** 以查看添加到作业中的变量列表。

注意

您在 **步骤 5** 中为变量提供的值，在您保存作业并退出时，或者在您安排作业在稍后时间运行时，将由 NetScaler Console 保留。

从纠正命令创建配置作业

您可以使用 NetScaler Console 中的审计模板功能来监控托管 NetScaler 实例的配置更改并排除配置错误。

使用审计模板审计配置更改的典型工作流程包括以下步骤

1. 创建审计模板，其中包含一组用于审计实例配置的有效/预期 NetScaler 命令。
2. 选择要运行审计模板的 NetScaler 实例，以检查运行配置与预期配置之间的任何差异。
3. 了解差异/纠正命令，并利用“创建作业”功能使实例配置达到所需状态

© 1997–2026 Citrix Systems, Inc. All rights reserved.

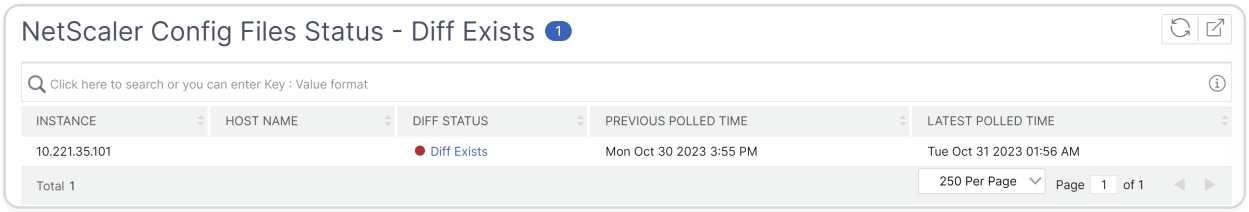
考虑一个场景，多个管理员正在管理五个 NetScaler 实例。所有这些管理员都会在需要更改时更新现有实例配置。超级管理员希望确保某些重要的配置保持不变，无论其他管理员进行何种更改。对于此用例，超级管理员会创建预期存在于 NetScaler 实例上的配置模板，并针对这些实例运行它。NetScaler Console 会将审计模板配置与运行配置进行比较，并在 **Configuration Audit** 仪表板上报告任何不匹配项。

如果您发现某些实例的配置发生更改，您可以使用 NetScaler Console 纠正命令功能，为特定的 NetScaler 实例创建包含已修改和已纠正配置命令的配置作业。

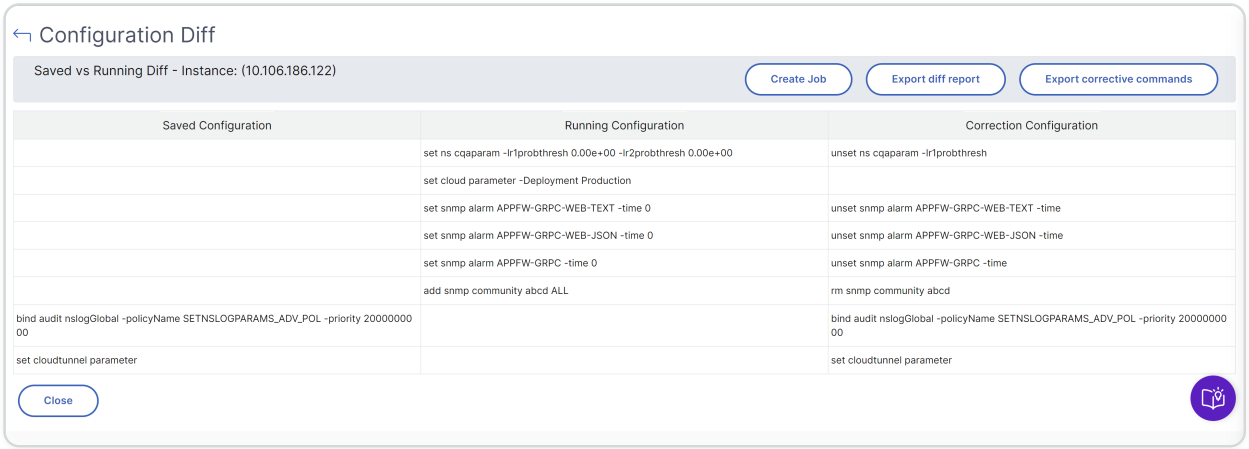
如果审计模板配置与运行配置之间存在任何差异，**Audit Report** 页面上将显示 **Diff Exists** 状态消息。单击 **Diff Exists** 链接将带您进入 **Configuration Diff** 页面，您可以在其中查看纠正命令。您还可以使用这些纠正命令创建配置作业，并在特定的 NetScaler 实例上运行该作业，以使它们恢复到所需的配置。

在 NetScaler Console 上从纠正命令创建配置作业

1. 导航到 **基础架构 > 配置审计**。
2. 在 **Configuration Audit** 页面上，单击任意两个环形图中的一个以访问 **Audit Reports** 页面。
3. 对于要纠正配置命令的实例，单击 **Diff Exists** 链接（在表格的 **Saved vs Running Diff** 列下）。将显示 **Configuration Diff** 页面，其中列出了该实例的保存配置、运行配置和纠正配置之间的差异。



4. 单击 **Create Job** 以转到 **Create Job** 页面，其中已预填充纠正命令。有关如何创建配置作业的说明，请参阅 如何在 NetScaler Console 上创建配置作业。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

将运行中和已保存的配置从一个 NetScaler 实例复制到另一个实例

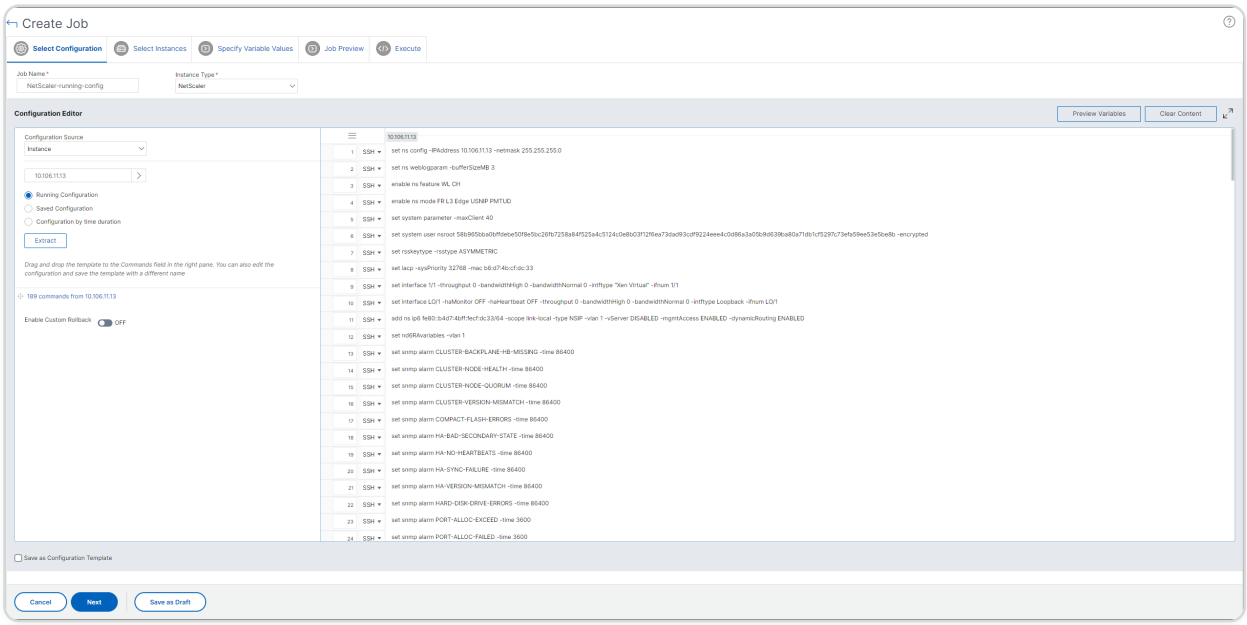
May 24, 2018

您现在可以将 NetScaler 实例的配置复制到其他实例。在 NetScaler Console 中配置作业时，请选择一个实例作为“配置源”，然后选择所选实例的运行中或已保存配置。

例如，当您选择“**运行配置**”并单击“**提取**”时，NetScaler Console 会向所选的 NetScaler 实例发送请求以查找运行配置，并将其显示为模板。您可以将模板拖到右侧窗格中的“**命令**”字段中。您可以修改命令、参数和实例。

要在 NetScaler Console 上将一个实例的运行中和已保存配置命令复制到另一个实例，请执行以下操作：

1. 导航到“**基础架构 > 配置作业**”，然后单击“**创建作业**”。
2. 指定作业名称和实例类型。例如，将 *NetScaler Running Config1* 指定为作业名称，将实例类型指定为 *NetScaler*。
3. 选择“**实例**”作为“**配置源**”，然后选择要将其配置复制到其他实例的源实例。
4. 您将看到以下三个选项：
   - 运行配置
   - 已保存配置
   - 按时间段配置
5. 选择“**运行配置**”，然后单击“**提取**”。将显示在该实例上运行的运行配置命令的数量。



6. 将命令拖到右侧窗格中的“**命令**”字段中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. 您可以在“命令”字段中编辑命令。例如，如果提取的命令用于设置 NetScaler 实例。这可能包括添加分区、设置负载平衡、将负载平衡服务器绑定到服务等。您可能希望编辑命令，以设置不带分区的新 NetScaler 实例。因此，要删除分区，请手动删除与创建分区相关的命令，然后单击“**下一步**”。
8. 单击“**添加实例**”并添加要应用运行配置命令的实例。单击“**确定**”，然后单击“**下一步**”。
9. 如果您在命令中指定了变量，请在“**指定变量值**”选项卡上，单击“**下载输入密钥文件**”。在下载的文件中，为变量指定值，然后将文件上传到 NetScaler Console。
10. 在“**作业预览**”选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。

11\. 在“**执行**”选项卡中，您可以选择立即运行作业或安排稍后运行。您还可以选择 NetScaler Console 在命令失败时必须采取的操作，以及是否希望发送有关作业成功或失败的电子邮件通知以及其他详细信息。

重用已运行的配置作业

配置作业允许您创建一组配置命令，您可以在一个或多个托管实例上运行这些命令。您还可以在修改命令、参数、配置源和作业中的实例后，运行同一组已保存的配置作业。当必须在不同实例上运行同一组命令时，或者当作业遇到错误并停止进一步执行时，这非常有用。

NetScaler Console 提供了一项功能，可以再次运行已完成的作业。通过此功能，已完全运行的作业可以在不更改作业名称的情况下再次运行。

注意

只有当执行模式为“立即”时运行的作业才能重新执行。

编辑已完成的作业：

1. 在 NetScaler Console 主页上，导航到 **基础架构 > 配置作业**。
2. 在**作业**页面中，选择一个执行摘要显示为“已完成”的作业，然后单击**编辑**。您还可以编辑计划的配置作业。
3. 在**配置作业**页面中，您可以看到作业名称和实例类型不可编辑。您可以修改其他字段，例如配置源、添加实例、编辑变量值和设置执行设置。
4. 单击**完成**以再次运行配置作业。

注意

您还可以选择作业并再次单击**执行**，以在不修改任何源、实例和命令的情况下运行作业。当您必须在同一实例上运行同一组命令时，这非常有用。有时，作业可能会遇到来自服务器端的瞬时错误，您可能需要再次运行作业。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

运行作业(/en-us/netscaler-application-delivery-management-software/media/executecompletedjob.png)

在配置作业中使用 SCP (put) 命令

您可以使用 NetScaler Console 的配置作业功能来创建配置作业、发送电子邮件通知以及检查所创建作业的执行日志。作业是一组配置命令，您可以在单个托管实例或多个托管实例上创建和运行。例如，您可以使用配置作业进行设备升级。

NetScaler Console 中的配置作业使用安全外壳 (SSH) 命令来配置实例，您可以配置一个配置作业以使用安全复制 (SCP) 安全地传输文件。SCP 基于 SSH 协议。您可以包含在配置作业中的 **SCP** 命令之一是“put”命令。您可以在配置作业中使用“put”命令将存储在系统本地目录中的一个或多个文件上传或传输到 NetScaler Console，然后再传输到 NetScaler 实例上的目录。

注意：

文件将上传到 NetScaler Console，然后复制（put）到选定的 NetScaler 实例。上传的文件存储在 NetScaler Console 中，并且仅在作业删除时才删除。这对于计划稍后运行的作业是必需的。

该命令具有以下语法：

```
put <local_filename> <remote_path/remote_filename>
```

其中，

\<local_filename\> 是要上传的本地文件的名称。

\<remote_path / remote_filename\> 是远程目录的路径，以及文件复制到该目录时要分配的名称。

注意：

如果远程目录包含与本地文件同名的文件，则 put 命令将覆盖远程文件。

在创建配置作业时，您可以将本地和远程文件名参数转换为变量。这使您可以在每次运行作业时，为同一组 NetScaler 实例将不同的文件分配给这些参数。此外，如果您在作业中的多个位置使用文件，并且想要重命名该文件，则可以重新定义变量，而无需在所有位置更改文件名。

要在配置作业中使用 put 命令上传文件，请执行以下操作：

1. 导航到 **基础架构 > 配置作业**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 在**作业**页面上，单击**创建作业**。
3. 在**创建作业**页面上，在“作业名称”字段中输入作业名称，并在**配置编辑器**窗格中输入“put”命令。

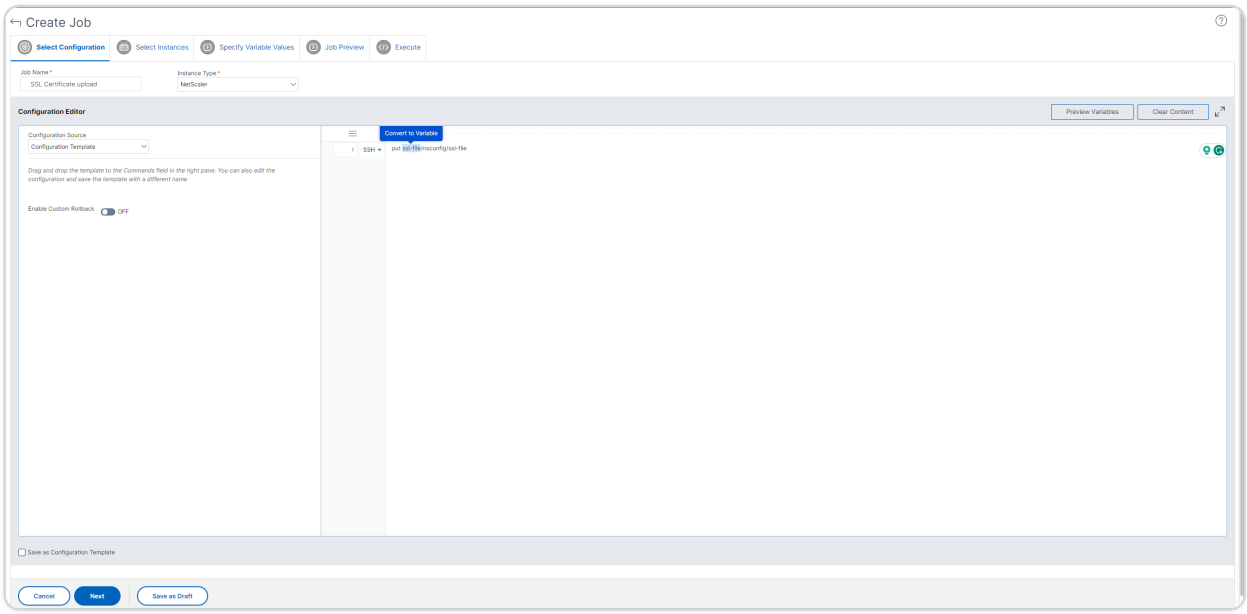
   例如，如果您想创建一个配置作业，将本地系统上保存的 SSL 证书文件复制到多个 NetScaler 实例，您可以添加一个使用变量而不是特定文件名的“put”命令，并将变量类型定义为“file”。

   `put scp-file /nsconfig/scp-file`

   在此示例中，

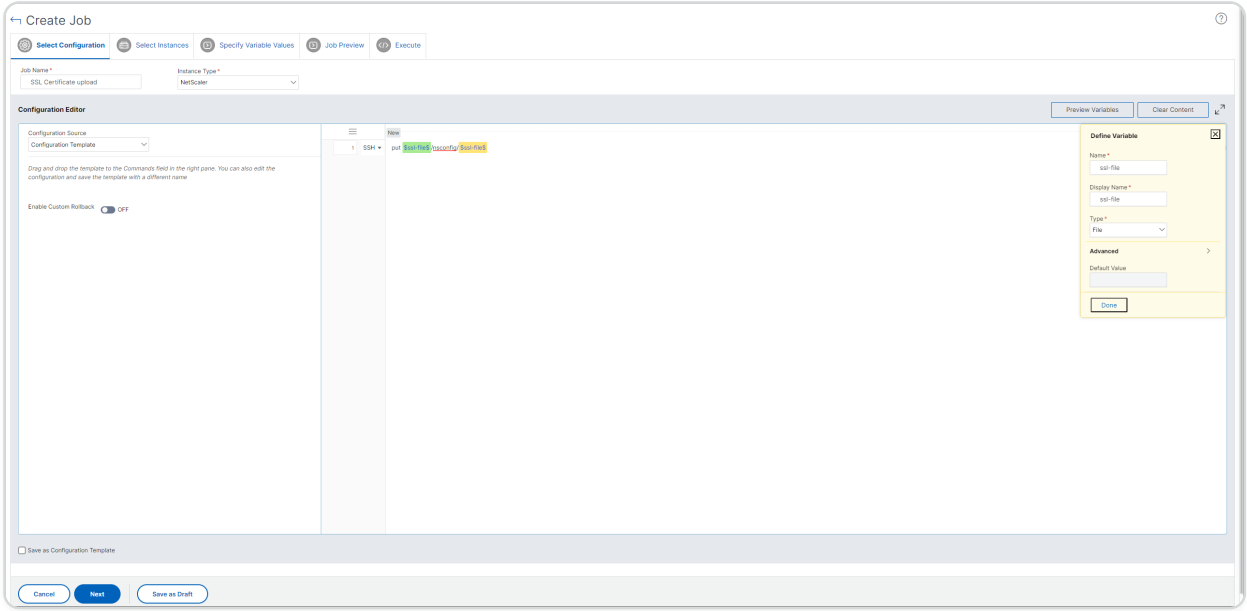
   - `scp-file` - 这是必须上传到 NetScaler 实例中的文件名称。
   - `/nsconfig/scp-file` - 这是实例上的目标文件夹，`scp-file` 将在任务执行后放置在此处。

4. 在您输入的命令中，选择要转换为变量的文件名，然后单击**转换为变量**，如下图所示。

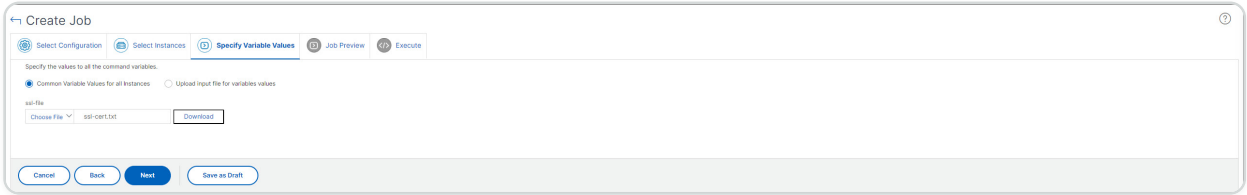


5. 验证文件名是否用美元符号括起来（表示它现在是一个变量），然后单击该变量。
6. 指定变量的详细信息，例如名称、显示名称和类型。
7. 从**类型**下拉列表中，选择**文件**。单击**保存**。将变量声明为“文件”类型允许您将文件上传到 NetScaler Console。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. 单击**下一步**并选择要复制文件的 NetScaler 实例。
9. 在**指定变量值**选项卡上，选择**所有实例的通用变量值**部分，从系统上的本地存储中选择文件，单击**上传**将文件上传到 NetScaler Console，然后单击**下一步**。



10. 在 **作业预览** 选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。
11. 在 **执行** 选项卡上，您可以立即运行作业或安排稍后运行。您还可以选择如果命令失败，NetScaler Console 必须采取什么操作。您还可以创建电子邮件通知，以接收有关作业成功或失败以及其他详细信息的通知。单击 **完成**。
12. 您可以通过导航到 **基础架构 > 配置作业**，并选择您配置的作业来查看作业详细信息。单击 **详细信息**，然后单击 **变量详细信息** 以列出添加到作业中的变量。

使用配置模板

配置模板使您能够保存和重用一组配置命令，以便在您的 NetScaler 实例中应用一致的配置。以下主题可帮助您创建和管理配置模板：

- 使用主配置模板
- 调度使用内置模板创建的作业
- 调度作业以配置从 NetScaler 到 Prometheus 的指标导出
- 使用配置模板创建审计模板
- 重新调度使用内置模板配置的作业

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在配置作业中重用配置审计模板
- 导入和导出配置模板

使用主配置模板

使用主配置模板是在多个 NetScaler 实例上创建和部署主配置的灵活选项。

作为管理员，您可能希望在 NetScaler 实例上进行配置更改并保存许可证、证书和其他文件。您可以将新配置保存为主配置模板（.conf 文件）。

要从 NetScaler 实例保存主配置模板，您可以执行以下操作之一：

- 在命令提示符处，输入 **save ns config**。配置将保存在实例的 FLASH 内存中的 /nsconfig/ns.conf 文件中。
- 从实例的 GUI 中，导航到 **Diagnostics** \> **View Configuration**。选择您要保存的配置类型。例如，如果要保存实例的已保存配置，请选择 **Saved configuratio**n。单击 **Save text to a file** 链接将“ns.conf”文件保存到本地计算机。

在创建作业时，通过使用“DeployMasterConfiguration”配置模板部署主配置模板时，您可以通过添加更多命令、修改现有命令以及在输入文件中提供不同的变量值来为每个特定的 NetScaler 实例进一步自定义它。

例如，作为管理员，您可能希望除了 ns.conf 文件之外，还将证书密钥上传到 NetScaler 实例，并同时在这些实例上部署主配置。

重要

您不能在 NetScaler CPX 实例、群集配置的实例或分区 NetScaler 实例上使用 DeployMasterConfiguration 模板运行配置作业。

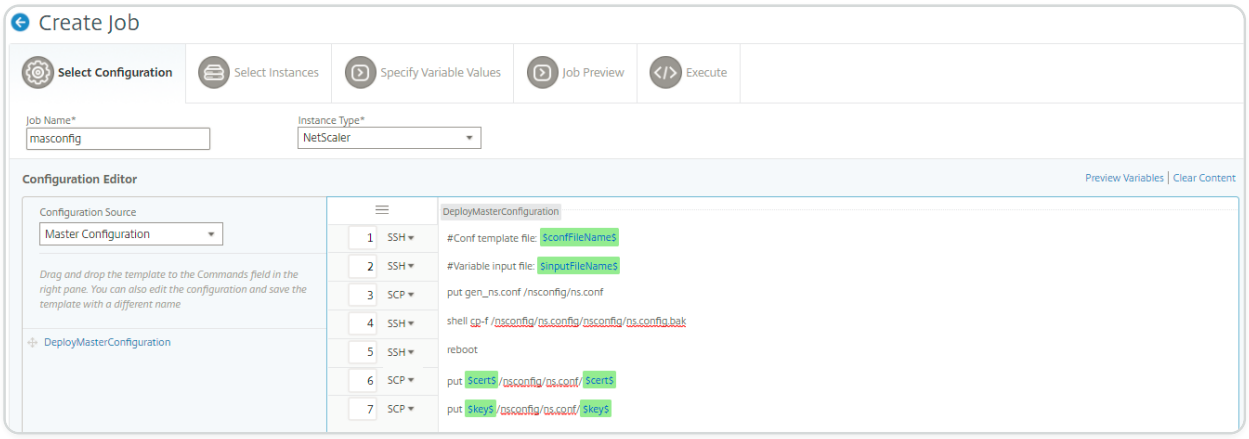
在 NetScaler Console 上使用主配置模板创建配置作业：

1. 在 NetScaler Console 中，导航到 **Infrastructure > Configuration Jobs**，然后单击 **Create Job**。
2. 在 **Create Job** 页面上，在 **Select Configuration** 选项卡中，指定 **Job Name** 并从下拉列表中选择 **Instance Type**。
3. 从 **Configuration Source** 下拉列表中选择 **Master Configuration**。将 DeployMasterConfiguration 模板的命令拖到右侧窗格。您也可以在右侧窗格中添加、修改或删除命令。单击 **Next**。

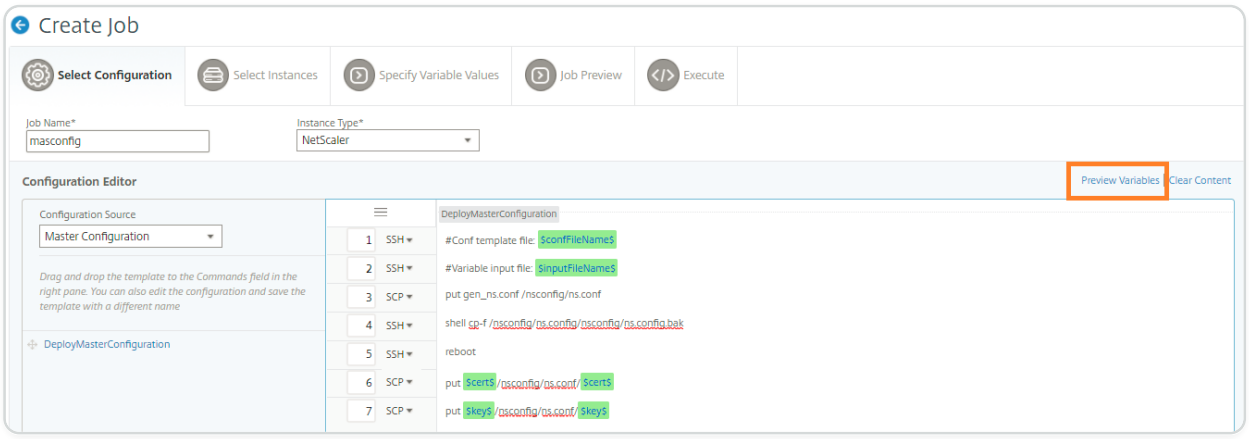
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

您可以添加 ***put*** 命令以将输入文件添加到模板。在我们的示例中，除了配置文件模板文件和变量输入文件之外，我们还必须上传证书和密钥文件。

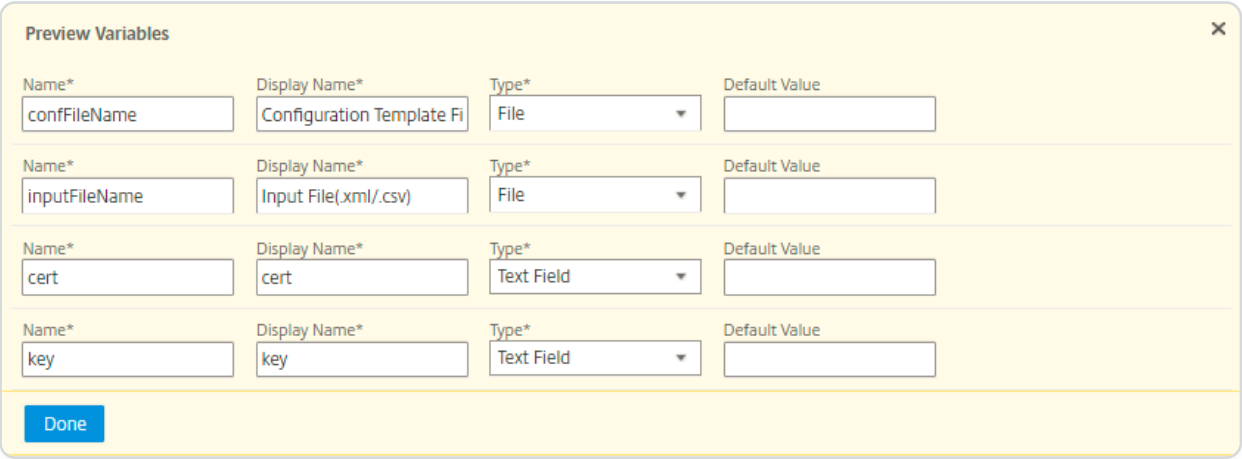


4. 您可以在一个合并视图中查看在创建或编辑配置作业时定义的所有变量。
5. 执行以下操作之一，以在单个合并视图中查看所有变量：
   - 创建配置作业时，导航到 **Infrastructure > Configuration Jobs**，选择 **Create Job**。在 **Create Job** 页面上，您可以查看在创建配置作业时添加的所有变量。
   - 编辑配置作业时，导航到 **Network \> Configuration Jobs**，选择作业名称，然后单击 **Edit** 。在 **Configure Job** 页面上，您可以查看在创建配置作业时添加的所有变量。
6. 然后，您可以单击 **Preview Variables** 选项卡，以在单个合并视图中预览在创建或编辑配置作业时定义的变量。



7. 将出现一个新弹出窗口，以表格形式显示变量的所有参数，例如名称、显示名称、类型和默认值。您还可以编辑和修改这些参数。编辑或修改任何参数后，单击 **Done** 按钮。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. 选择要运行配置作业的实例，然后单击 **Next**。
9. 在 **Specify Variable Values** 选项卡上，上传以下内容：

   - **Configuration Template File (.conf)** - 上传从 NetScaler 实例中提取的 .conf 文件。
   - **Upload the Input File (.xml/csv)** - 上传包含您在命令中定义的变量值的输入文件。

   此处提供了一个示例 xml 文件供您使用。确保 xml 文件包含与您正在使用的 NetScaler 实例相对应的详细信息。

```
<?xml version="1.0" encoding="UTF-8" ?>

<properties>

<!--

Provide inputs for all the parameters defined in the master config
file.

-  global. This tag contains all the common parameters and value.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

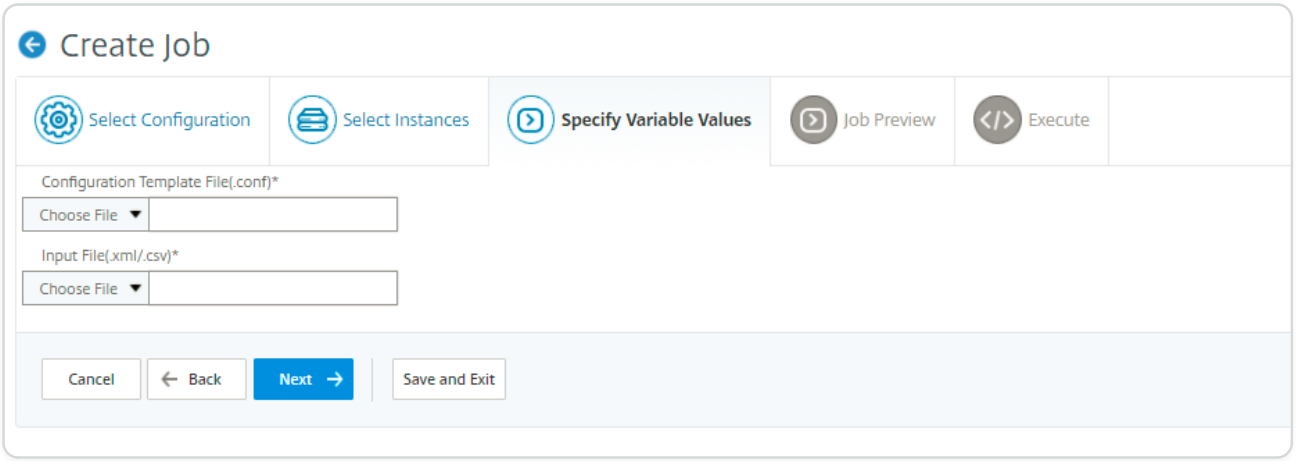
```
-  devicegroup. This tag contains all the instance group specific
parameters and values.



If the same parameters are defined in global and instance tags, the
instance specific parameters value will take precedence over the
instance group. The instance group specific parameters value will take
precedence over global parameters in the execution.



-  name. This attribute represents the name of the instance group.



-  device. This tag contains all the instance specific parameters and
value.



If the same parameters are defined in global and instance tags, the
instance specific parameters value will take precedence in the
execution.



-  name. This attribute represents the IP Address of the instance. Host
name is not supported for the attibute.



HA pair should be represented as <primaryip>-<secondaryip>. Example
10.102.2.1-10.102.2.2



In the template file, the parameter name must be specified within the
dollar sign,Example: $NSIP$, $CC_Trap_Dest$ and parameters names are
case sensitive.

-->
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<global>


</global>
<devicegroup name="BLR_DEVS">
</devicegroup>
<device name="10.106.101.209">
<param name="IP" value="10.106.101.209"/>
</device>


<!-- HA PAIR-->
<!--<device name="10.102.43.154-10.102.43.155">
<param name="NSIP" value="10.102.43.154"/>
<param name="HostName" value="NS43HA"/>
<param name="LBSERVER" value="haserver43http"/>
<param name="SNMPTrapDest" value="10.102.43.130"/>
</device>-->
</properties>
```

10. 点击**下一步**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



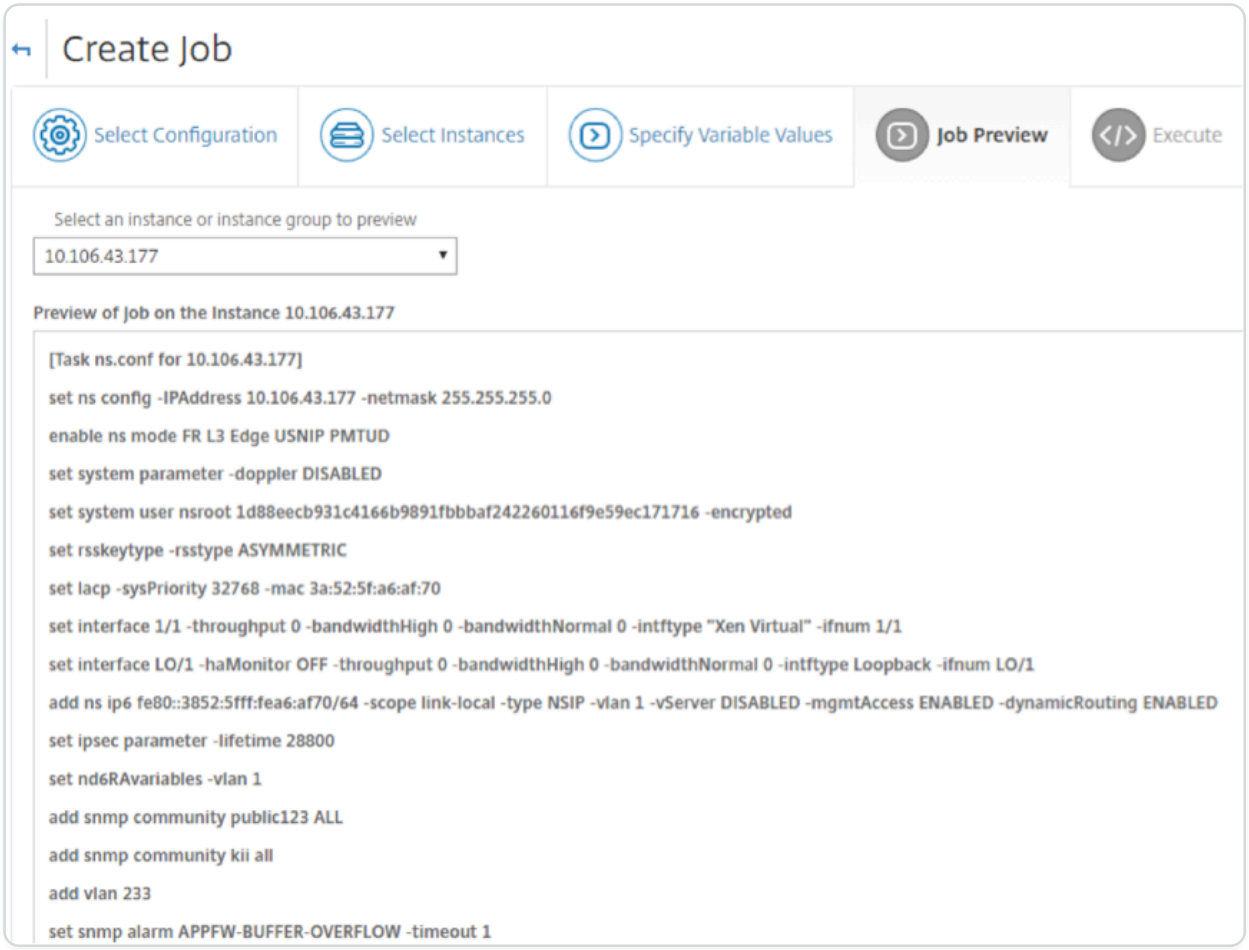
包含变量值的输入文件会（以相同的文件名）持久保存在配置作业中。您可以查看和编辑在创建或编辑配置作业时使用并上传的这些输入文件。

在创建配置作业时查看已运行的配置作业，导航到 **网络 \> 配置作业**，然后点击 **创建作业**。在 **创建作业** 页面中。在 **指定变量值** 选项卡上，选择 **所有实例的通用变量值** 选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑并上传文件（保持相同的文件名）。

在编辑配置作业时查看已运行的配置作业，导航到 **网络 \> 配置作业**，选择作业名称，然后点击 **编辑**。在 **配置作业** 页面中，在 **指定变量值** 选项卡上，选择 **所有实例的通用变量值** 选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑并上传文件（保持相同的文件名）。

1. 在 **作业预览** 选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令，然后点击 **下一步**。

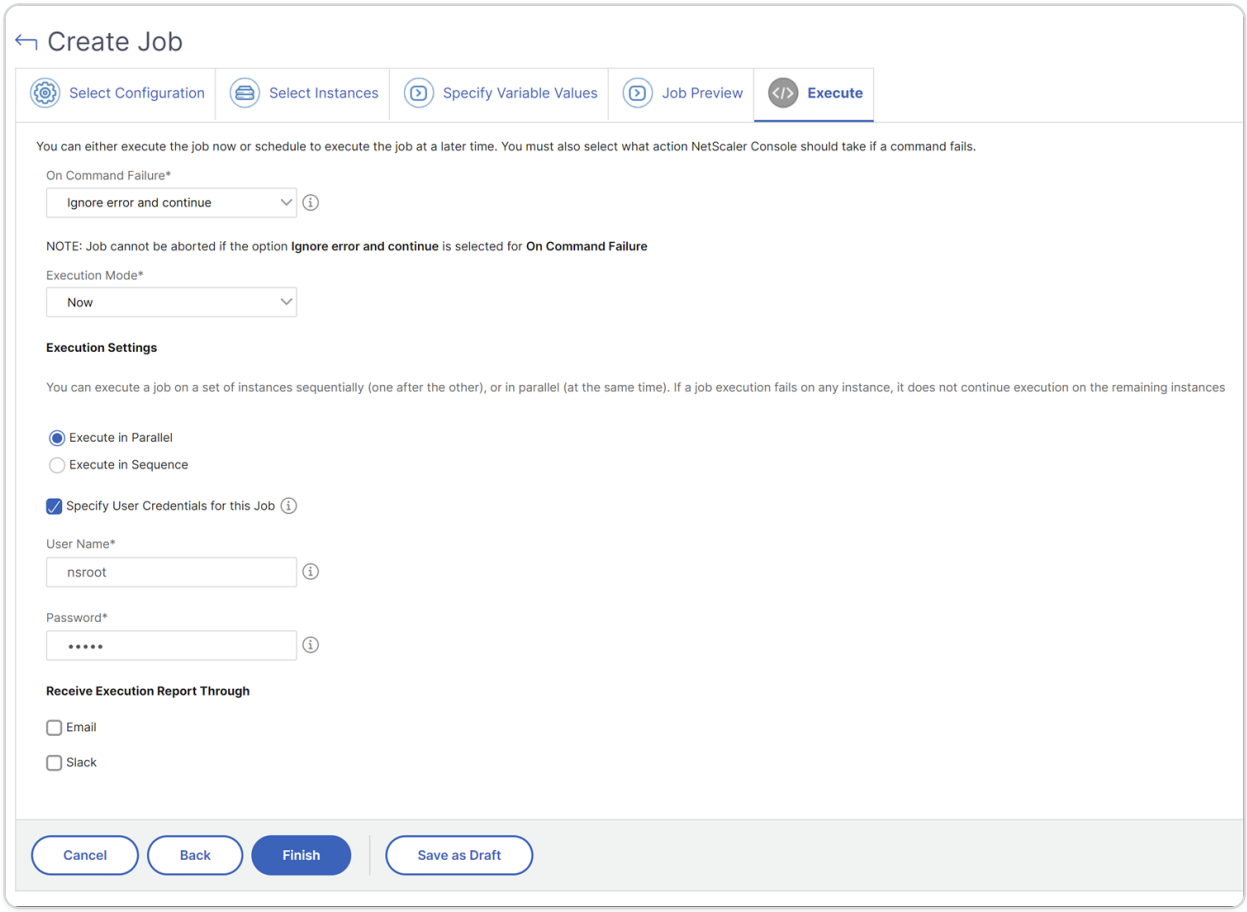
© 1997–2026 Citrix Systems, Inc. All rights reserved.



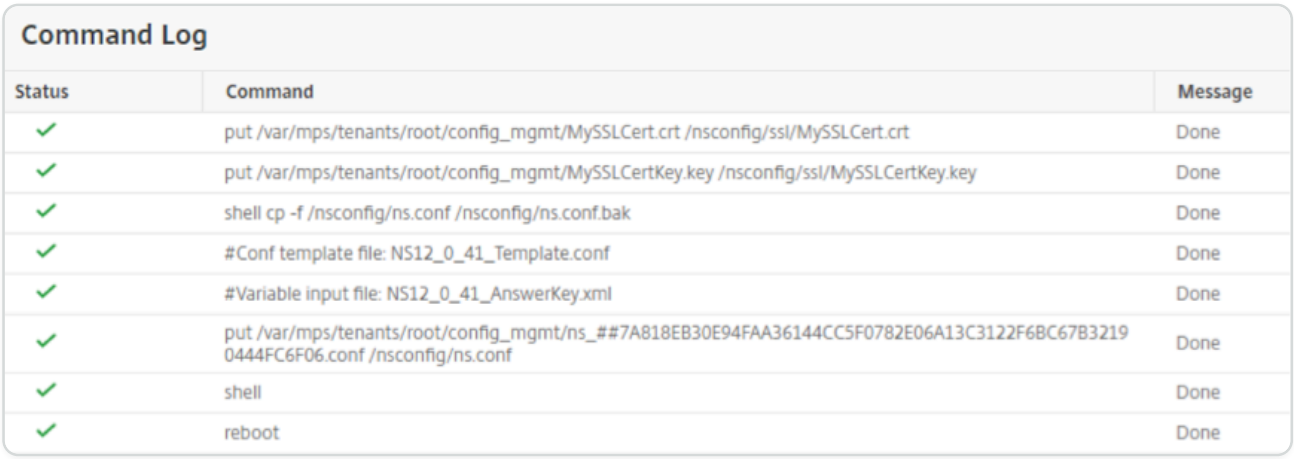
2. 在 **执行** 选项卡上，您可以选择立即运行作业或安排稍后运行。您还可以选择如果命令失败，NetScaler Console 必须采取什么操作。

   您还可以选择允许授权用户在您管理的实例上运行作业，并且可以选择是否发送有关作业成功或失败的电子邮件通知，以及其他详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



运行作业后，您可以通过导航到 **基础架构 > 配置作业** 并选择您配置的作业来查看作业详细信息。点击 **详细信息**，然后点击 **执行摘要** 以查看作业的详细信息。点击实例以查看 **命令日志**，从而查看作业上运行的命令。



Command Log

Status	Command	Message
✓	put /var/mps/tenants/root/config_mgmt/MySSLCert.crt /nsconfig/ssl/MySSLCert.crt	Done
✓	put /var/mps/tenants/root/config_mgmt/MySSLCertKey.key /nsconfig/ssl/MySSLCertKey.key	Done
✓	shell cp -f /nsconfig/ns.conf /nsconfig/ns.conf.bak	Done
✓	#Conf template file: NS12_0_41_Template.conf	Done
✓	#Variable input file: NS12_0_41_AnswerKey.xml	Done
✓	put /var/mps/tenants/root/config_mgmt/ns_##7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B3219 0444FC6F06.conf /nsconfig/ns.conf	Done
✓	shell	Done
✓	reboot	Done

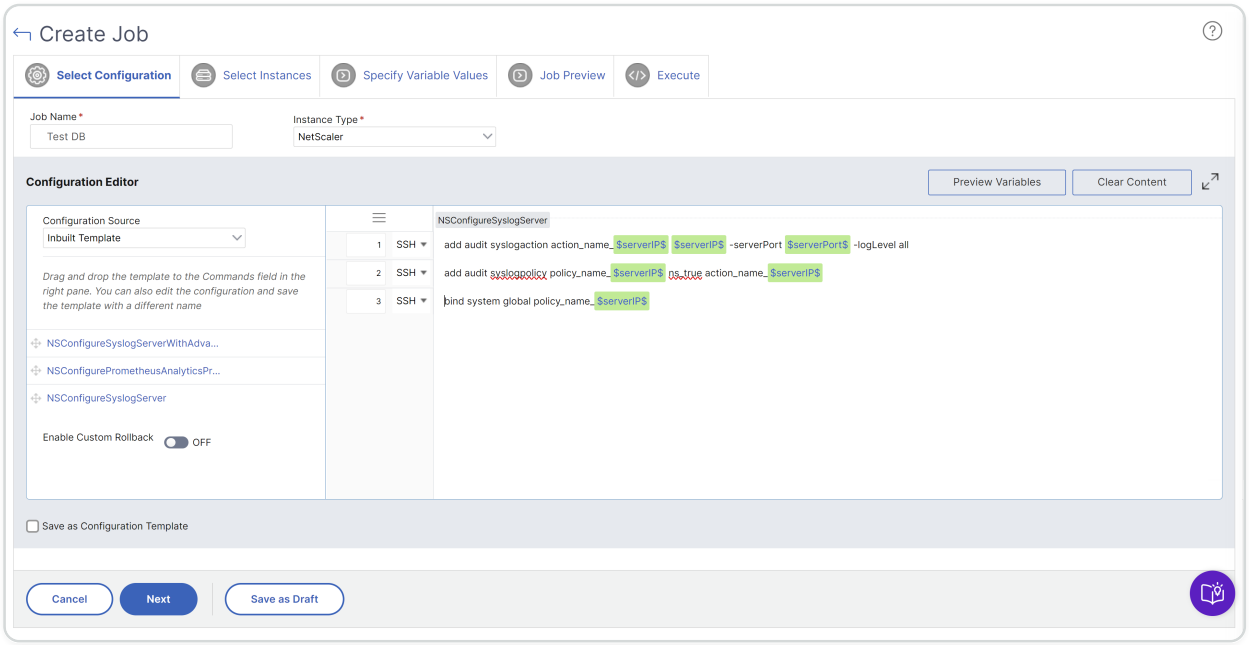
使用内置模板创建的计划作业

您可以使用内置模板选项计划作业。作业是一组配置命令，您可以在一个或多个托管实例上运行这些命令。例如，使用内置模板选项计划作业以配置 syslog 服务器。您还可以选择立即运行作业，或计划作业在稍后阶段运行。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 NetScaler Console 中使用内置模板计划作业

1. 在 NetScaler Console 中，导航到 **Infrastructure > Configuration Jobs**，然后单击 **Create Job**。
2. 在 **Create Job** 页面上，在 **Select Configuration** 选项卡中，指定 **Job Name** 并从下拉列表中选择 **Instance Type**。
3. 从 **Configuration Source** 下拉列表中选择 **Inbuilt Template**。将 ***NSConfigureSyslogServer** 命令拖动到右侧窗格，然后单击 **Next**。



4. 在 **Select Instances** 选项卡上，单击 **Add Instances**，选择要运行作业的实例，然后单击 **OK**。
5. 单击 **Next**。在 **Specify Variable Values** 选项卡上，选择以下选项之一来为实例指定变量：
   - **来自输入文件的变量值** - 下载输入文件以输入您在命令中定义的变量的值。然后，将文件上传到 NetScaler Console 服务器。
   - **所有实例的通用变量值** – 指定 syslog 服务器 IP 地址和端口。
6. 在 **Job Preview** 选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。
7. 单击 **Next**。
8. 在 **Execute** 选项卡上，设置以下条件：
   - **命令失败时** - 如果命令失败，您可以选择忽略错误并继续运行作业，或者停止作业的进一步执行。从下拉列表中选择要运行的操作。
   - **执行模式** - 您可以立即运行作业，也可以安排稍后运行作业。如果您想稍后安排作业，则必须为该作业指定执行频率设置。从下拉列表中选择您希望作业遵循的计划。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. 您还可以在**执行设置**下选择所需的方法，以顺序或并行方式在一组实例上运行作业。如果作业执行在任何实例上失败，则不会在其余实例上继续执行。

   您可以选择允许授权用户在您管理的实例上运行作业。还可以发送有关作业成功或失败的电子邮件通知，以及其他详细信息。

10. 单击**完成**。

安排一个作业，用于配置将指标从 NetScaler 导出到 Prometheus

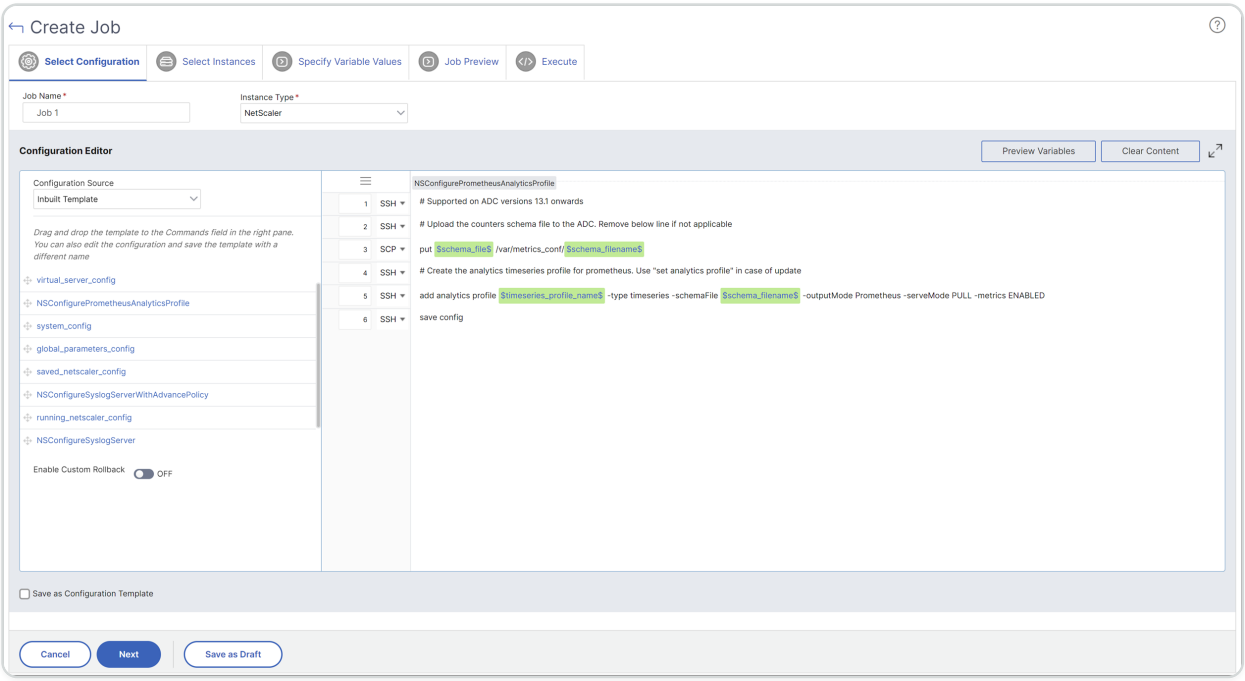
使用 `NSConfigurePrometheusAnalyticsProfile` 模板，您可以使用默认架构或带有修改参数的自定义架构，并将作业运行到所有托管实例。

先决条件

确保托管的 NetScaler 版本为 **13.1 build 39-27 或更高版本**。

安排作业：

1. 在 NetScaler Console 中，导航到 **基础架构 > 配置 > 配置作业**，然后单击 **创建作业**。
2. 在 **Create Job** 页面上，为作业指定一个名称，然后从 **Instance Type** 列表中选择 **NetScaler**。
3. 从 **Configuration Source** 列表中选择 **Inbuilt Template**。将 *NSConfigurePrometheusAnalyticsProfile* 命令拖动到右侧窗格，然后单击 **Next**。您也可以单击 **+** 添加模板。



4. 如果要使用默认架构：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 删除步骤 3 (`put $Schema_file /var/metrics.conf/$schema_filename$`)。将鼠标指针放在步骤 3 处，然后：

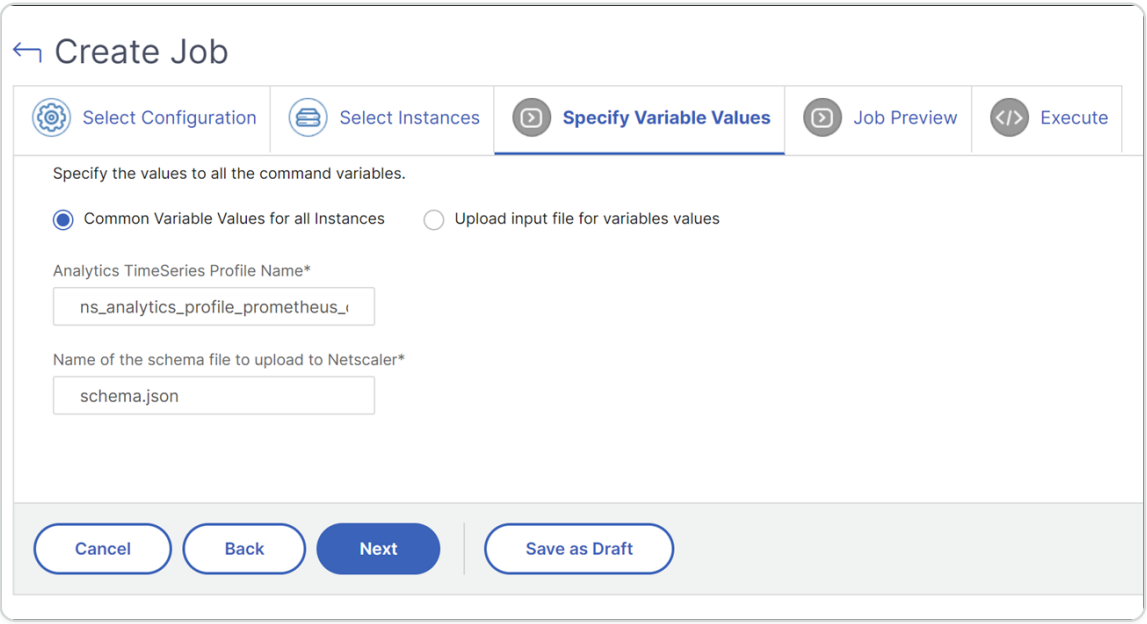
- 在 Windows 中，使用 Control + A 和 Delete。
- 在 Mac 中，使用 Command + A 和 Delete。

b. 删除后，单击 **Next**。

c. 在 **Select Instances** 选项卡上，单击 **Add Instances**，选择要运行作业的实例，然后单击 **Next**。

d. 在“**指定变量值**”选项卡上，选择“**所有实例的通用变量值**”。

- **分析时间序列配置文件名称** - 指定分析配置文件名称。有关更多信息，请参阅 `https://docs.netscaler.com/zh-cn/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html#configure-the-metrics-collector`。
- **要上传到 NetScaler 的架构文件名称** - 保留此文件名作为 `schema.json`，这是默认文件。



e. 从步骤 6 继续。

5. 如果要使用自定义架构计数器：

a. 从“**配置源**”列表中选择“**内置模板**”。将 `NSConfigurePrometheusAnalyticsProfile` 命令拖到右侧窗格，然后单击“**下一步**”。您也可以单击 + 添加模板。

b. 在“**选择实例**”选项卡上，单击“**添加实例**”，选择要运行作业的实例，然后单击“**下一步**”。

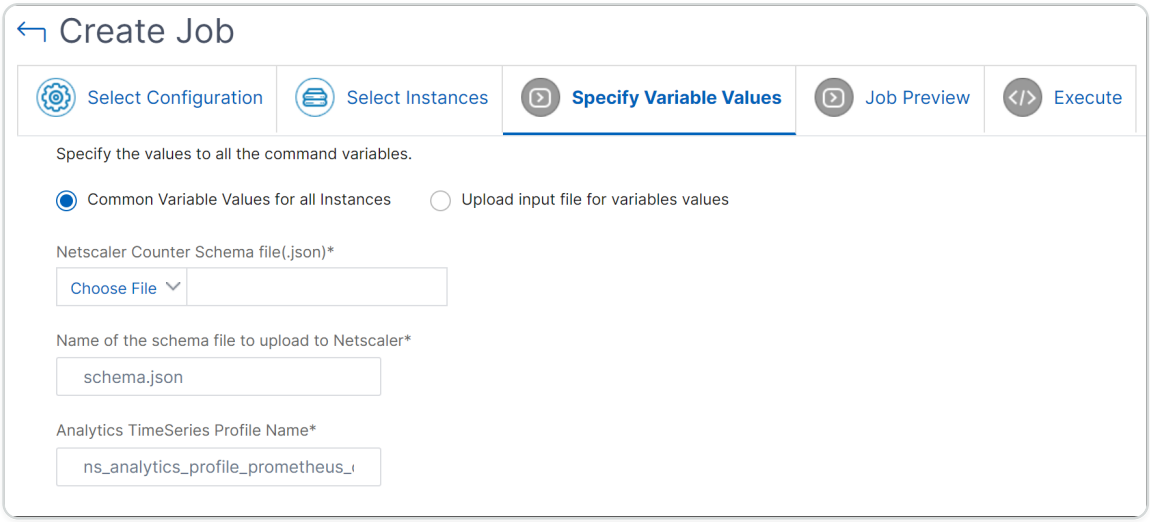
c. 在“**指定变量值**”选项卡上，选择“**所有实例的通用变量值**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **NetScaler 计数器架构文件(.json)** - 选择已使用参数修改的架构文件。在 NetScaler 中，包含所有受支持计数器的参考文件 `reference_schema.json` 位于路径 `/var/metrics_conf/` 下。

```
End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
 Done
> shell
root@ns# cd /var/metrics_conf/
root@ns# ls
reference_schema.json   schema.json
```

您可以使用 FTP 客户端将文件复制到本地，编辑所需的参数，保存，然后上传。



- **要上传到 NetScaler 的架构文件名称** - 指定要上传到 NetScaler 的架构文件名称。
- **分析时间序列配置文件名称** - 指定分析配置文件名称。有关更多信息，请参阅 `https://docs.netscaler.com/zh-cn/citrix-adc/current-release/ns-ag-appflow-intro-wrapper-con/ns-ag-appflow-config-tsk.html#configure-the-metrics-collector`。

6. 在“**作业预览**”选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。
7. 单击“**下一步**”。
8. 在“**执行**”选项卡上，设置以下条件：

   - **命令失败时** - 如果命令失败，您可以选择忽略错误并继续运行作业，或者停止作业的进一步执行。从下拉列表中选择要运行的操作。
   - **执行模式** - 您可以立即运行作业，也可以计划稍后运行作业。如果您想稍后计划作业，则必须指定该作业的执行频率设置。从下拉列表中选择作业要遵循的计划。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. 您还可以在“**执行设置**”下选择所需方法，以按顺序或并行方式在一组实例上运行作业。如果作业执行在任何实例上失败，则不会在其余实例上继续。

   您还可以选择允许授权用户在您管理的实例上运行作业，并且可以选择是否发送有关作业成功或失败的通知以及其他详细信息。

10. 单击“**完成**”。

    使用内置模板计划作业(/en-us/netscaler-application-delivery-management-software/media/dmc5.png)

使用配置模板创建审计模板

您现在可以使用以前保存为配置模板的配置命令来创建可应用于特定 NetScaler 实例的审计模板。在创建审计模板时，您可以将以前保存的配置模板拖到“命令”字段中，并编辑模板以满足您的要求。然后，您可以将审计模板应用于特定的 NetScaler 实例。NetScaler Console 会将这些实例与审计模板进行比较，并报告任何不匹配项。此过程可帮助您及时识别并纠正错误。

您可以在创建作业时创建配置模板，并将一组配置命令保存为模板。当您在“**创建作业**”页面上保存这些模板时，它们会自动显示在“**创建模板**”页面上。

例如，考虑一个基本的负载平衡配置，您可以在其中添加一个负载平衡虚拟服务器，添加两个服务，并将这些服务绑定到虚拟服务器。

此示例使用以下命令：

```
add lb vserver >servername> HTTP <ipaddress portnumber>
```

```
add service <servicename1 ipaddress1> HTTP 80
```

```
add service <servicename2 ipaddress2> HTTP 80
```

```
bind lb vserver <servername servicename1>
```

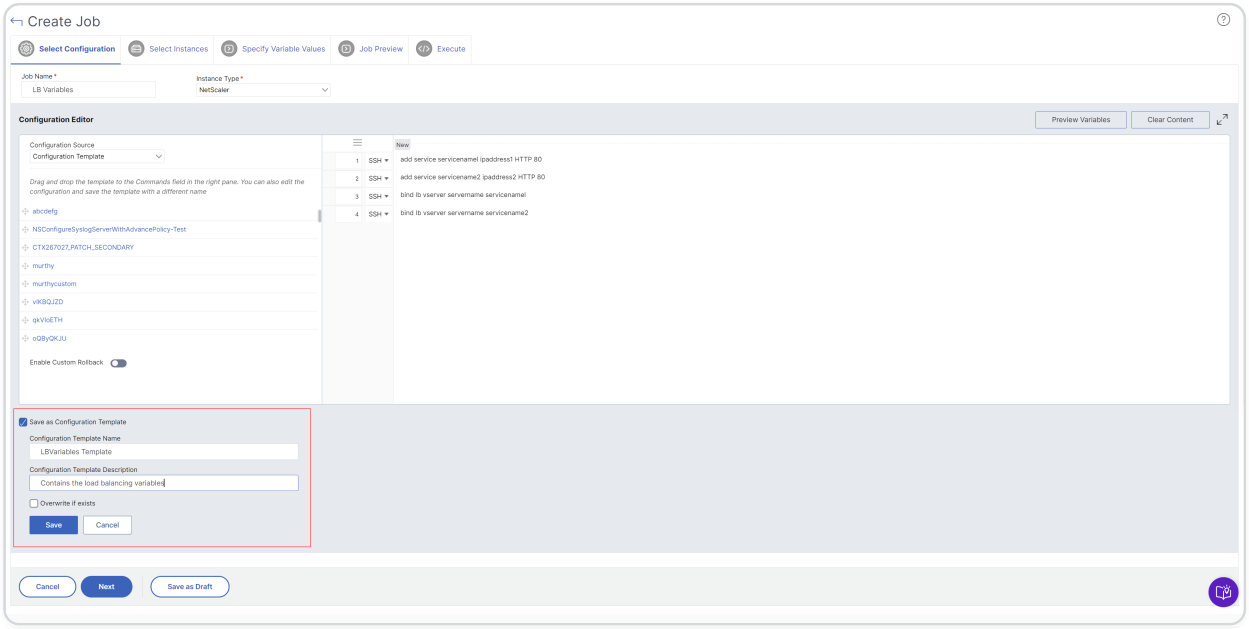
```
bind lb vserver <servername servicename2>
```

在 NetScaler Console 中保存配置模板：

1. 导航到“**基础架构 > 配置作业**”，然后单击“**创建作业**”。
2. 在“**创建作业**”页面上，指定作业名称和实例类型。
3. 选择“**配置模板**”作为配置源，并在“**命令**”字段中输入上述示例中的命令。
4. 选中“**另存为配置模板**”复选框，并为模板指定名称。您可以选择覆盖具有相同名称的其他现有模板。

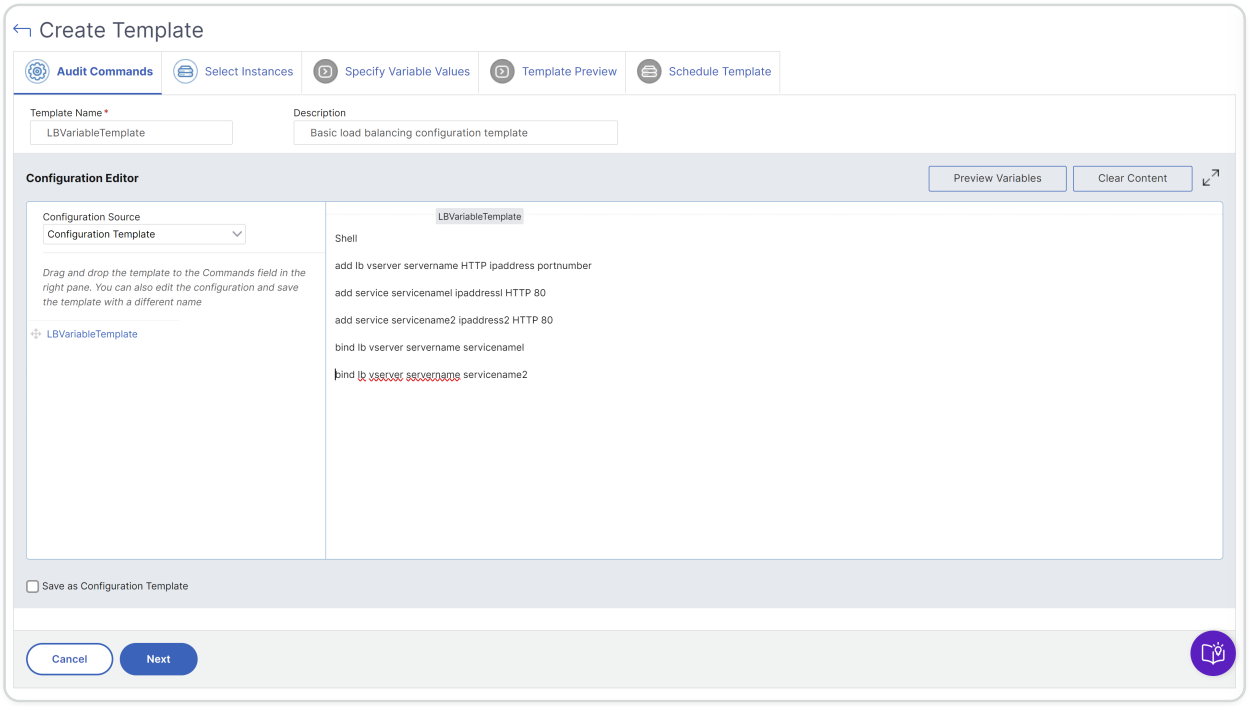
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 点击**保存**。



要在 NetScaler Console 中使用配置模板创建审计模板：

1. 导航到**基础架构 > 配置审计 > 审计模板**，然后点击**添加**。
2. 在**创建模板**页面上，指定模板名称，并输入描述。
3. 从**配置源**列表中，选择**配置模板**，然后将模板拖到右侧窗格中的“命令”字段中。您还可以编辑配置并以其他名称保存模板。点击**下一步**。
4. 在**选择实例**选项卡上，点击**添加实例**并添加要运行配置的实例。点击**确定**。
5. 点击**完成**。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

审计模板将显示在“审计模板”列表中，并每 12 小时针对指定实例的配置运行一次。

重新安排使用内置模板配置的作业

您可以重新安排在 NetScaler Console 中使用内置模板调度的作业。例如，您可以更改 NetScaler Console 在命令失败时必须采取的操作。如果您之前选择忽略错误并继续，则可以将其更改为在命令失败时回滚所有成功的命令。

重新安排在 NetScaler Console 中使用内置模板配置的作业

1. 在 NetScaler Console 中，导航到 **基础架构 > 配置作业**。
2. 选择要编辑的作业，添加或删除实例，指定变量值，然后更改执行操作和设置。
3. 单击 **Finish** 以重新安排作业。

注意

您还可以选择作业并单击 **Execute Again** 以运行作业，而无需修改任何源、实例和命令。当您必须在同一实例上运行同一组命令时，此功能非常有用。有时，作业可能会遇到来自服务器端的瞬时错误，您可能需要再次运行该作业。

在配置作业中重用配置审计模板

作为管理员，您现在可以在创建作业和运行配置审计时，将配置命令保存为一组可重用的配置模板。在配置作业中创建并保存的配置模板可在配置审计中使用，以创建可应用于特定 NetScaler 实例的审计模板。同样，在配置审计模块中创建的审计模板可在配置作业中使用，以便您可以将该模板作为配置作业运行。现在，对模板所做的任何更改在配置作业和配置审计模块中都可见。

以前，配置作业和配置审计模板必须针对相同的配置单独创建并保存为不同的文件。这导致在创建和维护模板方面重复工作。

NetScaler Console 允许您将此模板保存在系统中，以便审计模板也可在配置作业中使用。现在，审计模板可用于创建配置作业。这样，模板就可以在配置作业和配置审计之间互换使用。

例如，考虑一个基本的负载平衡配置，您可以在其中添加一个负载平衡虚拟服务器、添加两个服务并将这些服务绑定到虚拟服务器。

此示例使用以下命令：

```
add lb vserver servername HTTP ipaddress portnumber
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add service servicename1 ipaddress1 HTTP 80


add service servicename2 ipaddress2 HTTP 80


bind lb vserver servername servicename1


bind lb vserver servername servicename2
```

在配置审计中创建模板并在配置作业中重用

执行以下任务以在配置审计模块上创建模板并在配置作业模块中重用该模板。

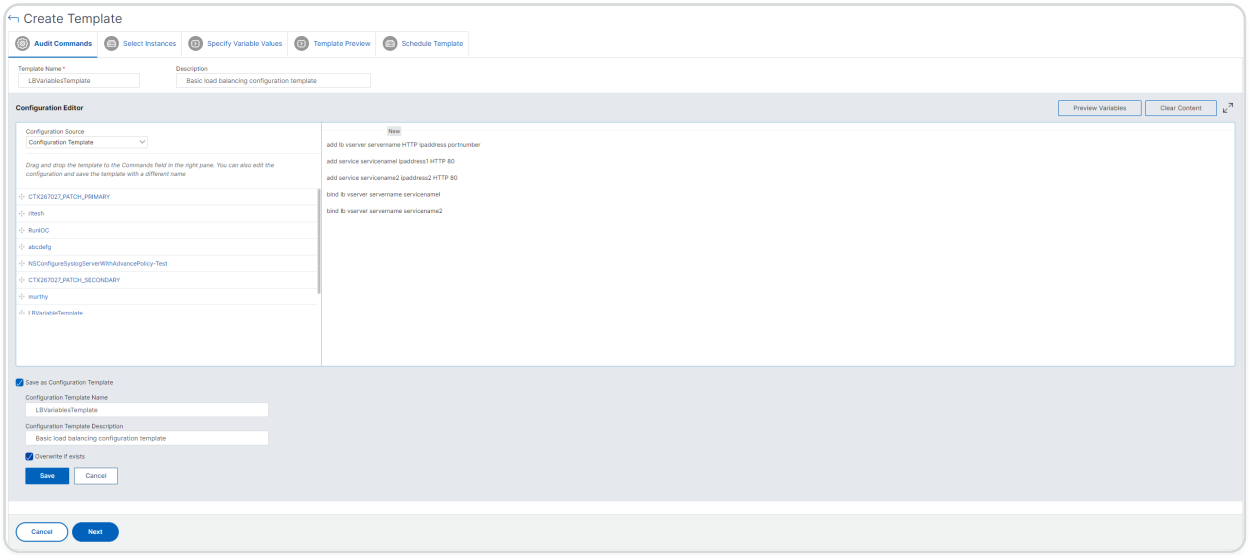
创建审计模板：

1. 在 NetScaler Console 中，导航到“**基础结构 > 配置审计 > 审计模板**”，然后单击“**添加**”。
2. 在“**创建模板**”页面上，指定模板名称。您还可以在“**描述**”字段中添加有关模板的更多信息。
3. 在“**命令**”窗格中，输入示例中的命令。
4. 选中“**另存为配置模板**”复选框并为模板指定名称，例如，您可以将此模板命名为“LBVariablesTemplate”。您可以选择覆盖具有相同名称的其他现有模板。

   注意
   审计模板名称可以与配置模板名称相同。

5. 单击“**保存**”，然后单击“**下一步**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 单击“**下一步**”。
7. 在“**选择实例**”选项卡中，选择要运行这些配置命令的 **NetScaler 实例**，然后单击“**完成**”。新模板现在在审核模板列表中可见。

8. 当您要运行这些配置命令时，导航到“**基础结构 > 配置作业**”，然后单击“**创建作业**”。您之前创建的审核模板将列为配置模板。

要在配置作业中重用审核模板，请执行以下操作：

1. 输入作业名称并选择实例类型，然后将模板拖到命令窗格中。

   创建配置作业时，您可以将本地和远程文件名参数转换为变量。这样，您就可以在每次运行作业时为同一组 NetScaler 实例将不同的文件分配给这些参数。

2. 在您输入的命令中，选择要转换为变量的文件名，然后单击“**转换为变量**”。
3. 在“**选择实例**”选项卡中，选择要运行这些命令的实例。
4. 如果您在命令中指定了任何变量，请在“**指定变量值**”选项卡中，选择以下选项之一来为您的实例指定变量：

   - 来自输入文件的变量值 - 下载输入文件以输入您在命令中定义的变量的值，然后将文件上传到 NetScaler Console 服务器。
   - 所有实例的通用变量值 – 指定 syslog 服务器 IP 地址和端口。

5. 在“**作业预览**”选项卡中，您可以评估和验证要在每个实例或实例组上运行的命令，然后单击“**下一步**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. 在“**执行**”选项卡中，单击“**完成**”以运行配置作业。现在，如果您想向此负载平衡服务器添加另一个服务并将该服务绑定到服务器，您可以在命令页面中编辑命令并保存它们。
7. 导航到**审计模板**，然后点击**添加**。
8. 将“LBVariablesTemplate”模板拖动到命令窗格。您可以看到该模板已使用新命令进行了更新。

审计模板出现在审计模板列表中，并每 12 小时针对指定实例的配置运行一次。您现在可以创建模板，并在配置作业和配置审计模块之间重用它们。

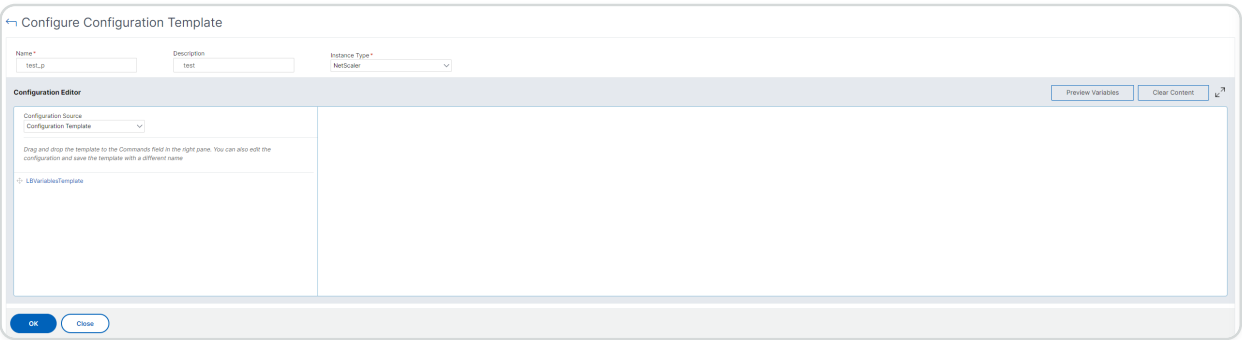
导入和导出配置模板

您可以从任何 NetScaler Console 导出配置模板。您也可以在将来的任何时候将文件导入到相同或另一个 NetScaler Console。配置模板数据（如配置命令、变量定义和参数）不会丢失。

您可以将配置模板导出为 **.json** 文件格式并将其保存在本地文件夹中。您可以将配置模板 **.json** 文件导入到 NetScaler Console。此文件可能是新文件，也可能是您从相同或另一个 NetScaler Console 导出的文件。

导出配置模板：

1. 导航到 **基础设施 > 配置作业 > 配置模板**。
2. 单击 **Add** 按钮以创建配置模板。
3. 在 **Create Configuration Template** 页面上，指定配置模板名称，然后选择实例类型。在 **Configuration Editor** 下，从下拉菜单中选择配置源为 Configuration Template。您可以将现有配置模板拖动到配置编辑器。单击 **Create**。



4. 导航到 **Infrastructure > Configuration Jobs > Configuration Templates** 以查看配置模板列表中的已创建模板。

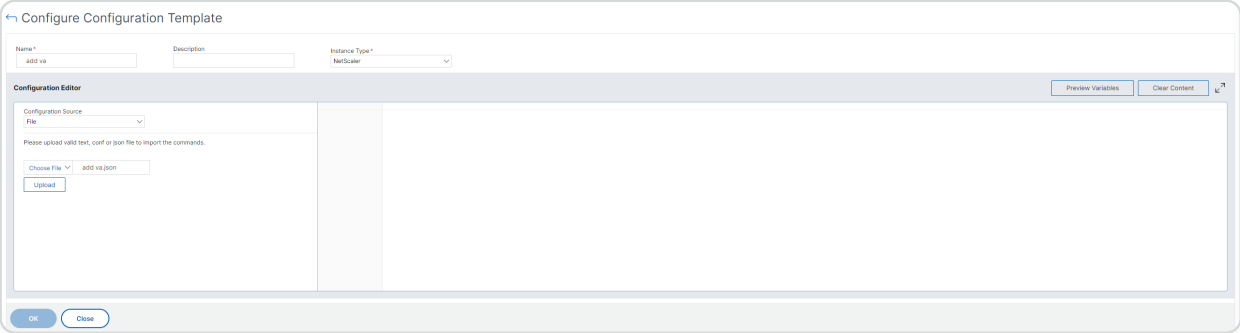
5. 选择新创建的配置模板，然后单击 **Export** 按钮。

相应的配置模板将以 **.json** 格式下载到您的本地系统。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

导入配置模板：

1. 导航到 **Infrastructure > Configuration Jobs > Configuration Templates**，然后单击 **Import** 按钮。选择包含配置模板 **.json** 文件的路径，然后上传 **.json** 文件。建议上传您已导出的 **.json** 文件。
2. 您还可以使用 Configuration Editor 上的 **File** 选项导入配置模板。
3. 在 **配置编辑器** 的下拉菜单中选择 **文件**。
4. 从本地系统选择 **选择文件**（**.json** 文件），并上传配置模板 **.json** 文件。



注意

- 每个新导入的模板都会存储一个新的 ID 字符串。
- 只有当文件以 **.json** 格式保存时，您才能导入配置模板。如果您从本地系统导入的配置模板不是 **.json** 文件，系统将显示错误并导致文件导入失败。

配置审计

本文档包含以下主题：

- 查看审计报告
- 审计跨实例的配置更改
- 获取网络配置建议
- 轮询 NetScaler 实例的配置审计
- 为 ConfigChange SNMP 陷阱生成配置审计差异

查看审计报告

(NetScaler Console) 允许您在配置审计部分查看和下载配置审计差异报告。配置审计部分允许您导出：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

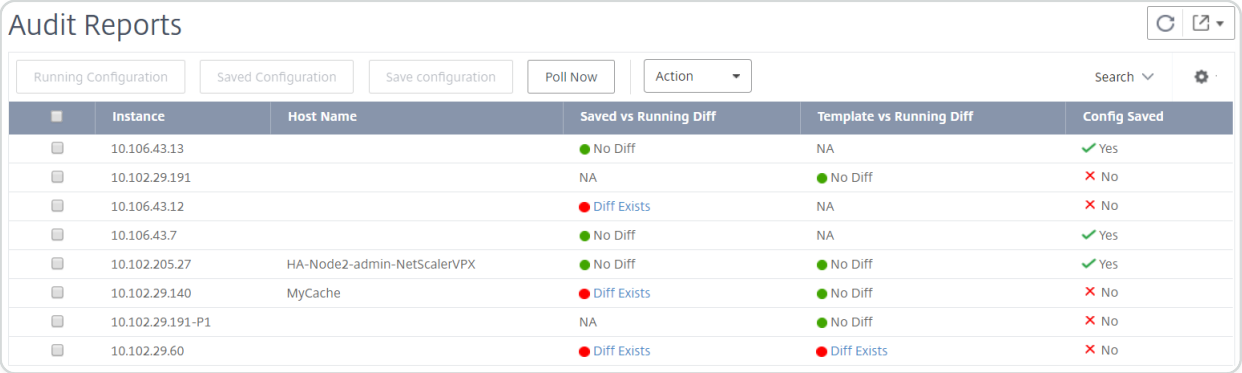
- 每个实例的跨所有实例的摘要报告
- 每个实例-模板对的粒度差异（diff）报告

“**审计模板**”中的审计模板在预定时间针对指定实例中的配置运行。“**配置审计**”仪表板上的“**NetScaler 配置漂移**”图表显示了已保存配置与未保存配置中配置更改的高级详细信息。当您单击“**NetScaler 配置漂移**”图表时，随后的“**审计报告**”页面会显示一个实例列表，其中包含“存在差异”和“无差异”。您可以下载 NetScaler Console 显示的差异报告。

NetScaler Console 还提供了一个选项，可将差异报告安排为邮件附件自动导出。

导出配置审计报告：

1. 在 NetScaler Console 中，导航到“**基础结构 > 配置 > 配置审计**”。
2. 在“**配置审计**”页面上，单击“**NetScaler® 配置漂移**”图表内部。
3. “**审计报告**”页面列出了存在差异的实例。该页面还显示了其运行配置中没有任何差异的实例列表。



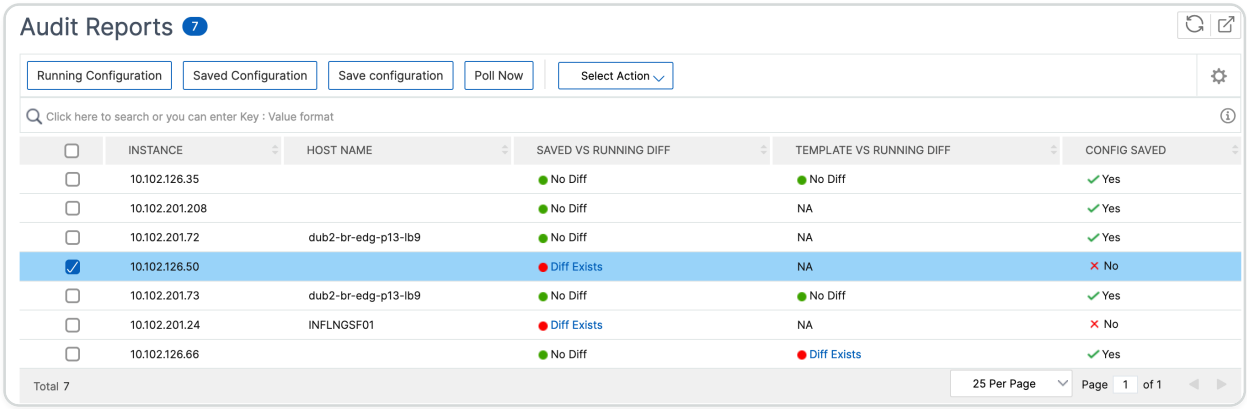
在图像中，您可以看到某些实例的差异仅存在于“**已保存与运行差异**”中，而某些实例的差异仅存在于“**模板与运行差异**”中。对于某些实例，“**已保存与运行差异**”和“**模板与运行差异**”中都存在差异。

已保存与运行差异

您可以查看实例上保存的配置与实例上当前运行的配置之间的差异报告。

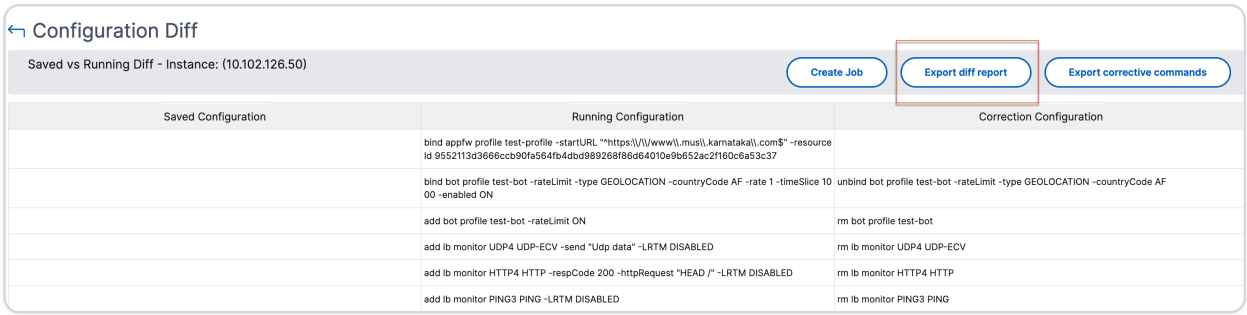
1. 在“**已保存与运行差异**”下，单击实例的“**存在差异**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以查看该实例的已保存配置与运行中配置差异的报告。

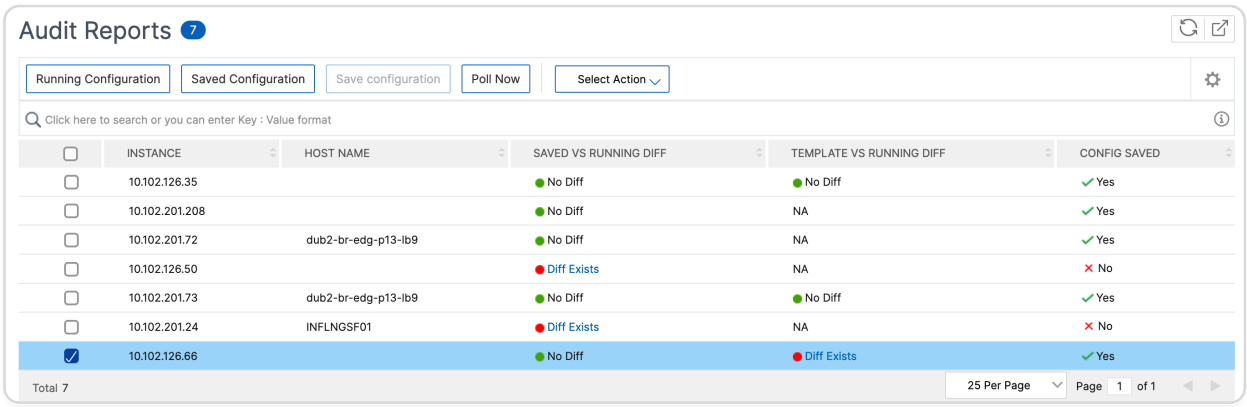
2. 单击“**导出差异报告**”以下载差异报告的 .csv 文件。您还可以单击“**导出纠正命令**”将命令导出到 .txt 文件。然后，您可以从“配置作业”在关联的 NetScaler Console 实例上运行这些命令，以纠正该实例中的配置。



模板与运行中配置差异

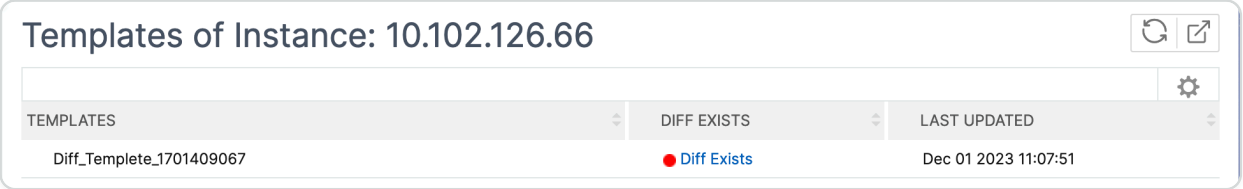
“**模板与运行中配置差异**”包括除作为默认模板的“**保存的配置与运行中的配置差异**”之外的所有模板。您可以查看模板与运行中配置之间存在的差异。

1. 在“**模板与运行中配置差异**”下，单击其中一个实例的“**存在差异**”。

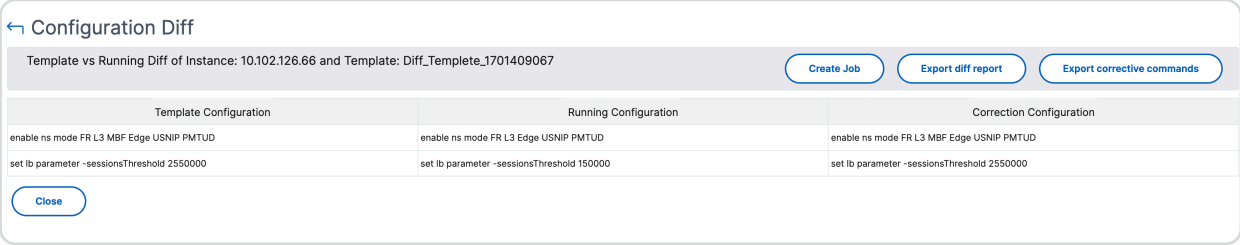


2. 当 NetScaler Console 实例偏离模板指定的配置时，模板会显示差异。

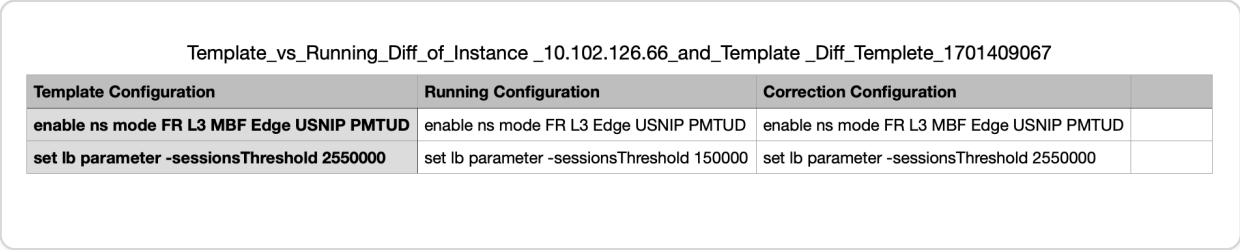
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 再次单击“**存在差异**”。下图显示了模板正在查找的配置、运行中配置以及纠正配置或用于纠正配置的命令。如果“**运行中配置**”为空白，则表示命令未配置或已删除。



4. 单击“**导出差异报告**”以下载差异报告的 .csv 文件。您还可以单击“**导出纠正命令**”将命令导出到 .txt 文件。然后，您可以在 CLI 中运行这些命令，以纠正实例中的配置。



Template_vs_Running_Diff_of_Instance _10.102.126.66_and_Template _Diff_Templete_1701409067

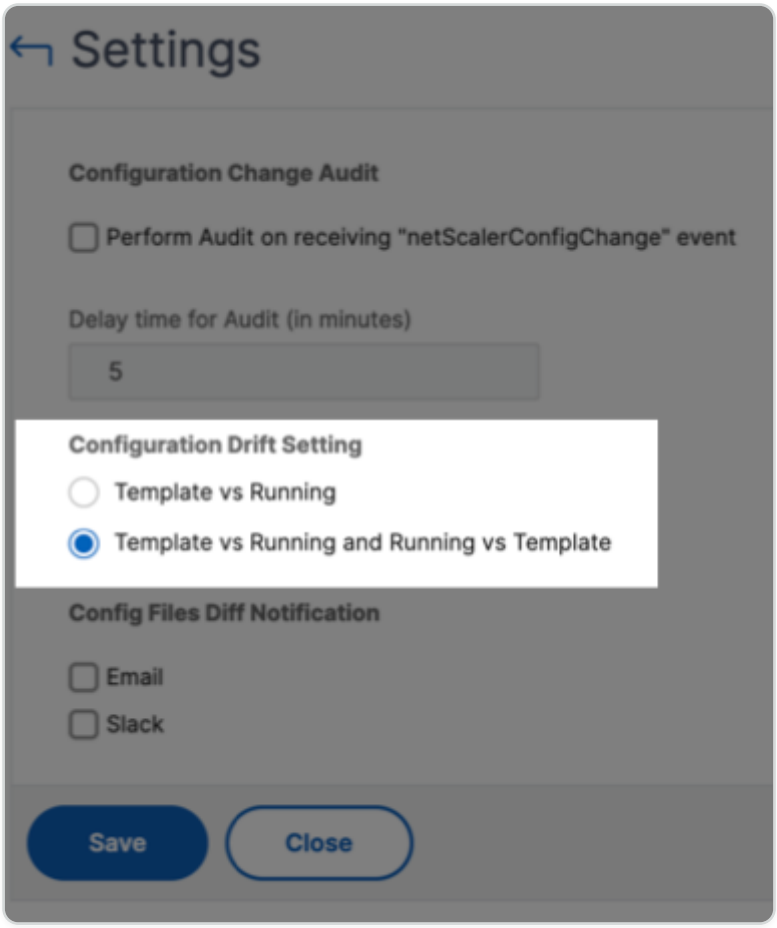
Template Configuration	Running Configuration	Correction Configuration	
enable ns mode FR L3 MBF Edge USNIP PMTUD	enable ns mode FR L3 Edge USNIP PMTUD	enable ns mode FR L3 MBF Edge USNIP PMTUD	
set lb parameter -sessionsThreshold 2550000	set lb parameter -sessionsThreshold 150000	set lb parameter -sessionsThreshold 2550000	

您还可以使用“模板与运行中”和“运行中与模板漂移”设置，从两种方式比较配置：

- 将审计模板配置与实例上的运行配置进行比较。
- 将实例上的运行配置与审计模板进行比较。

默认情况下，选择“模板与运行配置差异”设置。要修改差异设置，请在“**配置审计**”页面中选择“**设置**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



查看文件状态审计报告

使用“**NetScaler 文件状态**”图表监控 `nsconfig` 文件夹中是否有文件被添加、修改或删除。例如，如果 NetScaler 实例上的许可证文件已更新，您可以检查此文件上次更新的时间并采取所需的操作。

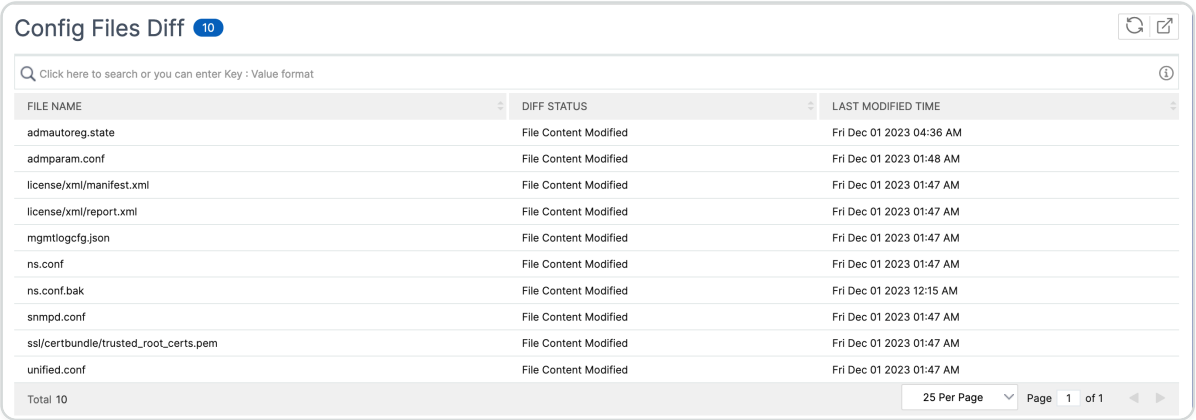
1. 导航到“**基础架构 > 配置 > 配置审计**”。
2. 在“**配置审计**”页面中，单击“**NetScaler 配置文件状态**”图表。

   “**审计报告**”页面列出了具有差异状态的实例。

   “**差异状态**”是根据“**上次轮询时间**”到“**最新轮询时间**”之间的时间间隔计算的。“**差异状态**”可以是以下之一：

   - “**存在差异**” - 此状态表示自“**上次轮询时间**”以来，实例的 `nsconfig` 文件夹中的文件已更改。要查看文件上的更改内容，请单击“**存在差异**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- “**无差异**” - 此状态表示 `nsconfig` 文件夹中的文件自上次轮询时间以来未发生更改。
- “**不适用**” - 此状态表示文件状态监控不适用。当 NetScaler Console 未轮询实例时，会出现此状态。例如，当新添加实例或实例状态不活动时，不会发生实例轮询。

从配置审计中排除文件

您可以从配置审计中排除特定文件，使其不被监控更改。对系统生成或频繁更新的文件（例如，每天更改的文件）使用排除项，以减少审计结果中的干扰并避免误报。

从配置审计文件差异中排除的文件名（或相对路径）示例：

- 有效的文件名（或相对路径）
  - `ns.conf`、`ssl/ns.cert`
- 无效的文件名（或相对路径）
  - `/ns.txt`、`\nsconfig\ns.conf`（排除的文件名必须是相对路径）
  - `ñs.conf`（排除的文件名必须只包含 ASCII 字符）
  - `C:/nsconfig/ns.conf`（排除的文件名不得使用驱动器盘符路径）
  - `ssl/../../ns.conf`（排除的文件名不得包含父目录遍历 `..`）

要从配置审计中排除文件，请执行以下步骤：

1. 导航到 **基础架构 > 配置 > 配置审计**。
2. 选择 **设置**。
3. 在 **NetScaler 配置文件设置** 下，添加您要从审计中排除的文件路径。
4. 单击 **保存**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

审计实例间的配置更改

您希望确保特定配置在特定实例上运行，以实现网络的最佳性能。您还希望监控托管的 NetScaler 实例上的配置更改，排查配置错误，并在系统突然关闭后恢复未保存的配置。

您可以创建包含特定配置的审计模板，以在某些实例上进行审计。NetScaler Console 会将这些实例与审计模板进行比较，并在配置不匹配时进行报告。配置差异报告使您能够排查和纠正不需要的配置更改。

您可以通过以下方式自动运行审计模板：

- 安排模板必须运行的时间。
- 设置 NetScaler Console 必须运行模板的频率。您可以每天、每周的特定一天或每月的特定日期运行模板。

您还可以选择将 NetScaler Console 生成的差异报告发送到您可以配置的指定电子邮件地址。通过此选项，用户可以以邮件附件或 Slack 通知的方式接收报告。他们无需登录 NetScaler Console 手动导出报告。

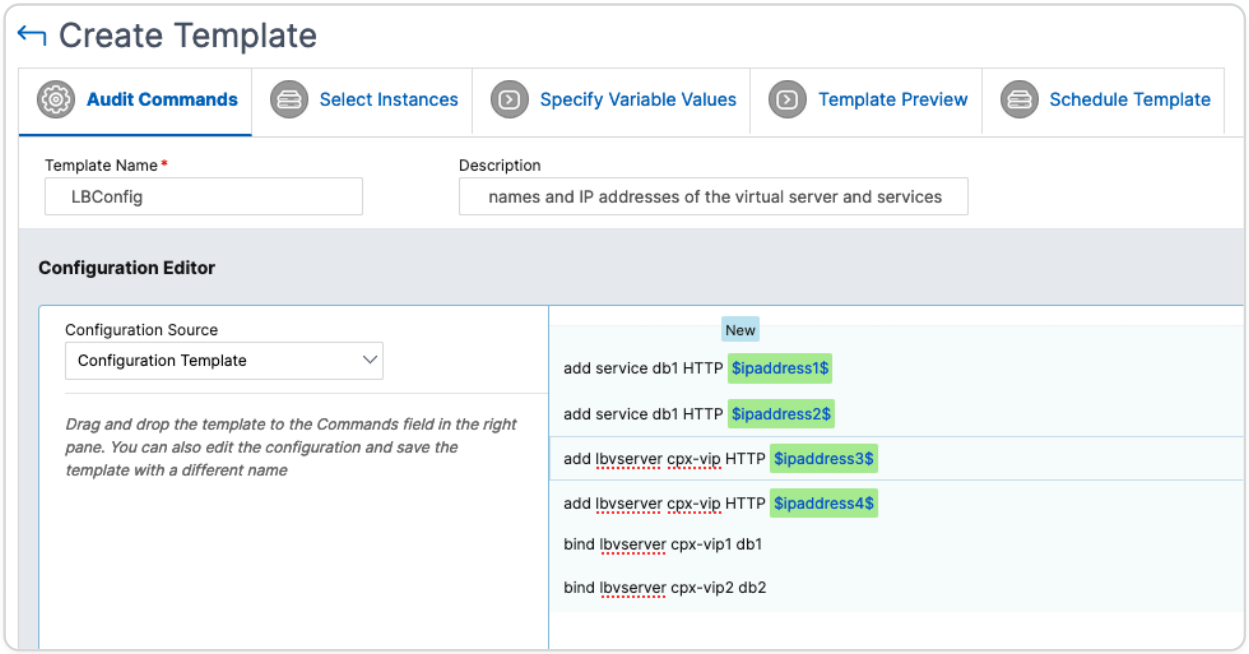
注意：

默认配置模板的“**重命名**”选项已禁用。但是，您可以重命名自定义配置模板。

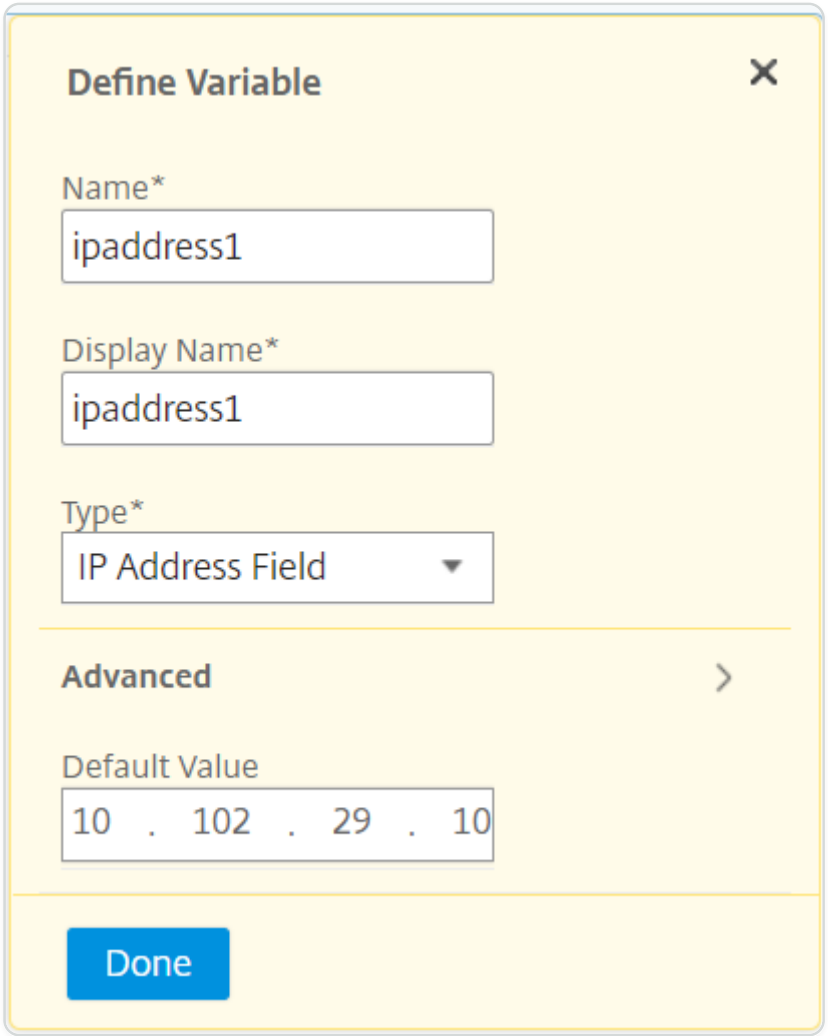
创建审计模板：

1. 导航到 **Infrastructure（基础架构）> Configuration（配置）> Configuration Audit（配置审计）> Audit Templates（审计模板）**，然后单击 **Add（添加）**。
2. 在“**创建模板**”页面和“**审计命令**”选项卡中，指定模板名称及其描述。
3. 在“**配置编辑器**”页面中，键入您的命令并将命令保存为配置模板。您还可以将现有模板从左侧窗格拖动到编辑器中。
4. 选择要转换为变量的值，然后单击“**转换为变量**”。例如，选择负载平衡服务器的 IP 地址“ipaddress1”，然后单击“**转换为变量**”。现在变量用“$”括起来。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

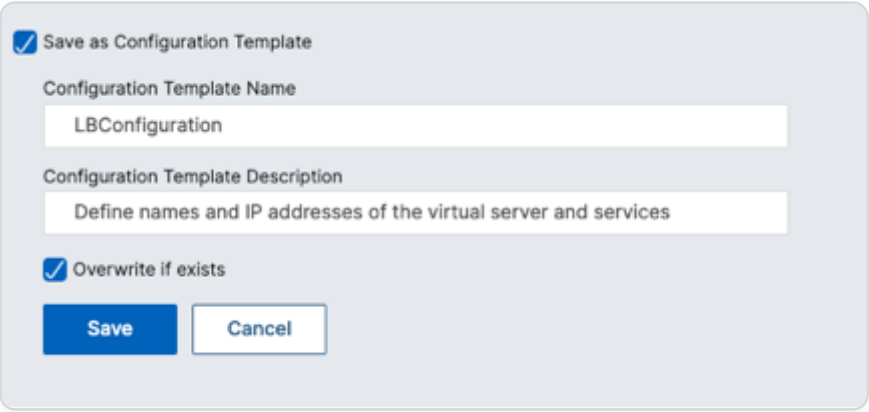


在“**定义变量**”窗口中，设置此变量的属性 - 名称、显示名称和变量类型。如果要进一步指定变量的默认值，请单击“**高级**”选项。

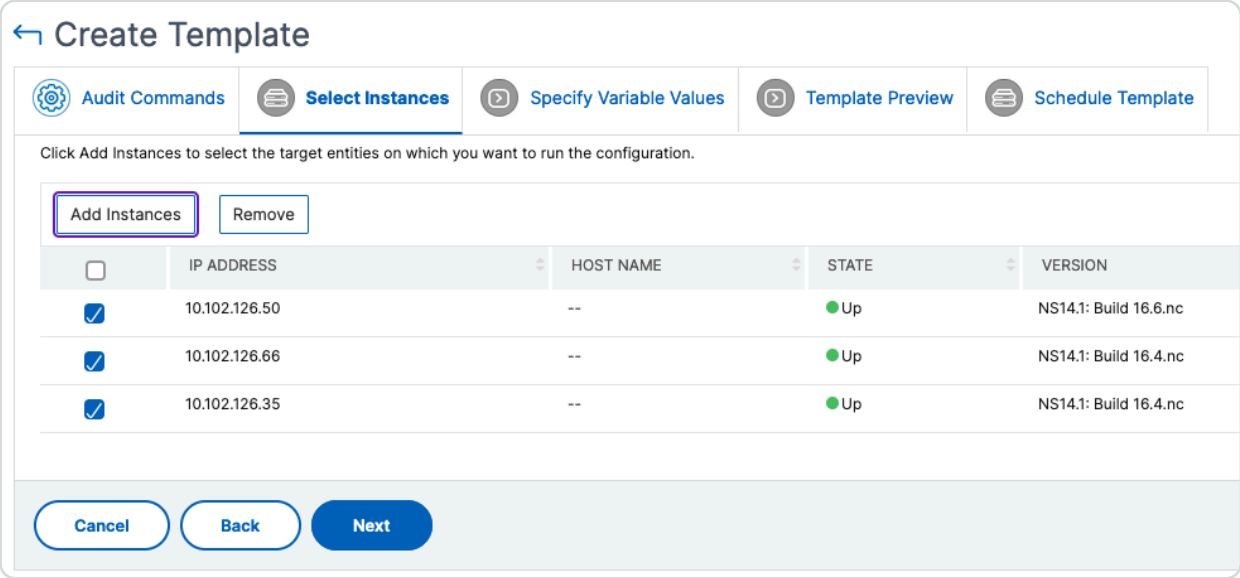


您还可以将命令另存为配置模板。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

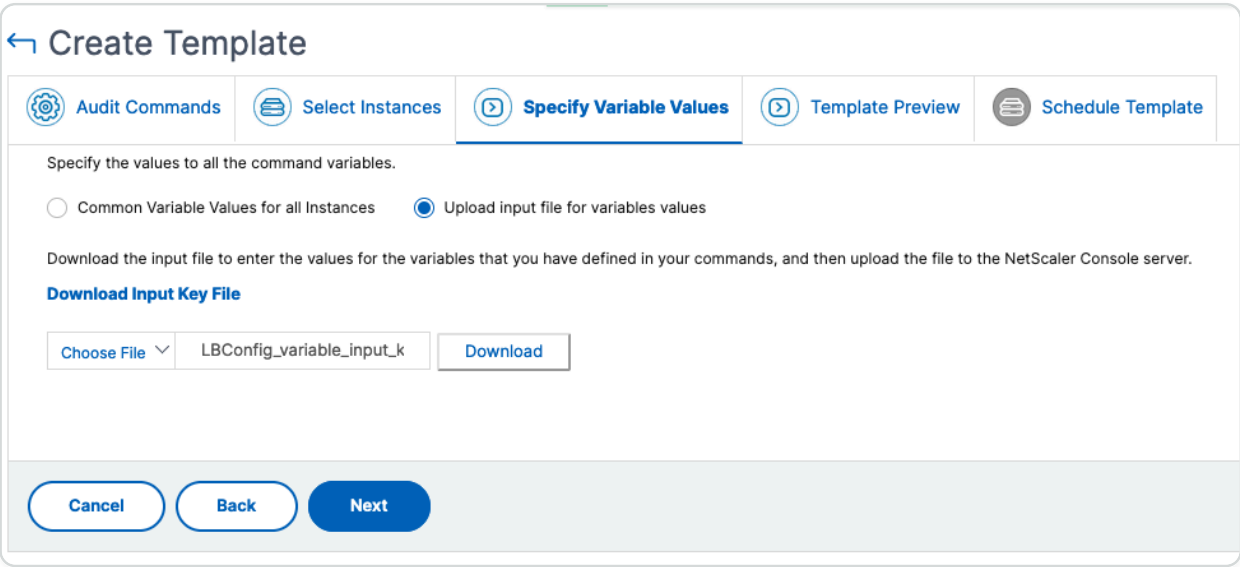


5. 单击“**保存**”，然后单击“**下一步**”。
6. 在“**选择实例**”选项卡中，选择要对其运行配置审计的实例，然后单击“**下一步**”。



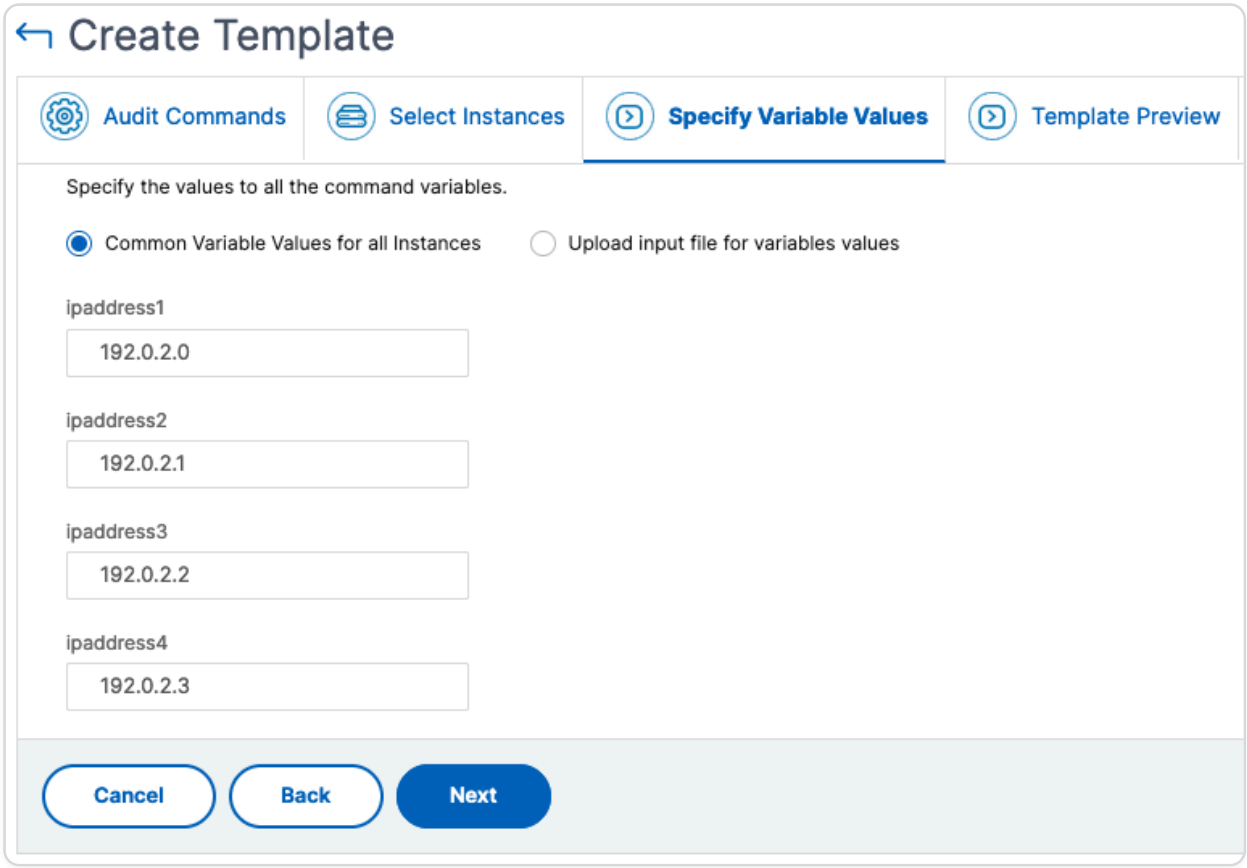
7. 在“**指定变量值**”选项卡中，您有两个选项：

   a. 下载输入文件，输入您在命令中定义的变量值。输入变量后，将文件上传到 NetScaler Console 服务器。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 为您为所有实例定义的变量输入通用值。

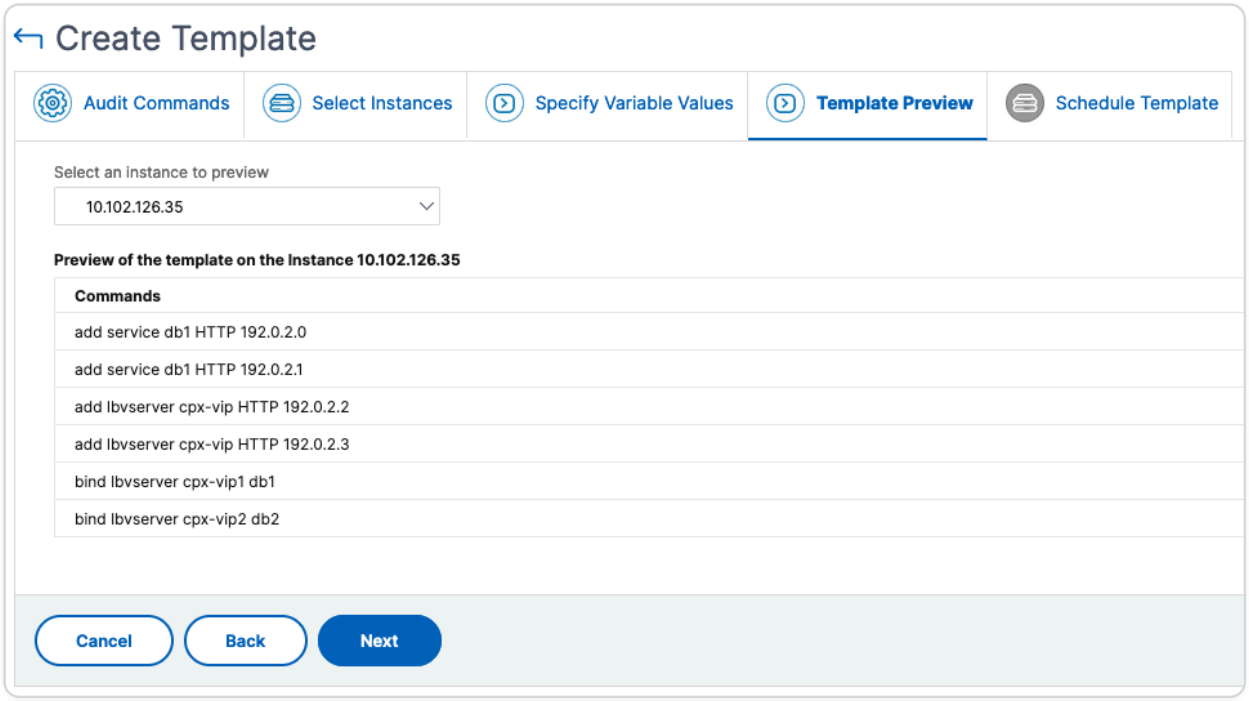


注意：

如果要使用不同的值审计每个实例，您必须在输入文件中为每个实例创建单独的变量。

8. 单击“**下一步**”。
9. 在**模板预览**选项卡中，您可以评估和验证要在每个实例或实例组上运行的命令。单击**下一步**。

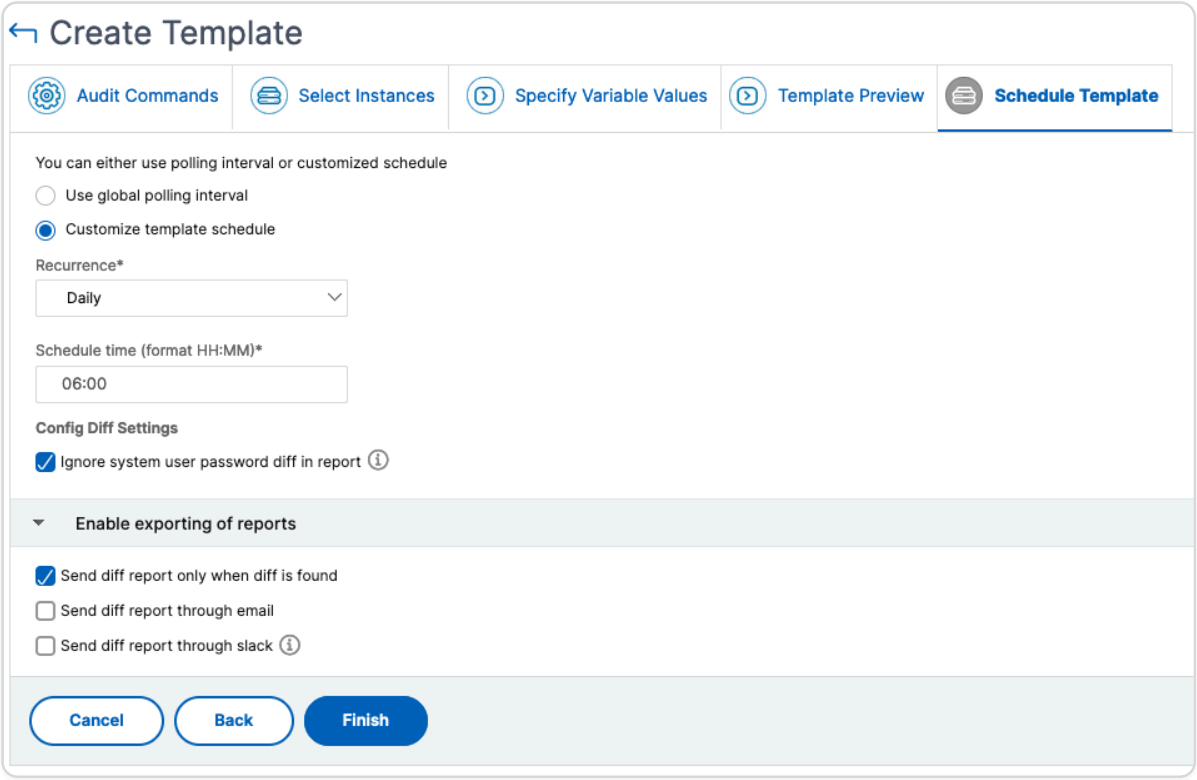
© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. 在**计划模板**选项卡中，您可以使用以下选项来计划模板的运行并配置用于发送差异报告的邮件地址。

    - **使用全局轮询间隔**。选择此选项可在 NetScaler Console 上全局配置的时间在实例上运行模板。
    - **自定义模板计划**。使用此选项可配置模板必须运行的时间和频率。
        - 指定审计模板执行的频率和时间。
    - **启用报告导出**。使用此选项可：
        - **仅当发现差异时发送差异报告**
        - **通过电子邮件发送差异报告**。配置邮件配置文件，差异报告将作为邮件附件发送到该配置文件。
        - **通过 Slack 发送差异报告**。配置 Slack 频道，差异报告将作为通知发送到该频道。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



11. 单击**完成**。

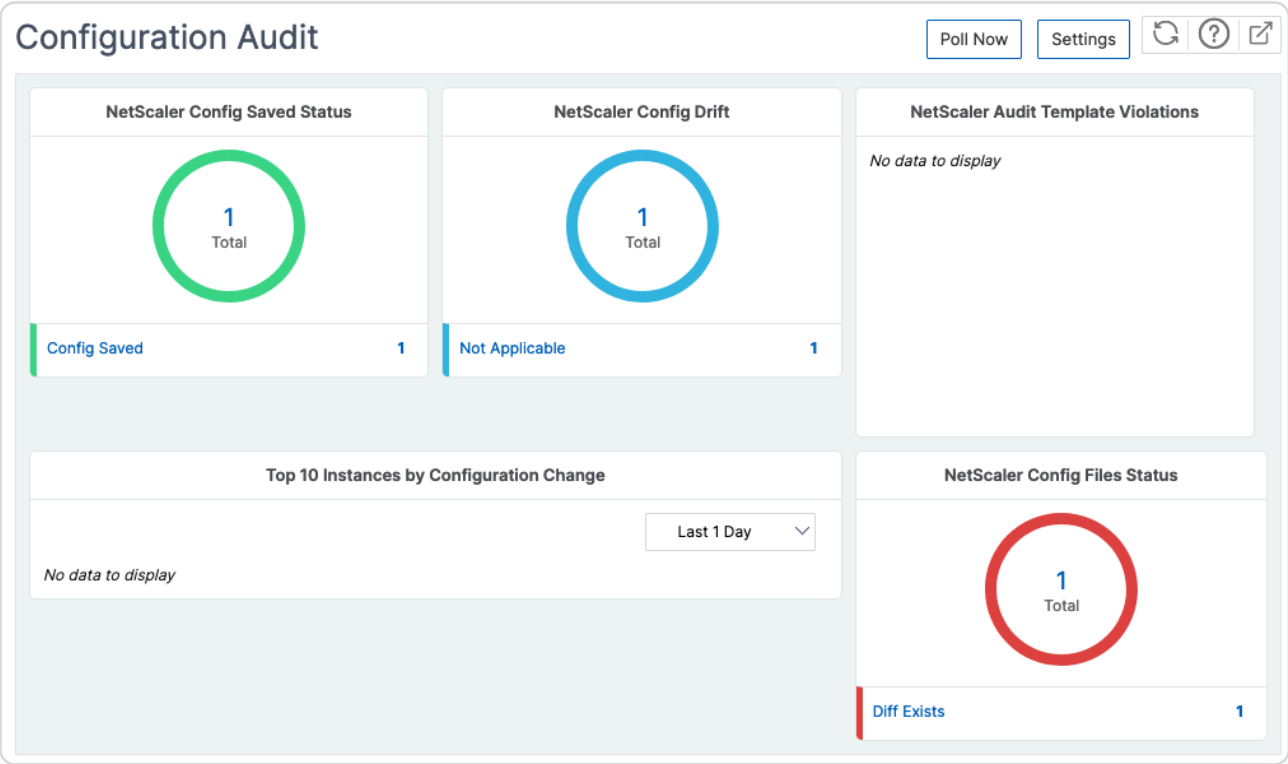
审计模板将显示在**审计模板**列表中，并按计划时间针对指定实例中的配置运行。

查看配置更改

您还可以使用**配置审计**仪表板查看有关配置更改的高级详细信息，例如：

- 按配置更改排名前 10 的实例
- 已保存和未保存的配置数量
- 在 `nsconfig` 文件夹中添加、删除或修改的文件

© 1997–2026 Citrix Systems, Inc. All rights reserved.

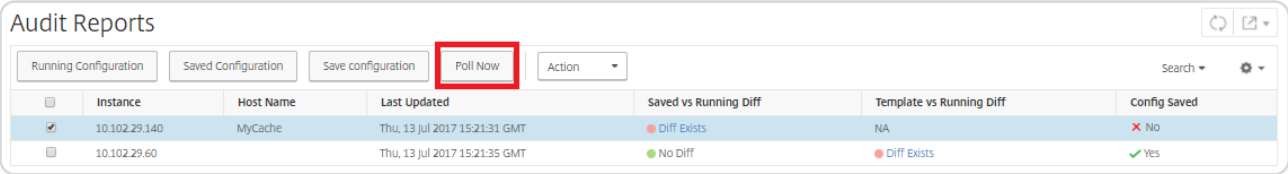


NetScaler Console 还允许您手动轮询配置审计，并将所有实例的配置审计立即添加到 NetScaler Console。为此，请导航到 **Infrastructure > Configuration > Configuration Audit**，单击 **Poll Now**，弹出的 **Poll Now** 页面为您提供了轮询网络中所有 NetScaler 实例或轮询选定实例的选项。

您还可以强制对实例执行审计。为此，请单击以下任意图表：

- **NetScaler 配置保存状态**
- **NetScaler 配置漂移**

在 **Audit Reports** 页面上，选择实例，然后在 **Action** 列表中选择 **Poll Now**。



NetScaler 配置文件状态 图表提供了 `nsconfig` 文件夹中存在的 NetScaler 文件的状态。NetScaler Console 记录并比较 `nsconfig` 文件夹中文件的更改并显示差异。请参阅 查看文件状态审计报告。

设置配置审计通知

1. 导航到 **基础架构 > 配置 > 配置审计**。
2. 在 **Configuration Audit** 页面中，单击 **Settings**。
3. 在 **Notification Settings** 页面中，单击 **Edit** 图标以启用通知设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 勾选“**已启用**”复选框。从下拉列表中选择一个电子邮件分发列表。您还可以通过单击“**+**”图标并指定电子邮件服务器详细信息来创建电子邮件分发列表。

获取网络配置建议

您使用最佳配置设置 NetScaler 实例，以便在应用程序上实现最佳性能。但是，某些配置可能不是标准配置，这可能会影响应用程序的性能。

为了帮助您优化应用程序性能，NetScaler Console 会分析 NetScaler 实例配置并为您提供建议。您可以从 NetScaler Console 应用推荐的配置。

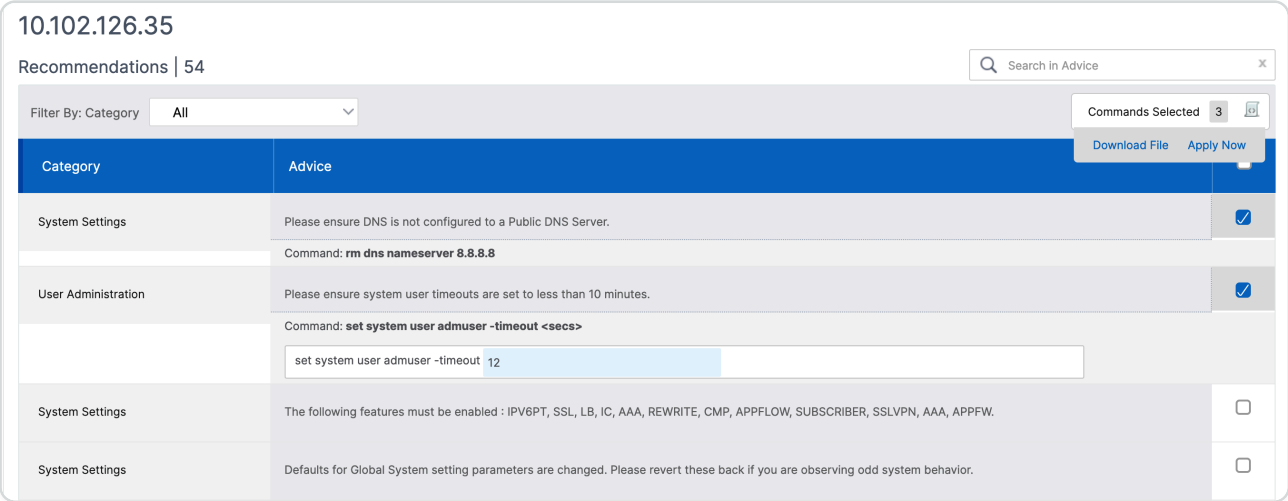
分析 NetScaler 实例：

1. 导航到 **Infrastructure（基础架构）> Configuration（配置）> Configuration Audit（配置审计）> Configuration Advice（配置建议）**。
2. 执行以下操作之一：

   单击 **上传配置文件** 并上传网络实例的配置文件。

   单击 **选择设备** 并选择要分析的 NetScaler 实例。

NetScaler Console 会分析实例上的配置，并提供配置建议列表，如以下图像所示。单击配置建议旁边的复选框以查看纠正命令。



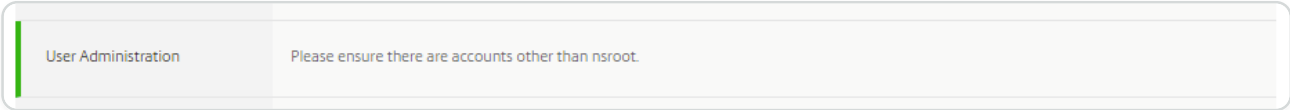
如果要更新配置，请指定纠正命令中变量的值，然后单击 **Apply Now（立即应用）**。

注意：

此处列出的命令仅为建议。具有读写访问权限的用户可以使用此功能编辑任何命令。请确保向您认为不应编辑命令的用户授予有限的特权访问权限。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

当命令在网络实例上成功运行后，建议旁边的复选框将消失。



如果您想查看在网络实例上运行的命令的详细信息，请导航到 **Infrastructure > Instances > `<Instance\_Type\>`**，选择实例的 IP 地址，然后从 **Actions** 下拉列表中单击 **Show Events**。

在 **Events** 页面上，查看配置更改的详细信息。

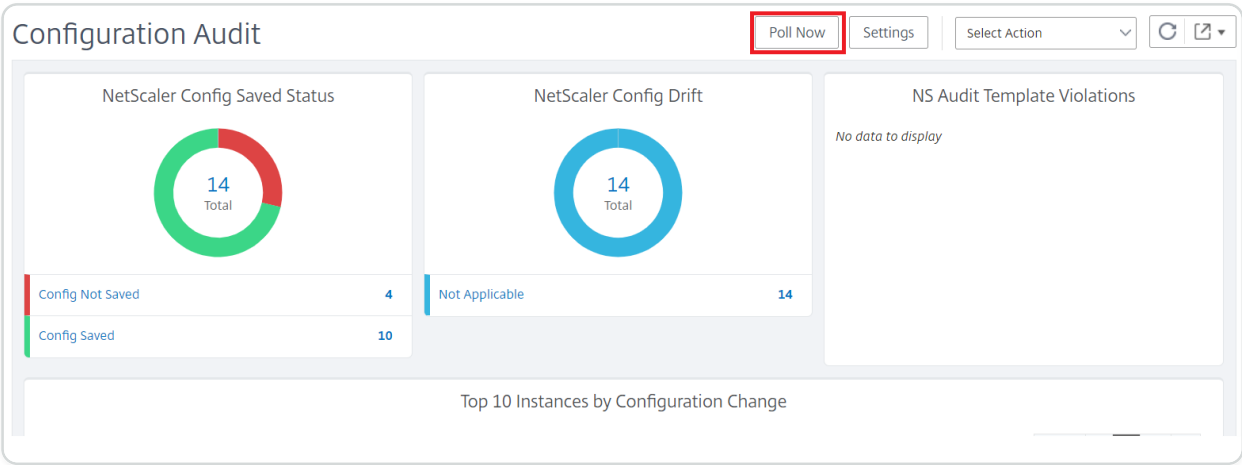
轮询 NetScaler® 实例的配置审计

NetScaler Console 每 10 小时自动轮询配置审计，以查找 NetScaler 实例上发生的配置更改。您也可以手动轮询配置审计以发现最近的更改，但轮询所有 NetScaler 实例的配置会对网络造成沉重负担。

您可以手动轮询选定一个或多个实例的配置审计，而不是轮询整个 NetScaler 实例的配置审计。

要轮询 NetScaler 实例的配置审计：

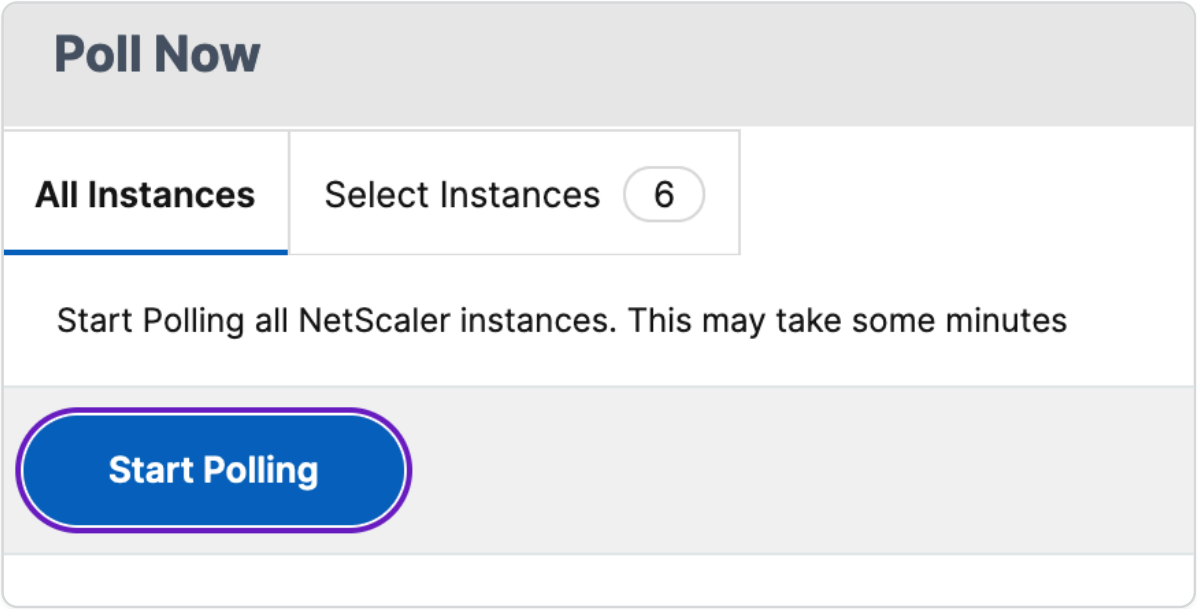
1. 在 NetScaler Console 中，导航到 **基础架构 > 配置 > 配置审计**。
2. 在 **配置审计** 中，单击 **立即轮询**。



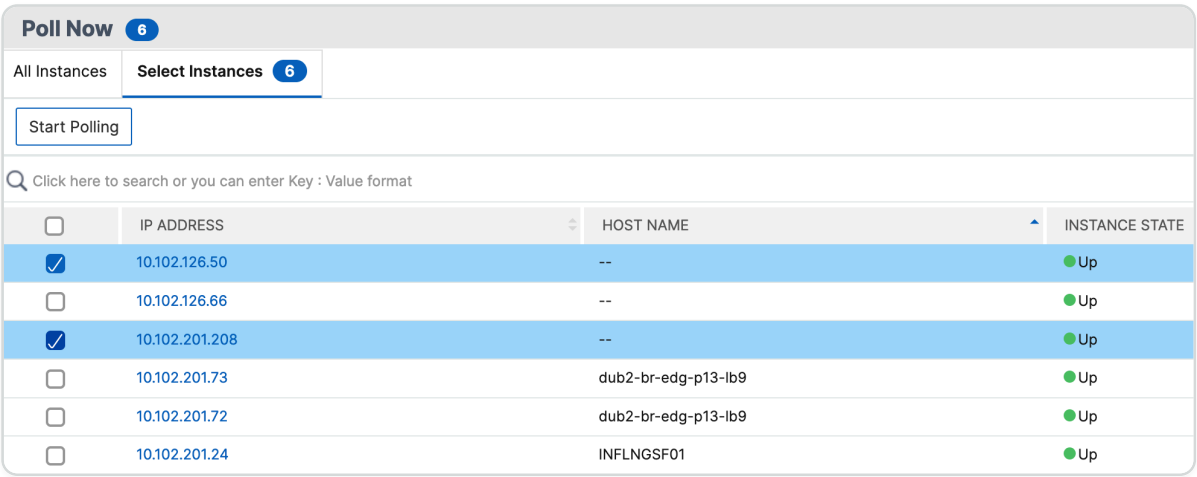
3. **立即轮询** 页面弹出，为您提供轮询网络中的所有 NetScaler 实例或轮询选定实例的选项。

   a. 要轮询所有 NetScaler 实例，请选择 **所有实例** 选项卡，然后单击 **开始轮询**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



b. 要轮询特定实例，请选择 **选择 实例** 选项卡，从列表中选择实例，然后单击 **立即轮询**。



为 ConfigChange SNMP 陷阱生成配置审计差异

每当网络中的 NetScaler 实例发生配置更改时，配置文件都会更新。该实例会向 NetScaler Console 发送一个 ConfigChange SNMP 陷阱。您可以启用 NetScaler Console 在实例发送 ConfigChange SNMP 陷阱时对该实例执行配置审计。

如果审计模板配置与运行配置之间存在差异，则“**审计报告**”页面上会显示“差异存在”状态消息。单击“**差异存在**”链接可转到“**配置差异**”页面，您可以在其中查看纠正命令。您可以使用这些纠正命令创建配置作业，并在特定的 NetScaler 实例上运行。运行配置作业后，实例将恢复到所需的配置。

有关如何从纠正命令创建配置作业的更多信息，请参阅如何在 NetScaler Console 上从纠正命令创建配置作业。

在收到 ConfigChange SNMP 陷阱时运行配置审计模板：

NetScaler Console 允许您启用在 NetScaler Console 中运行配置审计模板的选项。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 在 NetScaler Console 中，导航到“**基础结构 > 配置 > 配置审计**”。
2. 在“**配置审计**”页面上，单击“**设置**”。
3. 选择“**在收到‘netScalerConfigChange’事件时执行审计**”。

注意：

NetScaler Console 将对将来接收到 netScalerConfigChange SNMP 陷阱的每个实例执行配置审计。

1. 在“**运行审计模板的时间延迟**”（以分钟为单位）字段中，键入分钟数。NetScaler Console 在收到该实例的 ConfigChange SNMP 陷阱后，将在该时间延迟后在 NetScaler 实例上运行配置审计模板。

升级作业

重要提示：

基于文件的许可系统（也称为手动管理的授权），传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活所有 Citrix 产品套件的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler Flexed 许可证（Citrix Platform License/Universal Hybrid Multi-Cloud）、旧版 NetScaler Pooled 许可证和 NetScaler Fixed term Bandwidth 许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是兼容 LAS 的版本。

兼容 LAS 的最低 NetScaler 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：从 2025 年 9 月初开始支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： Console 本地部署的 LAS 支持从版本 14.1-51.x 开始。但是，自 April 15 2026 起，Console 本地部署 14.1-51.x 及更高版本和 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署 14.1-51.x 或 13.1-60.x 或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

所有其他形式的旧版 NetScaler 许可证，例如 NetScaler 虚拟 CPU 许可（池化 vCPU）、NetScaler VPX 签入和签出 (CICO)、永久许可证，将不支持 LAS。升级到上述软件版本后，使用没有有效维护的永久许可证的 NetScaler 实例将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。如果不遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法规定的其他补救措施。这些要求在法律或法规禁止的情况下不适用。
您可以使用 NetScaler Console 创建以下维护任务。然后，您可以安排在特定日期和时间执行这些维护任务。

- 升级 NetScaler 实例
- 升级 NetScaler SDX 实例
- 升级 NetScaler BLX 实例
- 升级自动扩缩组中的 NetScaler 实例
- 配置 NetScaler 实例的 HA 对
- 将实例的 HA 对转换为群集

注意：

- 如果升级作业失败，NetScaler Console 会删除构建文件和其他提取的文件，以确保 NetScaler 实例有足够的磁盘空间进行下一次升级尝试。
- 尽管您可以选择任意数量的 NetScaler 实例进行升级，但本地部署的 NetScaler Console 最多支持 40 个并发升级线程。这意味着只有 40 个实例可以同时升级。
- 不支持从非 FIPS 版本过渡到 FIPS 版本，也不支持跳过顺序升级的直接版本升级（例如，从 13.0 版到 14.1 版）。这些限制是必要的，因为不同构建类型之间存在架构差异，并且主要版本之间需要增量更改。为确保成功升级，您必须部署全新的 FIPS 版本或遵循所有中间版本的受支持顺序升级路径。

升级前验证

在 NetScaler 升级作业期间，NetScaler Console 执行以下验证：

- NetScaler Console 执行的升级前检查
- NetScaler 执行的升级前检查（从 NetScaler 14.1-66.x 及更高版本开始支持）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

这两个来源的结果会合并并以单个响应的形式呈现，以指导升级决策。无需额外配置即可启用 NetScaler 或 NetScaler Console 执行的升级前检查。升级前验证提供以下优势：

- 提高升级期间的信心和安全性
- 在升级启动前及早发现阻塞问题
- 在所有支持的 NetScaler 版本中提供一致的预检查体验

NetScaler Console 执行的预升级检查

NetScaler Console 执行以下检查：

- **`/var` 上的磁盘空间可用性**：验证 `/var` 分区上是否有足够的可用空间来安全地执行映像提取和安装操作。
- **/flash 上的磁盘空间可用性**：检查 `/flash` 分区是否具有支持安装期间基本系统操作所需的最小可用磁盘空间。
- **NSPEPI 配置检查**：验证 NetScaler 配置文件中是否存在不受支持或无效的策略，以防止安装或升级后出现配置错误。
- **高可用性 (HA) 配置检查**：验证 HA 状态和角色一致性，以确保 HA 设置健康且受支持。
- **SSH 连接检查**：确认 SSH 可访问性、信任验证以及与远程安装和管理操作所需的目标设备的连接。
- **降级匹配的 ns.conf**：确保有适当且兼容的 `ns.conf file` 可用于降级场景，以防止配置不兼容。

所有预检查结果统一分类如下：

- **严重（阻止）**：升级被阻止。必须在继续之前解决所有报告的问题。
- **警告**：经管理员批准后，可以继续升级。
- **建议**：经管理员批准后，可以继续升级。

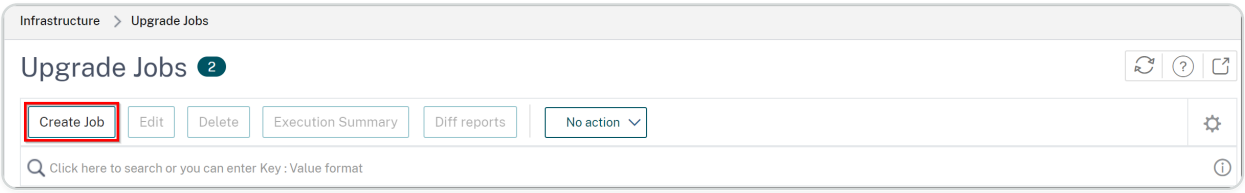
NetScaler 执行的预升级检查

有关 NetScaler 执行的预升级检查的详细信息，请参阅 NetScaler 预升级验证检查。

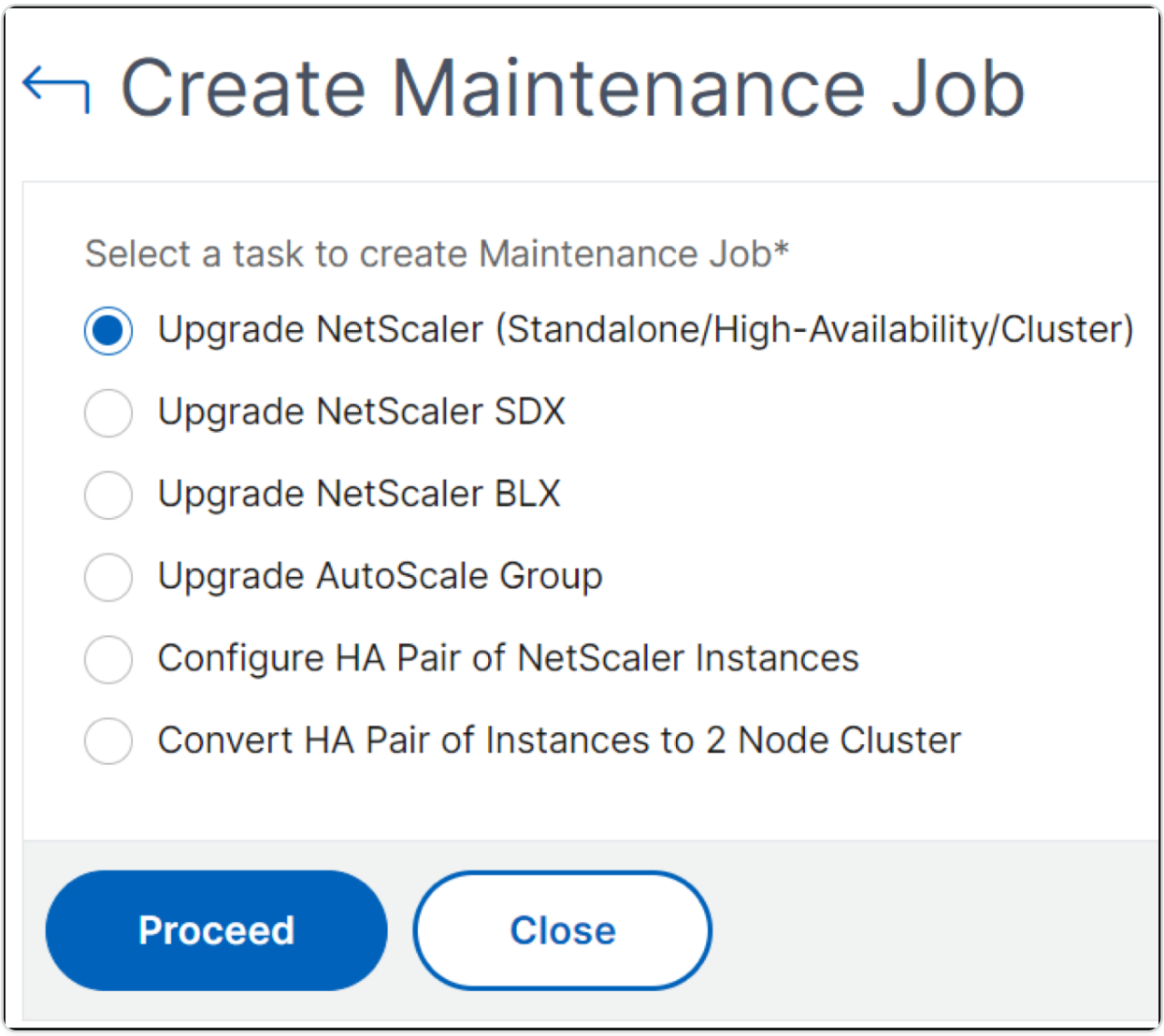
安排 NetScaler 实例升级

1. 导航到 **基础架构 > 升级作业**。单击 **创建作业**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

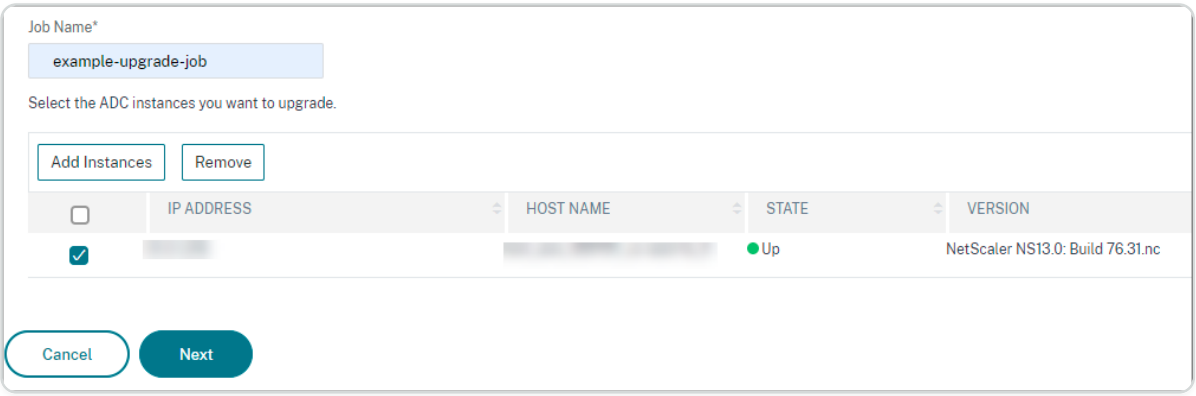


2. 在 **创建维护作业** 中，选择 **升级 NetScaler（独立/高可用性/群集）**，然后单击 **继续**。



3. 在 **Select Instance** 中，为 **Job Name** 键入您选择的名称。
4. 单击 **Add Instances** 以添加要升级的 NetScaler 实例。
   - 要升级 HA 对，请指定主节点或辅助节点的 IP 地址。但是，建议使用主实例升级 HA 对。
   - 要升级群集，请指定群集 IP 地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



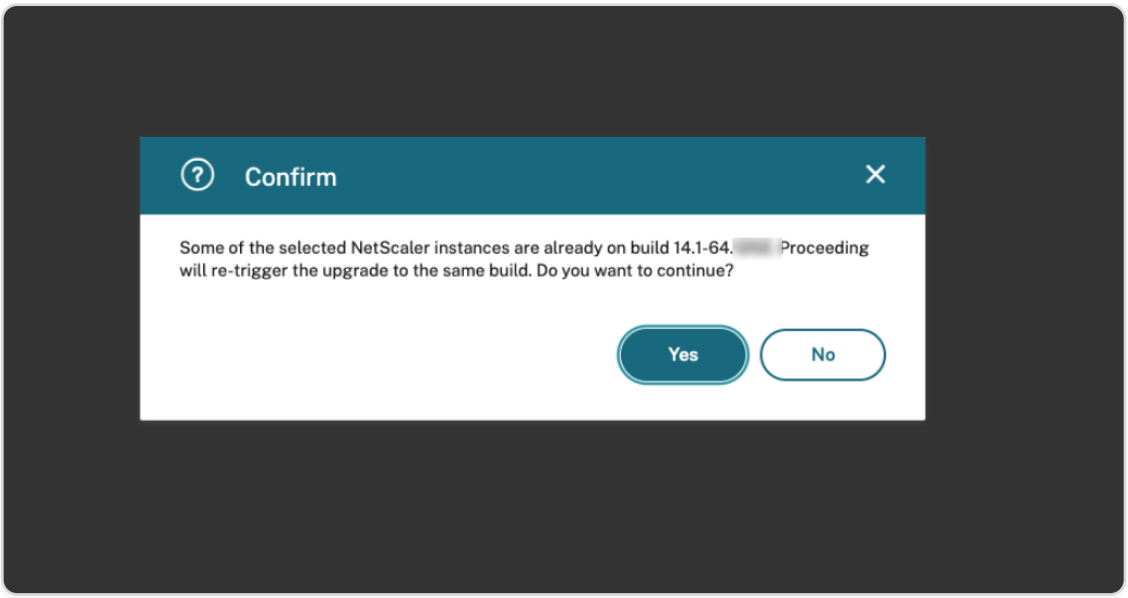
5. 单击 **Next** 以选择映像。从 **Software Image** 列表中选择以下选项之一：

   - **Local** - 从本地计算机中选择实例升级文件。
   - **Appliance** - 从 NetScaler Console 文件浏览器中选择实例升级文件。NetScaler Console GUI 显示 `/var/mps/mps_images` 处存在的实例文件。
     - **如果所选映像已可用，则跳过将映像上传到 NetScaler** - 如果映像已存在于 NetScaler 实例中，请选择此选项。
     - **成功升级后从 NetScaler 清理软件映像** - 选择此选项可在实例升级后清除 NetScaler 实例中上传的映像。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

- 如果所选实例已在目标版本上，则会显示警告。此警告有助于防止在升级作业期间选择错误的实例。如果您打算重新升级实例，请忽略此警告并继续升级。



- 如果所选实例已安排了现有升级作业，NetScaler Console 会显示警告消息。此警告消息有助于防止在同一 NetScaler 实例上无意中安排重复的升级作业。

6. 单击 **下一步** 以开始对所选实例进行升级前验证。

   升级前验证 选项卡显示失败的实例。删除失败的实例，然后单击 **下一步**。

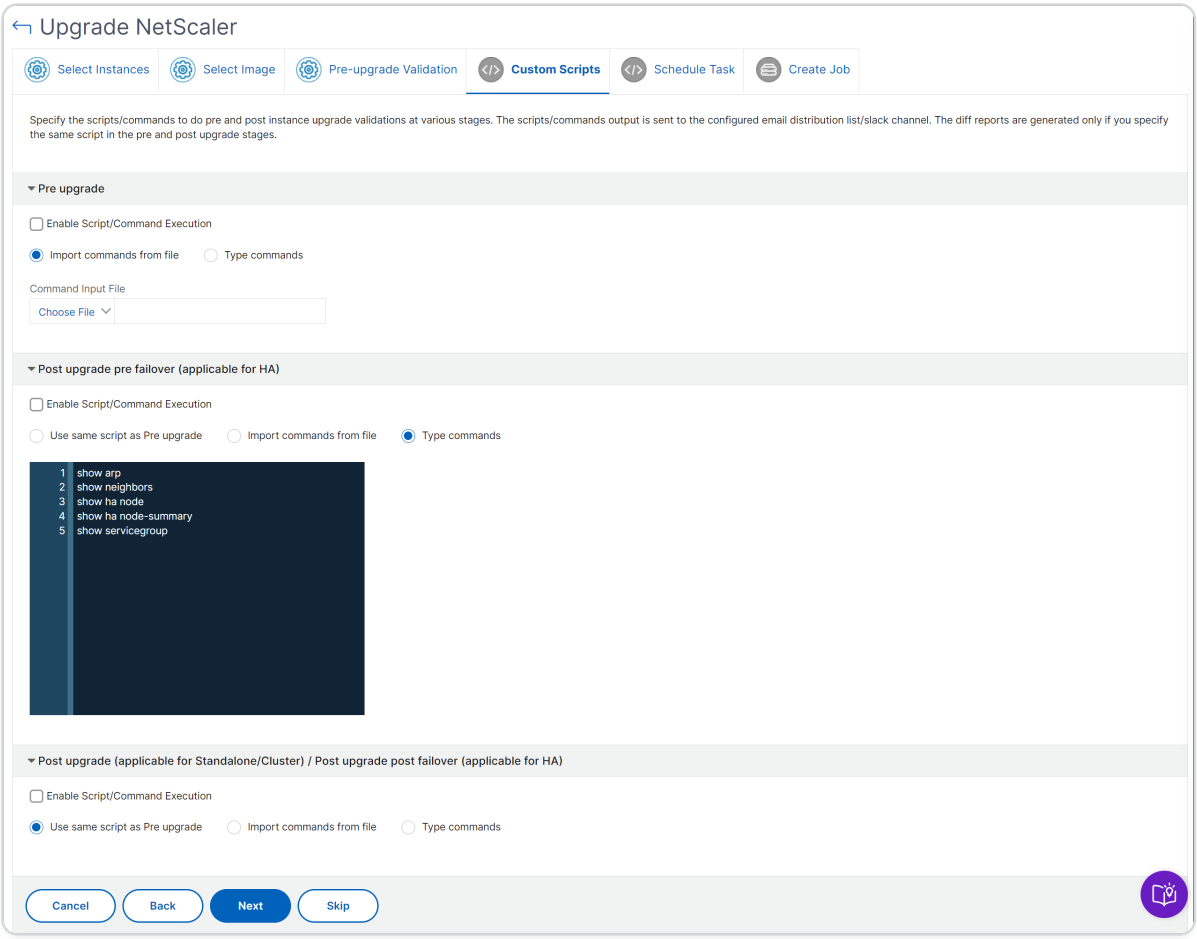
重要提示

如果您指定群集 IP 地址，NetScaler Console 仅对指定的实例执行升级前验证，而不对其他群集节点执行。

7. 可选，在 **自定义脚本** 中，指定在实例升级前后运行的脚本。使用以下方法之一运行命令：

   - **从文件导入命令** - 从本地计算机中选择命令输入文件。
   - **键入命令** - 直接在 GUI 上输入命令。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以使用自定义脚本检查实例升级前后的更改。例如：

- 升级前后的实例版本。
- 升级前后的接口、高可用性节点、虚拟服务器和服务的状态。
- 虚拟服务器和服务的统计信息。
- 动态路由。

8. 单击“**下一步**”。在“**计划任务**”中，选择以下选项之一：

   - “**立即升级**” - 升级作业立即运行。
   - “**稍后计划**” - 选择此选项可稍后运行此升级作业。指定要升级实例的“**执行日期**”和“**开始时间**”。

     如果要分两个阶段升级 NetScaler HA 对，请选择“**对 HA 中的节点执行两阶段升级**”。

     指定要升级 HA 对中另一个实例的“**执行日期**”和“**开始时间**”。

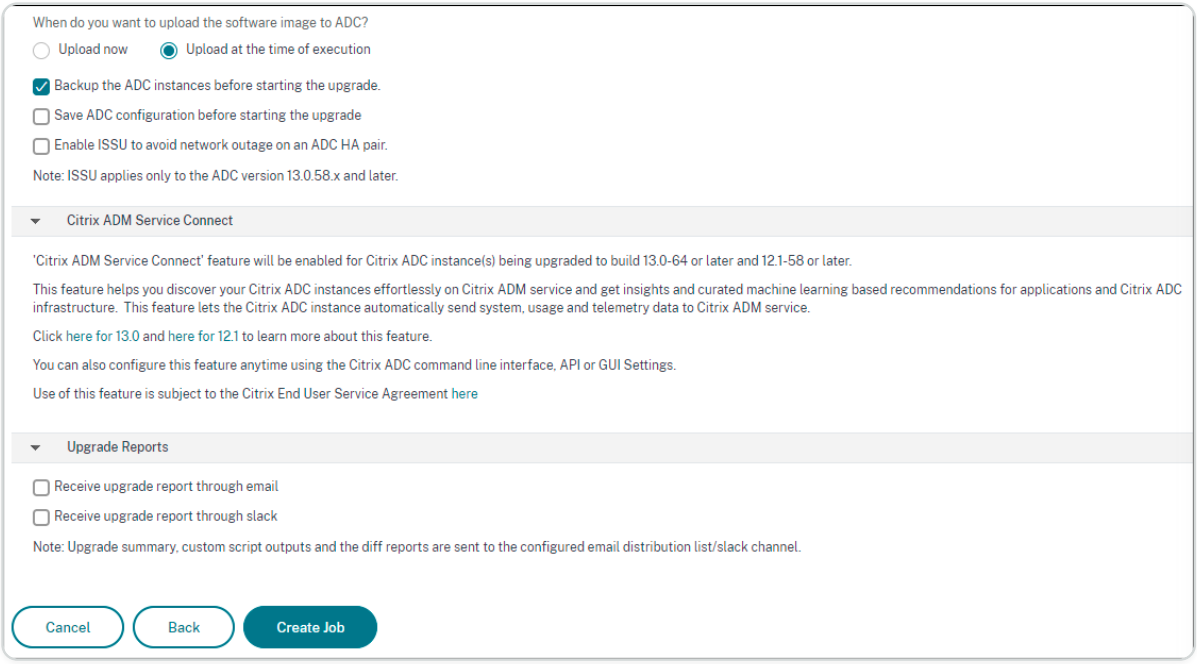
9. 单击“**下一步**”。在“**创建作业**”中，指定以下详细信息：

   a. 指定何时将映像上传到实例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- “**立即上传**” - 选择此选项可立即上传映像。但是，升级作业将在计划时间运行。
- “**在执行时上传**” - 选择此选项可在升级作业执行时上传映像。
- “**在开始升级之前备份 NetScaler 实例。**” - 创建所选 NetScaler 实例的备份。
- “**在开始升级之前保存 NetScaler 配置**” - 在升级之前保存实例上配置的配置作业。
- “**启用 ISSU 以避免 NetScaler HA 对上的网络中断**” - 启用在线软件升级 (ISSU) 允许您升级 NetScaler 高可用性 (HA) 对，而不会导致网络停机。ISSU 通过在节点之间无缝迁移活动会话来确保在升级期间遵守现有连接。在升级工作流中启用 ISSU 后，系统还可以在客户定义的延迟时间后触发 ISSU 迁移完成。NetScaler Console 触发完整的 ISSU 迁移完成可确保即使连接持续存在，升级也能完成。以分钟为单位指定 ISSU 迁移超时，以设置 NetScaler Console 完成迁移之前的等待时间。

- “**NetScaler Console Service Connect**” - 如果您要升级到版本 **13.0-64 或更高版本**和 **12.1-58 或更高版本**，NetScaler Console Service Connect 将自动启用。有关详细信息，请参阅使用 NetScaler Console 服务连接实现 NetScaler 实例的低接触式载入。
- **通过电子邮件接收执行报告** - 通过电子邮件发送执行报告。要添加电子邮件分发列表，请参阅创建电子邮件分发列表。
- **通过 Slack 接收执行报告** - 通过 Slack 发送执行报告。要添加 Slack 配置文件，请参阅创建 Slack 配置文件。



10. 单击**创建作业**。

安排升级 NetScaler SDX 实例

1. 导航到**基础架构 > 升级作业**。单击**创建作业**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 选择**升级 NetScaler SDX**，然后单击**继续**。
3. 在**升级 NetScaler SDX**页面上，在**实例选择**选项卡中：
   a. 添加**任务名称**。
   b. 从**软件映像**列表中，选择**本地**（您的本地计算机）或**设备**（构建文件必须存在于 NetScaler Console 虚拟设备上）。

      上传过程开始。
   c. 添加您要在其上运行升级过程的 NetScaler SDX 实例。
   d. 单击**下一步**。
4. 在**计划任务**选项卡上，从**执行模式**列表中选择**立即**以立即升级 NetScaler SDX 实例，然后单击**完成**。
5. 要稍后升级 NetScaler SDX 实例，请从**执行模式**列表中选择**稍后**。然后，您可以选择升级 NetScaler 实例的执行日期和开始时间，然后单击**完成**
6. 您还可以启用电子邮件和 Slack 通知，以接收正在升级的 NetScaler SDX 实例的执行报告。单击“**通过电子邮件接收执行报告**”复选框和“**通过 Slack 接收执行报告**”复选框以启用通知。

   有关配置电子邮件分发列表和 Slack 频道的更多信息，请参阅中的**步骤 8**。(#schedule-upgrading-of-pagecitrix-adc-generic-instances)

计划升级 NetScaler BLX 实例

1. 导航到“**基础结构 > 升级作业**”。单击“**创建作业**”。
2. 在“**创建维护作业**”中，选择“**升级 NetScaler BLX**”，然后单击“**继续**”。
3. 在“**选择实例**”中，为“**作业名称**”键入您选择的名称。
4. 单击“**添加实例**”以添加要升级的 BLX 实例。
   - 要升级 HA 对，请指定主节点或辅助节点的 IP 地址。但是，建议使用主实例升级 HA 对。
   - 要升级群集，请指定群集 IP 地址。
5. 单击“**下一步**”以选择映像。从“**软件映像**”列表中选择以下选项之一：
   - “**本地**” - 从本地计算机中选择实例升级文件。
   - “**设备**” - 从 NetScaler Console 文件浏览器中选择实例升级文件。NetScaler Console GUI 显示位于 `/var/mps/mps_images` 的实例文件。
     - “**如果所选映像已可用，则跳过将映像上传到 NetScaler**” - 如果映像已存在于 NetScaler 实例中，请选择此选项。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- “**成功升级后从 NetScaler 清理软件映像**” - 选择此选项可在实例升级后清除 NetScaler 实例中上传的映像。

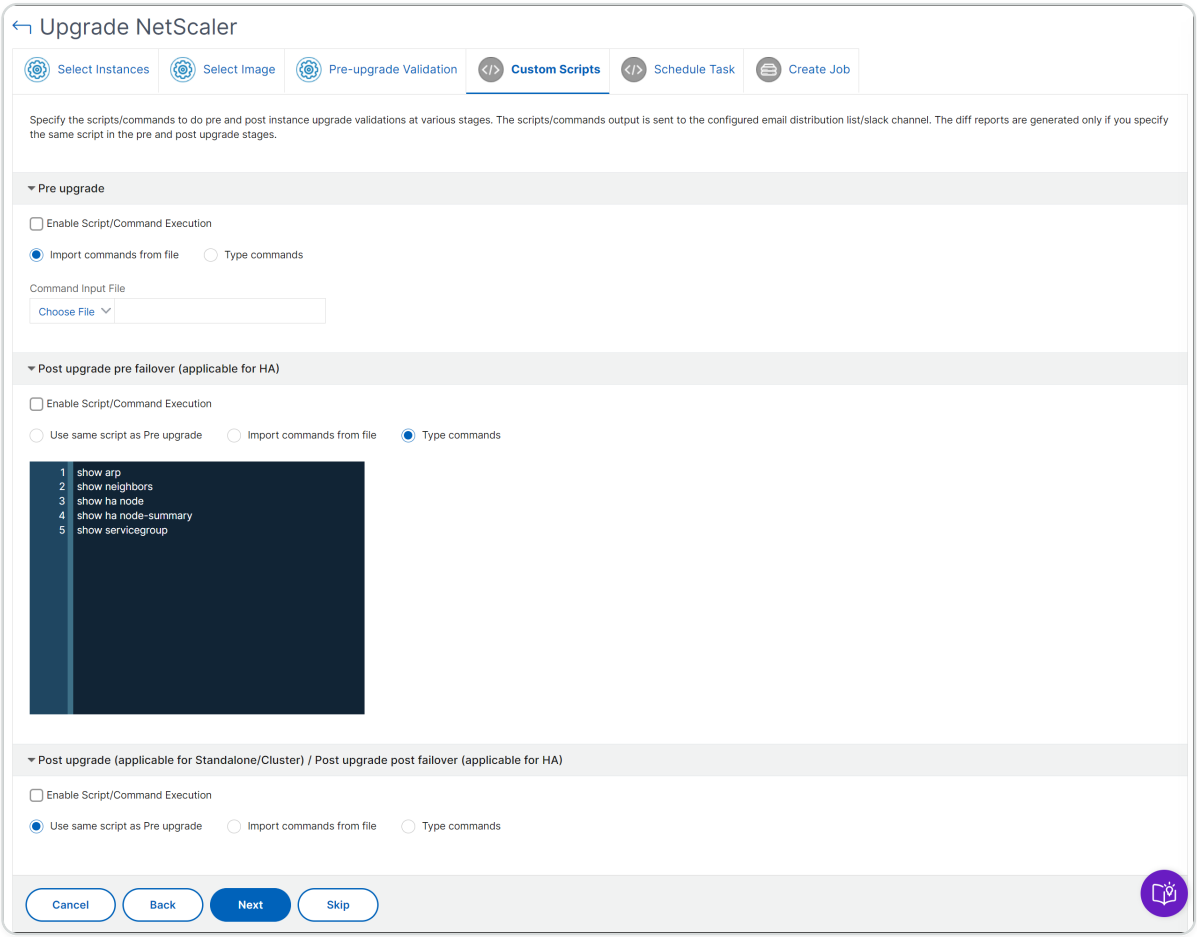
6. 单击“**下一步**”以开始对所选实例进行预升级验证。

   “**预升级验证**”选项卡显示失败的实例。删除失败的实例，然后单击“**下一步**”。

> **重要**
>
> 如果您指定集群 IP 地址，NetScaler Console 仅对指定的实例执行预升级验证，而不对其他集群节点执行。

7. 可选，在“**自定义脚本**”中，指定在实例升级前后运行的脚本。使用以下方法之一运行命令：

   - **从文件导入命令** - 从本地计算机选择命令输入文件。
   - **键入命令** - 直接在 GUI 上输入命令。



   您可以使用自定义脚本检查实例升级前后的更改。例如：

   - 升级前后的实例版本。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 升级前后的接口、高可用性节点、虚拟服务器和服务的状态。
- 虚拟服务器和服务的统计信息。
- 动态路由。

8. 单击“**下一步**”。在“**计划任务**”中，选择以下选项之一：

   - **立即升级** - 升级作业立即运行。
   - **稍后计划** - 选择此选项可稍后运行此升级作业。指定要升级实例的**执行日期**和**开始时间**。

     如果您想分两个阶段升级 HA 对，请选择 **对 HA 中的节点执行两阶段升级**。

     指定您希望升级 HA 对中另一个实例的**执行日期**和**开始时间**。

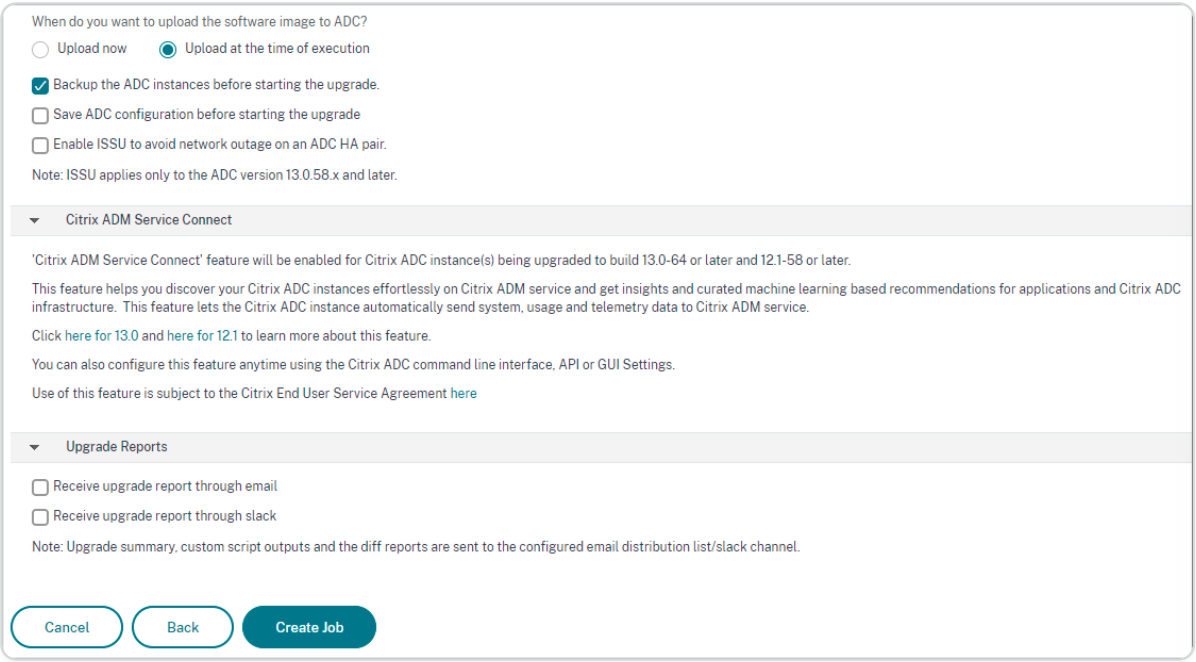
9. 单击**下一步**。在**创建作业**中，指定以下详细信息：

   a. 指定您希望何时将映像上传到实例：

      - **立即上传** - 选择此选项可立即上传映像。但是，升级作业将在计划时间运行。
      - **在执行时上传** - 选择此选项可在升级作业执行时上传映像。
      - **在开始升级之前备份 NetScaler 实例** - 创建所选 NetScaler 实例的备份。
      - **在开始升级之前保存 NetScaler 配置** - 保存升级之前在实例上配置的配置作业。
      - **启用 ISSU 以避免 NetScaler HA 对上的网络中断** - 启用在线软件升级 (ISSU) 允许您升级 NetScaler 高可用性 (HA) 对，而不会导致网络停机。ISSU 通过在节点之间无缝迁移活动会话来确保在升级期间保留现有连接。在升级工作流中启用 ISSU 后，系统还可以在客户定义的延迟时间后触发 ISSU 迁移完成。NetScaler Console 触发完整的 ISSU 迁移完成可确保即使连接持续存在，升级也能完成。以分钟为单位指定 ISSU 迁移超时，以设置 NetScaler Console 完成迁移之前的等待时间。

   - **NetScaler Console Service Connect** - 如果您正在升级到版本 **13.0-64 或更高版本**和 **12.1-58 或更高版本**，NetScaler Console Service Connect 将自动启用。有关更多信息，请参阅使用 NetScaler Console 服务连接实现 NetScaler 实例的低接触式载入。
   - **通过电子邮件接收执行报告** - 通过电子邮件发送执行报告。要添加电子邮件分发列表，请参阅创建电子邮件分发列表。
   - **通过 Slack 接收执行报告** - 通过 Slack 发送执行报告。要添加 Slack 配置文件，请参阅创建 Slack 配置文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. 单击**创建作业**。

计划升级 Autoscale™ 组

执行以下步骤，升级属于自动扩缩组的云服务中的所有实例：

1. 导航到 **基础架构 > 升级作业**。单击 **创建作业**。
2. 选择 **Upgrade Autoscale Group**，然后单击 **Proceed**。
3. 在 **Upgrade Settings** 选项卡中：
   a. 选择要升级的 **Autoscale Group**。
   b. 在 **Image** 中，选择 NetScaler 版本。此映像是自动扩缩组中 NetScaler 实例的现有版本。
   c. 在 **NetScaler Image** 中，浏览要升级到的 NetScaler 版本文件。

      如果选中 **Graceful Upgrade**，升级任务将等待直到指定的排空连接期到期。

   d. 单击 **Next**。
4. 在 **Schedule Task** 选项卡中：
   a. 从“执行模式”列表中选择以下选项之一：
      - **Now**：立即开始 NetScaler 实例升级。
      - **Later**：稍后开始 NetScaler 实例升级。
   b. 如果选择 **Later** 选项，请选择要开始升级任务的执行日期和开始时间。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您还可以启用电子邮件和 Slack 通知，以接收正在升级的自动扩缩组的执行报告。单击 **Receive Execution Report Through Email** 复选框和 **Receive Execution Report through slack** 复选框以启用通知。

5. 单击 **完成**。

计划配置 NetScaler 实例的 HA 对

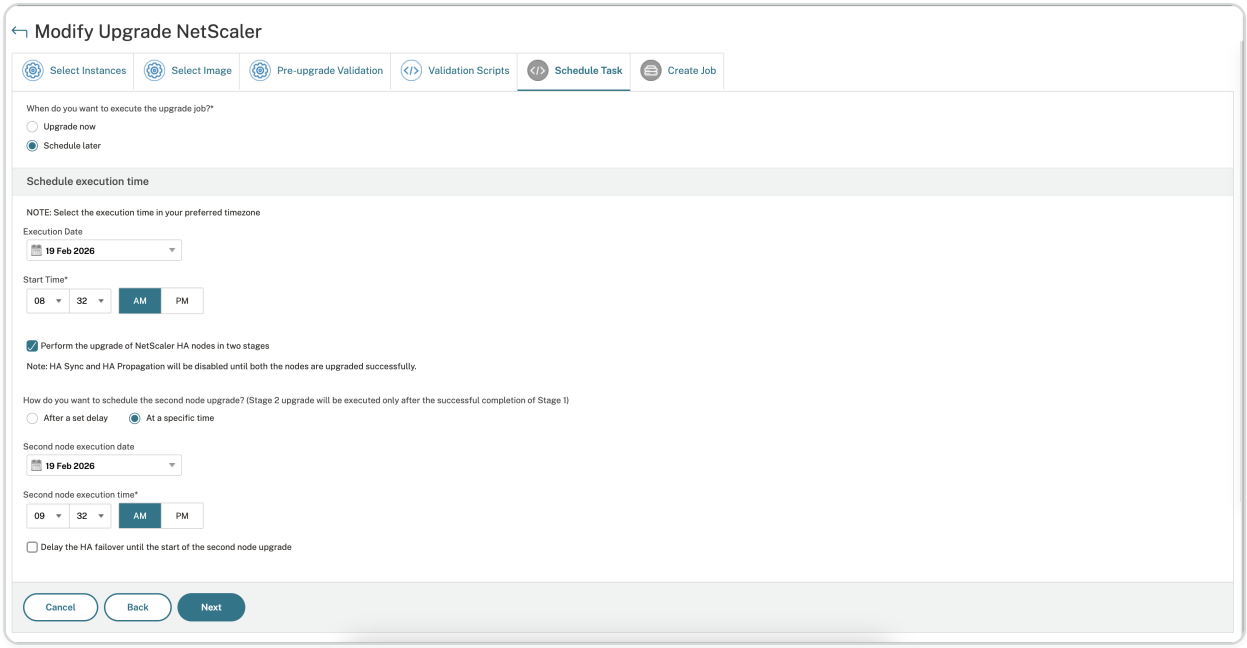
1. 导航到 **基础架构 > 升级作业**。单击 **创建作业**。
2. 选择 **配置 NetScaler 实例的 HA 对** 并单击 **继续**。
3. 在 **NetScaler HA 对** 页面上的 **实例选择** 选项卡中：
   a. 添加 **任务名称**。
   b. 选择主 IP 地址。
   c. 输入主 RPC 节点密码。
   d. 选择辅助 IP 地址。

   > **注意：**
   >
   > RPC 节点密码字段在 NetScaler 14.1 及更高版本中可用。

   e. 输入辅助 RPC 节点密码。
   f. 如果您的 HA 对实例位于两个子网中，请单击以启用 **启用 INC（独立网络配置）模式**。
4. 在 **计划任务** 选项卡上，选择以下选项之一：
   - **立即升级**：选择此选项以立即升级 NetScaler 实例。单击 **完成**。
   - **稍后安排**：选择此选项可稍后升级 NetScaler HA 对。
5. 如果选择“**稍后安排**”选项，请选择升级 NetScaler 实例的“**执行日期**”和“**开始时间**”。
   a. 选择“**分两个阶段执行 NetScaler HA 节点的升级**”。选择此选项后，HA 同步和 HA 传播将禁用，直到两个节点都成功升级。
   b. 选择以下选项之一来安排辅助节点升级。使用此选项，只有在阶段 1 成功完成后，才会运行阶段 2 升级。
      - **在设定的延迟后**：指定第一个节点升级完成后到第二个节点升级开始前的延迟（以小时为单位）。
      - **在特定时间**：选择辅助节点升级的日期和时间。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. 选择“**延迟 HA 故障转移，直到辅助节点升级开始**”。单击“**下一步**”。
7. 在“**计划任务**”选项卡上，从“**执行模式**”列表中选择“**立即**”以立即升级 NetScaler 实例，然后单击“**完成**”。



8. 您还可以启用电子邮件和 Slack 通知，以接收创建 NetScaler HA 对的执行报告。选中“**通过电子邮件接收执行报告**”复选框和“**通过 Slack 接收执行报告**”复选框以启用通知。

   有关配置电子邮件分发列表和 Slack 频道的更多信息，请参阅计划升级 NetScaler 实例中的**步骤 8**。

计划将 HA 实例对转换为群集

1. 导航到“**基础结构 > 升级作业**”。单击“**创建作业**”。
2. 选择“**将 HA 实例对转换为 2 节点群集**”，然后单击“**继续**”。
3. 在“**将 NetScaler HA 迁移到群集**”页面上，在“**实例选择**”选项卡中，添加“**任务名称**”。指定主 IP 地址、辅助 IP 地址、主节点 ID、辅助节点 ID、群集 IP 地址、群集 ID 和背板，然后单击“**下一步**”。
4. 在“**计划任务**”选项卡上，从“**执行模式**”列表中选择“**立即**”以立即升级 NetScaler 实例，然后单击“**完成**”。
5. 要稍后升级，请从“**执行模式**”列表中选择“**稍后**”。然后，您可以选择升级 NetScaler HA 对实例的“**执行日期**”和“**开始时间**”，然后单击“**完成**”。
6. 您还可以启用电子邮件和 Slack 通知，以接收升级 NetScaler SDX 实例的执行报告。单击“**通过电子邮件接收执行报告**”复选框和“**通过 Slack 接收执行报告**”复选框以启用通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关配置电子邮件分发列表和 Slack 频道的更多信息，请参阅计划升级 NetScaler 实例中的**步骤 8**。

使用作业升级 NetScaler® 实例

您可以使用 NetScaler Console 升级一个或多个 NetScaler 实例。在升级实例之前，您必须了解许可框架和许可证类型。

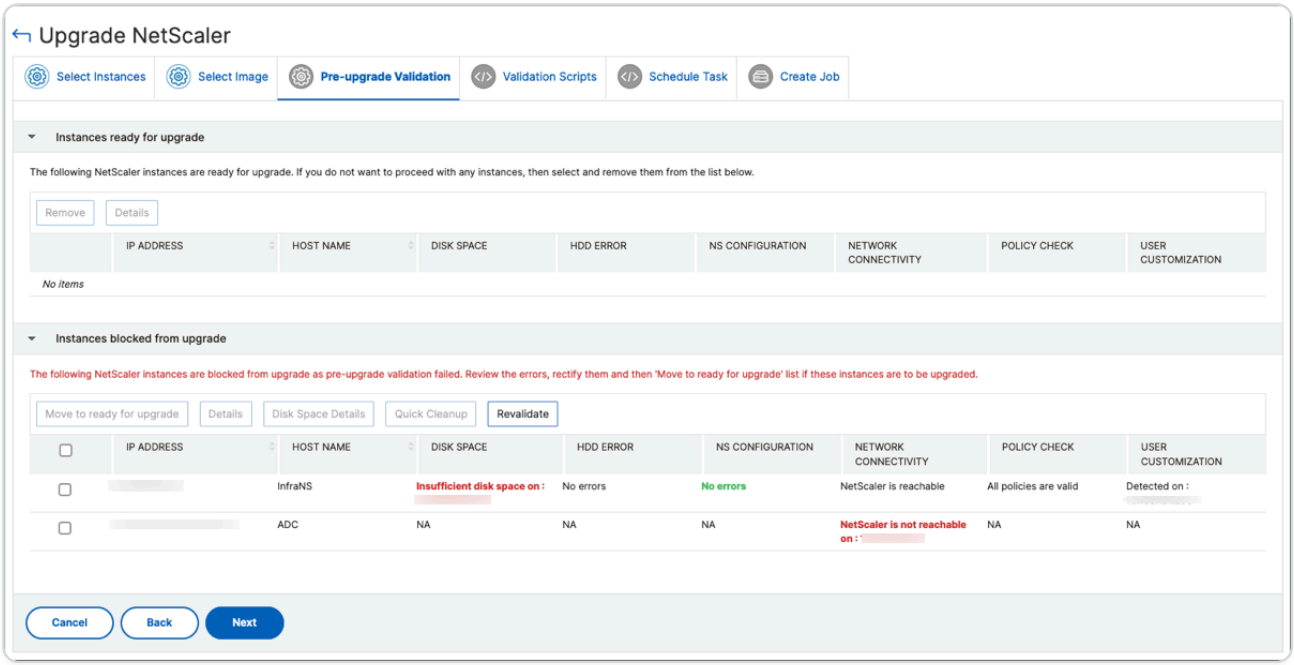
注意： 如果要升级具有经典策略的实例，建议您在使用 NSPEPI 工具升级实例之前，将经典策略转换为高级策略。这适用于 NSPEPI 工具支持的功能。有关更多信息，请参阅具有经典策略的配置的升级注意事项。

通过创建维护作业升级 NetScaler 实例时，请对要升级的实例执行预验证检查。

预验证检查

1. **检查自定义项** - 备份您的自定义项并将其从实例中删除。您可以在实例升级后重新应用已备份的自定义项。
2. **检查磁盘使用情况** - 如果 `/var` 文件夹的空间小于 6 GB，且 `/flash` 文件夹的空间小于 200 MB，请清理磁盘空间。检查以下文件夹路径以清理磁盘空间：
   - `/var/nstrace`
   - `/var/log`
   - `/var/nslog`
   - `/var/tmp/support`
   - `/var/core`
   - `/var/crash`
   - `/var/nsinstall`
   - `/var/netscaler/nsbackup`
3. **检查磁盘硬件问题** - 如果存在硬件问题，请解决。
4. **检查 STAYPRIMARY 和 STAYSECONDARY 节点** - 对于 NetScaler HA，处于 STAYPRIMARY 和 STAYSECONDARY 状态的节点将阻止升级。这些节点在预验证检查中被识别，并列在“**阻止升级的实例**”下。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler 高可用性对

升级 NetScaler HA 对时，请注意以下事项：

- 首先升级辅助节点。
- 在两个节点都成功升级之前，节点同步和传播将处于禁用状态。
- HA 对成功升级后，执行历史记录中会出现一条错误消息。如果 HA 对中的节点处于不同的内部版本或版本，则会出现此消息。此消息表示主节点和辅助节点之间的同步已禁用。

您可以分两个阶段升级 NetScaler HA 对：

1. 创建升级作业并立即在一个节点上运行，或稍后安排运行。
2. 稍后安排升级作业在剩余节点上运行。请务必在初始节点升级后安排此作业。

NetScaler 群集

升级 NetScaler 群集时，NetScaler Console 仅对指定实例执行升级前验证。在升级之前，请检查并解决群集节点上的自定义、磁盘使用情况和硬件问题。

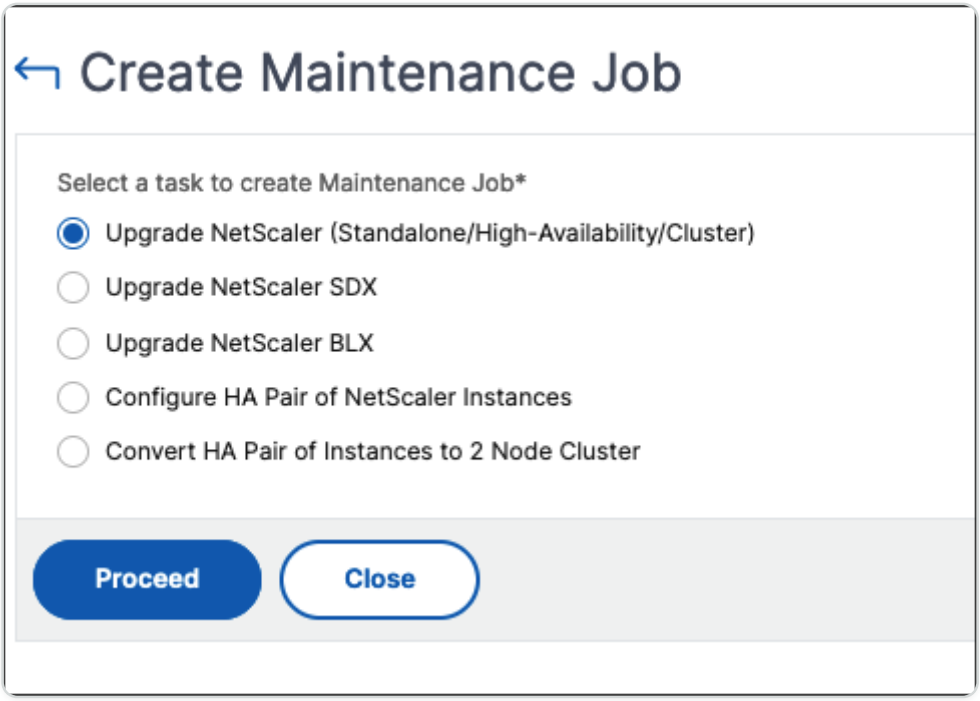
创建升级维护作业以升级 NetScaler 实例

注意

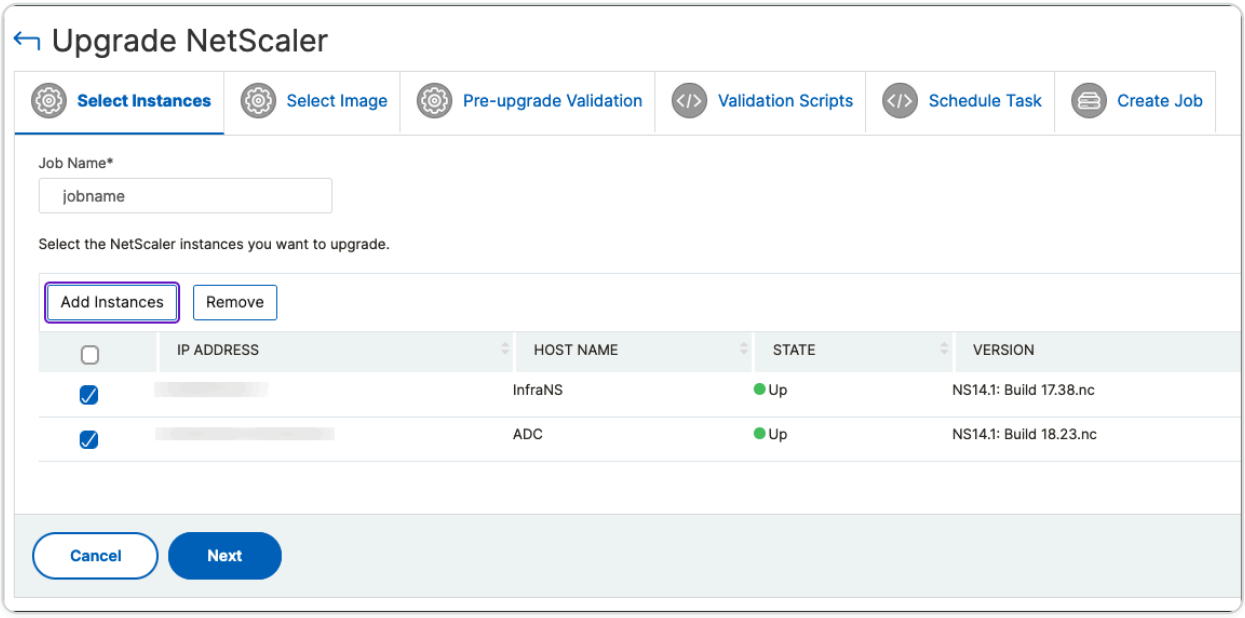
NetScaler 不支持从更高版本升级到更低版本。例如，如果您的 NetScaler 实例是 13.0 82.x，则无法将 NetScaler 实例降级到 13.0 79.x 或任何其他早期版本。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 在 NetScaler Console 中，导航到 **Infrastructure > Upgrade Jobs**。单击 **Create Job** 按钮。
2. 在 **创建维护作业** 中，选择 **升级 NetScaler（独立/高可用性/集群）**，然后单击 **继续**。



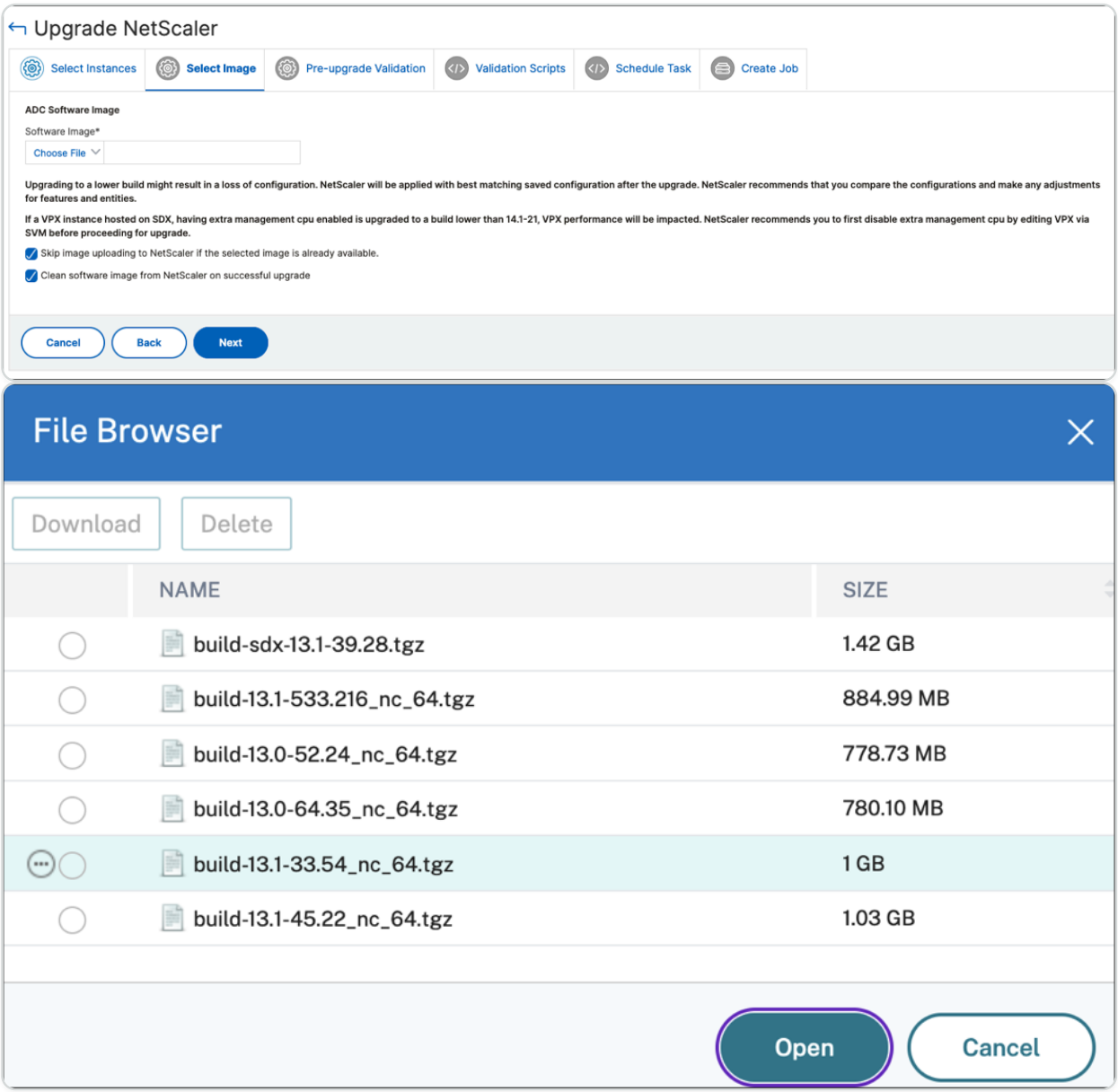
3. 在 **Select Instance** 中，为 **Job Name** 键入您选择的名称。
4. 单击 **Add Instances** 以添加要升级的 NetScaler 实例。
   - 要升级 NetScaler 高可用性对，请选择高可用性对的 IP 地址（由“S”和“P”的上标表示）。
   - 要升级群集，请选择群集 IP 地址（由“C”的上标表示）。



5. 在 **Select Image** 选项卡中，从本地驱动器或构建映像中选择 NetScaler 映像。
   - **Local** - 从本地计算机中选择实例升级文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Appliance** - 从 NetScaler Console 文件浏览器中选择实例升级文件。NetScaler Console GUI 显示 `/var/mps/ns_images` 处存在的实例文件。



- **如果所选映像已可用，则跳过将映像上传到 NetScaler** - 此选项检查所选映像在 NetScaler 中是否可用。升级作业会跳过上传新映像，并使用 NetScaler 中可用的映像。
- **成功升级后从 NetScaler 清理软件映像** - 此选项在实例升级后清除 NetScaler 实例中上传的映像。

单击**下一步**以开始对所选实例进行升级前验证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

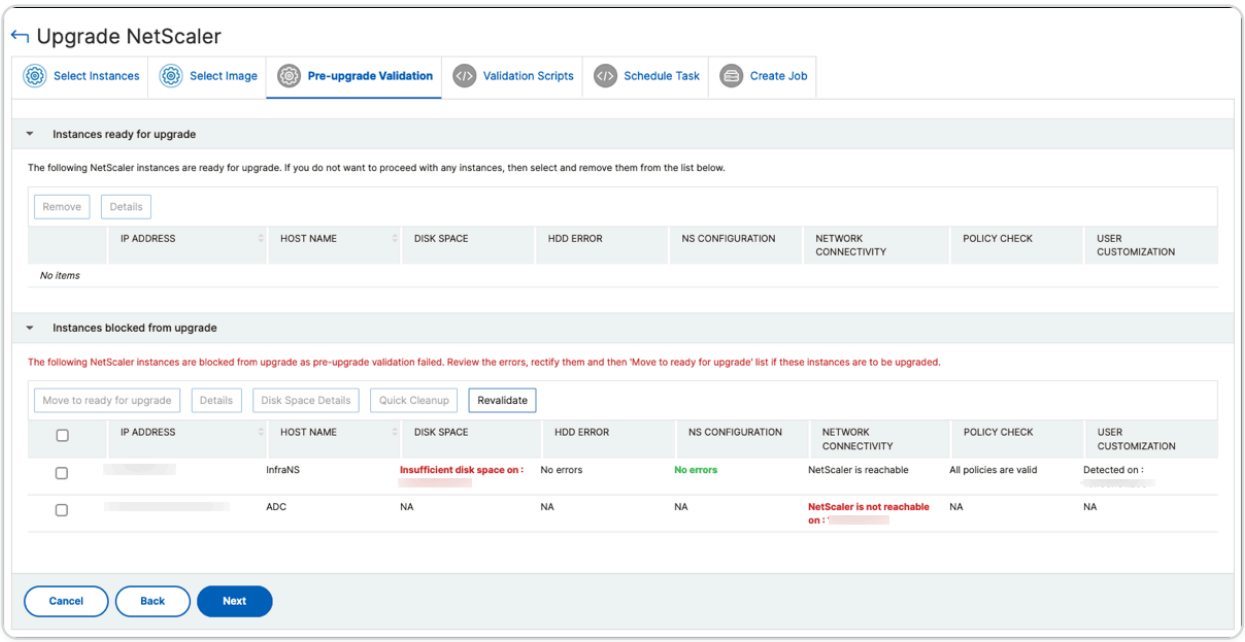
注意：

- 下载的 NetScaler 映像存储在 NetScaler Console 代理中，并位于 `/var/mps/adcimages`。这些缓存的映像可用于多次 NetScaler 升级，从而无需每次升级都下载映像。
- NetScaler Console 会根据映像的上次修改时间，每三天清除一次缓存的 NetScaler 映像。NetScaler Console 代理一次只缓存最新的两个映像文件。

6. **升级前验证**选项卡显示以下部分：

   - **准备升级的实例**。您可以继续升级这些实例。
   - **阻止升级的实例**。由于升级前验证错误，这些 NetScaler 实例被阻止升级。

   您可以查看、纠正错误，然后单击**移至准备升级**以升级它们。如果实例上磁盘空间不足，您可以检查并清理磁盘空间。请参阅，清理 NetScaler 磁盘空间。



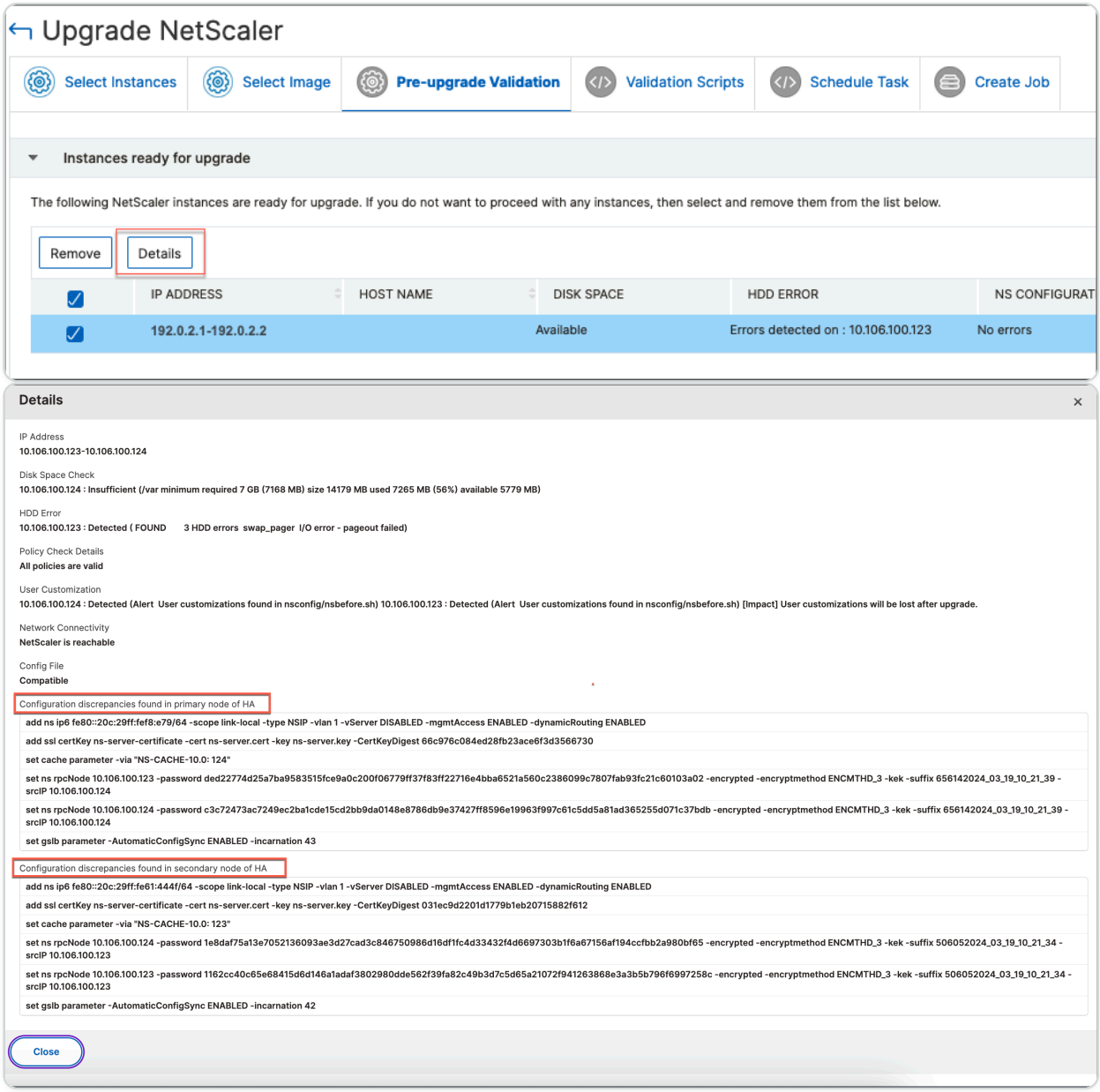
   - **策略检查**：如果 NetScaler Console 发现不支持的经典策略，您可以删除此类策略以创建升级作业。

重要提示：

如果指定群集 IP 地址，NetScaler Console 仅对指定的实例执行升级前验证，而不对其他群集节点执行。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要在升级期间查看主节点和辅助节点之间的差异，请选择高可用性节点，然后单击**详细信息**。



- **在 HA 主节点中发现的配置差异** - 显示在 NetScaler 高可用性对的辅助节点中找到但在主节点中缺失的所有配置。
- **在 HA 辅助节点中发现的配置差异** - 显示在 NetScaler 高可用性对的主节点中找到但在辅助节点中缺失的所有配置。

注意：

您可以忽略配置差异部分中可能出现的以下差异：

- 设备特定的配置，例如 IP 地址。
- 加密的密码或证书，即使密码相同，它们在节点之间也可能不同。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以查看这些差异，如果它们不相关，则选择忽略它们。

7. 在 **验证脚本** 中，指定在实例升级前后运行的脚本。您可以执行以下任一操作：

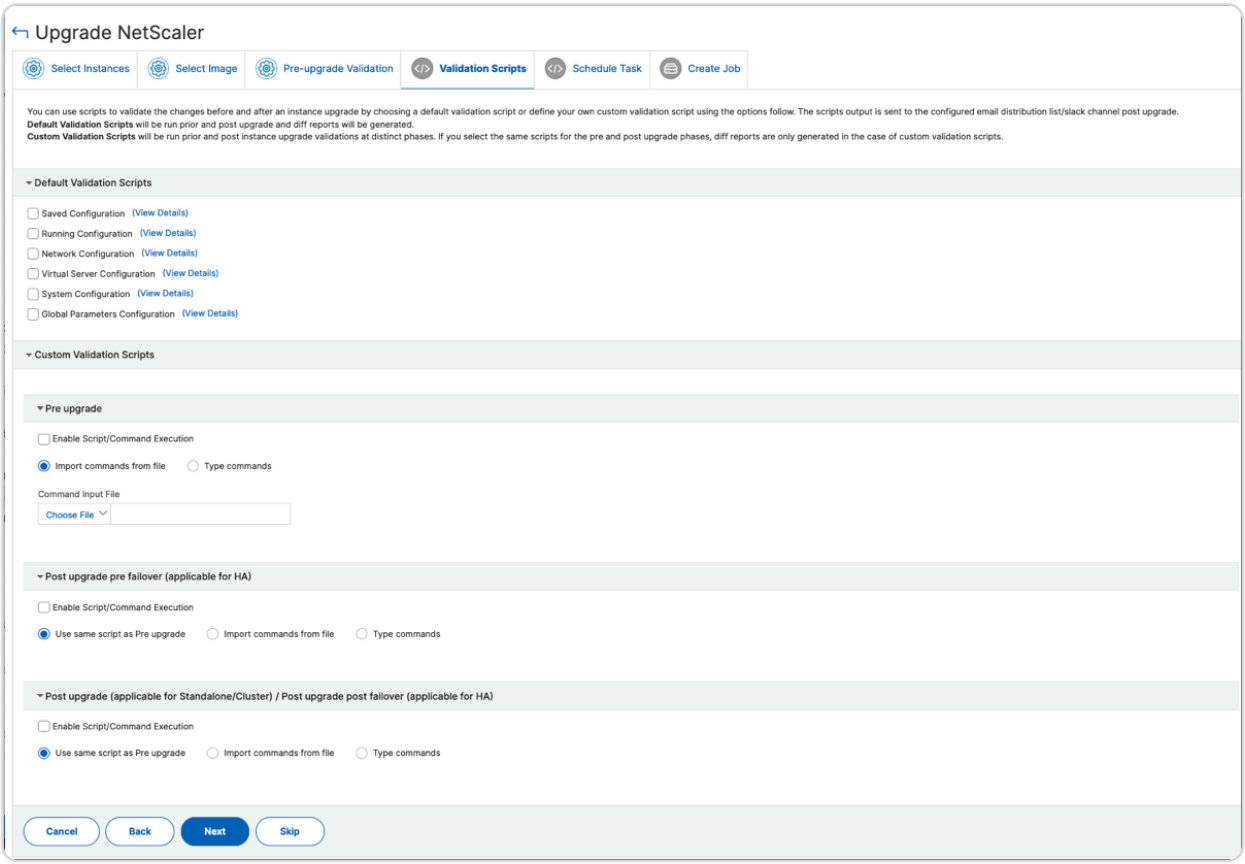
   - **默认验证脚本** - 选择此选项以运行预定义的验证脚本。这些脚本在升级作业之前和之后运行，为验证脚本生成差异报告。

     注意：

     您无法更改或编辑此预定义命令集。

   - **自定义验证脚本** - 选择此选项以运行您的验证脚本。您可以指定是希望在升级之前还是之后运行脚本。仅当在升级前后选择了相同的脚本时，才会生成差异报告。

   要了解每个配置中的命令集，请单击 **查看详细信息**。



   在 **自定义验证脚本** 中，指定在实例升级前后运行的脚本。使用以下方法之一运行 NetScaler CLI 命令：

   自定义脚本用于检查 NetScaler 实例升级前后的更改。例如：

   - 升级前后的实例版本。
   - 升级前后的接口、高可用性节点、虚拟服务器和服务的状态。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 虚拟服务器和服务的统计信息。
- 动态路由。

实例升级有多个阶段。您现在可以指定这些脚本在以下阶段运行：

- **升级前**：指定的脚本在升级实例之前运行。
- **升级后故障转移前（适用于 HA）**：此阶段仅适用于高可用性部署。指定的脚本在节点升级后但在其故障转移之前运行。
- **升级后（适用于独立部署）/ 升级后故障转移后（适用于 HA）**：指定的脚本在独立部署中升级实例后运行。在高可用性部署中，脚本在节点升级及其故障转移后运行。

> **注意：**
>
> 确保在所需阶段启用脚本执行。否则，指定的脚本将不会运行。

您可以在 NetScaler Console GUI 中直接导入脚本文件或键入 NetScaler CLI 命令。

- **使用与升级前相同的脚本**：对升级前、故障转移前和升级后使用相同的自定义脚本。
- **从文件导入命令**：从本地计算机中选择 NetScaler CLI 命令输入文件。
- **键入命令**：直接在 GUI 上输入 NetScaler CLI 命令。

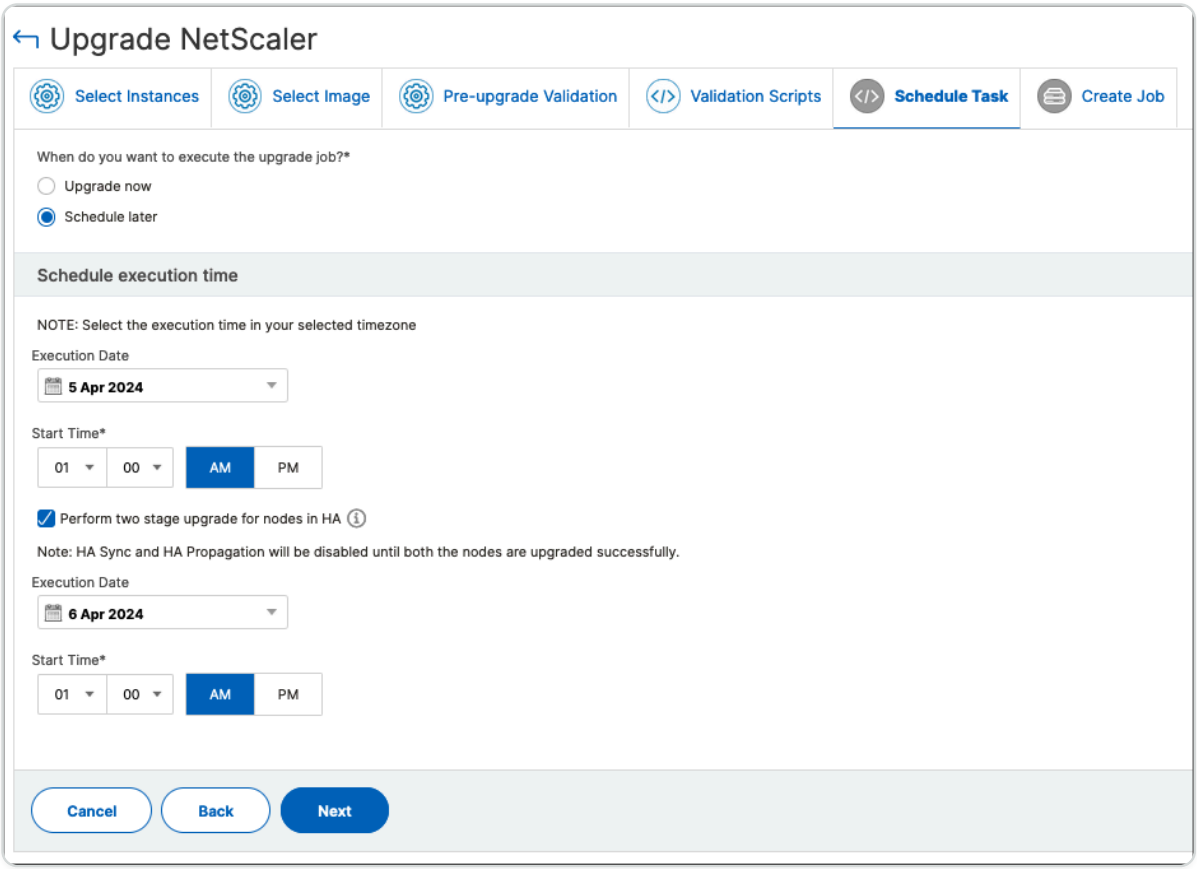
8. 在“**计划任务**”中，选择以下选项之一：

   - **立即升级** - 升级作业将立即运行。
   - **稍后计划** - 选择此选项可稍后运行此升级作业。指定您要升级实例的“**执行日期**”和“**开始时间**”。

     如果要分两个阶段升级 NetScaler HA 对，请选择“**对 HA 中的节点执行两阶段升级**”。

     指定“**执行日期**”和“**开始时间**”，以升级 HA 对中的另一个实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. 在“**创建作业**”中，指定以下详细信息：

   a. 从“**软件映像**”列表中选择以下选项之一：

      - **本地** - 从本地计算机中选择实例升级文件。
      - **设备** - 从文件浏览器中选择实例升级文件。NetScaler Console GUI 显示 `/var/mps/mps_images` 处存在的实例文件。

   b. 指定何时将映像上传到实例：

      - **立即上传** - 选择此选项可立即上传映像。但是，升级作业将在计划时间运行。
      - **在执行时上传** - 选择此选项可在升级作业执行时上传映像。

      对于高可用性对，您可以指定要上传映像的节点：

      - **上传到主节点和辅助节点**：将构建镜像文件上传到主节点和辅助节点。
      - **仅上传到辅助节点**：仅将构建镜像文件上传到辅助节点。辅助节点升级后，会发生故障转移，构建镜像文件将上传到新的辅助节点（即之前的主节点）。

   NetScaler 高可用性节点升级(/en-us/netscaler-application-delivery-management-software/media/upgrade-create-job-ns.png)

   有关高可用性对的可用调度方案的更多信息，请参阅为高可用性对调度升级作业。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **成功升级后从 NetScaler 清理软件镜像** - 选择此选项可在实例升级后清除 NetScaler 实例中上传的镜像。
- **在开始升级之前备份 NetScaler 实例。** - 创建所选 NetScaler 实例的备份。
- **升级后保持 HA 节点的主备状态**：如果您希望升级作业在每个节点升级后启动故障转移，请选择此选项。这样，升级作业将保持节点的主备状态。
- **在开始升级之前保存 NetScaler 配置** - 在升级 NetScaler 实例之前保存正在运行的 NetScaler 配置。
- **启用 ISSU 以避免 NetScaler HA 对的网络中断** - ISSU 确保 NetScaler 高可用性对的零停机升级。此选项提供迁移功能，可在升级期间保留现有连接。因此，您可以零停机升级 NetScaler HA 对。以分钟为单位指定 ISSU 迁移超时。
- **通过电子邮件接收执行报告** - 通过电子邮件发送执行报告。要添加电子邮件分发列表，请参阅创建电子邮件分发列表。
- **通过 Slack 接收执行报告** - 通过 Slack 发送执行报告。要添加 Slack 配置文件，请参阅创建 Slack 配置文件。

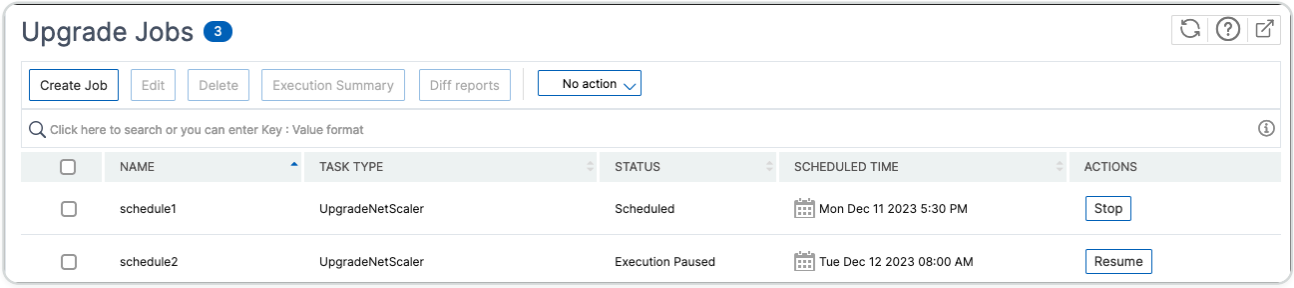
单击**创建作业**。

升级作业显示在**基础架构 > 升级作业**中。编辑现有作业时，如果必填字段已填写，则可以切换到任何选项卡。例如，如果您在**选择配置**选项卡中，则可以切换到**作业预览**选项卡。

暂停或恢复计划的升级作业

您还可以暂停计划的升级作业。

要使用此功能，请导航到 **Infrastructure > Upgrade Jobs**，选择一个现有的计划升级作业，然后单击 **Stop** 以暂停该作业。要恢复计划升级作业，请单击 **Resume**。



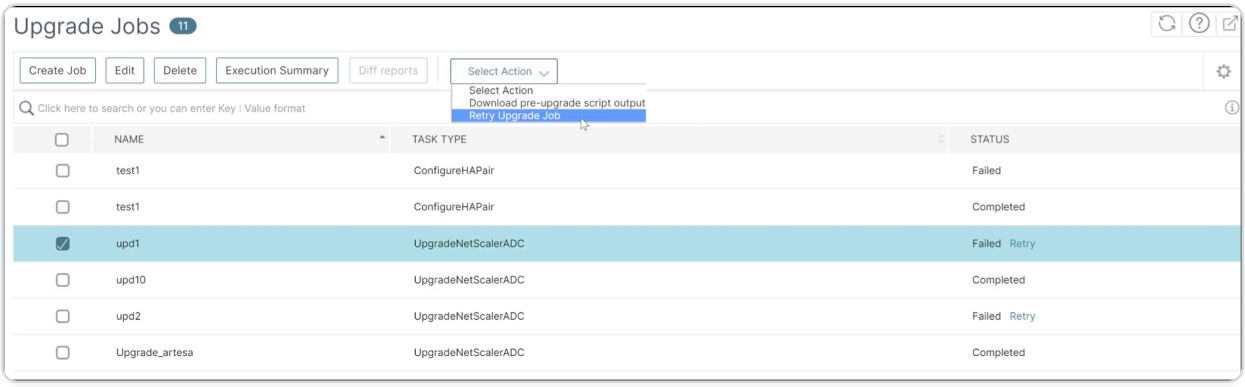
注意：

如果决定恢复升级作业后，其计划时间已过，则需要重新创建该升级作业。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重试失败的升级作业

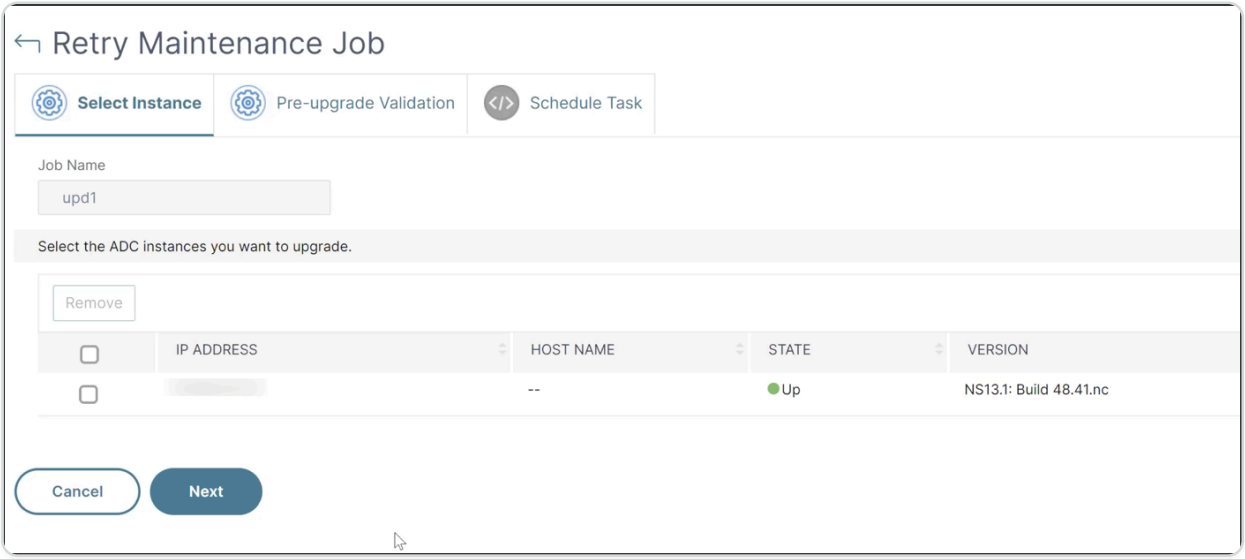
1. 在 **Infrastructure > Upgrade Jobs** 中，选择失败的升级作业，然后单击 **Retry**。或者，您也可以转到 **Select Action > Retry Upgrade Job** 以重试失败的作业。



2. 在 **Select Instance** 中，指定以下详细信息：

   - **作业名称** - 输入升级的名称。
   - 从列表中选择要升级的 NetScaler 实例。要删除任何实例，请单击 **Remove**。

   单击 **Next** 开始验证过程。

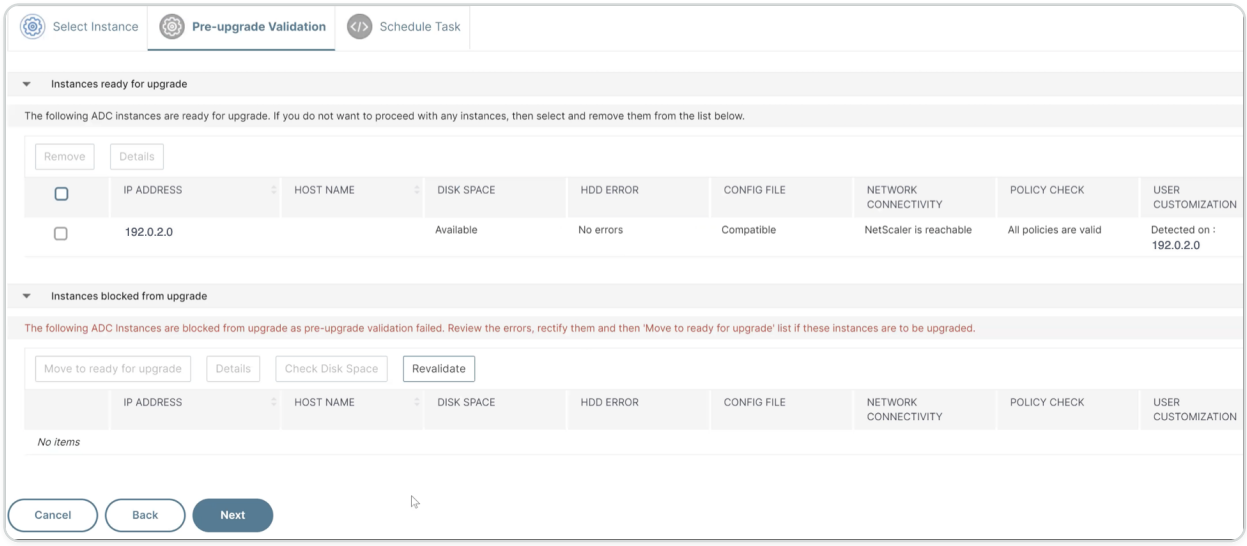


3. **升级前验证**选项卡显示以下部分：

   - **准备升级的实例**。您可以继续升级这些实例。
   - **被阻止升级的实例**。这些 NetScaler 实例因升级前验证错误而被阻止升级。

     您可以查看、纠正错误，然后点击 **Move to ready for upgrade** 来升级它们。如果实例上磁盘空间不足，您可以检查并清理磁盘空间。请参阅，清理 NetScaler 磁盘空间。
   - **策略检查**：如果 NetScaler Console 发现不支持的经典策略，您可以删除此类策略以创建升级作业。

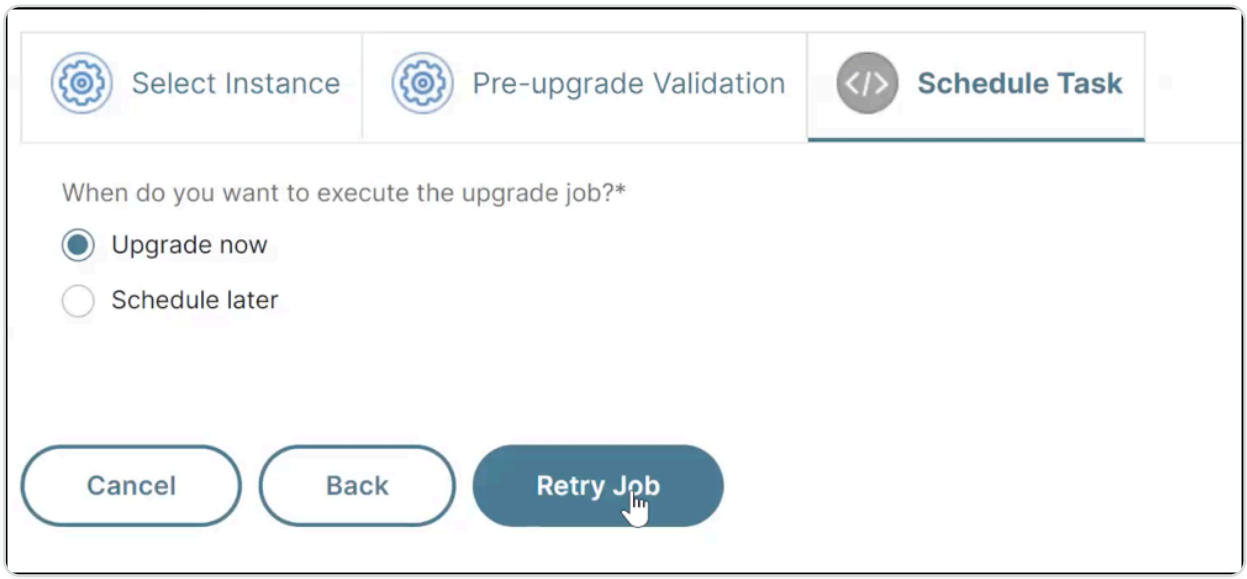
© 1997–2026 Citrix Systems, Inc. All rights reserved.



点击 **Next**。

4. 在 **Schedule Task** 中，选择以下选项之一：

   - **立即升级**：升级作业会立即运行。
   - **稍后计划**：选择此选项可稍后运行此升级作业。指定您要升级实例的**执行日期**和**开始时间**。



点击 **Retry**。

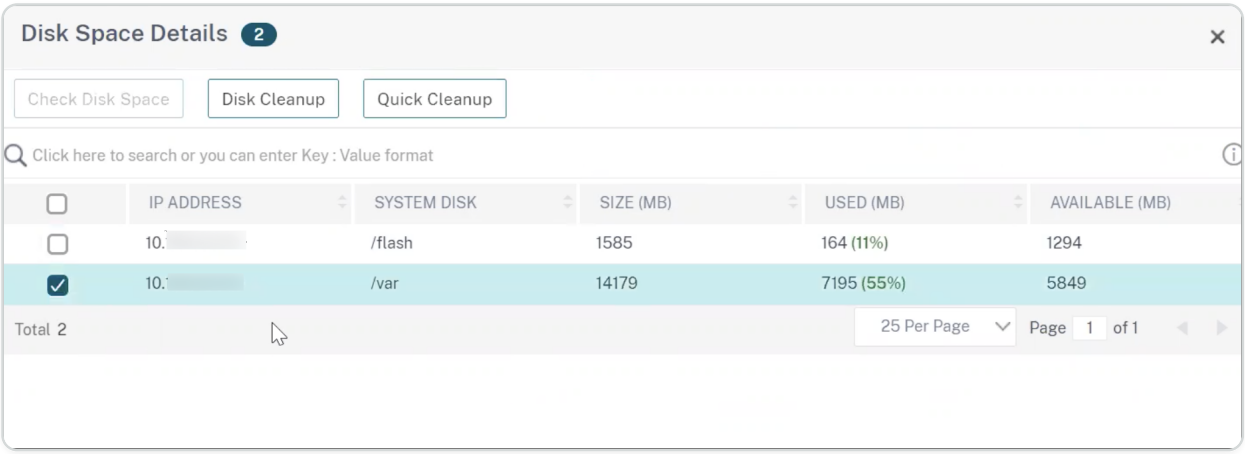
清理 NetScaler 磁盘空间

如果在升级 NetScaler 实例时遇到磁盘空间不足的问题，请直接从 NetScaler Console GUI 清理磁盘空间。

1. 在**升级前验证**选项卡中，**阻止升级的实例**部分显示因磁盘空间不足而升级失败的实例。选择存在磁盘空间问题的实例。
2. 点击 **检查磁盘空间**。

   将显示**磁盘空间详细信息**页面。此页面显示实例、已用内存和可用内存。

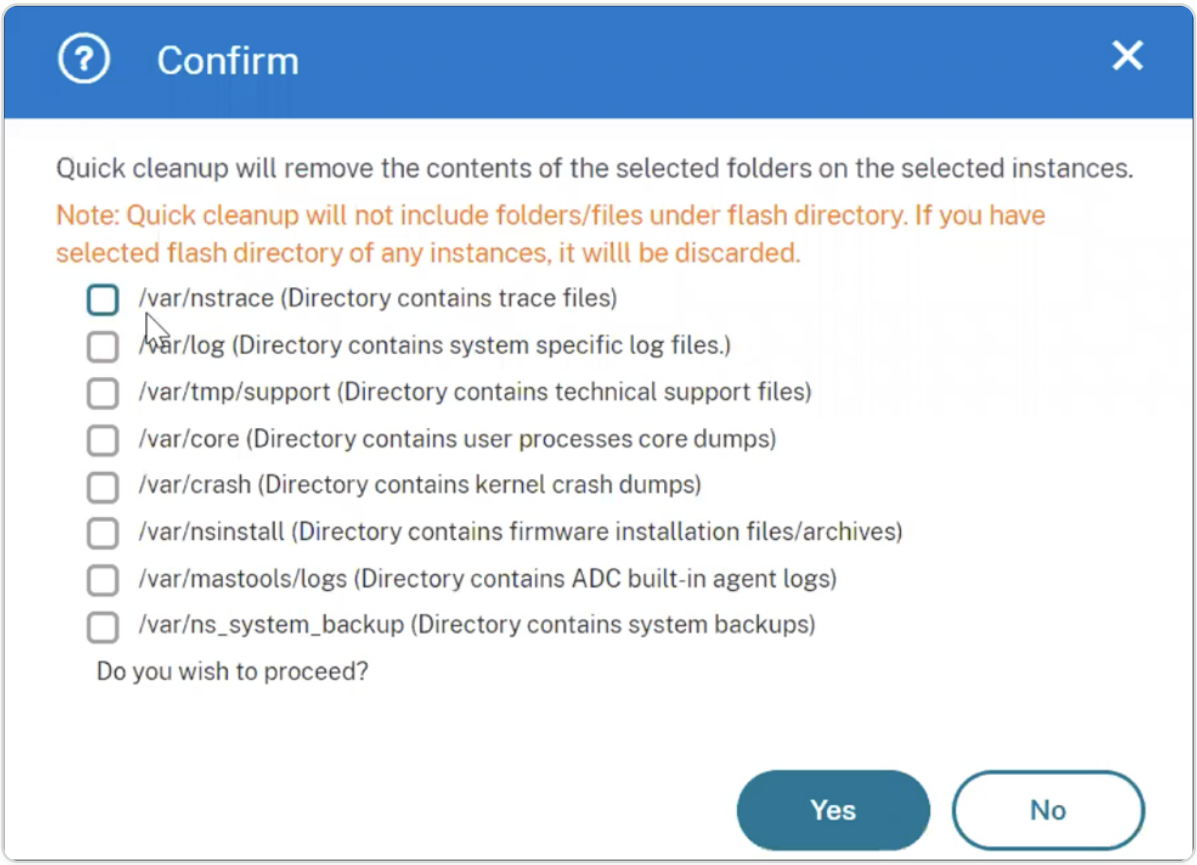
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 在“**磁盘空间详细信息**”窗格中，选择需要清理的实例，然后执行以下操作之一：

   a. **磁盘清理** - 导航到所需的文件夹或目录并将其删除以释放磁盘空间。

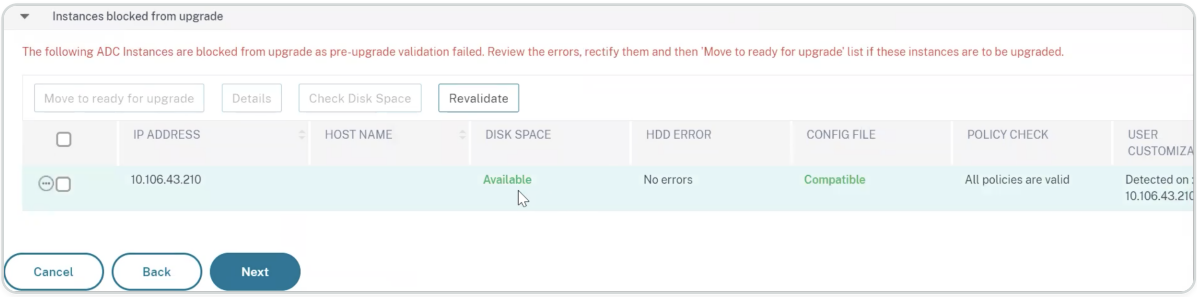
   b. **快速清理** - 通过删除多个文件夹快速清理磁盘空间。在出现的“**确认**”窗格中，选择要删除的文件夹，然后单击“**是**”。



   c. 清理磁盘空间后，您可以检查是否有足够的磁盘空间来升级实例。在“**阻止升级的实例**”部分中，单击“**重新验证**”。

   在以下示例中，磁盘空间可用。您现在可以单击“**移至准备升级**”以升级实例，或单击“**下一步**”以继续执行下一步。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



为 NetScaler 高可用性对安排升级作业

下表列出了“**计划任务**”页面中的不同计划方案以及“**创建作业**”页面中相应的升级选项：

您希望何时执行升级作业？	您希望何时将软件映像上传到 NETSCALER？	您希望如何将构建映像上传到 HA 节点？
立即升级	不适用	**上传到主节点和辅助节点**（默认选项）
	仅上传到辅助节点	
稍后安排	**在执行时上传**（默认选项）	**上传到主节点和辅助节点**（默认选项）
	仅上传到辅助节点	
	立即上传	不适用
稍后安排（当选择“**对 HA 中的节点执行两阶段升级**”时）	**在执行时上传**（默认选项）	**仅上传到辅助节点**（默认且唯一选项）
	立即上传	不适用

下载 NetScaler 升级作业的组合差异报告

如果指定了自定义脚本，您可以下载 NetScaler 升级作业的差异报告。差异报告包含升级前和升级后脚本输出之间的差异。通过此报告，您可以确定 NetScaler 实例在升级后发生了哪些更改。

注意

差异报告仅在您在升级前和升级后阶段指定相同脚本时生成。

要下载升级作业的差异报告，请执行以下操作：

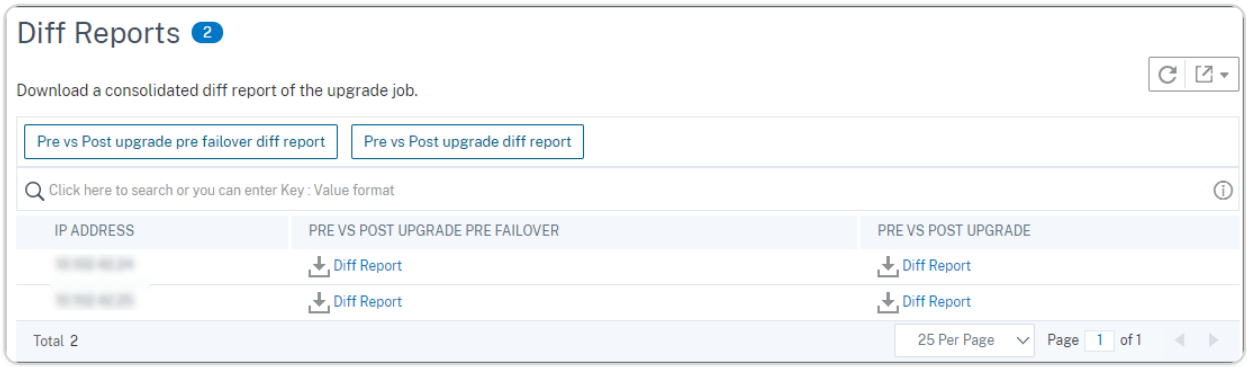
1. 导航到 **基础设施 > 升级作业**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 选择要下载差异报告的升级作业。
3. 单击 **Diff Reports**。
4. 在 **Diff Reports** 中，下载所选升级作业的合并差异报告。

   在此页面中，您可以下载以下任何差异报告：

   - **升级前与升级后故障转移前差异报告**
   - **升级前与升级后差异报告**



安全咨询

安全、可靠且具有弹性的基础设施是任何组织的生命线。组织必须跟踪新的常见漏洞和披露 (CVE)，并评估 CVE 对其基础设施的影响。他们还必须了解并规划补救措施以解决这些漏洞。

NetScaler Console 中的安全咨询功能使您能够：

- 分析您的 NetScaler 配置设置，以识别任何可能使您的系统面临攻击的错误配置、薄弱环节或偏离最佳实践的情况。
- 跟踪任何新的常见漏洞和披露 (CVE)，评估 CVE 的影响，了解补救措施，并解决这些漏洞。
- 检查您的 NetScaler 构建文件的完整性。

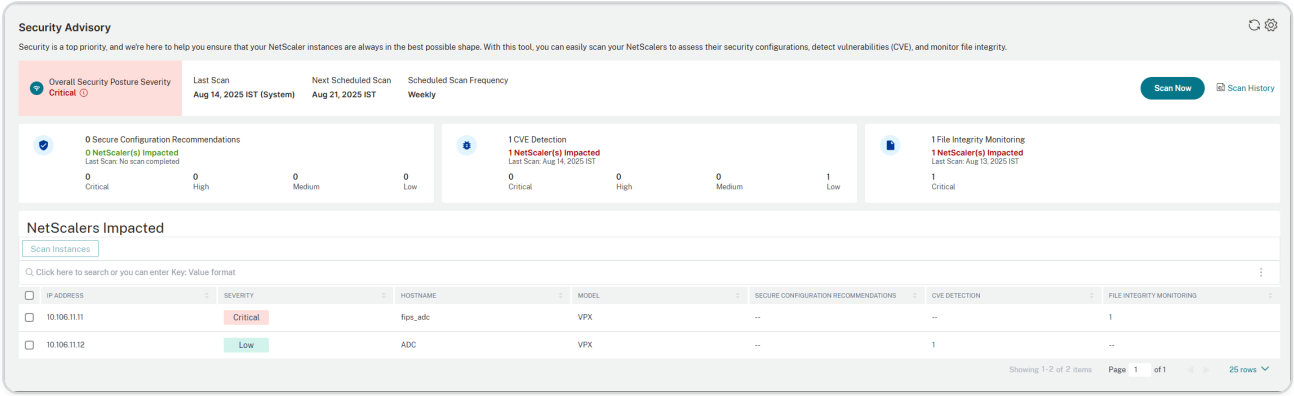
安全咨询登录页面

安全咨询登录页面提供了您的 NetScaler 部署安全状况的全面概览。该界面经过增强和设计，旨在为管理员和安全专业人员提供对其 NetScaler 基础设施整体健康状况和漏洞状态的即时洞察。

NetScaler Console 提供三种类型的安全咨询：

- **安全配置建议** - 使您能够根据最佳实践配置 NetScaler 实例。
- **常见漏洞和披露 (CVE) 检测** - 使您能够识别使您的 NetScaler 实例面临风险的 CVE，并推荐补救措施。
- **文件完整性监控** - 使您能够识别您的 NetScaler 构建文件是否已发生任何更改或添加。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler Console 安全咨询仪表板还包括以下内容：

- **整体安全态势严重性** - 表示安全态势的状态，并根据三种咨询类型的最大严重性计算。状态可以是以下之一：
  - **严重**：检测到多项严重程度的观察结果，必须以最高优先级处理。
  - **高**：检测到必须立即修复的严重漏洞或错误配置。尽管不如严重发现那样紧急，但这些问题对安全性和稳定性构成重大风险。
  - **中**：必须及时处理的重要安全观察结果。这些问题不会构成即时的严重威胁，但如果置之不理，可能会被利用或导致更严重的问题。
  - **低**：不构成重大安全风险的次要安全问题或最佳实践违规。尽管它们不是即时威胁，但修复这些问题以改善整体安全状况仍然是一个好主意。
- **上次扫描** - 上次扫描的日期。仪表板中提供的数据基于上次扫描的结果。
- **下次计划扫描** - 下次计划系统扫描的日期。
- **计划扫描频率** - 系统扫描运行的频率。
- **立即扫描** - 允许按需扫描，使您可以在系统扫描计划之外，根据需要随时扫描实例。
- **扫描历史记录** - 提供在您的 NetScaler 实例上运行的所有扫描的历史视图。
- **受影响的 NetScaler** - 列出受影响的 NetScaler 实例。
- **设置** - 允许您根据需要配置系统扫描设置并设置事件通知。

借助仪表板上提供的信息，您可以快速识别关键漏洞、安全配置建议（包括缓解步骤）以及相关文档链接。

登录页面允许您按严重性和 NetScaler IP 地址筛选问题。当选择特定的严重性级别时，仅显示该严重性级别的 NetScaler 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要提示：

在 **安全建议** GUI 或报告中，并非所有 CVE 都可能显示，您可能只看到一个 CVE。作为一种变通方法，请单击 **立即扫描** 并选择 **CVE** 以运行按需扫描。扫描完成后，所有范围内的 CVE（大约 15 个）将显示在 UI 或报告中。-->

安全配置建议

安全配置建议选项卡提供对配置观察结果的深入实例级分析，旨在为用户提供可操作的见解。有关更多信息，请参阅安全配置建议。

CVE 检测

CVE 检测主要侧重于识别和缓解安全漏洞。有关更多信息，请参阅CVE 检测。

文件完整性监控

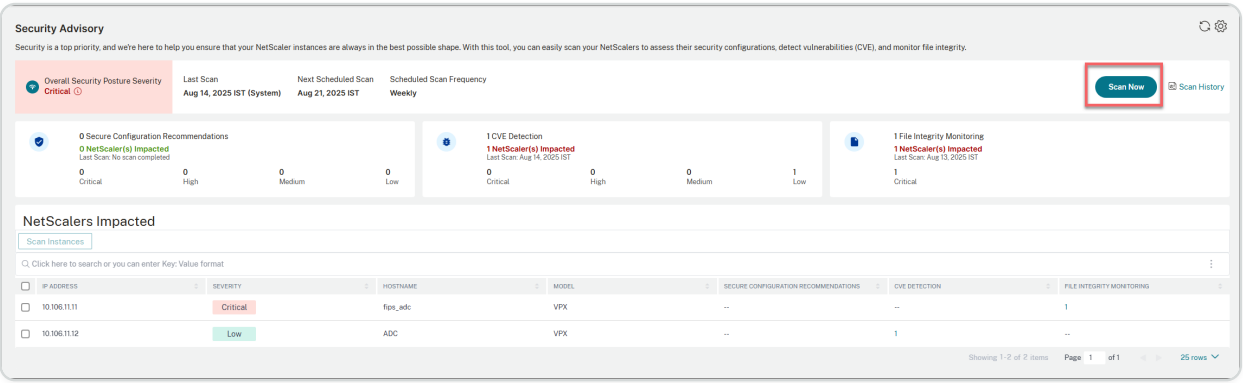
文件完整性监控检查 NetScaler 实例核心文件是否存在未经授权或恶意更改。它是安全建议的关键部分。有关更多信息，请参阅文件完整性监控。

立即扫描

您可以根据需要随时扫描实例，并根据您的安全要求选择要运行的扫描类型。

执行以下步骤运行扫描：

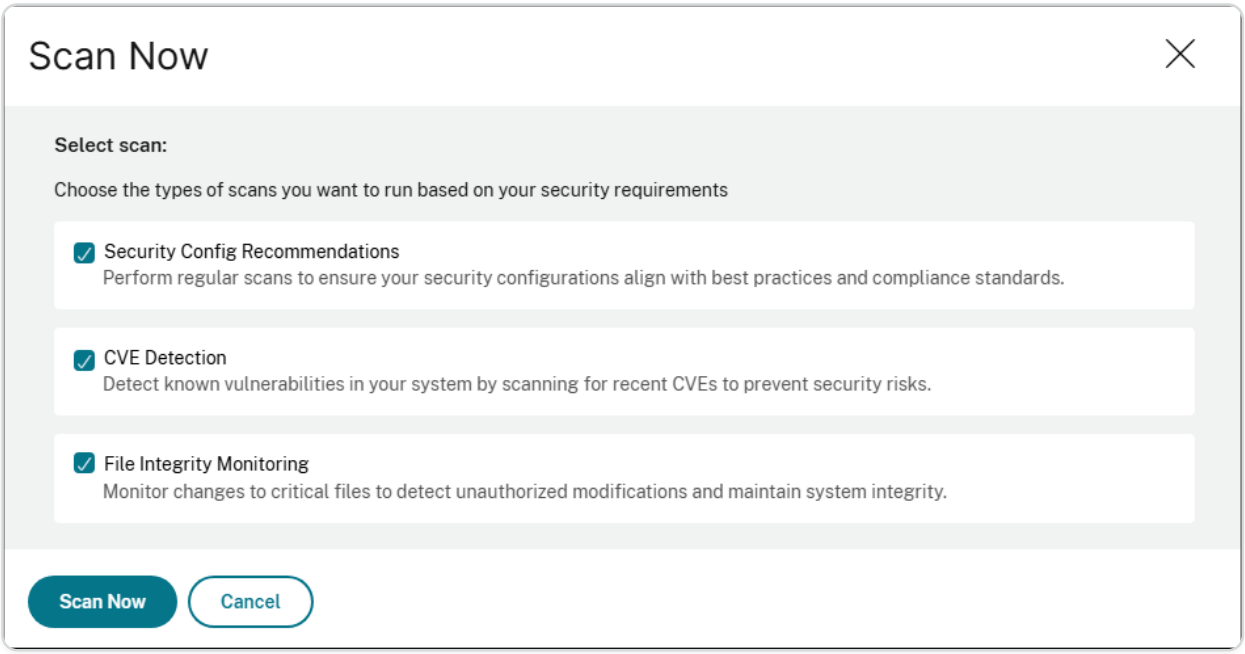
1. 单击**立即扫描**。



2. 选择要运行的扫描类型。

   - 安全配置建议
   - CVE 检测
   - 文件完整性监控

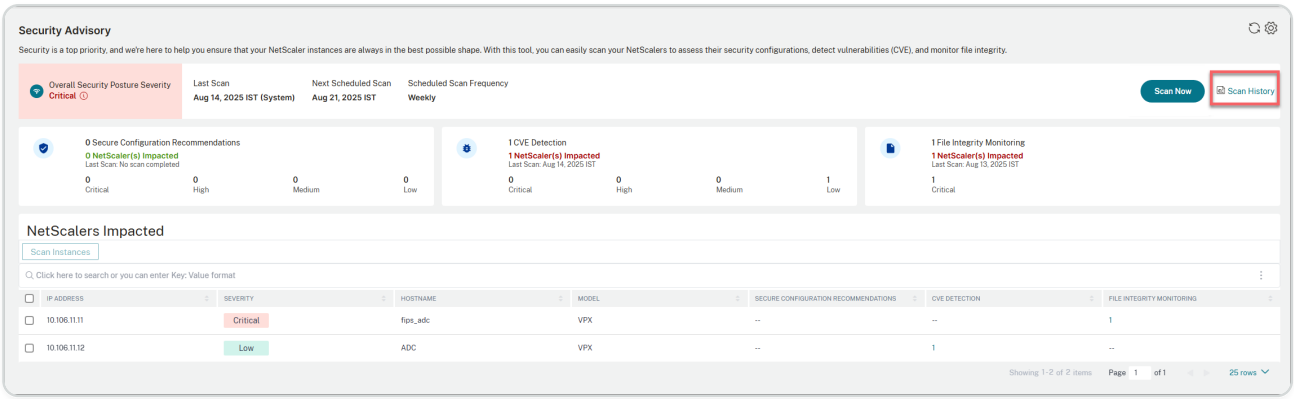
© 1997–2026 Citrix Systems, Inc. All rights reserved.



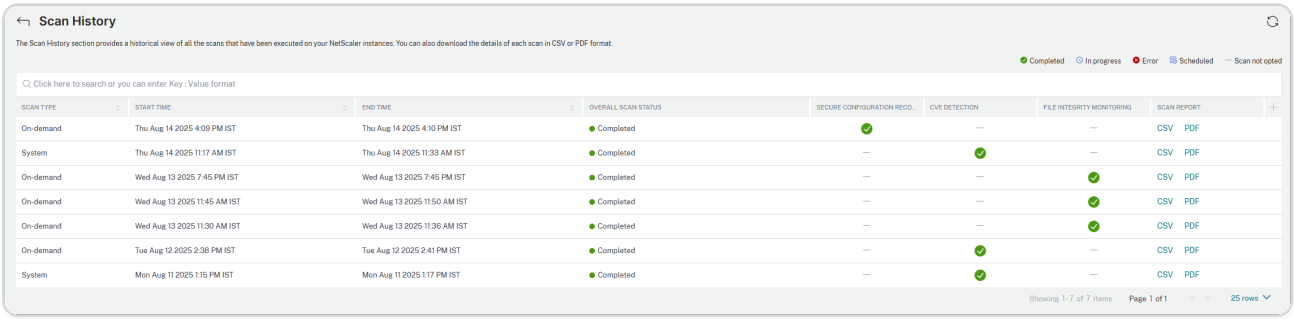
3. 单击**立即扫描**。扫描完成后，修订后的安全详细信息将显示在安全建议仪表板中。

扫描历史记录

单击**扫描历史记录**可查看在您的 NetScaler 实例上运行过的所有历史扫描。



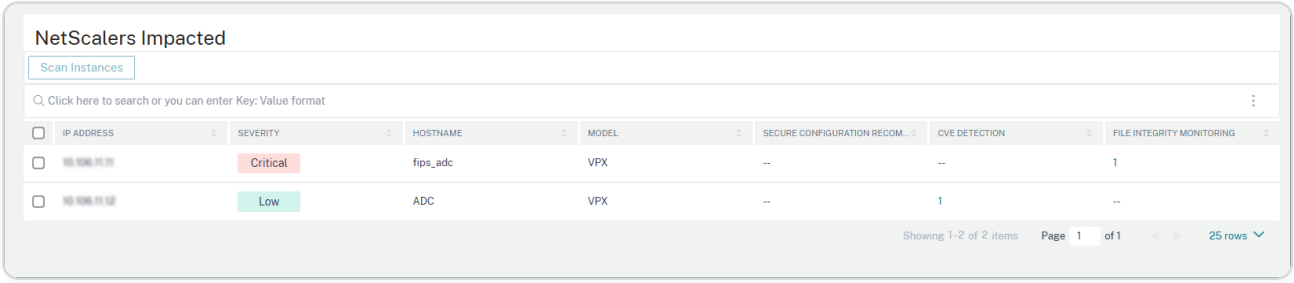
您可以查看扫描类型（按需扫描或系统扫描）、扫描的开始和结束时间、总体扫描状态，还可以下载 CSV 或 PDF 格式的每次扫描的详细信息。



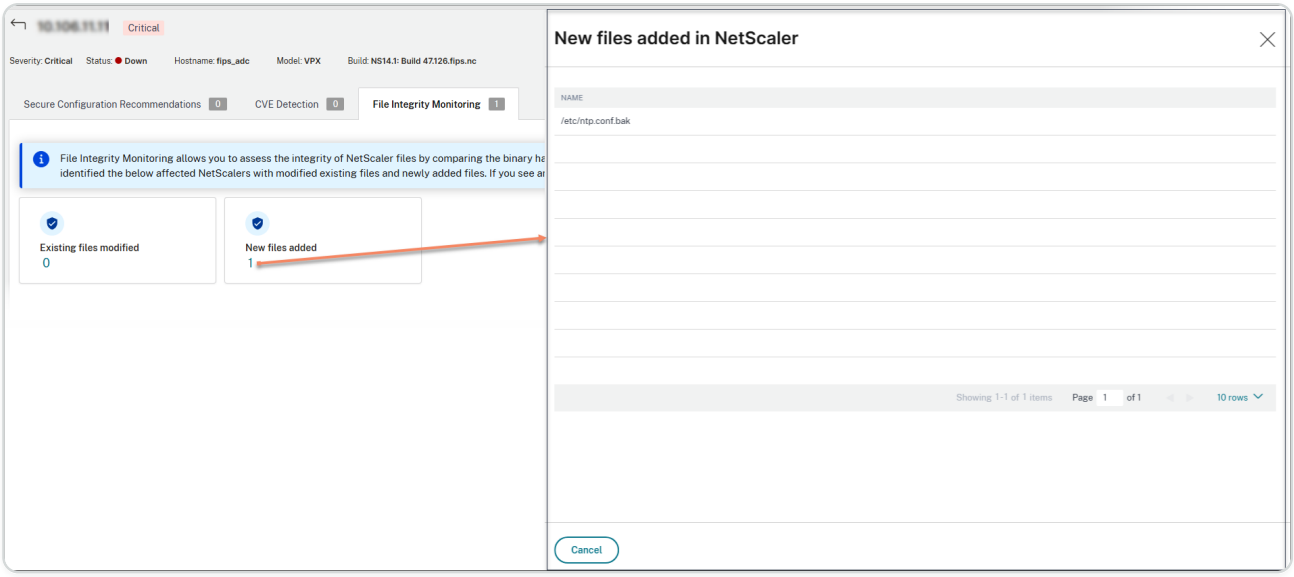
© 1997–2026 Citrix Systems, Inc. All rights reserved.

受影响的 NetScaler

受影响的 NetScaler 部分列出了受安全配置、CVE 和监视文件完整性检查影响的所有 NetScaler 实例。

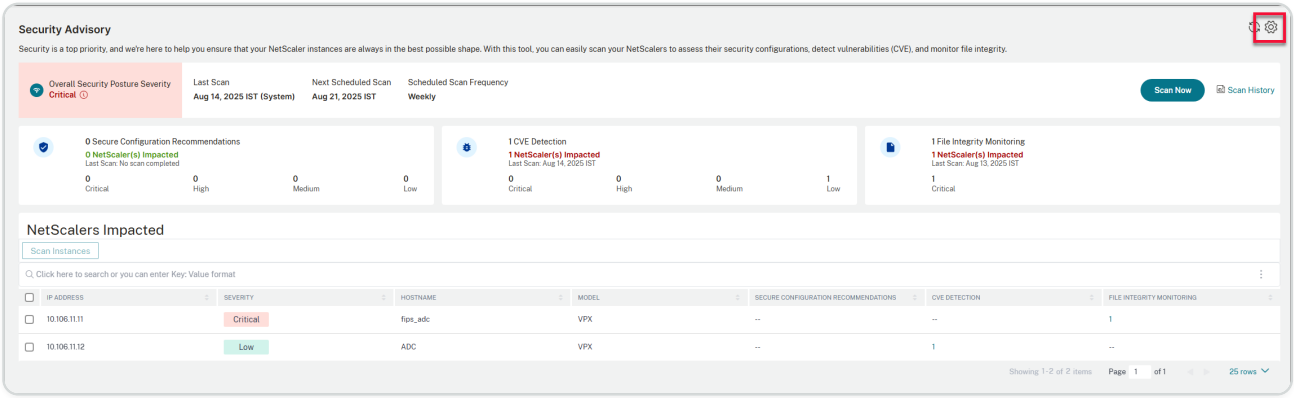


您还可以单击**安全建议配置**、**CVE 检测**或**文件完整性监控**下的数字以查看更多详细信息。以下是供您参考的示例图像。



设置

作为管理员，您可以接收 Citrix Cloud 通知，这些通知会告知有多少 NetScaler 实例存在 CVE 漏洞。要配置何时以及如何接收通知，请单击安全建议页面右上角的设置图标。



您可以执行以下操作：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 选择您必须接收通知的事件类型。
- 选择您希望如何收到通知。例如，通过电子邮件、Slack、PagerDuty。
- 选择必须包含在系统扫描中的扫描类型。默认情况下，系统扫描仅启用 CVE 扫描。
- 选择退出安全公告自定义扫描。

您还可以配置必须包含在系统扫描中的扫描类型。

Citrix Cloud 通知(/en-us/netscaler-application-delivery-management-software/media/secuirty-advisory-settings.png)

免责声明：

请注意，NetScaler 文件完整性监控（“该功能”）无法检测威胁行为者在针对相关环境时可能使用的所有技术、策略或程序 (TTP)。威胁行为者频繁更改 TTP 和基础设施，因此该功能对于某些威胁可能具有有限或不具有取证价值。强烈建议您聘请经验丰富的取证调查员来评估您的环境，以应对任何可能的威胁。

本文档及其包含的信息按“原样”提供。Cloud Software Group, Inc. 对本文档或其内容不作任何明示或暗示的保证或陈述，包括但不限于本文档或其中包含的信息没有错误或符合任何适销性或特定用途适用性条件。

安全配置建议

NetScaler 安全配置建议作为一份全面的指南，提供专家建议和具体说明，以增强 NetScaler 配置的安全态势。借助此功能，您可以保护您的应用交付控制器 (ADC) 基础设施免受潜在漏洞和不断演变的网络威胁。通过严格遵循建议的指导方针，您可以主动降低风险，增强系统弹性，并有效防御未经授权的访问和恶意活动。

此功能不仅扫描 NetScaler 配置中的潜在漏洞，还主动建议精确的命令来修复这些配置。网络管理员可以快速识别安全漏洞并实施必要的更改，以加强其 NetScaler 部署。

“**安全配置建议**”选项卡提供了一个按严重性精心分类的全面视图，从而可以优先处理潜在的配置漏洞。

基于严重性的优先级划分

按严重性分类使用户能够有效地分配精力。观察结果通常分为以下几个级别：

- **关键**：对 NetScaler 实例的安全性和完整性构成即时且重大风险的问题。这些问题必须以最高优先级解决。

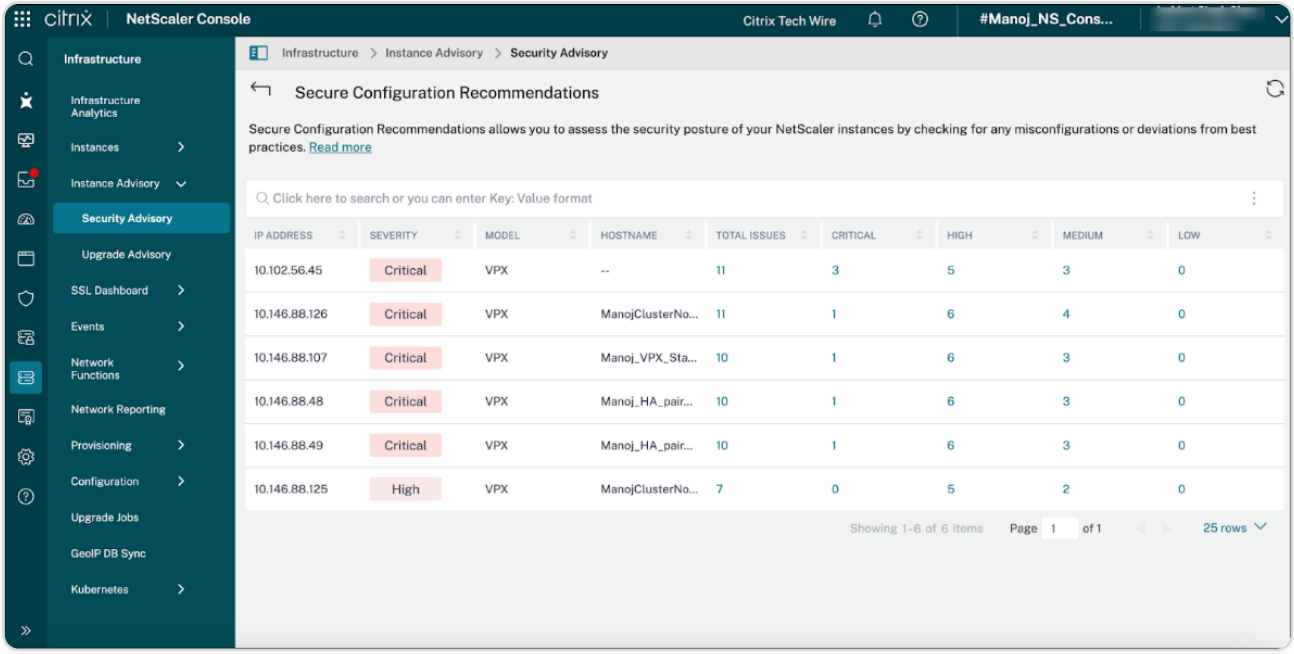
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **高**：如果被利用，可能导致重大安全漏洞的配置，需要立即关注。
- **中**：表明潜在弱点或错误配置的观察结果。虽然这些问题不属于关键问题，但如果置之不理，可能会导致更大的安全事件。
- **低**：改善整体安全态势的次要建议或最佳实践。这些问题不构成即时威胁。

详细实例级视图的优势

- **有针对性的修复**：用户收到的不是通用建议，而是针对每个 NetScaler 实例量身定制的具体建议，确保精确有效的修复。
- **减少攻击面**：通过系统地解决观察到的错误配置，组织可以显著减少其攻击面，并最大限度地降低成功利用的可能性。
- **合规性**：详细的观察结果可以帮助组织识别和纠正可能违反法规合规性标准的配置（例如，GDPR、HIPAA、PCI DSS）。
- **增强安全态势**：主动识别和解决配置弱点有助于建立更强大的整体安全态势，并增强抵御网络威胁的能力。
- **运营效率**：通过提供清晰且可操作的见解，系统简化了安全修复流程，节省了时间和资源。

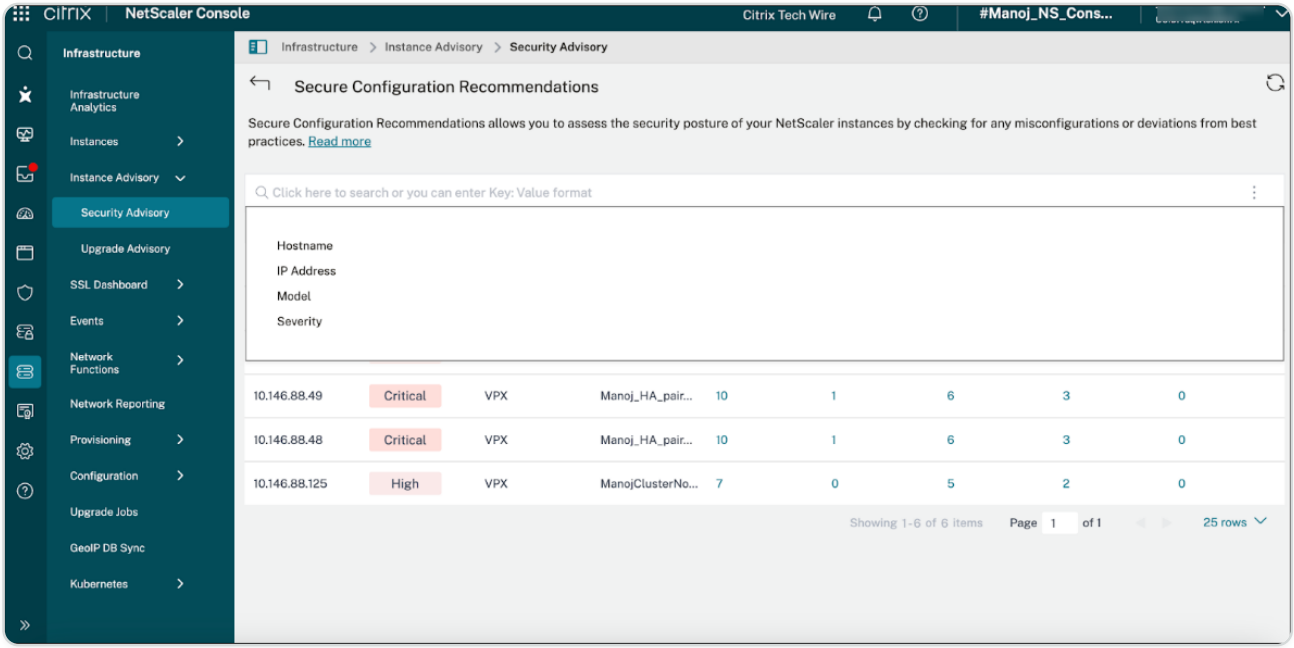
您可以根据优先级、风险承受能力和可用资源，**选择**要首先解决的观察结果。这种灵活性确保了最紧迫的安全问题能够及时解决，同时仍提供必要的信息，以便随着时间的推移实现全面的配置强化。此选项使安全管理员能够做出明智的决策并采取果断行动来保护其 NetScaler 部署。



自由文本搜索功能使您能够根据各种关键标识符缩小搜索结果范围。例如，您可以通过实例的唯一主机名高效地搜索实例，从而提供一种直接定位特定设备的方法。此外，通过 IP 地址搜索提供了另一种精确定位实例的方式，这在以网络为中心的环境中特别有用。

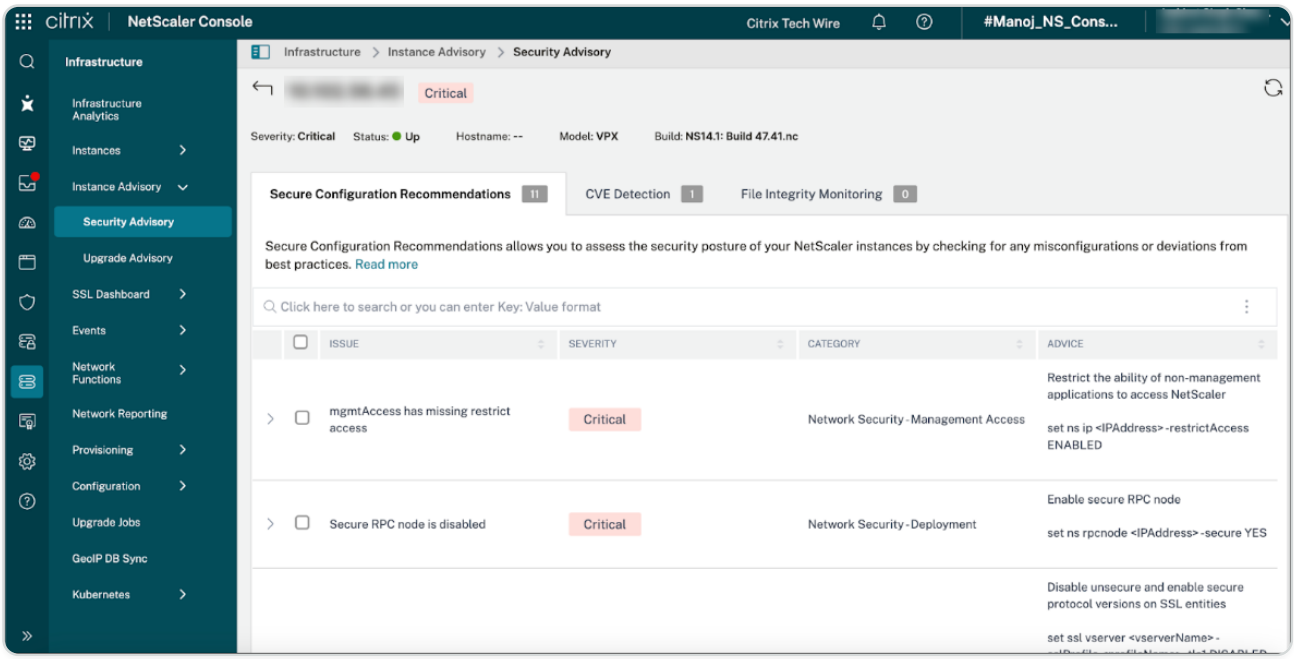
© 1997–2026 Citrix Systems, Inc. All rights reserved.

除了基本识别之外，搜索还支持按 NetScaler 型号进行筛选。这意味着您可以指定 MPX、SDX 或 VPX 等型号，以仅查看属于特定硬件或软件类别的实例。您还可以按严重性级别优化搜索，从而根据实例的关键性（从信息性警报到严重警告）对其进行优先级排序。



修复配置建议

在您评估了配置观察结果并确定了需要采取行动的项后，系统会显示推荐配置的全面视图。然后，系统会显示一个专用页面（如以下图像所示），其中显示根据您的选择量身定制的修复步骤。例如，如果您选择仅解决特定 NetScaler 实例（在此特定场景中，IP 地址为 10.102.56.45 的实例）的严重性问题，则该页面会动态填充相关的、高优先级的建议，以有效地指导修复过程。



配置建议可分为两种类型：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

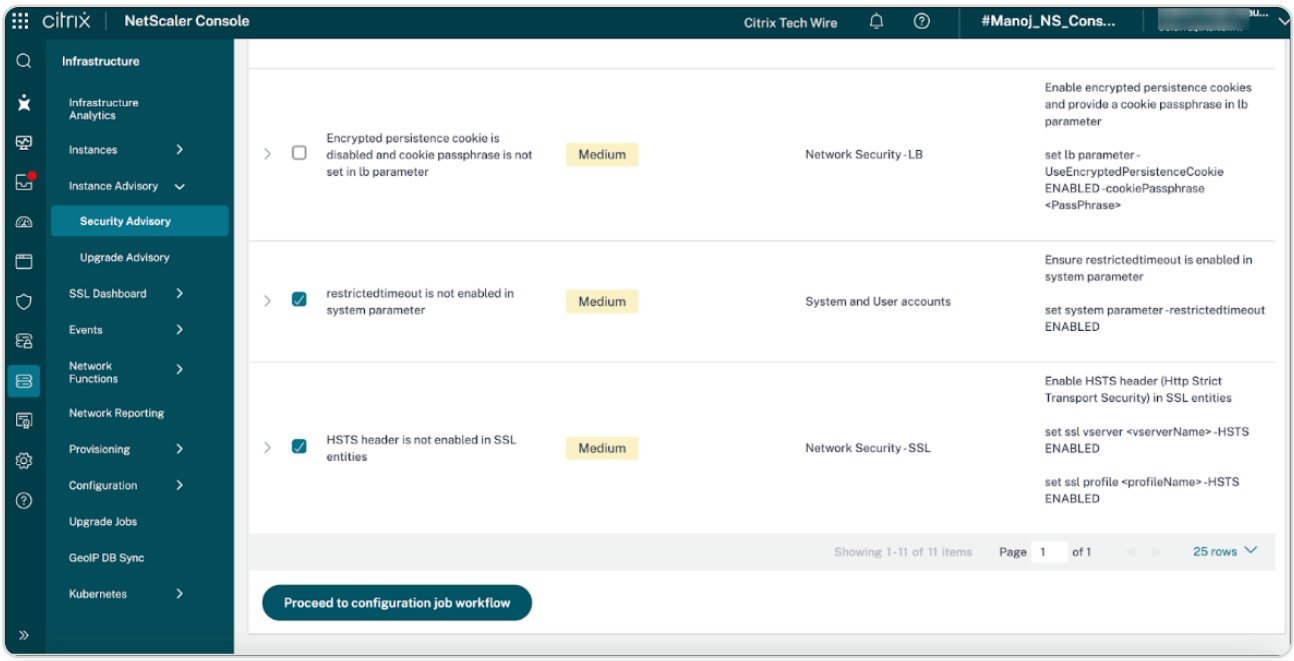
- **需要用户输入的建议**：此类别包含需要 NetScaler 管理员或安全团队提供特定上下文信息或决策的配置建议。这些通常是通用默认值可能不适用，或者最佳设置取决于独特的操作环境、安全策略或应用程序要求的场景。以下是一些建议示例：
  - **定义特定的 IP 地址或 IP 范围**：例如，配置防火墙规则以仅允许来自受信任的内部子网或特定客户端 IP 地址的流量。系统无法推断这些唯一的网络详细信息。
  - **设置自定义端口号**：虽然许多服务都有标准端口，但应用程序可能出于安全或操作原因配置为使用非默认端口。网络管理员必须指定端口号。
  - **指定主机名或域名**：在配置 SSL 证书、负载平衡虚拟服务器或内容切换策略时，用户必须提供 NetScaler 实例服务或与之交互的确切主机名或域名。
  - **提供身份验证服务器详细信息**：将 NetScaler 与 LDAP、RADIUS、SAML 或 OAuth 等外部身份验证系统集成需要用户输入服务器 IP 地址、共享密钥、目录路径和其他特定于协议的详细信息。
  - **设置特定的 URL 重写或内容切换策略**：这些高级功能的精确 URL、模式和目标目的地高度依赖于应用程序架构，必须由用户定义。
  - **影响**：这些建议通常需要更深入地了解部署的具体需求、安全策略和网络拓扑。用户输入中的错误可能导致服务中断或安全漏洞，因此需要仔细规划和验证。实施这些功能的自动化工具或脚本通常会提示输入必要的参数，或者从配置文件中读取这些参数。
- **无需用户输入的建议**：此类别包括可以普遍应用或涉及不依赖于独特环境变量的标准最佳实践的配置建议。这些通常是基础性的安全增强或性能优化，对大多数 NetScaler 部署都有益。以下是一些建议示例：
  - **禁用弱密码或协议**：建议您禁用 SSL/TLS 版本（例如 SSLv3 或 TLS 1.0）或特定的弱密码套件（例如 RC4、3DES），因为这些是已知的漏洞，并且移除它们是通用的安全最佳实践。系统无需特定输入即可知道哪些密码是弱的。
  - **启用 HTTP 严格传输安全 (HSTS)**：这是一项由 Web 浏览器强制执行的策略，仅使用安全的 HTTPS 连接与服务器交互。启用它是一个标准的安全强化步骤。
  - **设置安全 Cookie 标志（例如，`Secure`、`HttpOnly`）**：这些标志增强了会话 Cookie 的安全性，防止它们通过未加密的通道传输或通过客户端脚本访问。它们的应用是一个通用建议。
  - **启用常见安全标头**：X-Frame-Options、X-Content-Type-Options 和 Content-Security-Policy（带有默认安全策略）等标头无需特定用户输入即可推荐，因为它们普遍提高了客户端安全性。
  - **为常见攻击实施默认速率限制**：虽然自定义速率限制可能需要输入，但建议对常见攻击向量（例如，过多的登录失败尝试）应用通用速率限制可能适用于作为基线。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

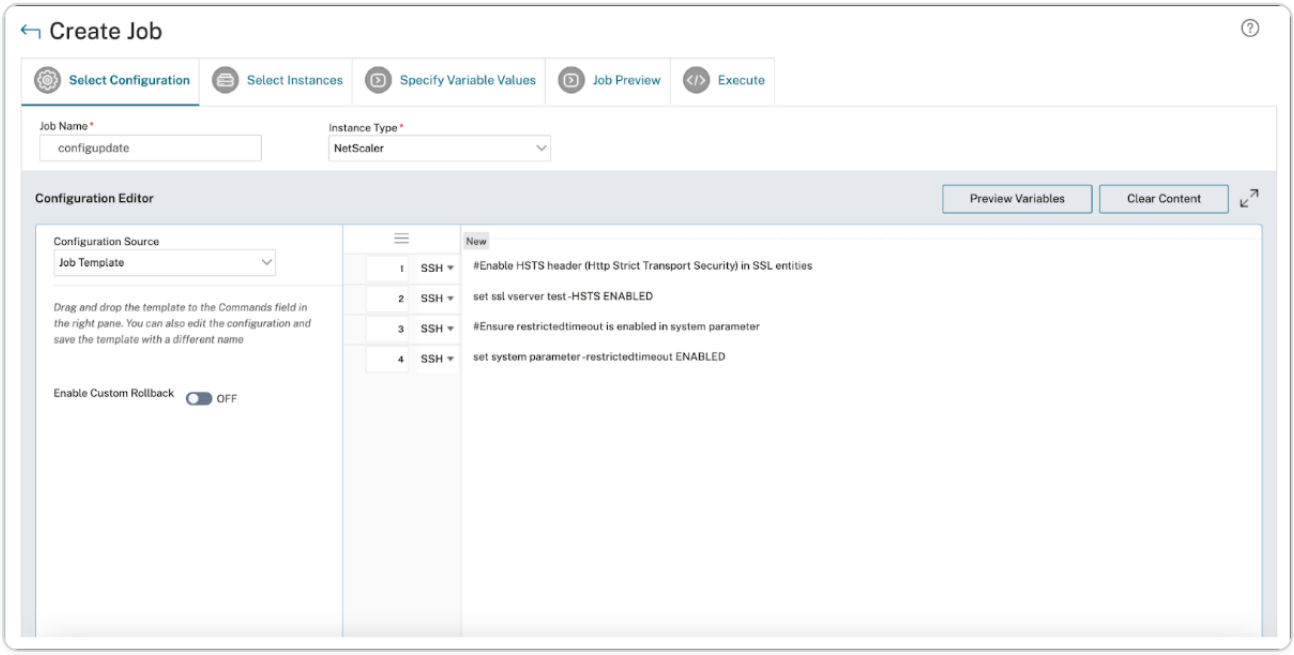
  - **配置最佳缓冲区大小或超时**：与内部缓冲区大小或连接超时相关的通用性能建议，这些建议由系统架构而非特定应用程序逻辑决定。
  - **确保安全事件的适当日志记录级别**：确保对安全相关事件进行一定级别的日志记录的建议是审计和事件响应的通用最佳实践。

- **影响**：这些建议通常是自动化或基线配置脚本的绝佳选择，因为它们可以统一应用于多个 NetScaler 实例，而无需手动干预具体细节。它们通过解决常见漏洞和强制执行广泛接受的标准来增强强大的安全态势。

总而言之，根据用户输入要求对配置建议进行分类可以简化实施过程。需要输入的建议要求用户仔细收集和验证数据，而不需要输入的建议通常可以作为标准安全基线或通过自动化部署机制应用。

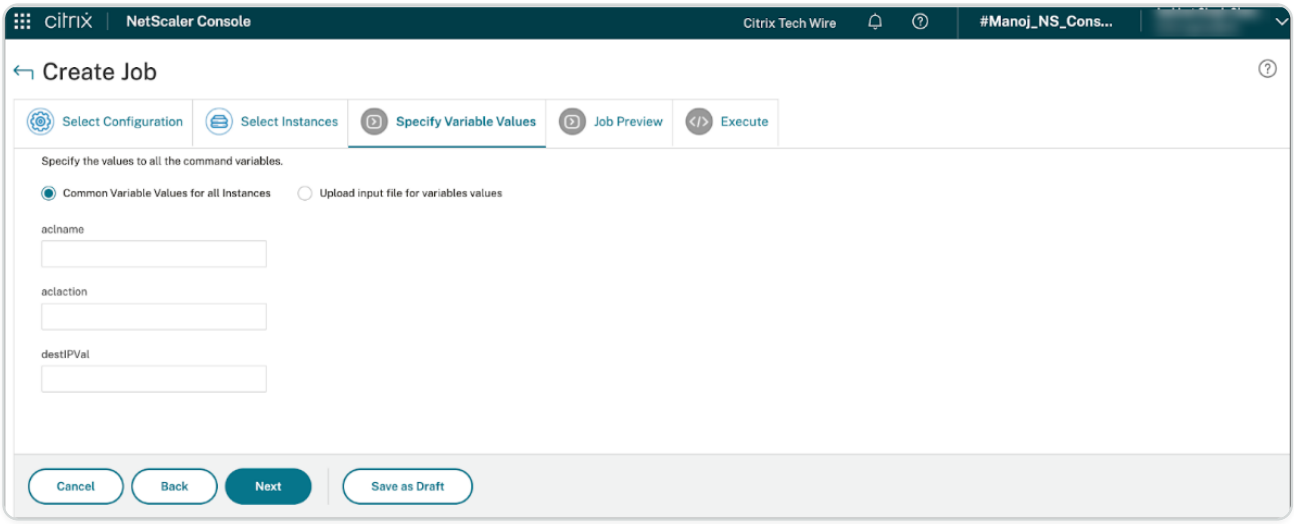


一旦用户决定要处理的配置，现有的配置作业工作流将接管以推送配置更改。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

例如，这是一个需要用户输入的配置建议示例。您可以逐个输入配置值，也可以选择上传包含配置值的文件，如下图所示。

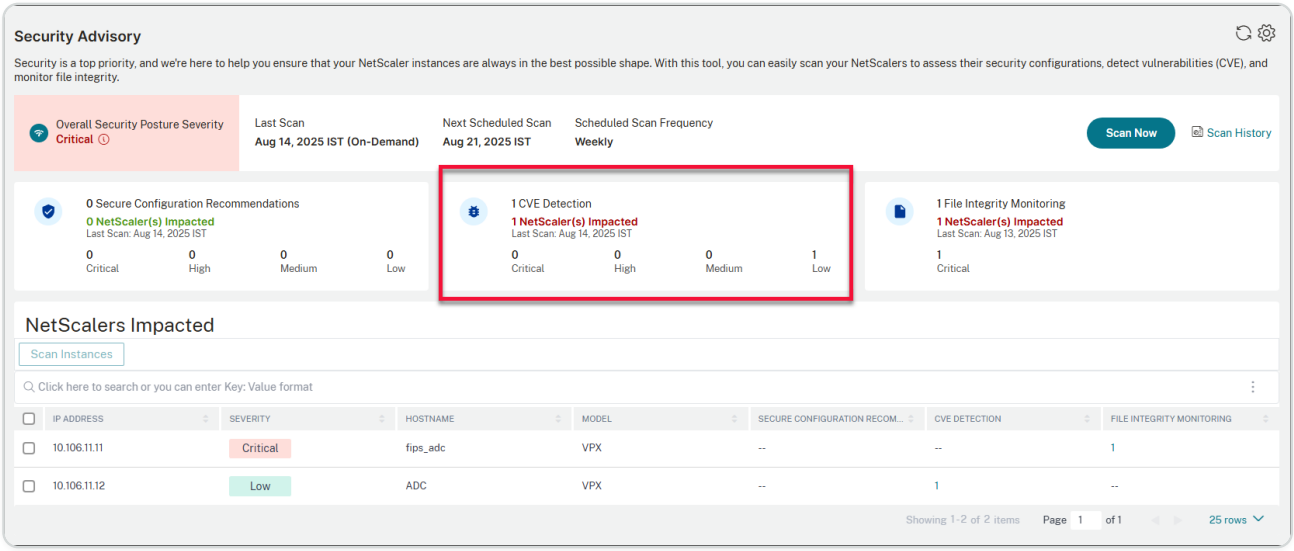


CVE 检测

NetScaler 通过扫描实例版本、配置和系统文件来检测 CVE，以识别漏洞。它使用更新的 CVE 存储库，并提供详细的影响分析和补救建议。

安全建议仪表板中的**CVE 检测**部分列出了以下内容：

- 检测到的 CVE 数量
- 受影响的 NetScaler 实例数量
- 上次扫描运行的日期
- 按严重性（严重、高危、中危和低危）分类的受影响 NetScaler 实例

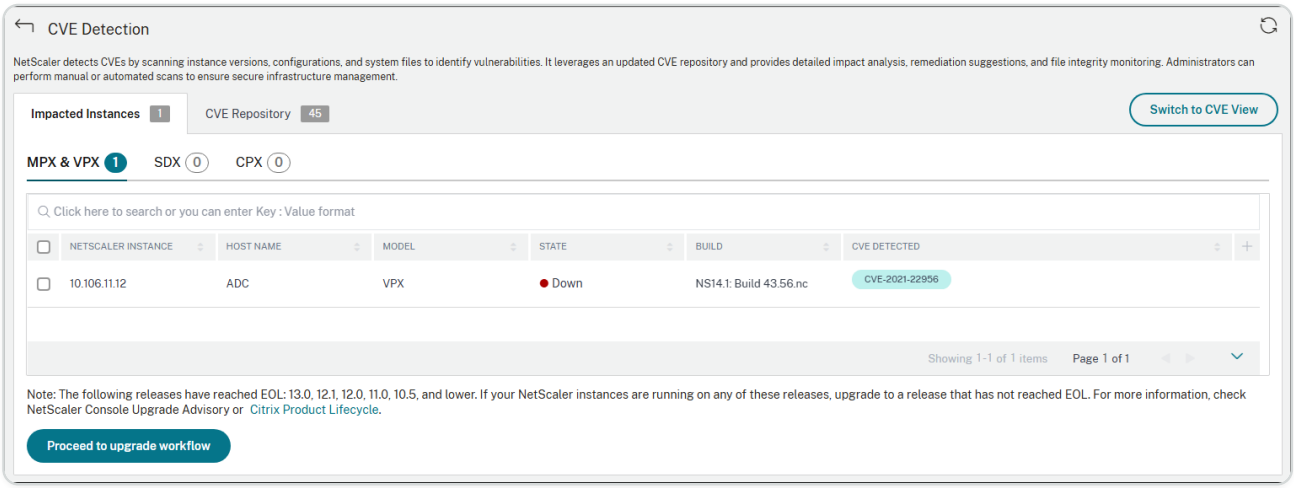


作为管理员，您可以允许 NetScaler 运行定期计划的系统扫描，也可以根据需要选择运行按需扫描。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **系统扫描** - 默认扫描所有托管实例。NetScaler Console 决定系统扫描的日期和时间，您无法更改它们。
- **按需扫描** - 您可以在需要时手动扫描实例。如果上次系统扫描后经过的时间很长，您可以运行按需扫描以评估当前安全状况。或者在应用补救措施后进行扫描，以评估修订后的状况。要运行按需扫描，请单击安全建议中的**立即扫描**。

您可以单击**CVE 检测**部分以查看详细信息。



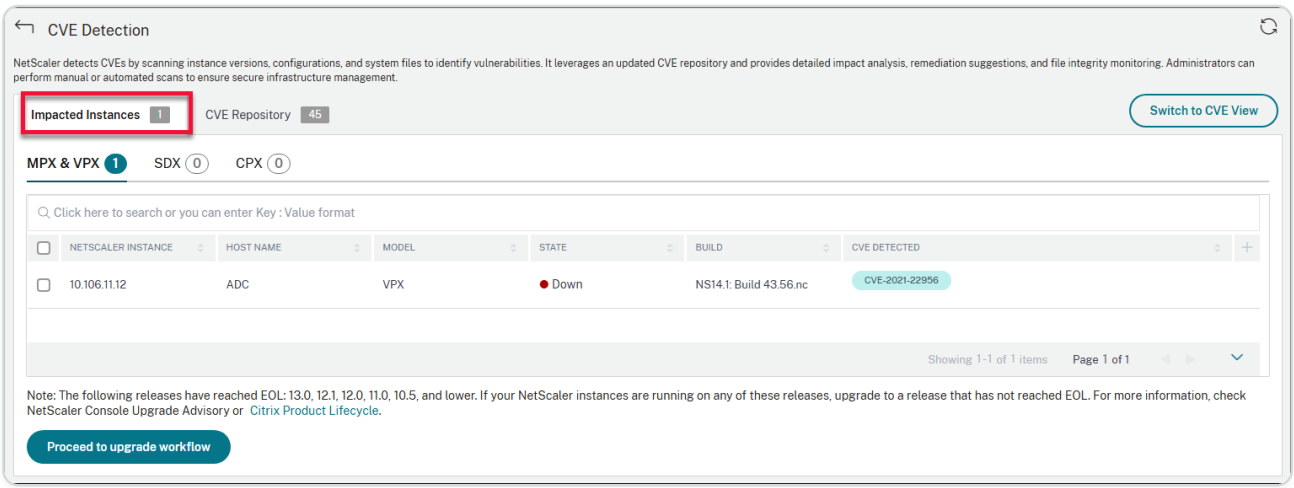
CVE 检测部分有两种视图：

- 实例视图
- CVE 视图

实例视图

实例视图包含**受影响的实例**和**CVE 存储库**选项卡。

受影响的实例选项卡显示受影响的 NetScaler 实例列表。



受影响的实例根据以下因素进行分类：

- MPX 和 VPX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SDX
- CPX
- BLX

您还可以根据以下条件搜索实例：

- 检测到的 CVE
- 主机名
- 型号
- NetScaler 实例
- 状态

该表显示以下详细信息：

- NetScaler IP 地址
- 主机名
- NetScaler 型号
- NetScaler 状态
- 软件版本和内部版本
- 影响 NetScaler 的 CVE 列表。

大多数 CVE 需要升级作为补救措施，而其他 CVE 则需要升级和额外的步骤作为补救措施。

- 有关 CVE-2020-8300 补救措施，请参阅 修复 CVE-2020-8300 的漏洞。
- 有关 CVE-2021-22927 和 CVE-2021-22920，请参阅 修复 CVE-2021-22927 和 CVE-2021-22920 的漏洞。
- 有关 CVE CVE-2021-22956，请参阅 识别并修复 CVE-2021-22956 的漏洞
- 有关 CVE CVE-2022-27509，请参阅 修复 CVE-2022-27509 的漏洞

> **注意**
>
> 如果您的 NetScaler 实例有自定义项，请在规划 NetScaler 升级之前参阅 自定义 NetScaler 配置的升级注意事项。

您可以将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。要升级，请执行以下操作之一：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **升级工作流** - 选择一个实例，然后单击**继续升级工作流**。
- **配置作业工作流** - 选择一个实例，然后单击**配置作业工作流**。

升级工作流启动，易受攻击的 NetScaler 会自动填充为目标 NetScaler。有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅使用作业升级 NetScaler 实例。

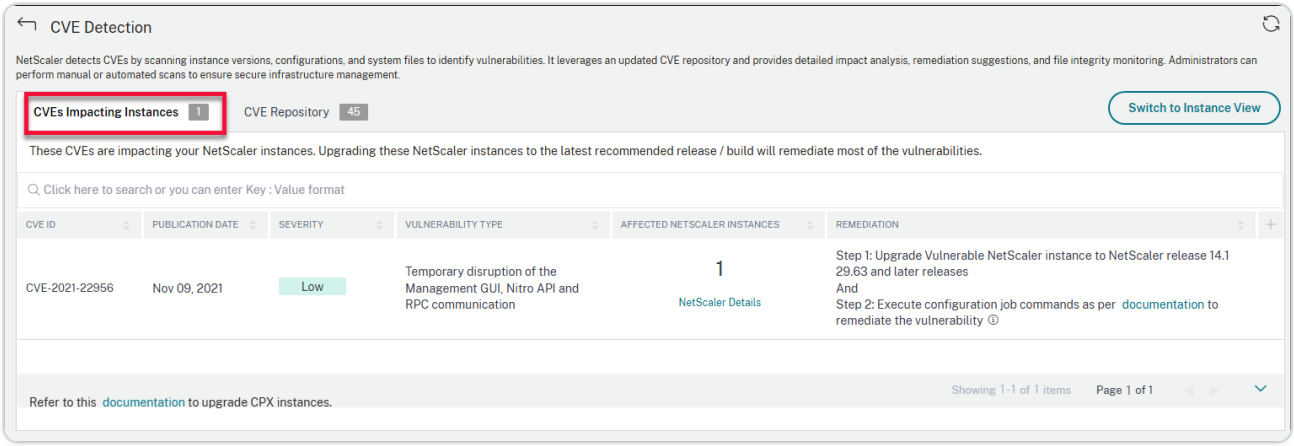
注意：

- 版本 13.0、12.1、12.0、11.0、10.5 及更低版本已达到生命周期结束 (EOL)。如果您的 NetScaler 实例运行在这些版本中的任何一个上，请升级到受支持的版本。
- 您要升级到的版本和内部版本由您自行决定。请参阅修复列下的建议，了解哪些版本和内部版本包含安全修复程序。并相应地选择一个尚未达到生命周期结束的受支持版本和内部版本。

要切换到 CVE 视图，请单击**切换到 CVE 视图**。

CVE 视图

CVE 视图显示影响您基础设施的所有 CVE 以及所有受影响的 NetScaler 实例的结果，并提供修复建议。您可以使用此信息应用修复程序来解决安全风险。



显示影响 NetScaler 实例的 CVE 数量的表包含以下详细信息。

- **CVE ID**：影响实例的 CVE 的 ID。
- **发布日期**：该 CVE 的安全公告发布日期。
- **严重性分数**：严重性类型（高/中/危急）和分数。要查看分数，请将鼠标悬停在严重性类型上。
- **漏洞类型**：此 CVE 的漏洞类型。
- **受影响的 NetScaler 实例**：受此 CVE ID 影响的实例数量。将鼠标悬停在其上方时，将显示 NetScaler 实例列表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

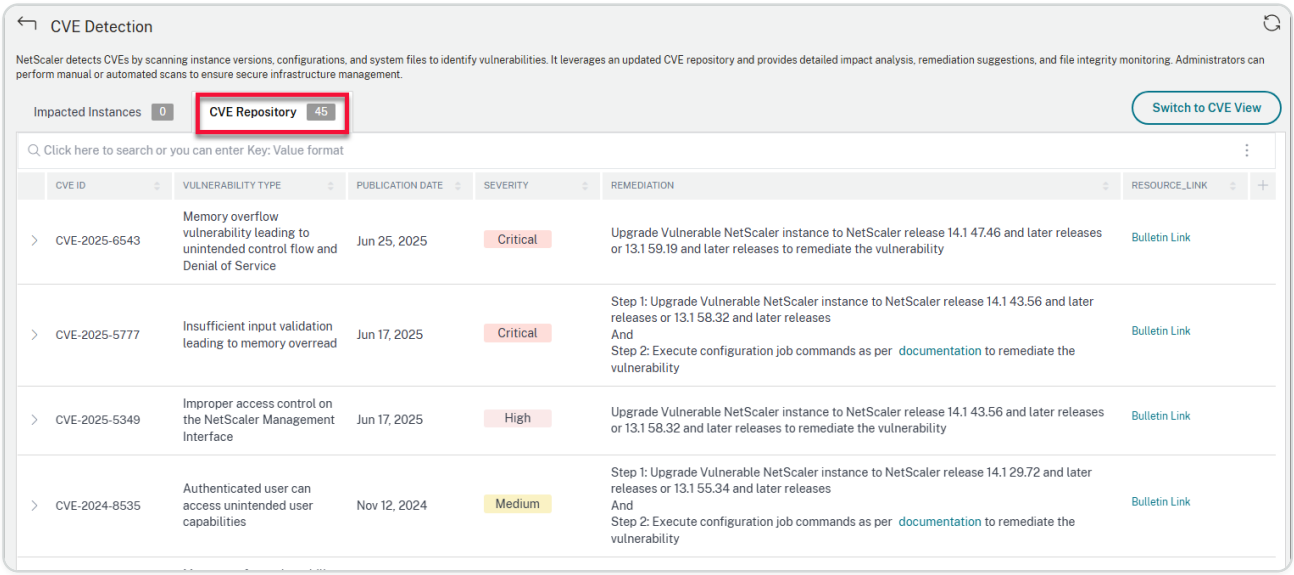
- **补救措施**：可用的补救措施，通常是升级实例或应用配置包。

同一个实例可能受到多个 CVE 的影响。此表可帮助您查看一个特定 CVE 或多个选定 CVE 影响了多少实例。要检查受影响实例的 IP 地址，请将鼠标悬停在“**受影响的 NetScaler 实例**”下的“NetScaler 详细信息”上。要检查受影响实例的详细信息，请单击表底部的“**查看受影响的实例**”。 您还可以通过单击加号来添加或删除表中的列。

CVE 存储库

实例视图和 CVE 视图都包含“**CVE 存储库**”选项卡。此选项卡详细显示了 Citrix 自 2019 年 12 月以来发布的所有可能影响您的 NetScaler 基础架构的 NetScaler 相关 CVE。

- CVE ID
- 漏洞类型
- 发布日期
- 严重级别
- 补救措施
- 安全公告链接



您可以使用此视图了解安全公告范围内的 CVE，并了解有关 CVE 的更多信息。有关不受支持的 CVE 的信息，请参阅安全公告中不受支持的 CVE。

注意事项

- 安全通报不支持已达到生命周期结束 (EOL) 的 NetScaler 版本。我们建议您升级到 NetScaler 支持的版本。
- 支持 CVE 检测的实例：所有 NetScaler（SDX、MPX、VPX）和 Gateway。
- 支持文件完整性监控的实例：MPX、VPX 实例和 Gateway。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 支持的 CVE：2019 年 12 月之后的所有 CVE。

> **注意：**
>
> NetScaler Console 安全通报不支持检测和修复影响适用于 Windows 的 NetScaler Gateway 插件的漏洞。有关不受支持的 CVE 的信息，请参阅 安全通报中不受支持的 CVE 。

- NetScaler Console 安全通报在识别漏洞时，不考虑任何类型的特性配置错误。
- NetScaler Console 安全通报仅支持 CVE 的识别和修复。它不支持识别和修复安全文章中强调的安全问题。
- NetScaler、Gateway 版本的范围：此功能仅限于主要版本。安全通报不包括任何特殊版本。
  - 安全通报在管理分区中不受支持。
- 针对 CVE，可进行以下类型的扫描：
  - **版本扫描**：此扫描需要 NetScaler Console 将 NetScaler 实例的版本与提供修复的版本和内部版本进行比较。此版本比较有助于 NetScaler Console 安全通报识别 NetScaler 是否易受 CVE 攻击。例如，如果某个 CVE 在 NetScaler 版本和内部版本 xx.yy 上得到修复，则安全通报会将内部版本低于 xx.yy 的所有 NetScaler 实例视为易受攻击。版本扫描目前在安全通报中受支持。
  - **配置扫描**：此扫描需要 NetScaler Console 将 CVE 扫描的特定模式与 NetScaler 配置文件 (`nsconf`) 进行匹配。如果 NetScaler ns.conf 文件中存在特定的配置模式，则该实例被视为易受该 CVE 攻击。此扫描通常与版本扫描一起使用。 配置扫描目前在安全通报中受支持。
  - **自定义扫描**：此扫描需要 NetScaler Console 连接到托管的 NetScaler 实例，向其推送脚本并运行该脚本。脚本输出有助于 NetScaler Console 识别 NetScaler 是否易受 CVE 攻击。示例包括特定的 shell 命令输出、特定的 CLI 命令输出、某些日志以及某些目录或文件的存在或内容。对于需要自定义扫描的 CVE，脚本会在每次计划扫描或按需扫描运行时运行。有关收集的数据以及特定自定义扫描选项的更多信息，请参阅该 CVE 的安全通报文档。
- 扫描不会影响 NetScaler 上的生产流量，也不会更改 NetScaler 上的任何 NetScaler 配置。
- NetScaler Console 安全通告不支持 CVE 缓解。如果您已对 NetScaler 实例应用了缓解措施（临时解决方案），NetScaler Console 仍会将该 NetScaler 识别为易受攻击的 NetScaler，直到您完成修复。
- 对于 FIPS 实例，不支持 CVE 扫描。

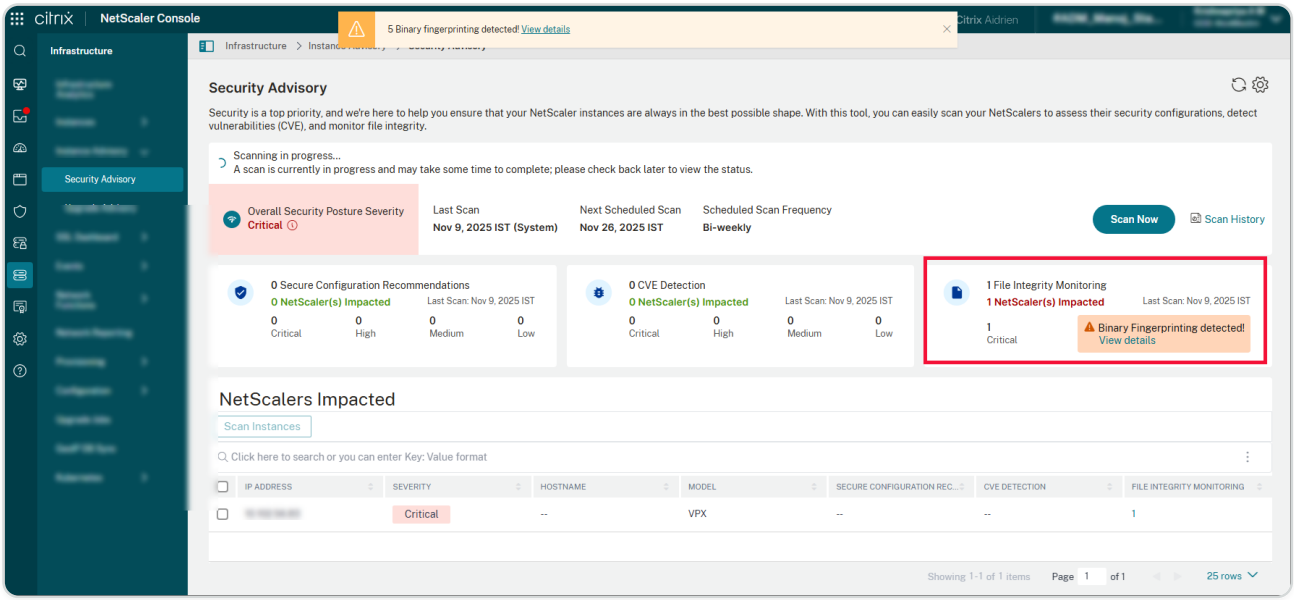
© 1997–2026 Citrix Systems, Inc. All rights reserved.

文件完整性监控

文件完整性监控使您能够识别 NetScaler 文件系统是否发生了任何更改或添加。此功能通过将当前 NetScaler 版本的二进制哈希值与链接到同一 NetScaler 版本的原始二进制哈希值进行比较，来评估 NetScaler 文件的完整性。

“**安全建议**”仪表板中的“**文件完整性监控**”部分列出了以下内容：

- 检测到的问题数量
- 受影响的 NetScaler 实例数量
- 上次扫描运行的日期
- 按严重性（关键、高、中、低）分类的受影响 NetScaler 实例
- 使用二进制签名和验证报告问题的受影响 NetScaler 实例



作为管理员，您可以允许 NetScaler 运行定期计划的系统扫描，也可以根据需要选择运行按需扫描。

- **系统扫描** - 默认情况下扫描所有托管实例。NetScaler Console 决定系统扫描的日期和时间，并且默认情况下禁用系统扫描。
- **按需扫描** - 您可以在需要时手动触发扫描。要运行按需扫描，请在安全建议仪表板上单击“**立即扫描**”。

您可以单击“**文件完整性监控**”部分以查看详细信息。

控制台检测

“**控制台检测**”选项卡通过比较当前版本的二进制哈希与原始版本的哈希来检测已修改或新添加的文件，从而列出受影响的 NetScaler 实例。该表显示以下详细信息：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- IP 地址 - 受影响实例的 IP 地址。
- 扫描状态 - 显示扫描错误结果。
- 现有文件已修改 - 已修改的现有文件列表。
- 新增文件 - 新增文件列表。
- 扫描时间 - 上次扫描的时间。
- 主机名 - 受影响的 NetScaler 的主机名。
- 型号 - 受影响的 NetScaler 的型号名称。

扫描错误结果显示在主仪表板视图中，这样您就不必单击单个扫描结果或行项目来访问错误详细信息。任何完整性问题，例如哈希不匹配或扫描错误，都会以清晰、易于访问的格式呈现在仪表板上，帮助您快速识别和理解问题。

单击“**现有文件已修改**”和“**新增文件**”下的数字以查看详细信息。

文件完整性监控部分(/en-us/netscaler-application-delivery-management-software/media/file-integrity-monitoring.png)

您可以创建自定义允许列表，并从文件完整性监控扫描中排除特定文件。通过定义要从扫描中排除的文件，您可以简化监控并减少对受信任文件的非必要警报。

要从文件完整性监控扫描中排除特定文件，请执行以下操作：

1. 单击“**排除文件/目录**”。
2. 选择所需的文件或目录。

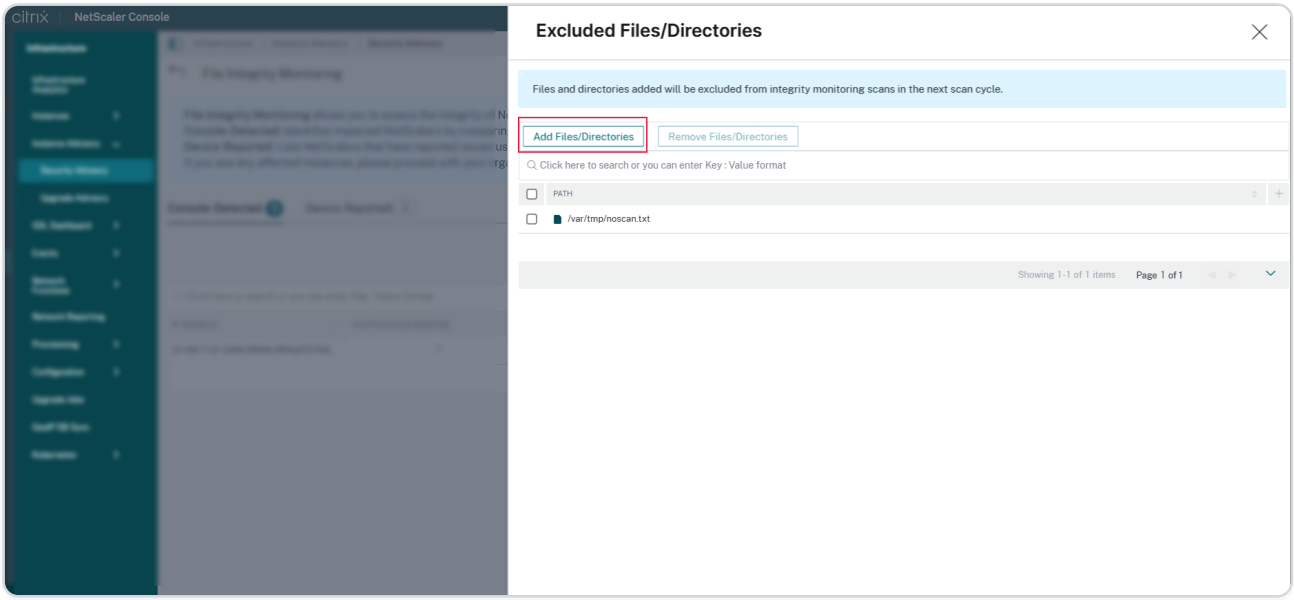
   或

   点击 **添加文件/目录** 以添加新文件。您可以添加标准 shell glob 模式，并排除任何符合定义条件的路径。添加目录时，其所有文件都将从扫描中排除。点击 **添加**。

   您还可以执行搜索以查找特定文件或文件夹。您还可以通过在 `path` 选项下的搜索栏中输入文件或文件夹的一部分来查找排除列表路径。搜索功能使管理和审查排除路径变得更加容易。

如果您不想从扫描中排除文件，您可以选择所需的文件或目录，然后点击 **删除文件/目录**。指定的文件或目录将包含在下一次计划扫描中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



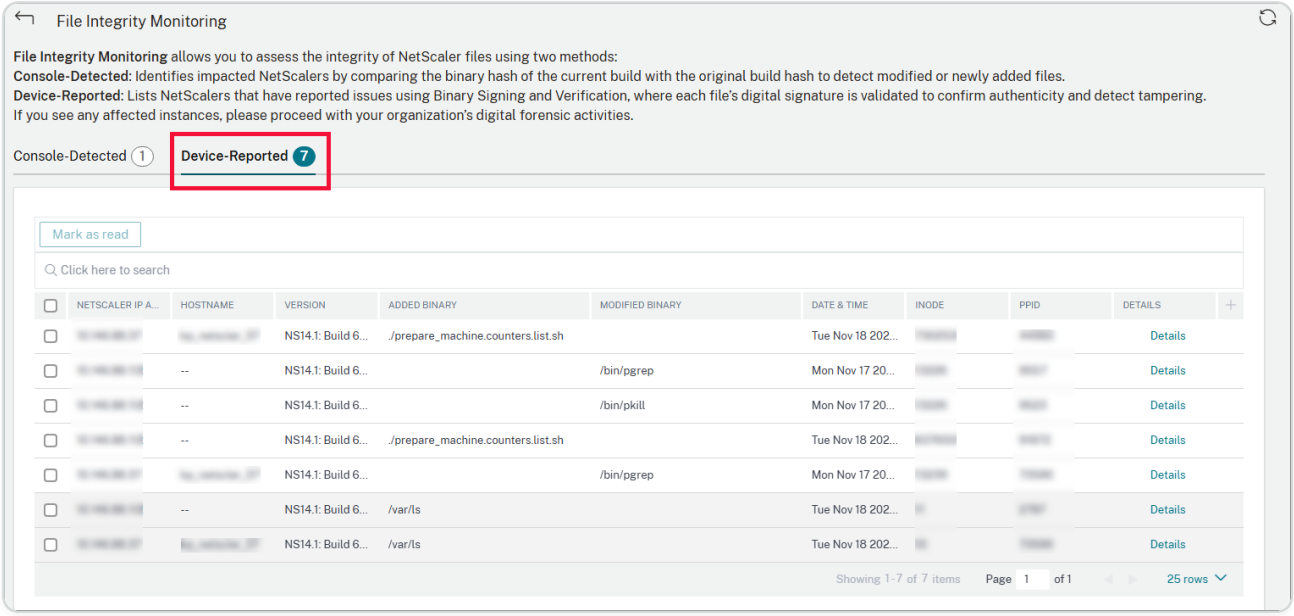
注意事项

- 文件完整性监控支持的实例：MPX、VPX 实例和 Gateway。
- 文件完整性监控提供以下扫描：
  - **文件完整性监控扫描**：此扫描需要 NetScaler Console 连接到受管 NetScaler 实例。NetScaler Console 通过在 NetScaler 中运行脚本并收集 NetScaler 系统文件的当前二进制哈希值来比较哈希值。比较后，NetScaler Console 提供结果，其中包含已修改的现有文件总数和新添加的文件总数。作为管理员，您可以联系您组织的数字取证部门，对扫描结果进行进一步调查。
- 以下是不支持的平台列表：BLX

设备报告

设备报告 选项卡列出了使用二进制签名和验证报告问题的 NetScaler 实例。通过此验证，可以验证每个文件的数字签名，以确认真实性并检测篡改。如果您看到任何受影响的实例，您可以继续进行您组织的数字取证活动。该表列出了受影响的 NetScaler 实例以及其他详细信息，例如主机名、添加的二进制文件、修改的二进制文件。您可以点击所需实例对应的 **详细信息** 以查看详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler Console 中的入侵指标检测

NetScaler Console 中的入侵指标 (IoC) 检测功能旨在检测您的 NetScaler 设备是否可能已受到漏洞影响。

如果存在 CVE 事件，首要关注点之一是恶意行为者是否已成功利用该漏洞。漏洞利用会对客户业务造成灾难性损害，因此，立即检测此类事件至关重要。过去，NetScaler 的入侵指标通过支持渠道分发，这满足了客户需求，但需要额外付出通过支持流程提交工单、与支持专业人员沟通的努力，这有时可能并不理想。NetScaler Console 中的入侵指标检测功能旨在缩短当前以支持为导向的流程，并帮助客户快速评估其 NetScaler 基础设施。

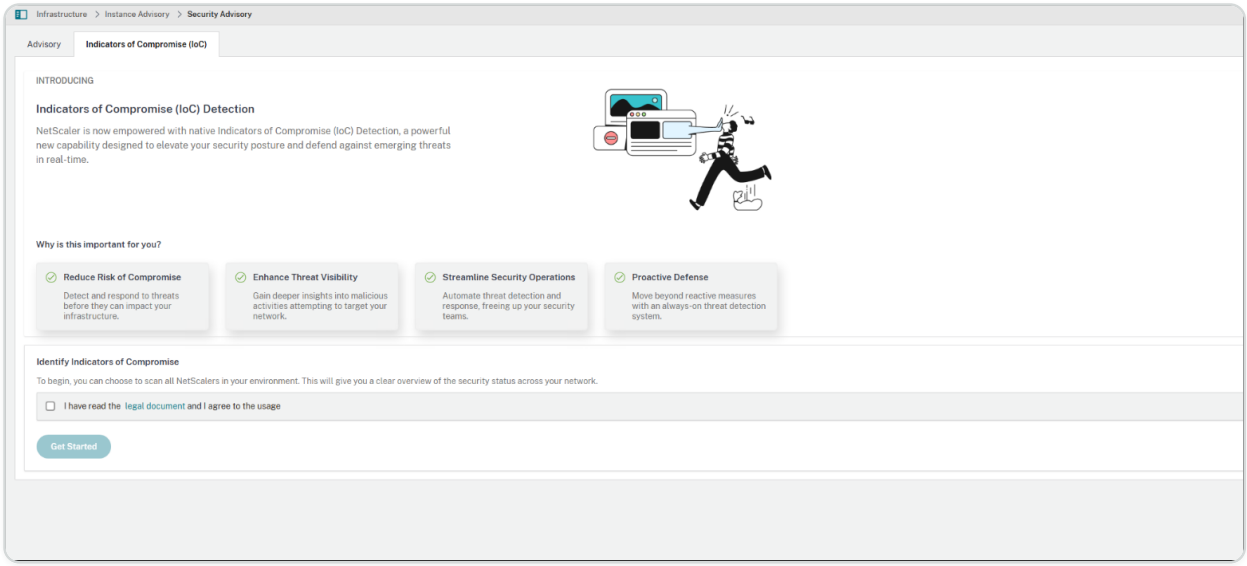
先决条件

此功能要求您发送产品使用遥测数据。有关 NetScaler 遥测的更多信息，请参阅 `<https://docs.netscaler.com/zh-cn/netscaler-application-delivery-management-software/current-release/ns-telemetry.html>`。

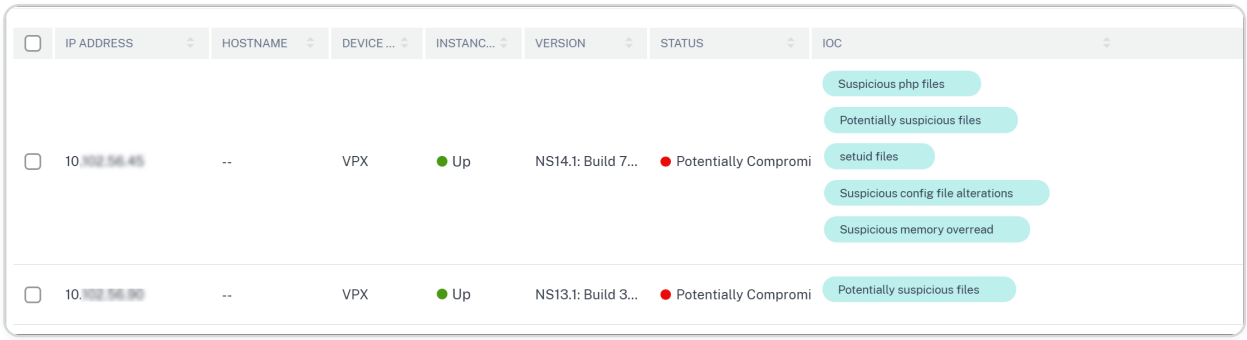
优势

- 您可以从 NetScaler Console 的“**安全建议**”页面运行入侵检测扫描。

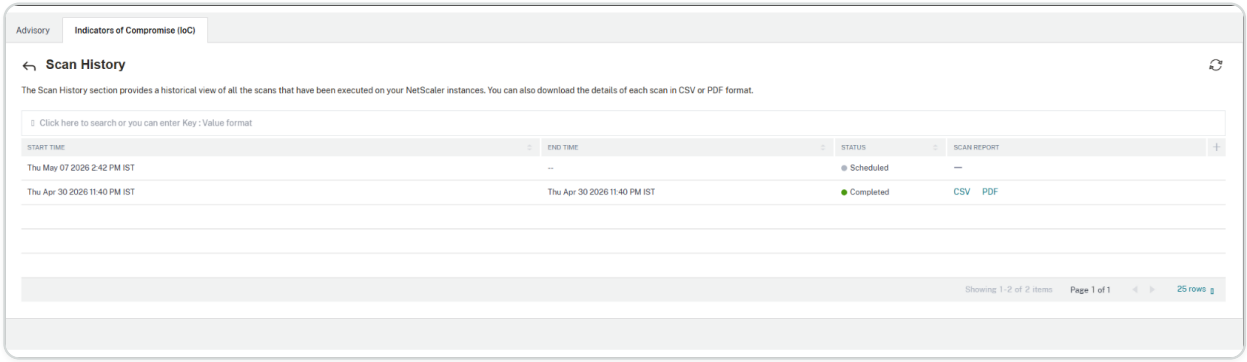
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 扫描提供以下结果之一：
  - **可能已受入侵** – 如果检测逻辑已检测到某个 CVE 可能已受入侵。
  - **未检测到入侵** – 如果检测逻辑未检测到任何入侵。
  - **已跳过** – 如果已针对特定 NetScaler 实例手动跳过扫描。
  - **执行失败** – 如果扫描未成功运行。
  - **正在执行** – 如果扫描正在进行中。
- 随着发现更多 IoC，IoC 逻辑会不断更新。在这种情况下，主页会显示有可用更新。
- 每当 IoC 检测逻辑有可用更新时，您都可以在登录页面上看到它。



- 较早扫描的结果已保存，可随时查看。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 该解决方案采用中心辐射型架构，其中中央云服务从安全的云位置摄取资产，并将其安装到目标设备上。

注意：

IoC 信息不包含威胁行为者在针对相关环境时可能使用的所有技术、策略或程序（“TTP”）。此外，威胁行为者会频繁更改 TTP 和基础设施。由于这些原因以及其他原因，IoC 信息可能具有有限的取证价值，并且可能无法识别实际的妥协。建议您聘请经验丰富的取证调查员来评估您的环境。

通过安全通告支持的 CVE

在您的本地 NetScaler Console 中，如果您已通过 Cloud Connect 或自动启用通道启用了安全通告，则支持完整版安全通告。有关更多信息，请参阅 安全通告。

最新支持的 CVE

下表提供了您可以在安全通告中识别和修复的最新支持的 CVE 详细信息：

发布日期	CVE ID	识别	修复	资源链接
27 Sep 2026	CVE-2026-88771	需要版本扫描。	升级到安全公告中提及的建议版本。	安全公告
27 Sep 2026	CVE-2026-88772	需要版本扫描。	升级到安全公告中提及的推荐版本。	安全公告
27 Sep 2026	CVE-2026-88773	需要版本扫描。	升级到安全公告中提及的推荐版本。	安全公告
27 Sep 2026	CVE-2026-88774	需要版本扫描。	升级到安全公告中提及的推荐版本。	安全公告
27 Sep 2026	CVE-2026-88775	需要版本扫描。	升级到安全公告中提及的推荐版本。	安全公告

© 1997–2026 Citrix Systems, Inc. All rights reserved.

发布日期	CVE ID	识别	修复	资源链接
27 Sep 2026	CVE-2026-88776	需要版本扫描。	升级到安全公告中提及的推荐版本。	安全公告
27 Sep 2026	CVE-2026-88777	需要版本扫描。	升级到安全公告中提及的推荐版本。	安全公告
27 Sep 2026	CVE-2026-88778	需要版本扫描。	升级到安全公告中提及的推荐版本，并应用配置作业。	安全公告

注意：

安全通报不支持已达到生命周期结束 (EOL) 的 NetScaler 版本。我们建议您升级到 NetScaler 支持的版本。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅使用作业升级 NetScaler 实例。

注意：

安全通报系统扫描可能需要几个小时才能完成，并在安全通报模块中反映 CVE 的影响。要更快地查看影响，您可以点击“**立即扫描**”启动按需扫描。

支持的 CVE

以下是安全通报中支持的现有 CVE：

发布日期	CVE ID	资源链接
19 Aug 2026	CVE-2026-19490	安全公告
19 Aug 2026	CVE-2026-19489	安全公告
30 Jun 2026	CVE-2026-13474	安全公告
30 Jun 2026	CVE-2026-10817	安全公告

© 1997–2026 Citrix Systems, Inc. All rights reserved.

发布日期	CVE ID	资源链接
30 Jun 2026	CVE-2026-10816	安全公告
30 Jun 2026	CVE-2026-8655	安全公告
30 Jun 2026	CVE-2026-8452	安全公告
30 Jun 2026	CVE-2026-8451	安全公告
Mar 23, 2026	CVE-2026-4368	安全公告
Mar 23, 2026	CVE-2026-3055	安全公告
Nov 11, 2025	CVE-2025-12101	安全公告
Aug 26, 2025	CVE-2025-8424	安全公告
Aug 26, 2025	CVE-2025-7776	安全公告
Aug 26, 2025	CVE-2025-7775	安全公告
Jun 25, 2025	CVE-2025-6543	安全公告
Jun 17, 2025	CVE-2025-5349	安全公告
Jun 17, 2025	CVE-2025-5777	安全公告
Nov 12, 2024	CVE-2024-8535	安全公告
Jul 09, 2024	CVE-2024-5491	安全公告
Jul 09, 2024	CVE-2024-5492	安全公告
Jan 16, 2024	CVE-2023-6549	安全公告
Jan 16, 2024	CVE-2023-6548	安全公告
Oct 10, 2023	CVE-2023-4967	安全公告
Oct 10, 2023	CVE-2023-4966	安全公告
Jul 18, 2023	CVE-2023-3519	安全公告

© 1997–2026 Citrix Systems, Inc. All rights reserved.

发布日期	CVE ID	资源链接
Jul 18, 2023	CVE-2023-3467	安全公告
Jul 18, 2023	CVE-2023-3466	安全公告
May 09, 2023	CVE-2023-24488	安全公告
May 09, 2023	CVE-2023-24487	安全公告
Dec 13, 2022	CVE-2022-27518	安全公告
Nov 08, 2022	CVE-2022-27516	安全公告
Nov 08, 2022	CVE-2022-27513	安全公告
Nov 08, 2022	CVE-2022-27510	安全公告
Jul 26, 2022	CVE-2022-27509	安全公告
May 25, 2022	CVE-2022-27508	安全公告
May 25, 2022	CVE-2022-27507	安全公告
Nov 09, 2021	CVE-2021-22956	安全公告
Nov 09, 2021	CVE-2021-22955	安全公告
Jul 19, 2021	CVE-2021-22927	安全公告
Jul 19, 2021	CVE-2021-22920	安全公告
Jul 19, 2021	CVE-2021-22919	安全公告
Jun 08, 2021	CVE-2020-8300	安全公告
Jun 08, 2021	CVE-2020-8299	安全公告
Sep 17, 2020	CVE-2020-8247	安全公告
Sep 17, 2020	CVE-2020-8246	安全公告
Sep 17, 2020	CVE-2020-8245	安全公告

© 1997–2026 Citrix Systems, Inc. All rights reserved.

发布日期	CVE ID	资源链接
Jul 07, 2020	CVE-2020-8197	安全公告
Jul 07, 2020	CVE-2020-8199	安全公告
Jul 07, 2020	CVE-2020-8195	安全公告
Jul 07, 2020	CVE-2020-8196	安全公告
Jul 07, 2020	CVE-2020-8193	安全公告
Jul 07, 2020	CVE-2020-8187	安全公告
Jul 07, 2020	CVE-2020-8191	安全公告
Jul 07, 2020	CVE-2020-8190	安全公告
Jul 07, 2020	CVE-2019-18177	安全公告
Jul 07, 2020	CVE-2020-8194	安全公告
Jul 07, 2020	CVE-2020-8198	安全公告
Dec 17, 2019	CVE-2019-19781	安全公告

识别并修复 CVE-2026-88771 漏洞

在 NetScaler Console® 安全通报仪表板中，单击“**CVE 检测**”。在“**受影响实例**”选项卡上，搜索 CVE-2026-88771。将显示受 CVE-2026-88771 影响的 NetScaler 实例列表。

CVE-2026-sep 的安全通报仪表板(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-sep.png)

有关安全通报仪表板的更多信息，请参阅安全通报。

注意：

安全通报系统扫描可能需要几个小时才能完成，并在安全通报模块中反映 CVE-2026-88771 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

修复 CVE-2026-88771

对于受 CVE-2026-88771 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。

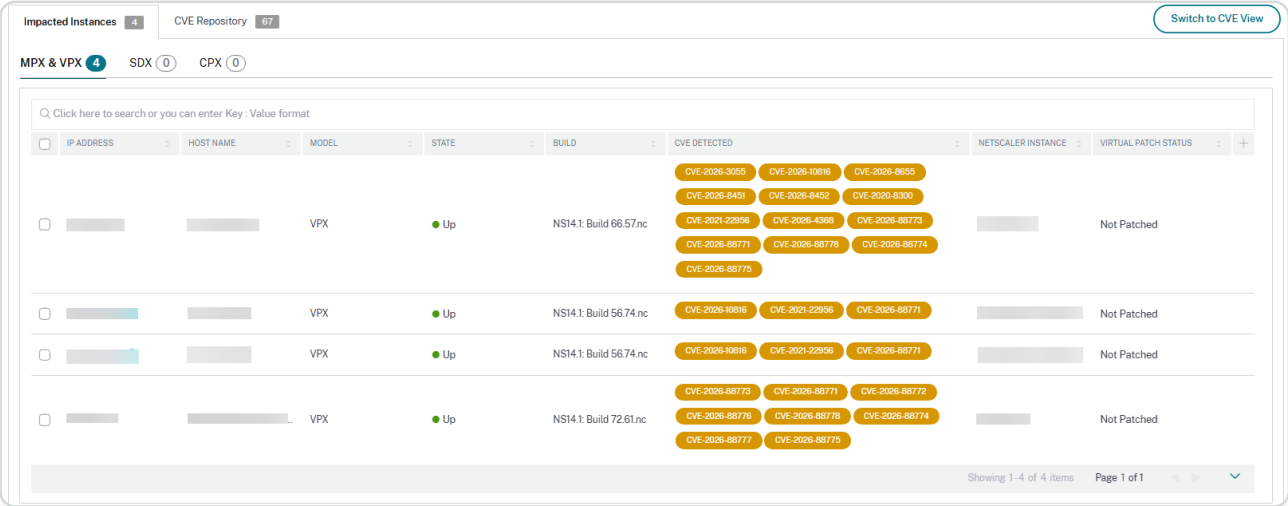
在 GUI 中，在“**CVE 检测 > 受影响实例**”下，选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。

此步骤可以一次性完成所有易受攻击的 NetScaler 实例。有关更多信息，请参阅CVE 检测。

识别并修复 CVE-2026-88772 漏洞

在 NetScaler Console® 安全通报仪表板中，单击“**CVE 检测**”。在“**受影响的实例**”选项卡上，搜索 CVE-2026-88772。将显示受 CVE-2026-88772 影响的 NetScaler 实例列表。



有关安全通报仪表板的更多信息，请参阅安全通报。

注意：

安全通报系统扫描可能需要几个小时才能完成，并在安全通报模块中反映 CVE-2026-88772 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

修复 CVE-2026-88772

对于受 CVE-2026-88772 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。

在 GUI 中，在“**CVE 检测 > 受影响的实例**”下，选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充了易受攻击的 NetScaler 实例。

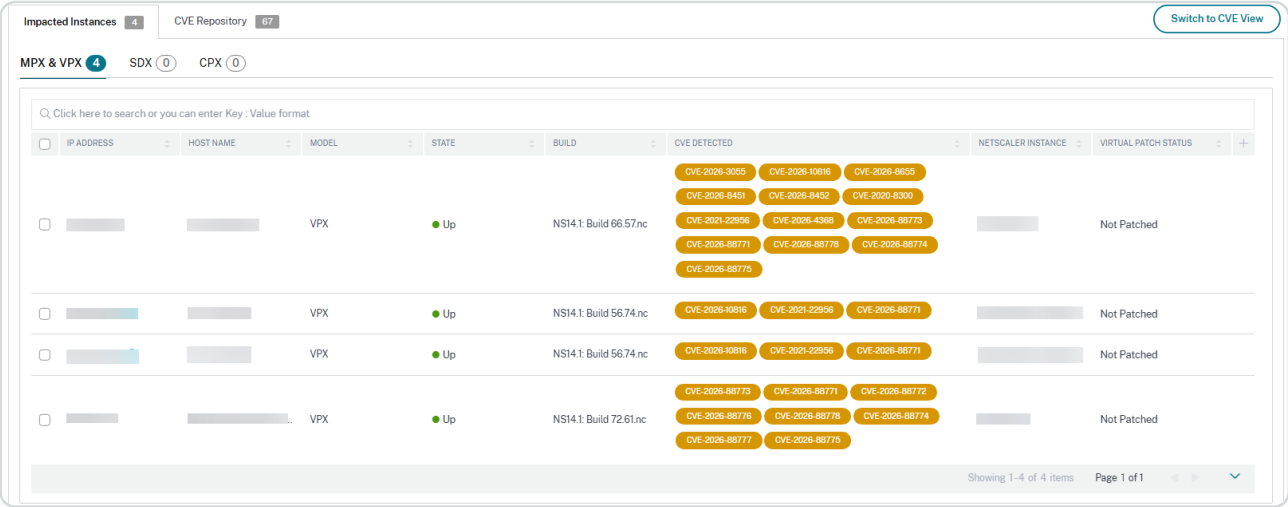
© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。

此步骤可以一次性完成所有易受攻击的 NetScaler 实例。有关更多信息，请参阅CVE 检测。

识别并修复 CVE-2026-88773 漏洞

在 NetScaler Console® 安全通告仪表板中，单击“**CVE 检测**”。在“**受影响的实例**”选项卡上，搜索 CVE-2026-88773。将显示受 CVE-2026-88773 影响的 NetScaler 实例列表。



有关安全通告仪表板的更多信息，请参阅安全通告。

注意：

安全通告系统扫描可能需要几个小时才能完成，并在安全通告模块中反映 CVE-2026-88773 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

修复 CVE-2026-88773

对于受 CVE-2026-88773 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。

在 GUI 中，在“**CVE 检测 > 受影响的实例**”下，选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。

此步骤可以一次性为所有易受攻击的 NetScaler 实例完成。有关更多信息，请参阅CVE 检测。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

识别并修复 CVE-2026-88774 的漏洞

在 NetScaler Console® 安全通告仪表板中，单击“**CVE 检测**”。在“**受影响实例**”选项卡上，搜索 CVE-2026-88774。将显示受 CVE-2026-88774 影响的 NetScaler 实例列表。

CVE-2026-sep 的安全通告仪表板(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-sep.png)

有关安全通告仪表板的更多信息，请参阅 安全通告。

注意：

安全通告系统扫描可能需要几个小时才能完成，并在安全通告模块中反映 CVE-2026-88774 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

修复 CVE-2026-88774

对于受 CVE-2026-88774 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。

在 GUI 中，在“**CVE 检测 > 受影响实例**”下，选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

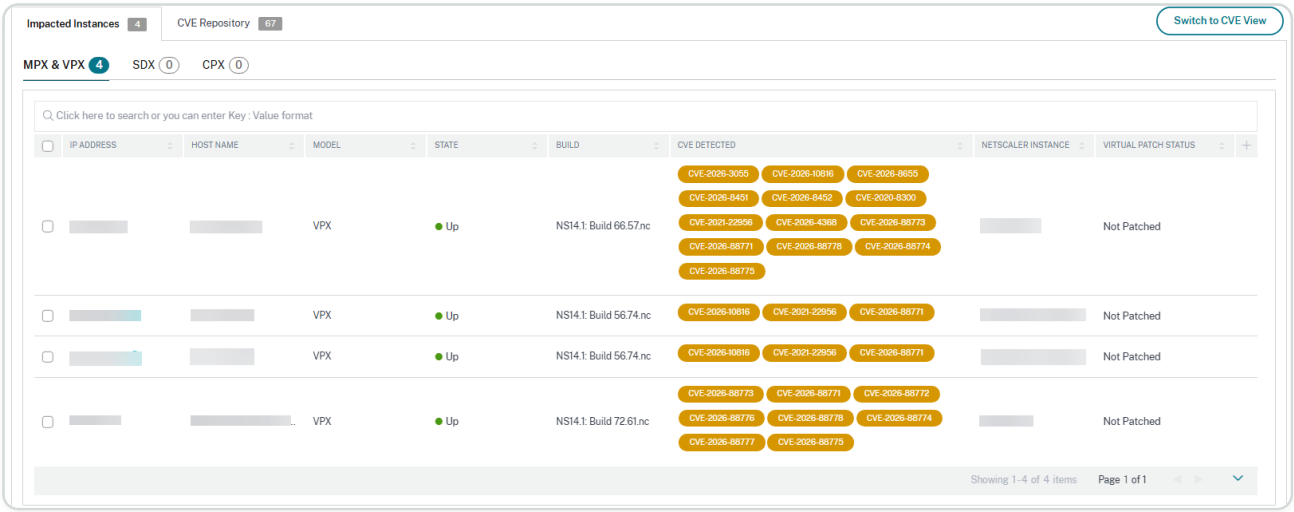
有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。

此步骤可以一次性完成所有易受攻击的 NetScaler 实例。有关更多信息，请参阅 CVE 检测。

识别并修复 CVE-2026-88775 的漏洞

在 NetScaler Console® 安全通报仪表板中，单击**CVE 检测**。在**受影响实例**选项卡上，搜索 CVE-2026-88775。将显示受 CVE-2026-88775 影响的 NetScaler 实例列表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关安全通报仪表板的更多信息，请参阅 安全通报。

注意：

安全通报系统扫描可能需要几个小时才能完成，并在安全通报模块中反映 CVE-2026-88775 的影响。要更快地查看影响，请单击**立即扫描**启动按需扫描。

修复 CVE-2026-88775

对于受 CVE-2026-88775 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。

在 GUI 中，在**CVE 检测 > 受影响实例**下，选择实例并单击**继续升级工作流**。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。

此步骤可以一次性完成所有易受攻击的 NetScaler 实例。有关更多信息，请参阅 CVE 检测。

识别并修复 CVE-2026-88776 的漏洞

在 NetScaler Console® 安全通告仪表板中，单击“**CVE 检测**”。在“**受影响的实例**”选项卡上，搜索 CVE-2026-88776。将显示受 CVE-2026-88776 影响的 NetScaler 实例列表。

CVE-2026-sep 的安全通告仪表板(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-sep.png)

有关安全通告仪表板的更多信息，请参阅 安全通告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

安全通告系统扫描可能需要几个小时才能完成并在安全通告模块中反映 CVE-2026-88776 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

修复 CVE-2026-88776

对于受 CVE-2026-88776 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复的发行版本和内部版本。

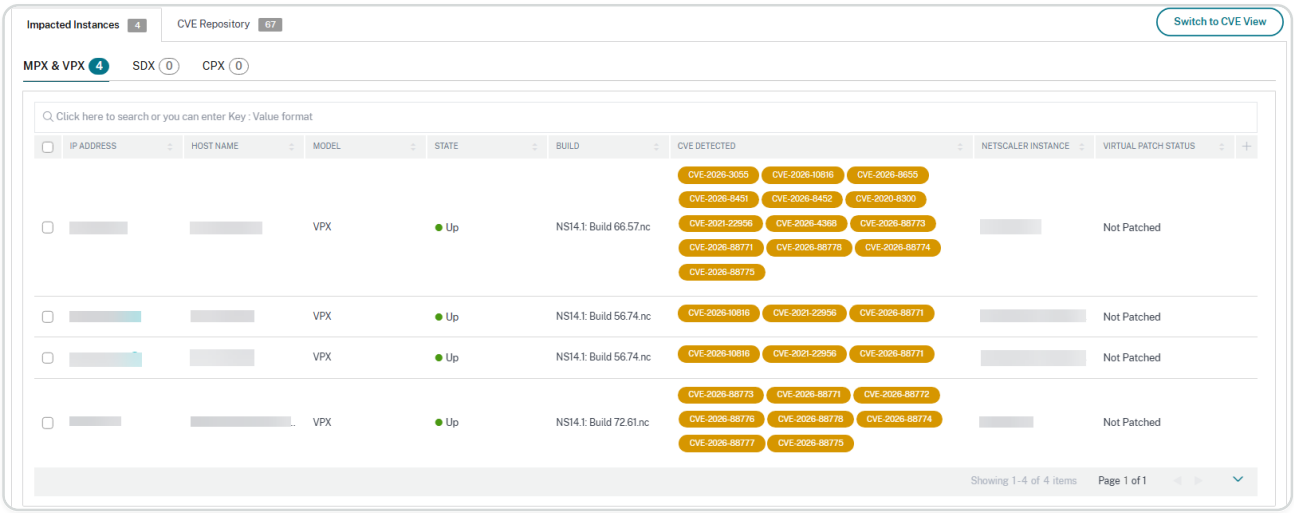
在 GUI 中，在“**CVE 检测 > 受影响的实例**”下，选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。

此步骤可以一次性完成所有易受攻击的 NetScaler 实例。有关更多信息，请参阅 CVE 检测。

识别并修复 CVE-2026-88777 的漏洞

在 NetScaler Console® 安全通报仪表板中，单击 **CVE 检测**。在 **受影响实例** 选项卡上，搜索 CVE-2026-88777。将显示受 CVE-2026-88777 影响的 NetScaler 实例列表。



有关安全通报仪表板的更多信息，请参阅 安全通报。

注意：

安全通报系统扫描可能需要几个小时才能完成，并在安全通报模块中反映 CVE-2026-88777 的影响。要更快地查看影响，请通过单击 **立即扫描** 启动按需扫描。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

修复 CVE-2026-88777

对于受 CVE-2026-88777 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。

在 GUI 中，在 **CVE 检测 > 受影响实例** 下，选择实例并单击 **继续升级工作流**。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。

此步骤可以一次性完成，适用于所有易受攻击的 NetScaler 实例。有关更多信息，请参阅 CVE 检测。

修复 CVE-2026-88778 的漏洞

在 NetScaler Console 安全公告仪表板中，在 **当前 CVE `<number of>` 受 CVE 影响的 NetScaler 实例** 下，您可以看到所有因 CVE-2026-88778 而易受攻击的实例。要查看受 CVE 影响的实例的详细信息，请选择 CVE-2026-88778，然后单击**查看受影响的实例**。

CVE-2026-sep 的安全公告仪表板(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-sep.png)

修复 CVE-2026-88778

对于受 CVE-2026-88778 影响的 NetScaler 实例，修复是一个两步过程。在 GUI 中，在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您可以看到步骤 1 和 2。

CVE-2026-sep 的安全公告仪表板(/en-us/netscaler-application-delivery-management-software/media/sep-cves-cve-info.png)

这两个步骤包括：

1. 将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。
2. 在配置作业中使用可自定义的内置配置模板应用所需的配置命令。

在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您会看到此两步修复过程的两个独立工作流：它们是 **继续升级工作流** 和 **继续配置作业工作流**。

步骤 1：升级受影响的 NetScaler 实例

要升级易受攻击的实例，请选择实例并单击**继续升级工作流**。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

受影响的 NetScaler 实例(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-sep.png)

步骤 2：应用配置命令

升级受影响的实例后，在 `<number of>` **受 CVE 影响的 NetScaler 实例** 窗口中，选择受 CVE-2026-88778 影响的实例，然后单击**继续配置作业工作流**。该工作流包括以下步骤。

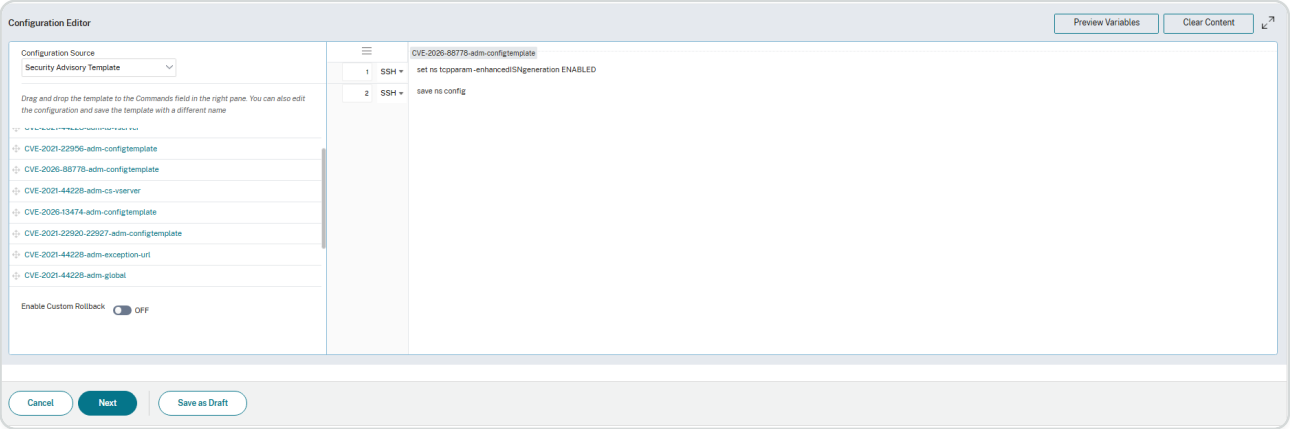
1. 自定义配置。
2. 审查自动填充的受影响实例。
3. 为作业指定变量输入。
4. 审查填充了变量输入的最终配置。
5. 运行作业。

在选择实例并点击“**Proceed to configuration job workflow**”之前，请记住以下几点：

- 对于仅受 CVE-2026-88778 影响的多个 NetScaler 实例：您可以一次性在所有实例上运行配置作业。例如，您有 NetScaler 1、NetScaler 2 和 NetScaler 3，并且它们都仅受 CVE-2026-88778 影响。选择所有这些实例并点击“**Proceed to configuration job workflow**”，内置配置模板将自动填充在“**Select configuration**”下。

步骤 1：选择配置

在配置作业工作流中，内置配置基本模板将自动填充在“**Select configuration**”下。



步骤 2：选择实例

受影响的实例将自动填充在“**Select Instances**”下。选择实例。点击“**Next**”。在下一步中预览配置。点击“**Next**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

对于集群模式下的 NetScaler 实例，使用安全建议，NetScaler Console 仅支持在集群配置协调器 (CCO) 节点上运行配置作业。请单独在非 CCO 节点上运行命令。

步骤 3：运行配置

点击 **完成** 以运行配置作业。

作业运行后，它会显示在 **基础架构 > 配置 > 配置作业** 下。

完成针对所有易受攻击的 NetScaler 实例的这两个补救步骤后，您可以运行按需扫描以查看修订后的安全状况。

识别并修复 CVE-2026-19490 的漏洞

在 NetScaler Console® 安全通告仪表板中，单击 **CVE 检测**。在**受影响的实例**选项卡上，搜索 CVE-2026-19490。将显示受 CVE-2026-19490 影响的 NetScaler 实例列表。

CVE-2026-19490 的安全通告仪表板 (/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-19490.png)

有关安全通告仪表板的更多信息，请参阅 安全通告。

注意：

安全通告系统扫描可能需要几个小时才能完成并在安全通告模块中反映 CVE-2026-19490 的影响。要更快地查看影响，请单击**立即扫描**启动按需扫描。

修复 CVE-2026-19490

对于受 CVE-2026-19490 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。

在 GUI 中，在 **CVE 检测 > 受影响的实例**下，选择实例并单击**继续升级工作流**。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

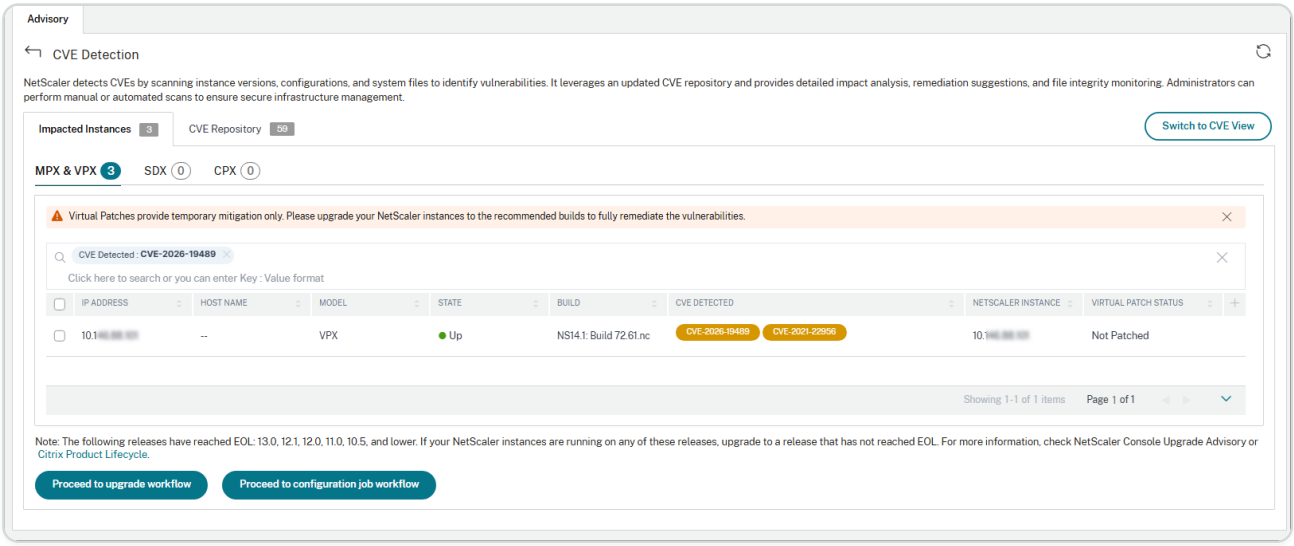
有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。

此步骤可以一次性为所有易受攻击的 NetScaler 实例完成。有关更多信息，请参阅 CVE 检测。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

识别并修复 CVE-2026-19489 的漏洞

在 NetScaler Console® 安全通告仪表板中，单击 **CVE 检测**。在 **受影响的实例** 选项卡上，搜索 CVE-2026-19489。将显示受 CVE-2026-19489 影响的 NetScaler 实例列表。



有关安全通告仪表板的更多信息，请参阅 安全通告。

注意：

安全通告系统扫描可能需要几个小时才能完成，并在安全通告模块中反映 CVE-2026-19489 的影响。要更快地查看影响，请单击 **立即扫描** 启动按需扫描。

修复 CVE-2026-19489

对于受 CVE-2026-19489 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和构建。

在 GUI 中，在 **CVE 检测 > 受影响的实例** 下，选择实例并单击 **继续升级工作流**。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

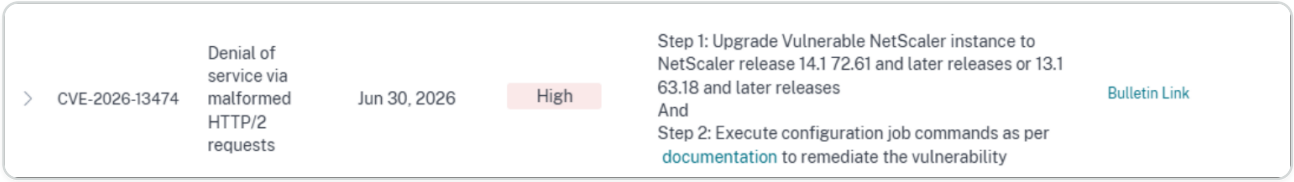
有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。

此步骤可以一次性完成所有易受攻击的 NetScaler 实例。有关更多信息，请参阅 CVE 检测。

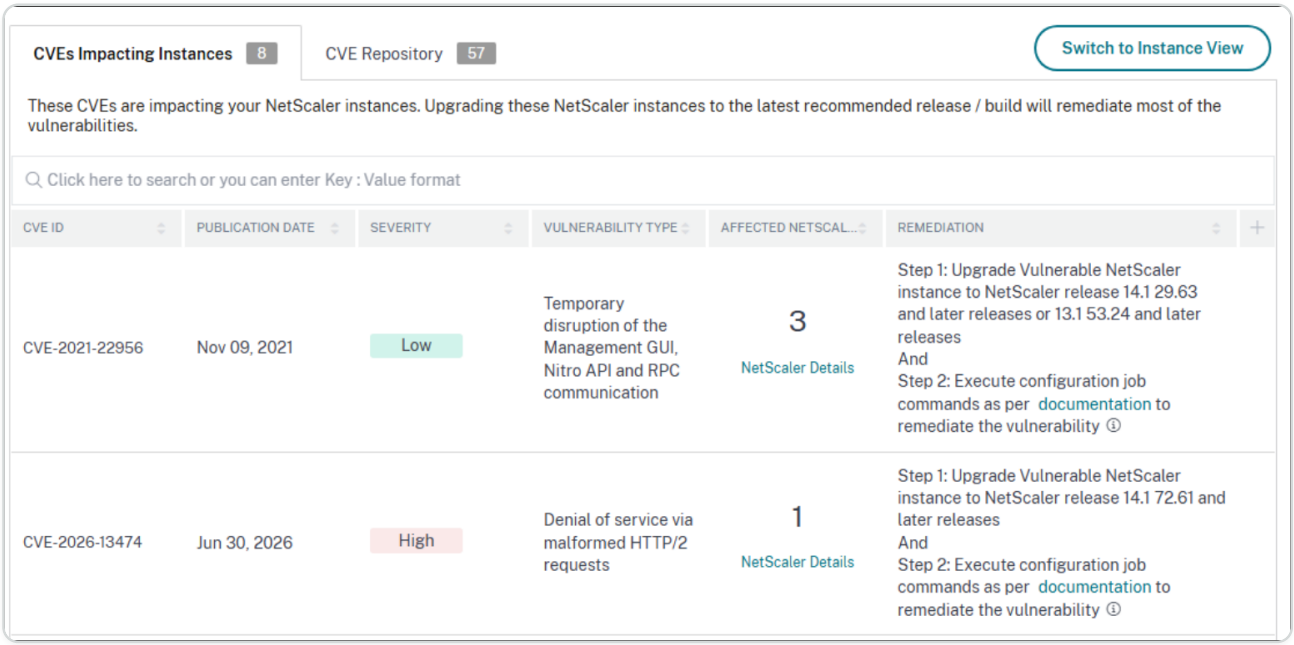
修复 CVE-2026-13474 的漏洞

在 NetScaler Console 安全通告仪表板中，在 **当前 CVE > `<number of>` 受常见漏洞和披露 (CVE) 影响的 NetScaler 实例** 下，您可以看到所有受此特定 CVE 影响的易受攻击实例。要查看受 CVE-2026-13474 影响的实例的详细信息，请选择 **CVE-2026-13474** 并单击 **查看受影响的实例**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



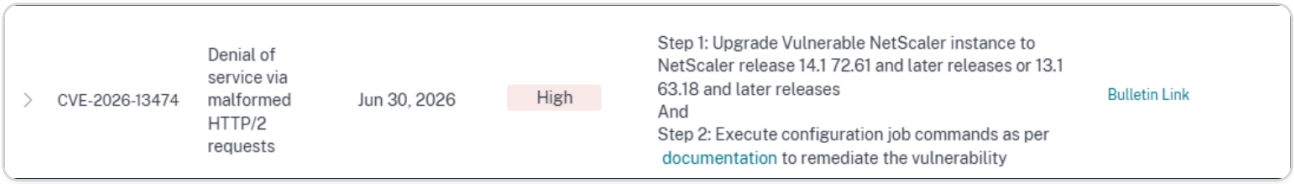
`<number of>` **受 CVE 影响的 NetScaler 实例** 窗口随即出现。在此处，您可以看到受 CVE-2026-13474 影响的 NetScaler 实例的数量和详细信息。



有关安全通告仪表板的更多信息，请参阅 安全通告。

修复 CVE-2026-13474

对于受 CVE-2026-13474 影响的 NetScaler 实例，修复是一个两步过程。在 GUI 中，在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您可以看到步骤 1 和 2。



这两个步骤包括：

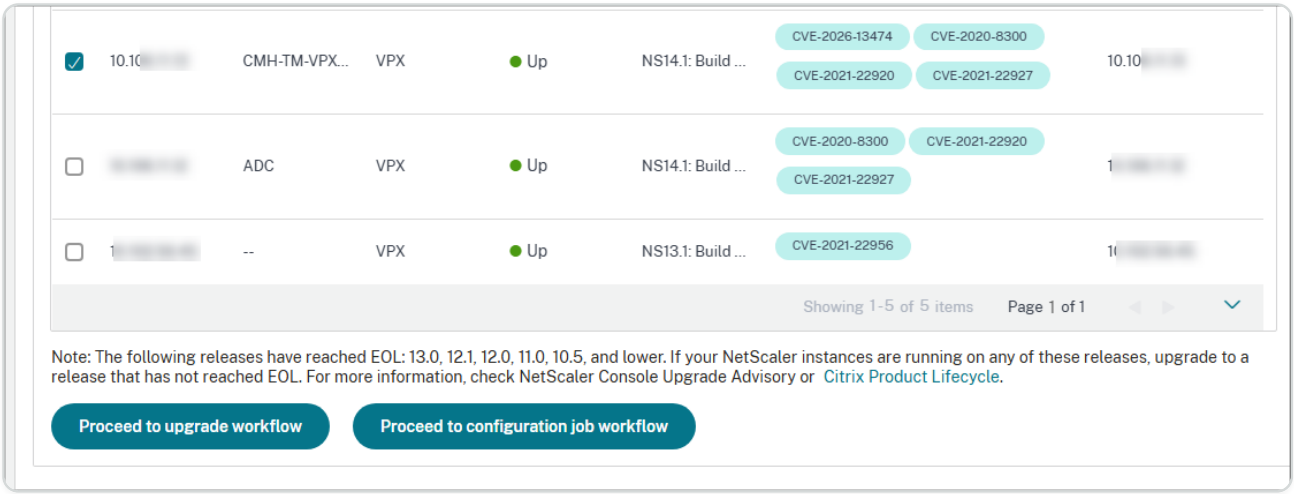
1. 将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。
2. 使用配置作业中可自定义的内置配置模板应用所需的配置命令。

在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您会看到此两步修复过程的两个独立工作流，分别是 **继续升级工作流** 和 **继续配置作业工作流**。

步骤 1：升级受影响的 NetScaler 实例

要升级易受攻击的实例，请选择这些实例并单击 **继续升级工作流**。升级工作流将打开，其中已填充了易受攻击的 NetScaler 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。

步骤 2：应用配置命令

升级受影响的实例后，在 `<number of>` **受 CVE 影响的 NetScaler 实例** 窗口中，选择受 CVE-2026-13474 影响的实例，然后单击 **继续执行配置作业工作流程**。该工作流程包括以下步骤。

1. 自定义配置。
2. 查看自动填充的受影响实例。
3. 为作业指定变量输入。
4. 查看填充了变量输入的最终配置。
5. 运行作业。

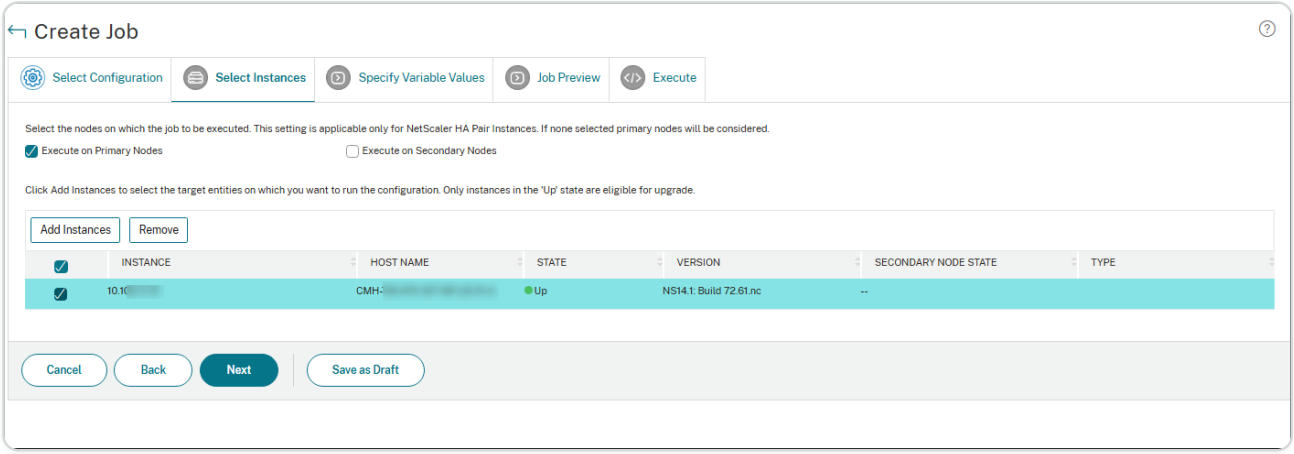
在选择实例并单击 **继续执行配置作业工作流程** 之前，请记住以下几点：

- 对于仅受 CVE-2026-13474 影响的多个 NetScaler 实例：您可以一次性在所有实例上运行配置作业。例如，您有 NetScaler 1、NetScaler 2 和 NetScaler 3，并且它们都仅受 CVE-2026-13474 影响。选择所有这些实例，然后单击 **继续执行配置作业工作流程**，内置配置模板将在 **选择配置** 下自动填充。

步骤 1：选择配置

在配置作业工作流程中，内置配置基本模板将在 **选择配置** 下自动填充。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



步骤 2：选择实例

受影响的实例会在“**选择实例**”下自动填充。选择实例，然后单击“**下一步**”。在下一步中，预览配置，然后单击“**下一步**”。

> **注意：**
>
> 对于集群模式下的 NetScaler 实例，使用安全建议时，NetScaler Console 仅支持在集群配置协调器 (CCO) 节点上运行配置作业。请在非 CCO 节点上单独运行命令。

CVE-2026-13474 的补救步骤(/en-us/netscaler-console-service/media/cve-2026-13474-remediation-step-2.png)

步骤 3：运行配置

单击“**完成**”以运行配置作业。

CVE-2026-13474 的补救步骤(/en-us/netscaler-console-service/media/cve-2026-13474-remediation-step-3.png)

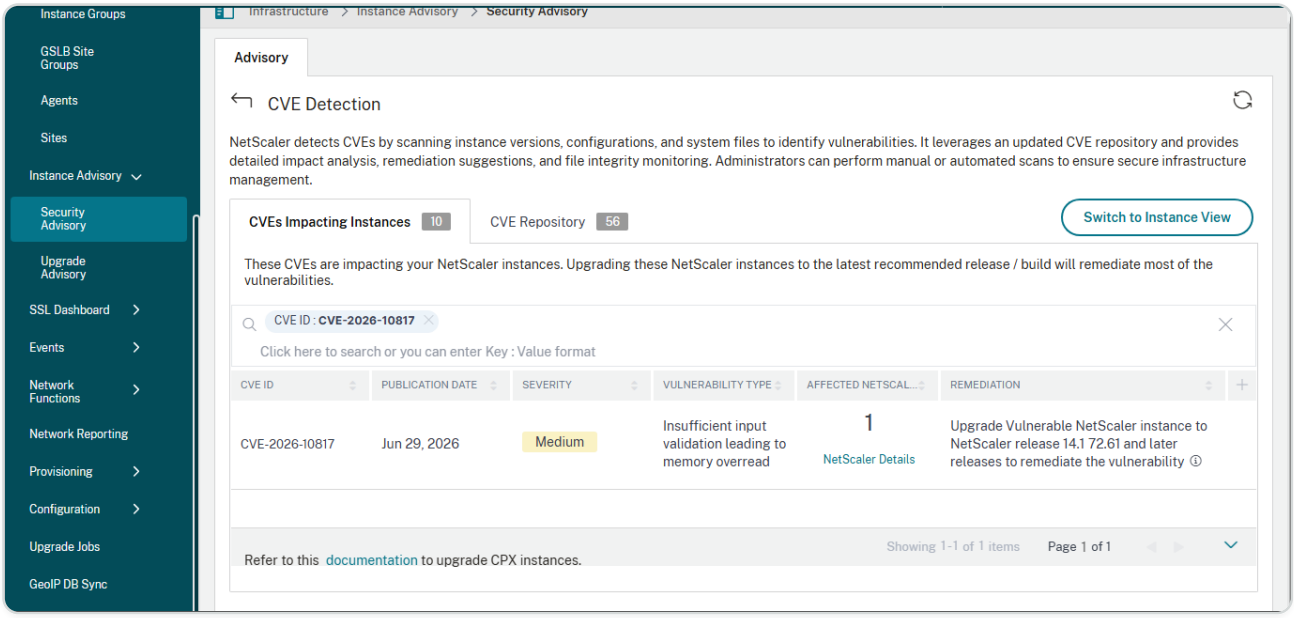
作业运行后，它会显示在“**基础架构 > 配置 > 配置作业**”下。

完成所有易受攻击的 NetScaler 实例的两个补救步骤后，您可以运行按需扫描以查看修订后的安全状况。

识别并修复 CVE-2026-10817 的漏洞

在 NetScaler Console® 安全通告仪表板中，单击“**CVE 检测**”。在“**受影响的实例**”选项卡上，搜索 CVE-2026-10817。将显示受 CVE-2026-10817 影响的 NetScaler 实例列表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关安全通告仪表板的更多信息，请参阅安全通告。

注意：

安全通告系统扫描可能需要几个小时才能完成，并在安全通告模块中反映 CVE-2026-10817 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

修复 CVE-2026-10817

对于受 CVE-2026-10817 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复的发行版本和内部版本。

在 GUI 中，在“**CVE 检测 > 受影响的实例**”下，选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充了易受攻击的 NetScaler 实例。

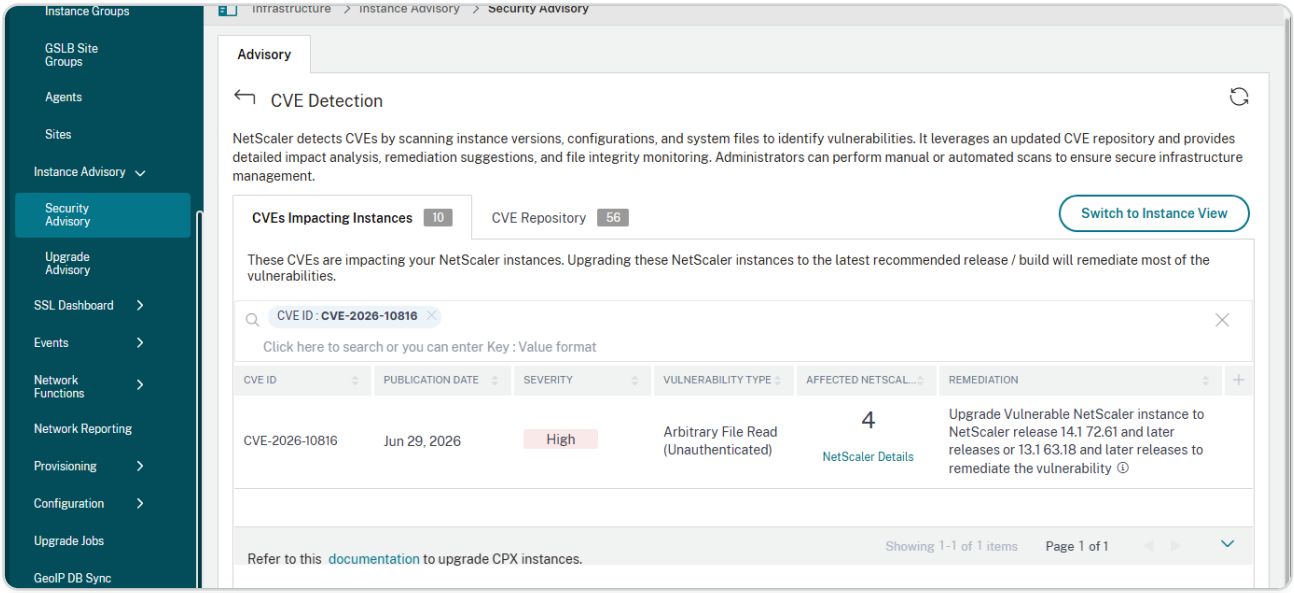
有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。

此步骤可以一次性完成所有易受攻击的 NetScaler 实例。有关更多信息，请参阅CVE 检测。

识别并修复 CVE-2026-10816 的漏洞

在 NetScaler Console® 安全通报仪表板中，单击 **CVE 检测**。在**受影响的实例**选项卡上，搜索 CVE-2026-10816。将显示受 CVE-2026-10816 影响的 NetScaler 实例列表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关安全通报仪表板的更多信息，请参阅安全通报。

注意：

安全通报系统扫描可能需要几个小时才能完成，并在安全通报模块中反映 CVE-2026-10816 的影响。要更快地查看影响，请单击 **立即扫描** 启动按需扫描。

修复 CVE-2026-10816

对于受 CVE-2026-10816 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。

在 GUI 中，在 **CVE 检测 > 受影响的实例** 下，选择实例并单击 **继续升级工作流**。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。

此步骤可以一次性完成所有易受攻击的 NetScaler 实例。有关更多信息，请参阅CVE 检测。

识别并修复 CVE-2026-8655 漏洞

在 NetScaler Console® 安全通报仪表板中，单击“**CVE 检测**”。在“**受影响的实例**”选项卡上，搜索 CVE-2026-8655。将显示受 CVE-2026-8655 影响的 NetScaler 实例列表。

CVE-2026-8655 的安全通报仪表板(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2026-8655.png)

有关安全通报仪表板的更多信息，请参阅安全通报。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

安全通报系统扫描可能需要几个小时才能完成，并在安全通报模块中反映 CVE-2026-8655 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

修复 CVE-2026-8655

对于受 CVE-2026-8655 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。

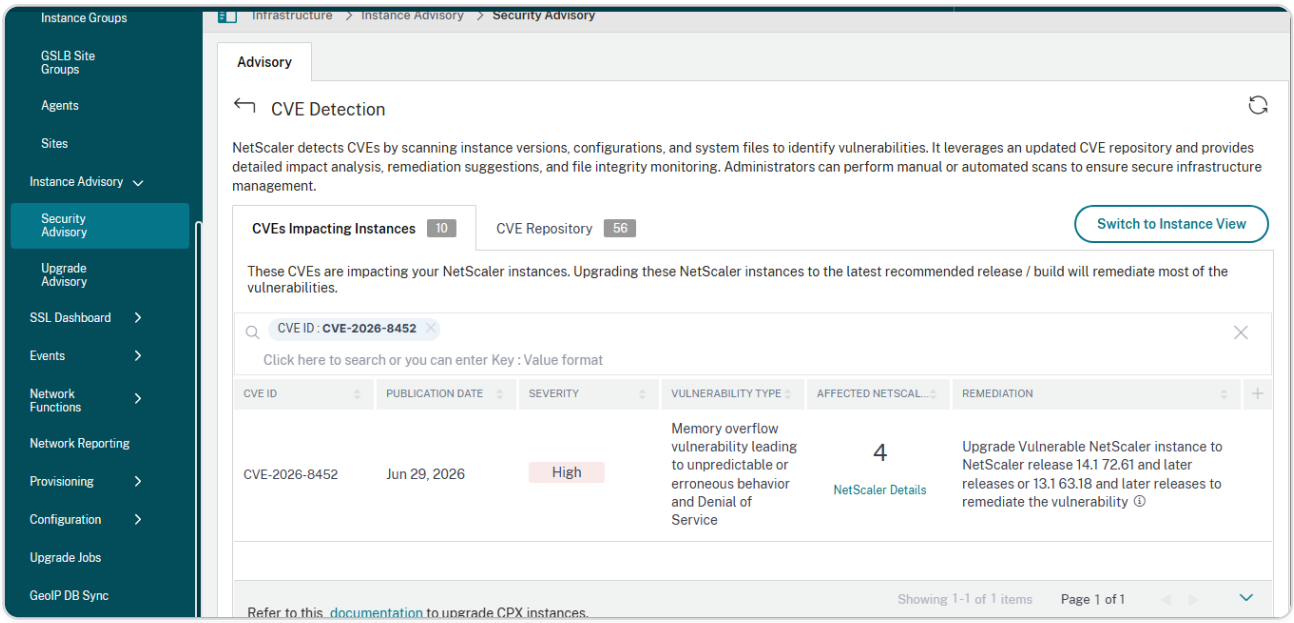
在 GUI 中，在“**CVE 检测 > 受影响的实例**”下，选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。

此步骤可以一次性完成所有易受攻击的 NetScaler 实例。有关更多信息，请参阅CVE 检测。

识别并修复 CVE-2026-8452 的漏洞

在 NetScaler Console® 安全通报仪表板中，单击“**CVE 检测**”。在“**受影响的实例**”选项卡上，搜索 CVE-2026-8452。将显示受 CVE-2026-8452 影响的 NetScaler 实例列表。



有关安全通报仪表板的更多信息，请参阅安全通报。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

安全通报系统扫描可能需要几个小时才能完成，并在安全通报模块中反映 CVE-2026-8452 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

修复 CVE-2026-8452

对于受 CVE-2026-8452 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。

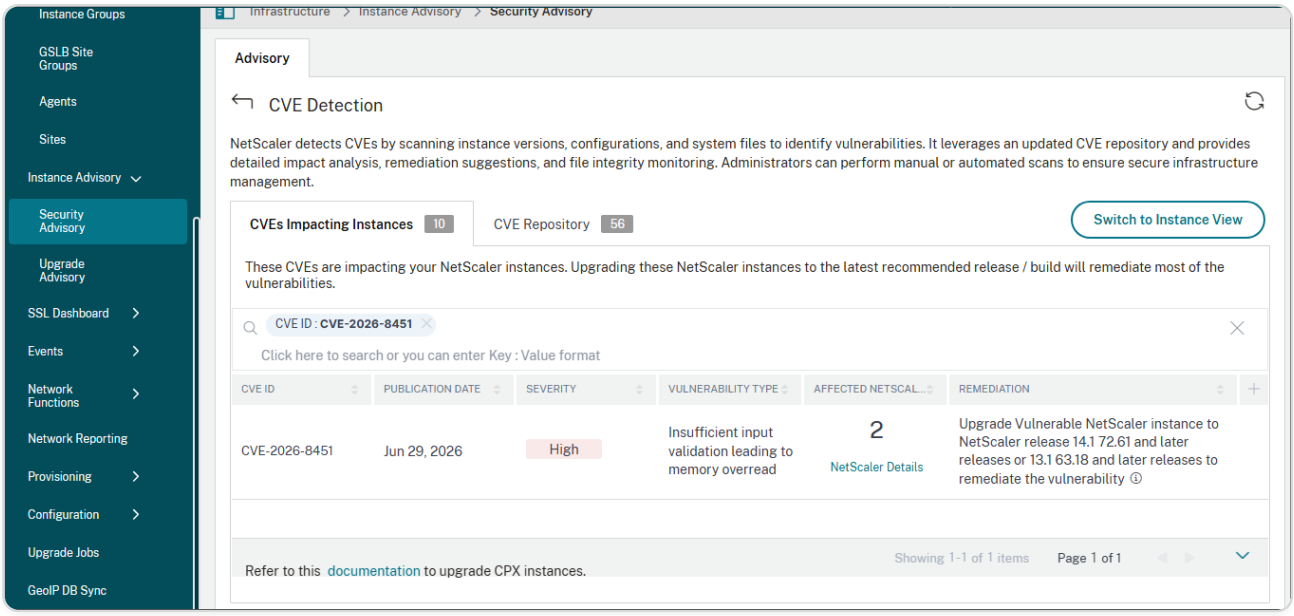
在 GUI 中，在“**CVE 检测 > 受影响的实例**”下，选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。

此步骤可以一次性完成所有易受攻击的 NetScaler 实例。有关更多信息，请参阅CVE 检测。

识别并修复 CVE-2026-8451 漏洞

在 NetScaler Console® 安全通告仪表板中，单击“**CVE 检测**”。在“**受影响的实例**”选项卡上，搜索 CVE-2026-8451。将显示受 CVE-2026-8451 影响的 NetScaler 实例列表。



有关安全通告仪表板的更多信息，请参阅安全通告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

安全通告系统扫描可能需要几个小时才能完成，并在安全通告模块中反映 CVE-2026-8451 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

修复 CVE-2026-8451

对于受 CVE-2026-8451 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。

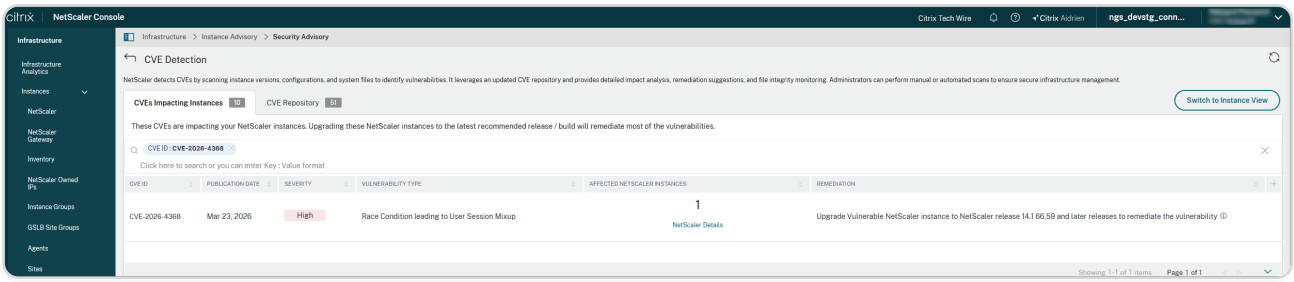
在 GUI 中，在“**CVE 检测 > 受影响的实例**”下，选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。

此步骤可以一次性完成所有易受攻击的 NetScaler 实例。有关更多信息，请参阅CVE 检测。

识别并修复 CVE-2026-4368 漏洞

在 NetScaler Console® 安全通告仪表板中，点击**CVE 检测**。在**受影响的实例**选项卡中，搜索 CVE-2026-4368。将显示受 CVE-2026-4368 影响的 NetScaler 实例列表。



有关安全通告仪表板的更多信息，请参阅安全通告。

注意：

安全通告系统扫描可能需要几个小时才能完成，并在安全通告模块中反映 CVE-2026-4368 的影响。要更快地查看影响，请点击**立即扫描**启动按需扫描。

修复 CVE-2026-4368

对于受 CVE-2026-4368 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复的版本和构建。

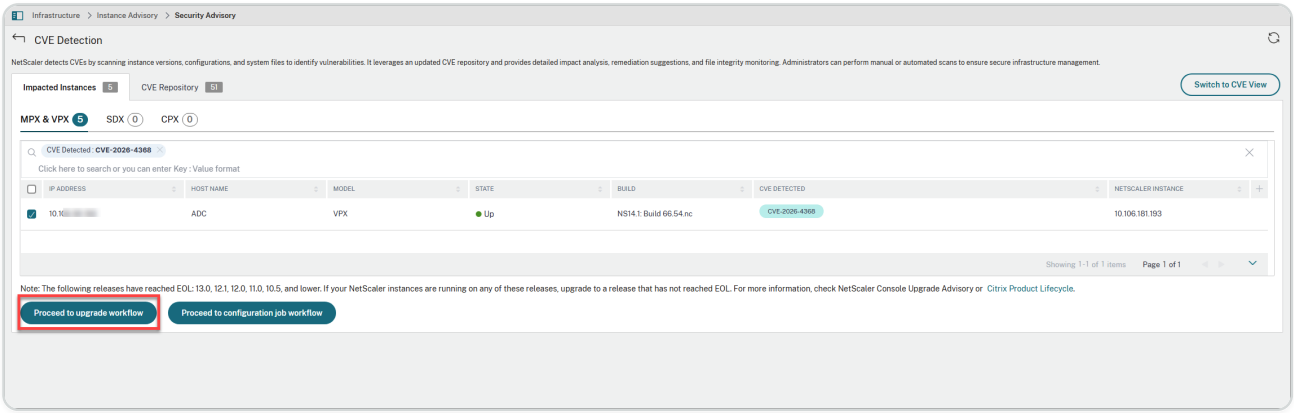
© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 GUI 中，在**CVE 检测 > 受影响的实例**下，选择实例并点击**继续升级工作流**。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

重要提示

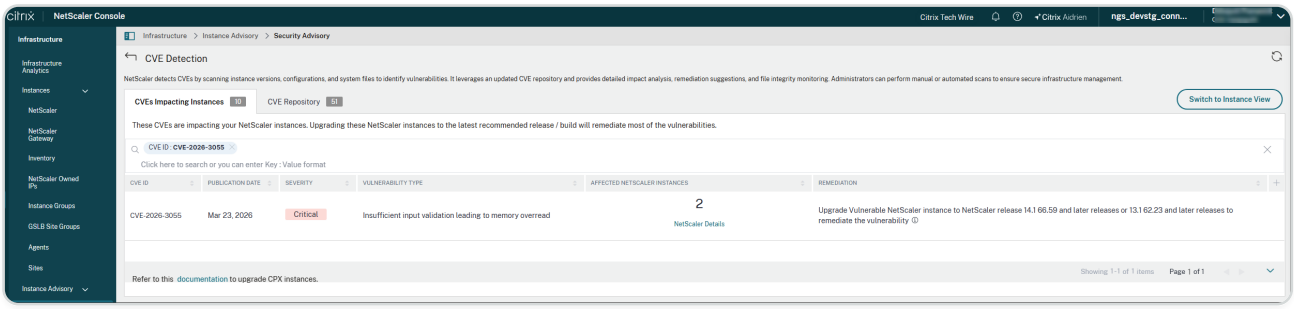
如果您的易受攻击的 NetScaler 实例已将 /etc/httpd.conf 文件复制到 /nsconfig 目录，请在规划 NetScaler 升级之前参阅自定义 NetScaler 配置的升级注意事项。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。



识别并修复 CVE-2026-3055 漏洞

在 NetScaler Console® 安全通报仪表板中，单击“**CVE 检测**”。在“**受影响的实例**”选项卡上，搜索 CVE-2026-3055。将显示受 CVE-2026-3055 影响的 NetScaler 实例列表。



有关安全通报仪表板的更多信息，请参阅安全通报。

注意：

安全通报系统扫描可能需要几个小时才能完成，并在安全通报模块中反映 CVE-2026-3055 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

修复 CVE-2026-3055

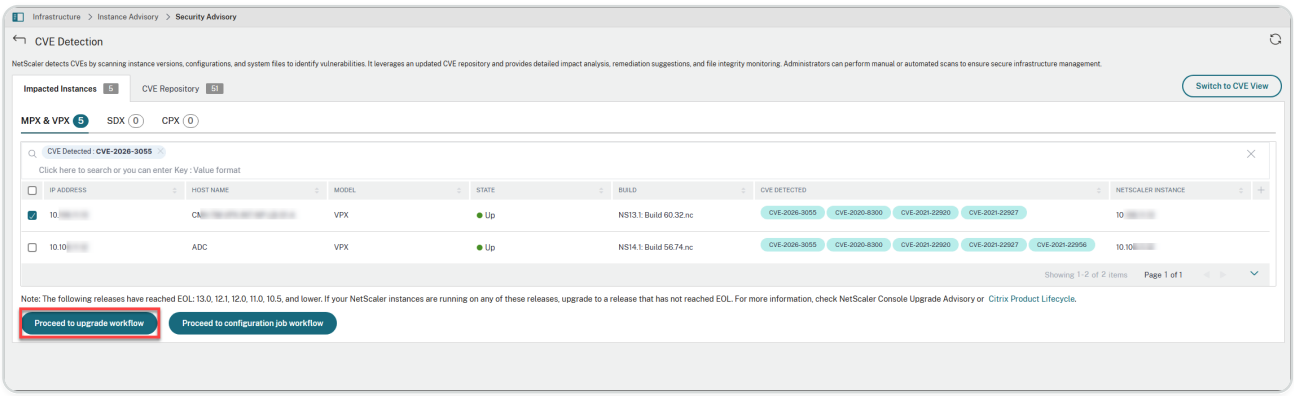
对于受 CVE-2026-3055 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。

在 GUI 中，在“**CVE 检测 > 受影响的实例**”下，选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

重要提示

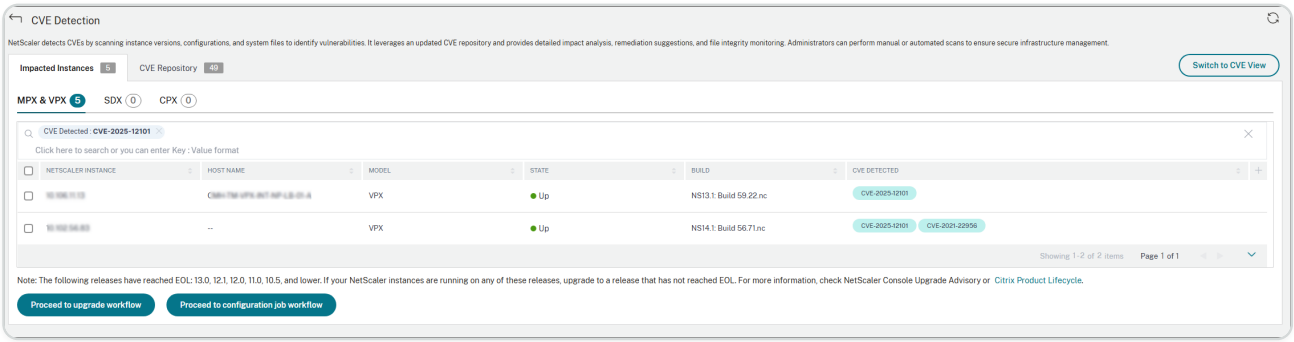
如果您的易受攻击的 NetScaler 实例已将 /etc/httpd.conf 文件复制到 /nsconfig 目录，请在规划 NetScaler 升级之前参阅自定义 NetScaler 配置的升级注意事项。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。



识别并修复 CVE-2025-12101 的漏洞

在 NetScaler Console® 安全通报仪表板中，单击“**CVE 检测**”。在“**受影响实例**”选项卡上，搜索 CVE-2025-12101。将显示受 CVE-2025-12101 影响的 NetScaler 实例列表。



有关安全通报仪表板的更多信息，请参阅安全通报。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

安全通报系统扫描可能需要几个小时才能完成，并在安全通报模块中反映 CVE-2025-12101 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

修复 CVE-2025-12101

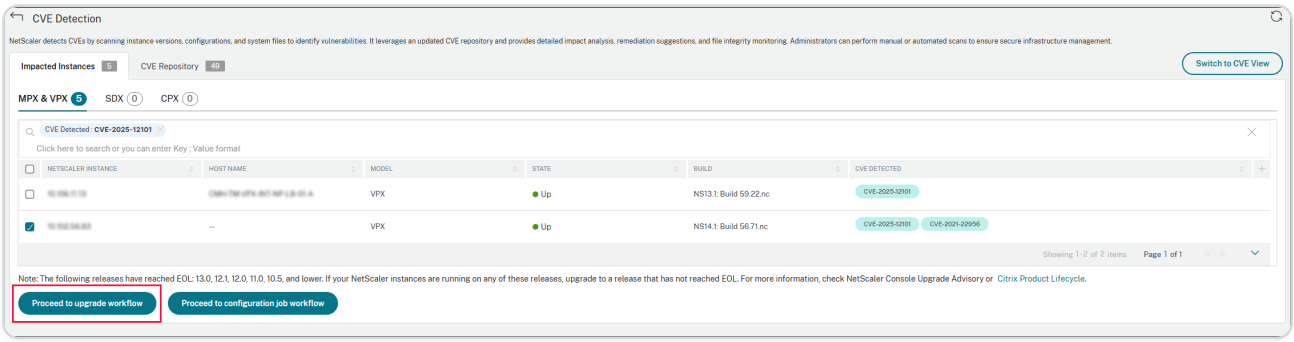
对于受 CVE-2025-12101 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。

在 GUI 中，在“**CVE 检测 > 受影响实例**”下，选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

重要提示

如果您的易受攻击的 NetScaler 实例已将 /etc/httpd.conf 文件复制到 /nsconfig 目录，请在规划 NetScaler 升级之前参阅自定义 NetScaler 配置的升级注意事项。

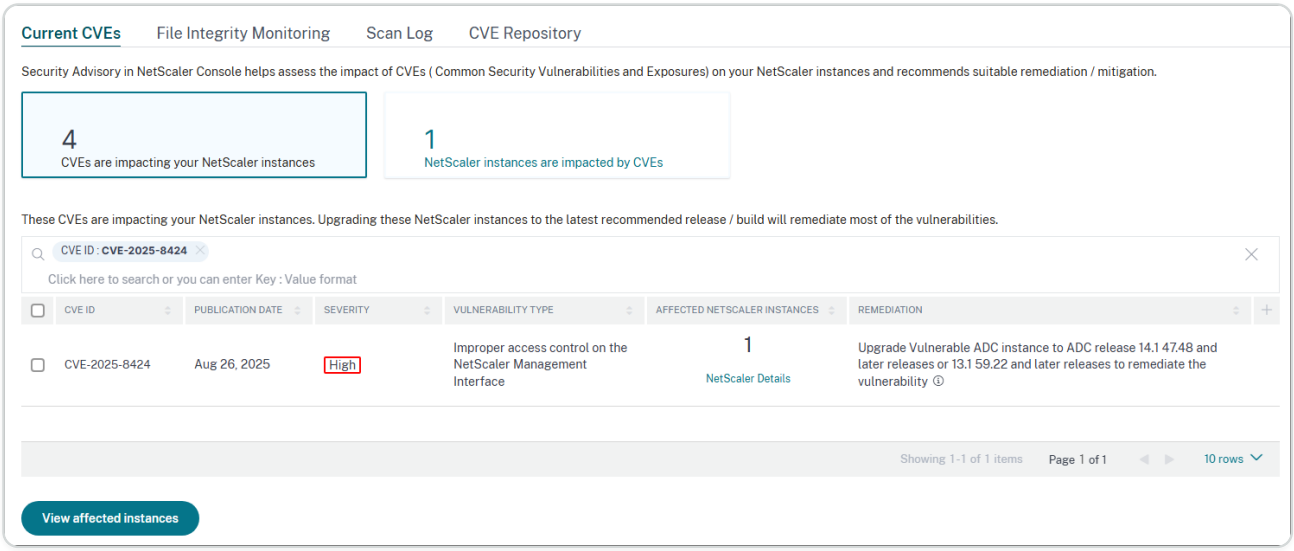
有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。



识别并修复 CVE-2025-8424 漏洞

在 NetScaler Console 安全通告仪表板中，在 **当前 CVE `<number of>` 受 CVE 影响的 NetScaler 实例** 下，您可以看到所有因 CVE-2025-8424 而易受攻击的实例。要查看受 CVE 影响的实例的详细信息，请选择 CVE-2025-8424 并单击 **查看受影响的实例**。

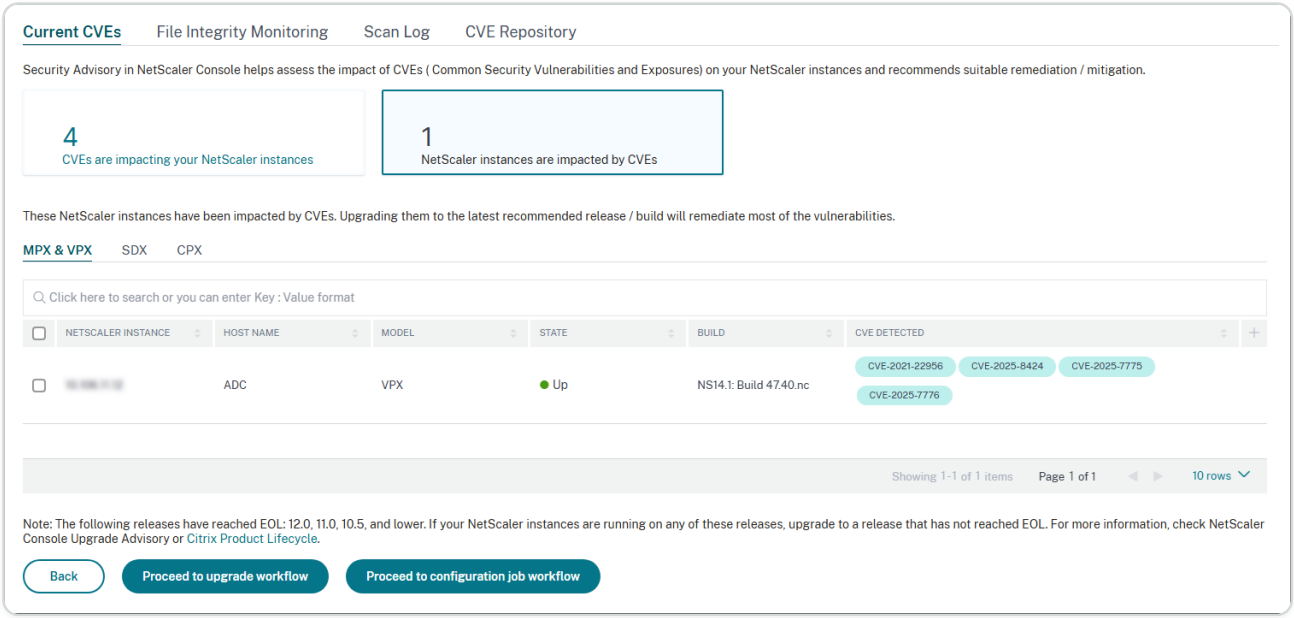
© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

要了解 NetScaler 漏洞的原因，请在安全通告的 **扫描日志** 选项卡中下载 CSV 报告。

出现 `<number of>` **受 CVE 影响的 NetScaler 实例** 窗口。在以下屏幕截图中，您可以看到受 CVE-2025-8424 影响的 NetScaler 实例的数量和详细信息。



有关安全通告仪表板的更多信息，请参阅 安全通告。

注意：

安全通告系统扫描可能需要几个小时才能完成并在安全通告模块中反映 CVE-2025-8424 的影响。要更快地查看影响，请单击 **立即扫描** 启动按需扫描。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

修复 CVE-2025-8424

对于受 CVE-2025-8424 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和构建。在 GUI 中，在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您可以看到修复步骤。

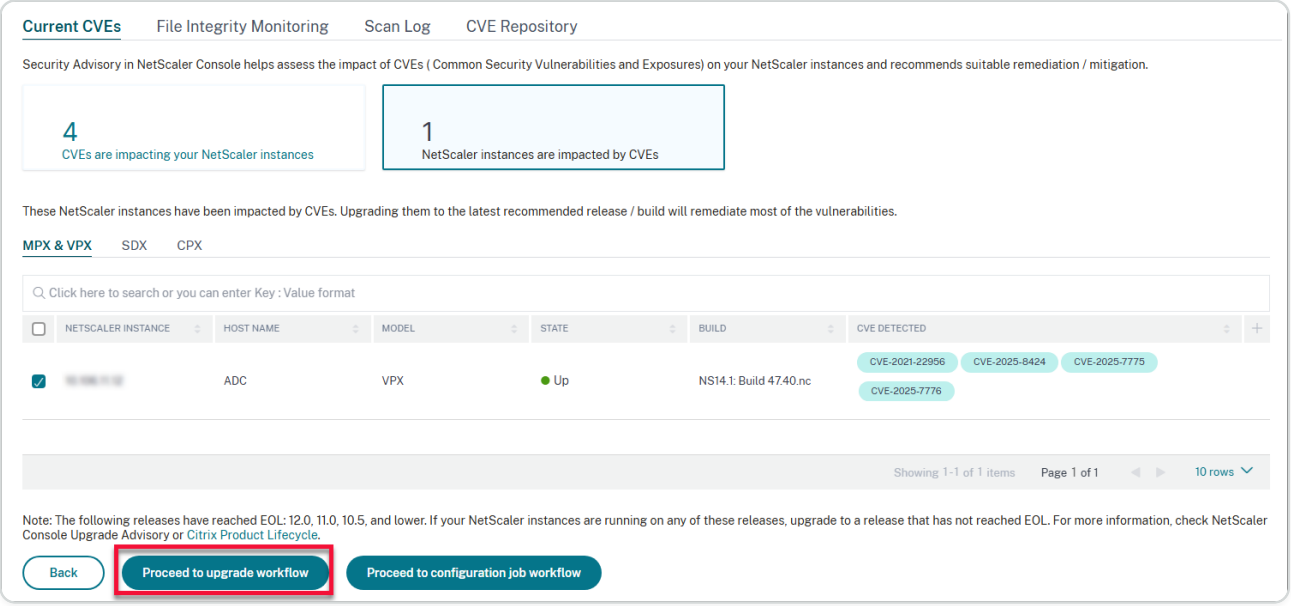
在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您会看到此单步修复过程的以下工作流，即 **继续升级工作流**。

要升级易受攻击的实例，请选择实例并单击 **继续升级工作流**。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

重要提示

如果您的易受攻击的 NetScaler 实例已将 /etc/httpd.conf 文件复制到 /nsconfig 目录，请在规划 NetScaler 升级之前参阅自定义 NetScaler 配置的升级注意事项。

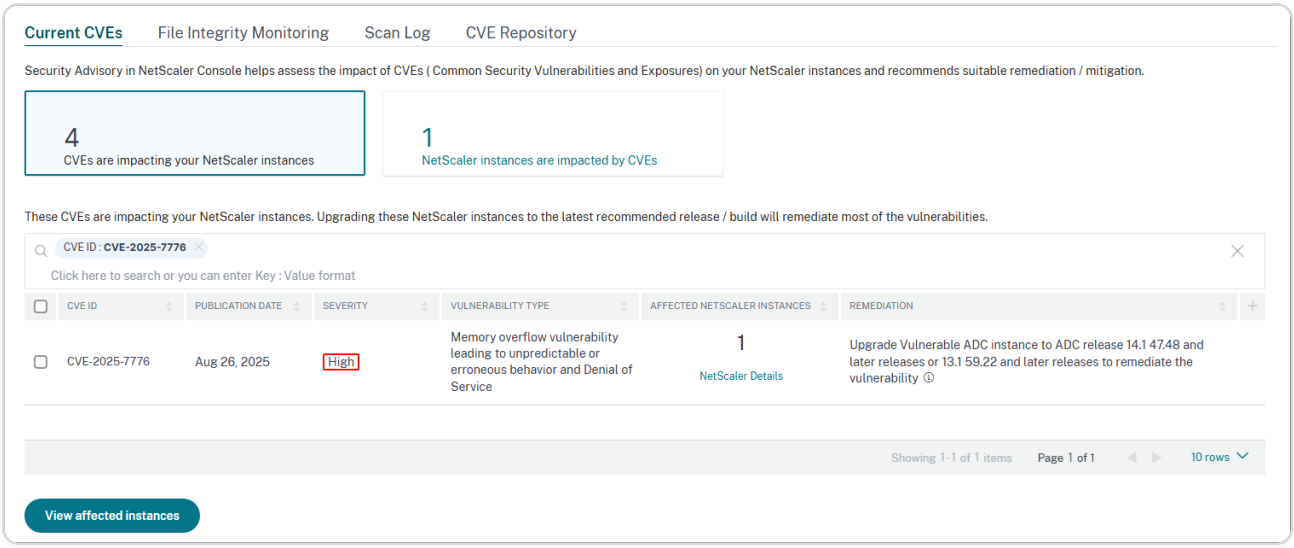
有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。



识别并修复 CVE-2025-7776 的漏洞

在 NetScaler Console 安全通告仪表板中，在“**当前 CVE** `<number of>` **受 CVE 影响的 NetScaler 实例**”下，您可以看到所有因 CVE-2025-7776 而易受攻击的实例。要查看受 CVE 影响的实例的详细信息，请选择 CVE-2025-7776，然后单击“**查看受影响的实例**”。

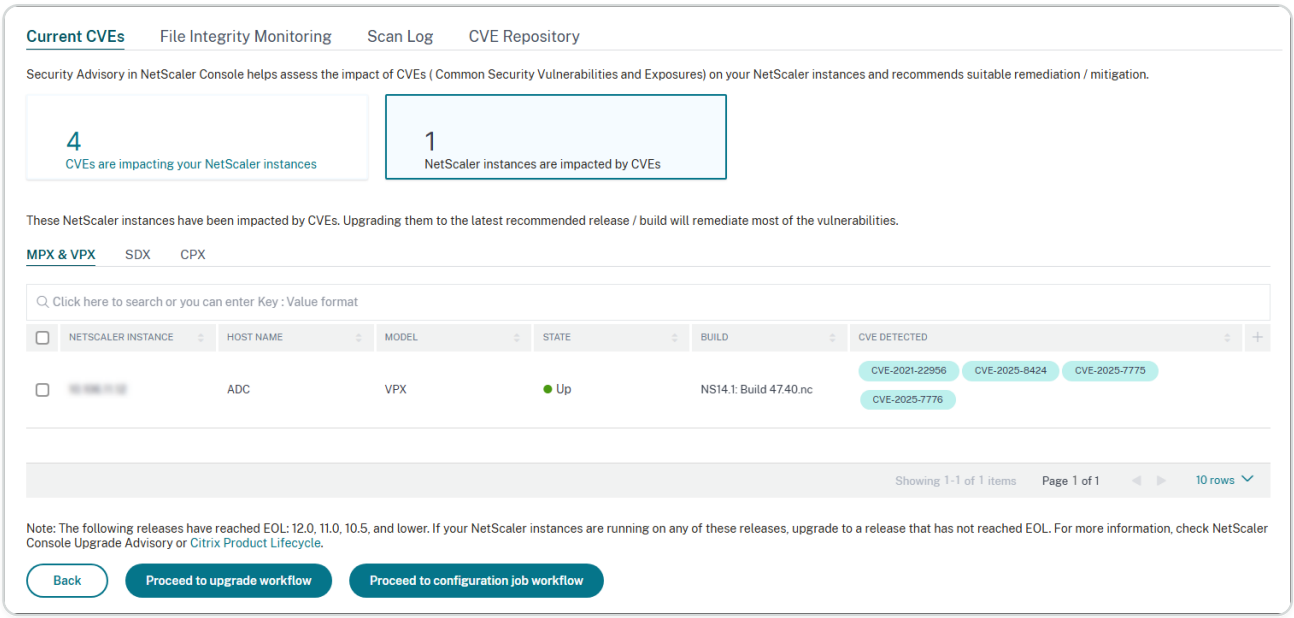
© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

要了解 NetScaler 漏洞的原因，请在安全通告的“**扫描日志**”选项卡中下载 CSV 报告。

“`<number of>` **受 CVE 影响的 NetScaler 实例**”窗口随即出现。在以下屏幕截图中，您可以看到受 CVE-2025-7776 影响的 NetScaler 实例的数量和详细信息。



有关安全通告仪表板的更多信息，请参阅安全通告。

注意：

安全通告系统扫描可能需要几个小时才能完成，并在安全通告模块中反映 CVE-2025-7776 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

修复 CVE-2025-7776

对于受 CVE-2025-7776 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复的发行版和版本。在 GUI 中，在“**当前 CVE > 受 CVE 影响的 NetScaler 实例**”下，您可以看到修复步骤。

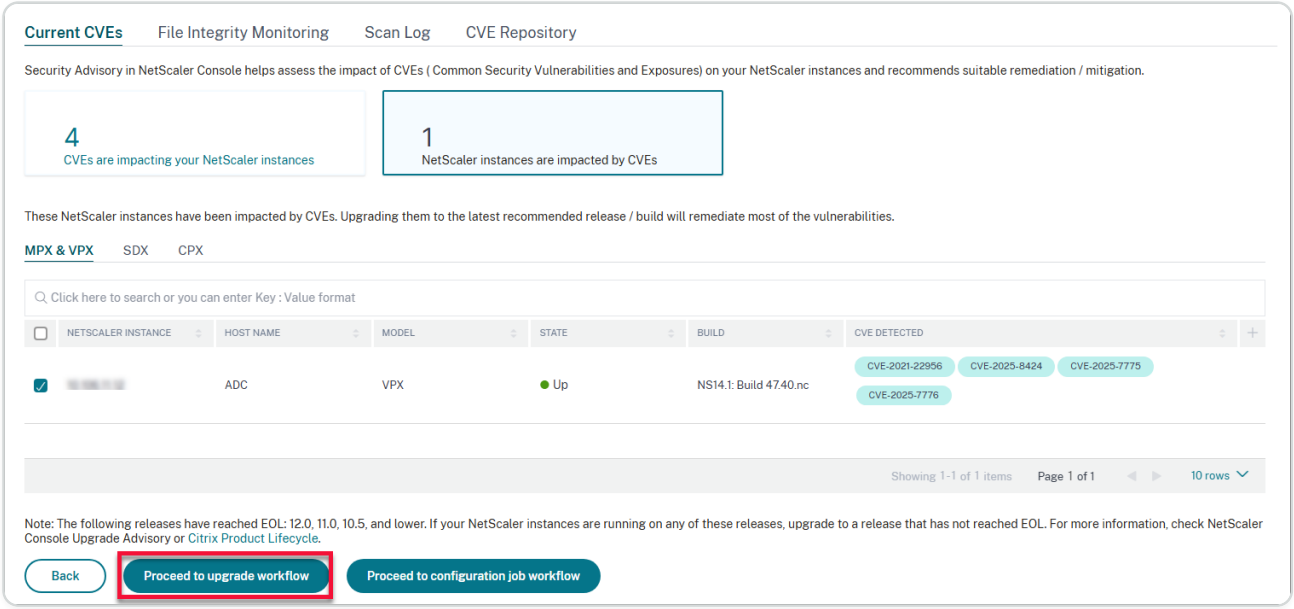
在“**当前 CVE > 受 CVE 影响的 NetScaler 实例**”下，您会看到此单步修复过程的以下工作流，即“**继续升级工作流**”。

要升级易受攻击的实例，请选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

重要提示

如果您的易受攻击的 NetScaler 实例已将 /etc/httpd.conf 文件复制到 /nsconfig 目录，请在规划 NetScaler 升级之前参阅 自定义 NetScaler 配置的升级注意事项。

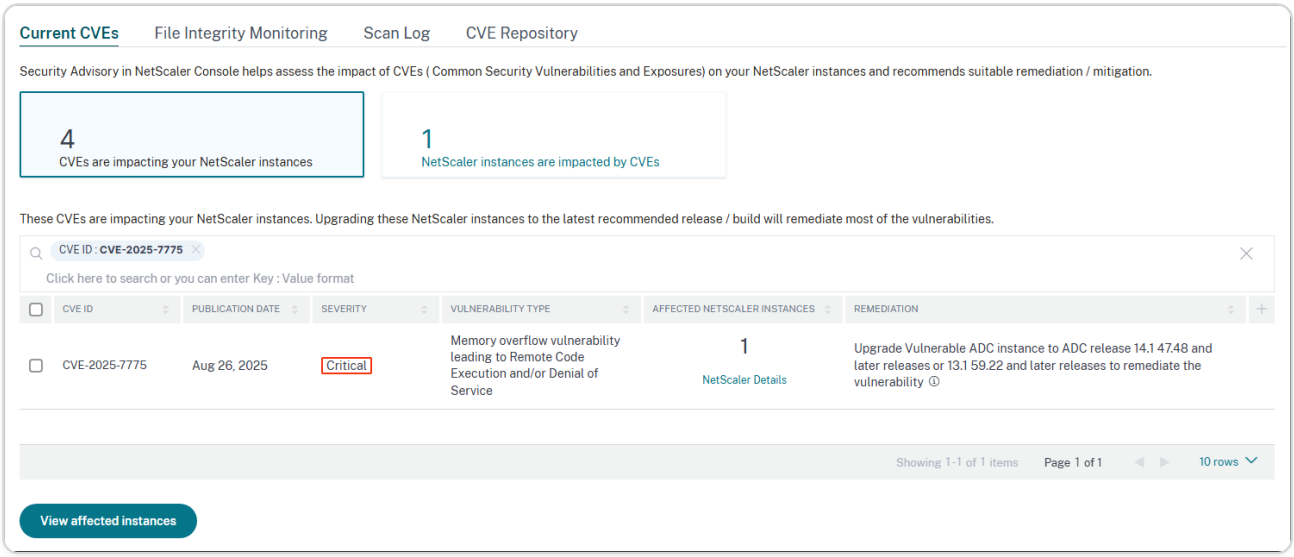
有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。



识别并修复 CVE-2025-7775 的漏洞

在 NetScaler Console 安全通报仪表板中，在“**当前 CVE `<number of>` 受 CVE 影响的 NetScaler 实例**”下，您可以看到所有因 CVE-2025-7775 而易受攻击的实例。要查看受 CVE 影响的实例的详细信息，请选择 CVE-2025-7775，然后单击“**查看受影响的实例**”。

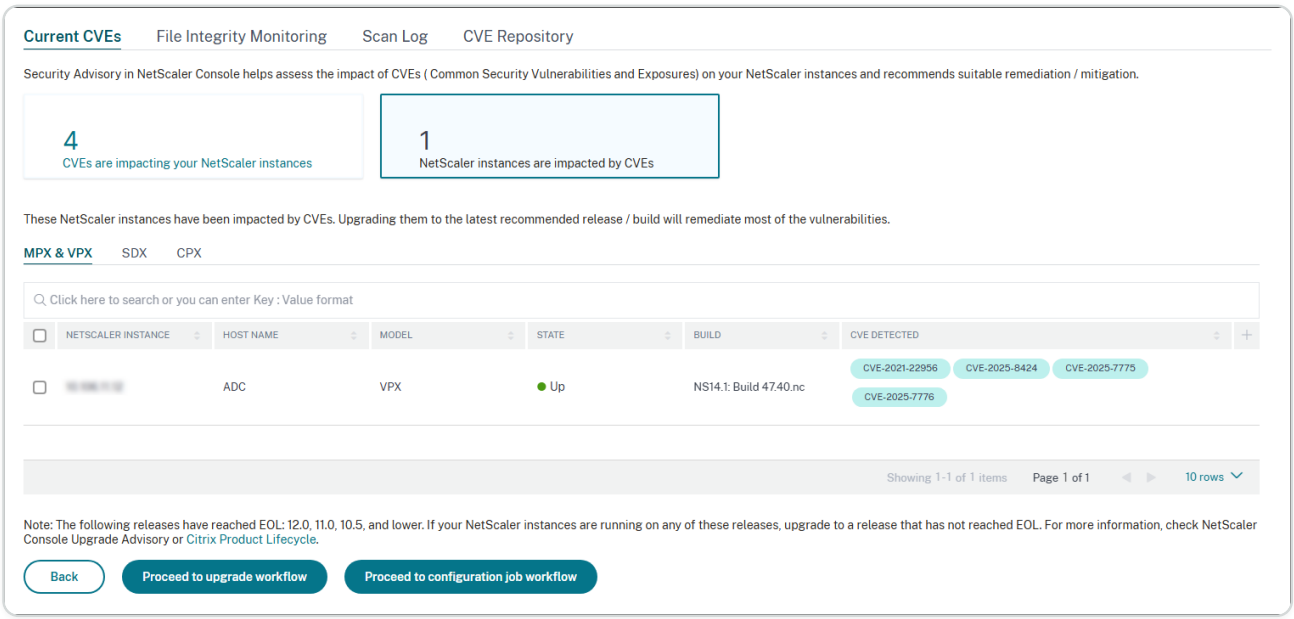
© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

要了解 NetScaler 漏洞的原因，请在安全通报的“**扫描日志**”选项卡中下载 CSV 报告。

“`<number of>` **受 CVE 影响的 NetScaler 实例**”窗口随即出现。在以下屏幕截图中，您可以看到受 CVE-2025-7775 影响的 NetScaler 实例的数量和详细信息。



有关安全通报仪表板的更多信息，请参阅安全通报。

注意：

安全通报系统扫描可能需要几个小时才能完成，并在安全通报模块中反映 CVE-2025-7775 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

修复 CVE-2025-7775

对于受 CVE-2025-7775 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。在 GUI 中，在“**当前 CVE > 受 CVE 影响的 NetScaler 实例**”下，您可以看到修复步骤。

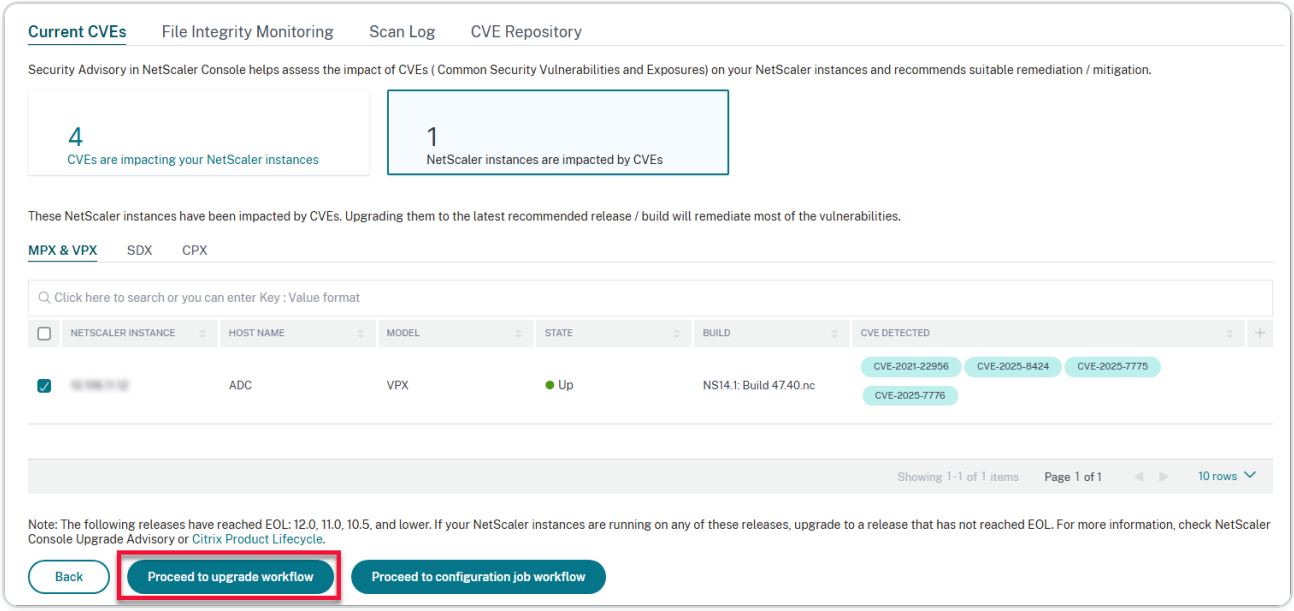
在“**当前 CVE > 受 CVE 影响的 NetScaler 实例**”下，您会看到此单步修复过程的以下工作流，即“**继续升级工作流**”。

要升级易受攻击的实例，请选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充了易受攻击的 NetScaler 实例。

重要提示

如果您的易受攻击的 NetScaler 实例已将 /etc/httpd.conf 文件复制到 /nsconfig 目录，请在规划 NetScaler 升级之前参阅 自定义 NetScaler 配置的升级注意事项。

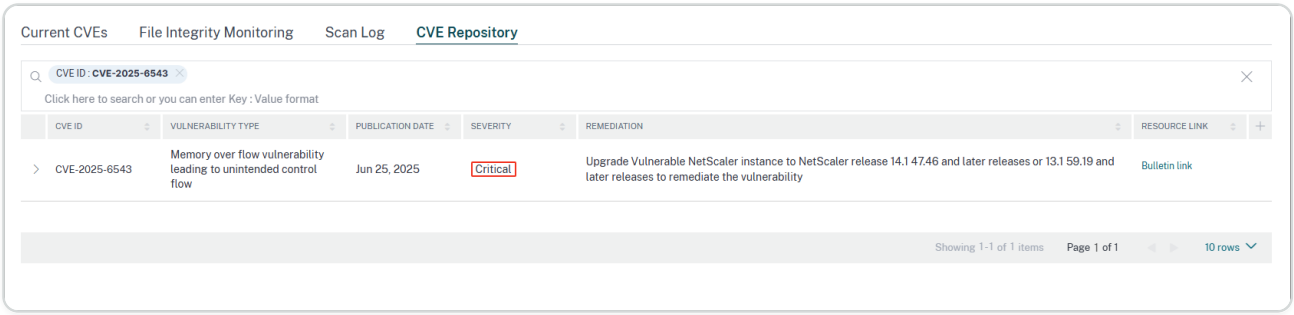
有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。



识别并修复 CVE-2025-6543 漏洞

在 NetScaler Console 安全通告仪表板中，在 **当前 CVE** `<number of>` **受 CVE 影响的 NetScaler 实例** 下，您可以看到所有因 CVE-2025-6543 而易受攻击的实例。要查看受 CVE 影响的实例的详细信息，请选择 CVE-2025-6543 并单击 **查看受影响的实例**。

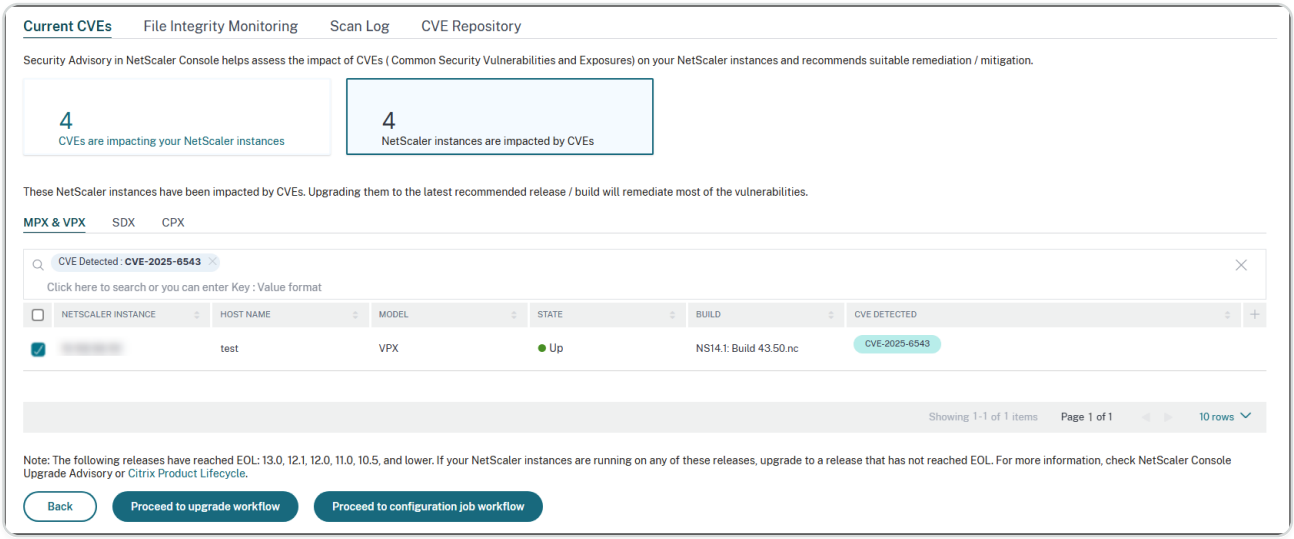
© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

要了解 NetScaler 漏洞的原因，请在安全通告的 **扫描日志** 选项卡中下载 CSV 报告。

`<number of>` **受 CVE 影响的 NetScaler 实例** 窗口随即出现。在以下屏幕截图中，您可以看到受 CVE-2025-6543 影响的 NetScaler 实例的数量和详细信息。



有关安全通告仪表板的更多信息，请参阅 安全通告。

注意：

安全通告系统扫描可能需要几个小时才能完成并在安全通告模块中反映 CVE-2025-6543 的影响。要更快地查看影响，请单击 **立即扫描** 启动按需扫描。

修复 CVE-2025-6543

对于受 CVE-2025-6543 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。在 GUI 中，在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您可以看到修复步骤。

在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您会看到此单步修复过程的以下工作流，即 **继续升级工作流**。

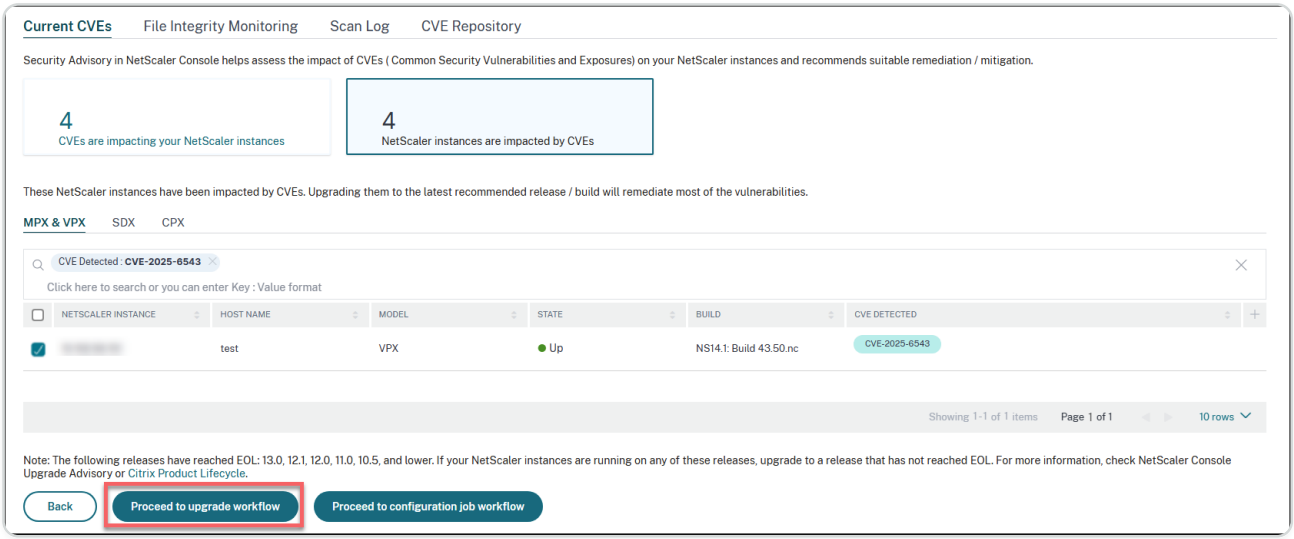
© 1997–2026 Citrix Systems, Inc. All rights reserved.

要升级易受攻击的实例，请选择实例并单击 **继续升级工作流**。升级工作流将打开，其中已填充了易受攻击的 NetScaler 实例。

重要提示

如果您的易受攻击的 NetScaler 实例已将 /etc/httpd.conf 文件复制到 /nsconfig 目录，请在规划 NetScaler 升级之前参阅 自定义 NetScaler 配置的升级注意事项。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。



识别并修复 CVE-2025-5349 漏洞

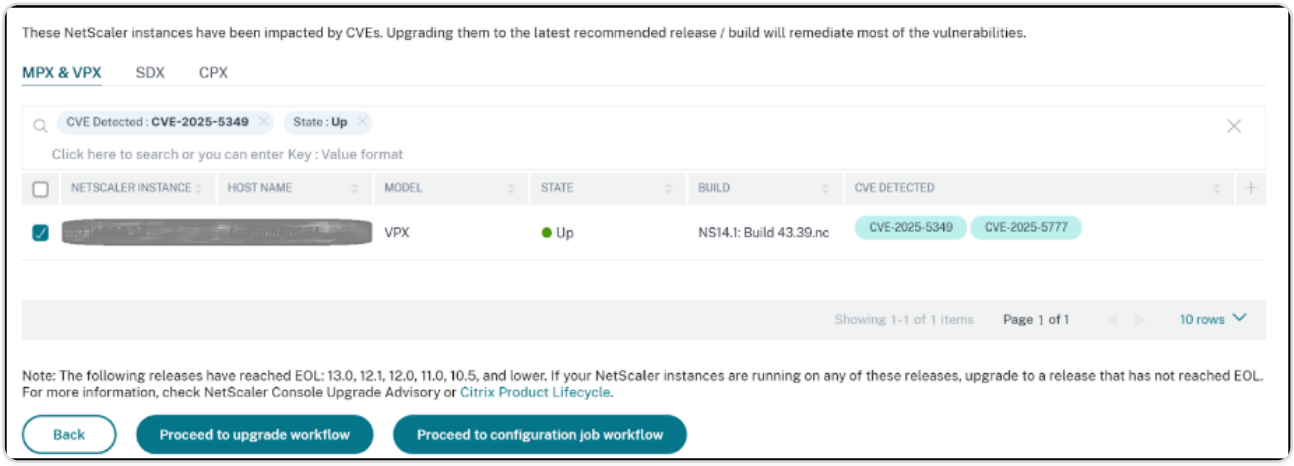
在 NetScaler Console 安全通告仪表板中，在 **当前 CVE** `<number of>` **受 CVE 影响的 NetScaler 实例** 下，您可以看到所有因 CVE-2025-5349 而易受攻击的实例。要查看受 CVE 影响的实例的详细信息，请选择 CVE-2025-5349 并单击 **查看受影响的实例**。

注意：

要了解 NetScaler 漏洞的原因，请在安全通告的 **扫描日志** 选项卡中下载 CSV 报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`<number of>` **受 CVE 影响的 NetScaler 实例** 窗口随即出现。在以下屏幕截图中，您可以看到受 CVE-2025-5349 影响的 NetScaler 实例的数量和详细信息。



有关安全通告仪表板的更多信息，请参阅 安全通告。

注意：

安全通告系统扫描可能需要几个小时才能完成，并在安全通告模块中反映 CVE-2025-5349 的影响。要更快地查看影响，请单击 **立即扫描** 启动按需扫描。

修复 CVE-2025-5349

对于受 CVE-2025-5349 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。在 GUI 中，在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您可以看到修复步骤。

在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您会看到此单步修复过程的以下工作流程，即 **继续升级工作流程**。

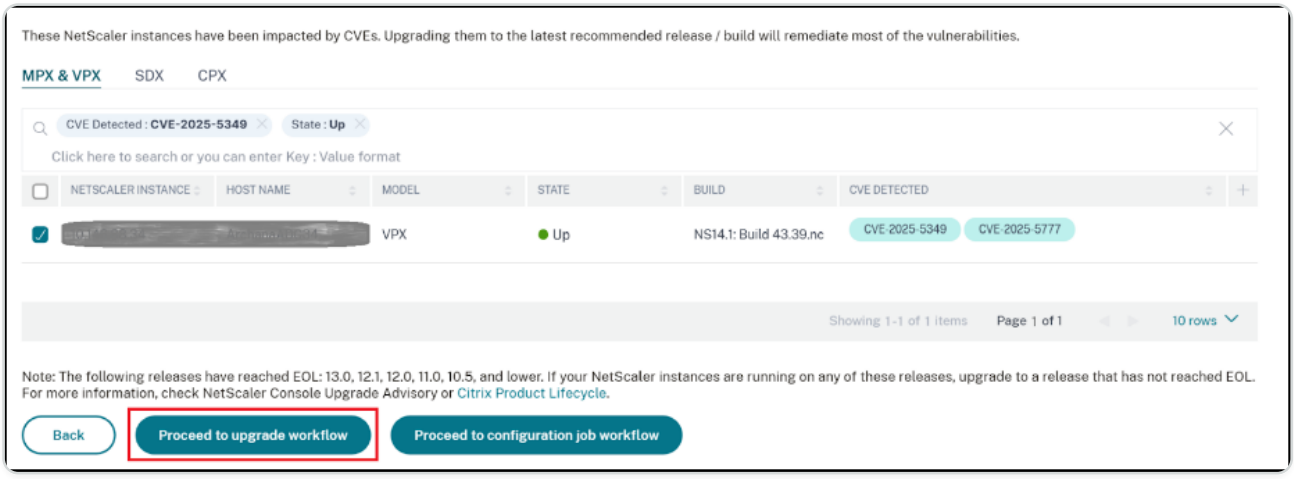
要升级易受攻击的实例，请选择实例并单击 **继续升级工作流程**。升级工作流程将打开，其中已填充易受攻击的 NetScaler 实例。

重要

如果您的易受攻击的 NetScaler 实例已将 /etc/httpd.conf 文件复制到 /nsconfig 目录，请在规划 NetScaler 升级之前参阅 自定义 NetScaler 配置的升级注意事项。

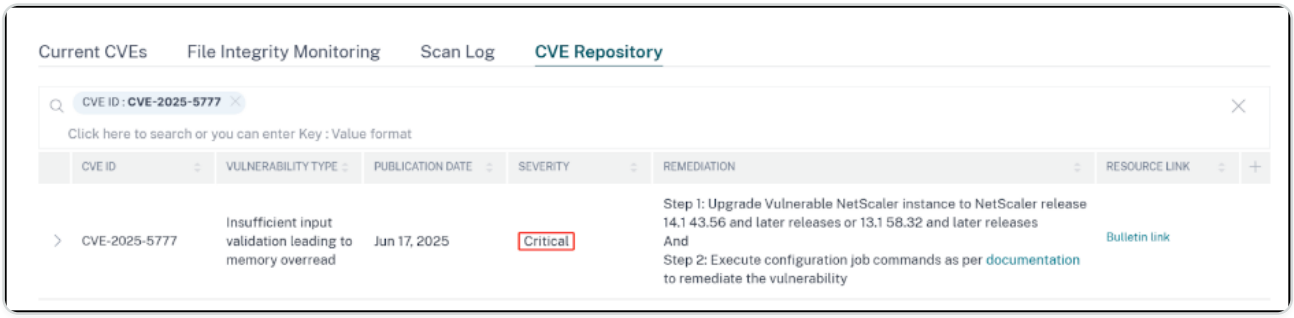
有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



修复 CVE-2025-5777 的漏洞

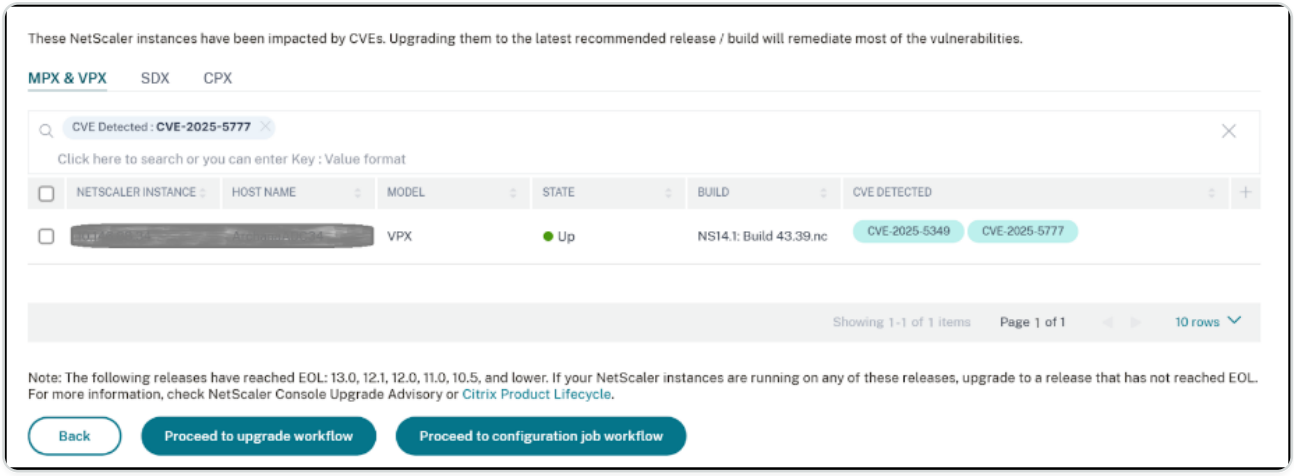
在 NetScaler Console 安全公告仪表板中，在**当前 CVE `<number of>` 受 CVE 影响的 NetScaler 实例**下，您可以看到所有因 CVE-2025-5777 而易受攻击的实例。要查看受 CVE 影响的实例的详细信息，请选择 CVE-2025-5777 并单击**查看受影响的实例**。



注意：

要了解 NetScaler 漏洞的原因，请在安全公告的**扫描日志**选项卡中下载 CSV 报告。

`<number of>` 受 CVE 影响的 NetScaler 实例窗口随即出现。在以下屏幕截图中，您可以看到受 CVE-2025-5777 影响的 NetScaler 实例的数量和详细信息。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关安全公告仪表板的更多信息，请参阅安全公告。

注意：

安全公告系统扫描可能需要几个小时才能完成，并在安全公告模块中反映 CVE-2025-5777 的影响。要更快地查看影响，请单击**立即扫描**启动按需扫描。

修复 CVE-2025-5777

对于受 CVE-2025-5777 影响的 NetScaler 实例，修复是一个两步过程。在 GUI 中，在**当前 CVE > 受 CVE 影响的 NetScaler 实例**下，您可以看到步骤 1 和 2。

这两个步骤包括：

1. 将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。
2. 在配置作业中使用可自定义的内置配置模板应用所需的配置命令。

在“**当前 CVE > 受 CVE 影响的 NetScaler 实例**”下，您会看到此两步补救过程的两个独立工作流：它们是“**继续升级工作流**”和“**继续配置作业工作流**”。

步骤 1：升级易受攻击的 NetScaler 实例

要升级易受攻击的实例，请选择这些实例，然后单击“**继续升级工作流**”。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。

注意：

此步骤可以一次性为所有易受攻击的 NetScaler 实例完成。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

步骤 2：应用配置命令

升级受影响的实例后，在“`<number of` **> 受 CVE 影响的 NetScaler 实例**”窗口中，选择受 CVE-2025-5777 影响的实例，然后单击“**继续配置作业工作流**”。该工作流包括以下步骤。

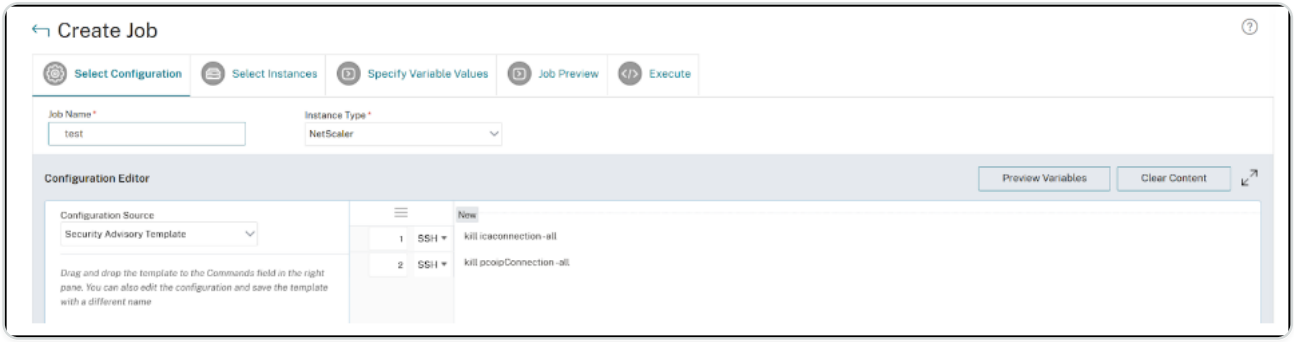
1. 自定义配置。
2. 查看自动填充的受影响实例。
3. 运行作业。

在选择实例并单击“**继续配置作业工作流**”之前，请记住以下几点：

- 对于受多个 CVE（例如 CVE-2020-8300、CVE-2021-22927、CVE-2021-22920、CVE-2021-22956 和 CVE-2025-5777）影响的 NetScaler 实例：当您选择该实例并单击“**继续配置作业工作流**”时，内置配置模板不会在“**选择配置**”下自动填充。您必须手动将“**安全通告模板**”下相应的配置作业模板拖放到右侧的配置作业窗格中。
- 对于仅受 CVE-2025-5777 影响的多个 NetScaler 实例：您可以一次性在所有实例上运行配置作业。例如，您有 NetScaler 1、NetScaler 2 和 NetScaler 3，并且它们都仅受 CVE-2025-5777 影响。选择所有这些实例并单击“**继续配置作业工作流**”，内置配置模板将在“**选择配置**”下自动填充。
- 对于受 CVE-2025-5777 和一个或多个其他 CVE（例如 CVE-2020-8300、CVE-2021-22927 和 CVE-2021-22920）影响的多个 NetScaler 实例，需要每次对一个 NetScaler 应用修复：当您选择这些实例并单击“**继续配置作业工作流**”时，会出现一条错误消息，提示您每次只能在一个 NetScaler 上运行配置作业。

步骤 1：选择配置

在配置作业工作流中，内置配置基本模板会在“**选择配置**”下自动填充。



步骤 2：选择实例

受影响的实例会在“**选择实例**”下自动填充。选择该实例。如果此实例是 HA 对的一部分，请选择“**在辅助节点上执行**”。单击“**下一步**”。

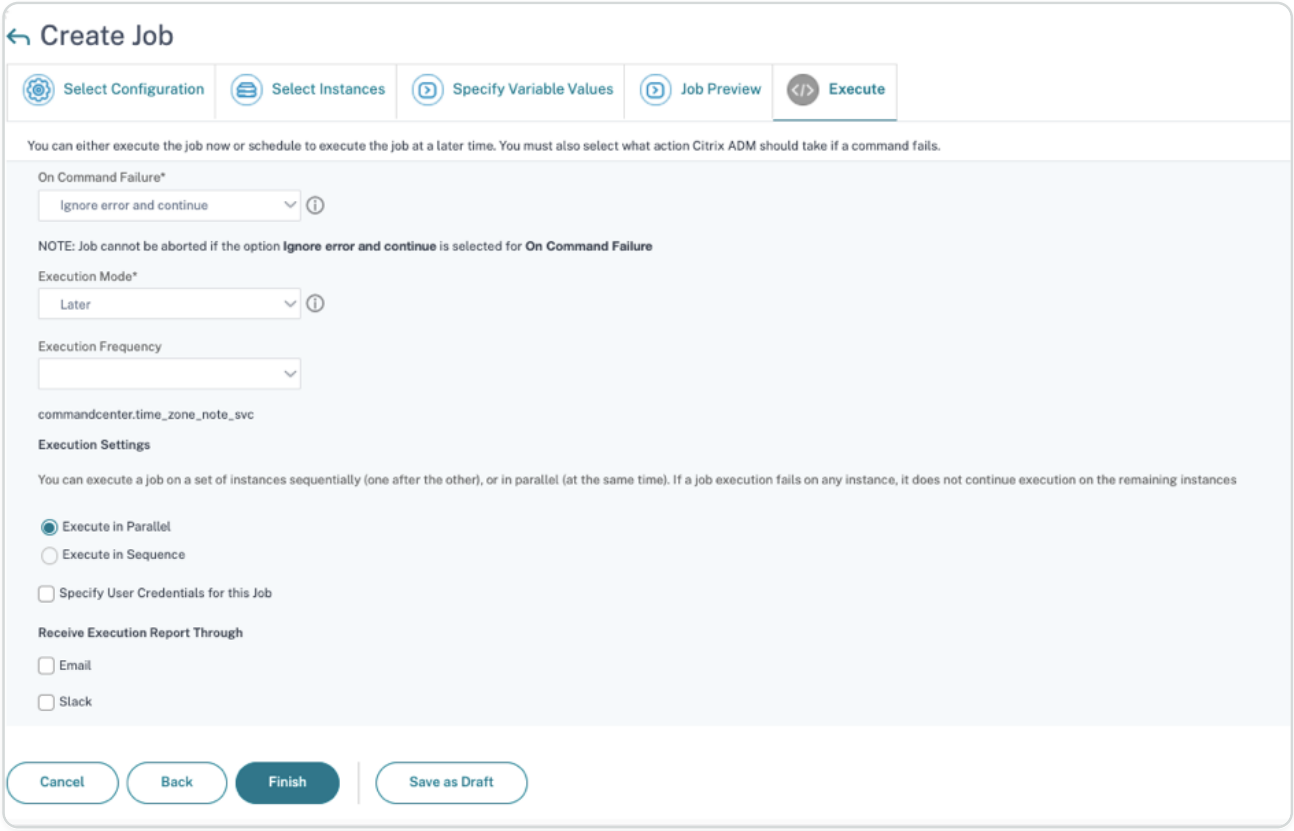
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

对于处于群集模式的 NetScaler 实例，使用安全建议时，NetScaler Console 仅支持在群集配置协调器 (CCO) 节点上运行配置作业。在非 CCO 节点上单独运行命令。

步骤 3：运行作业

单击“**完成**”以运行配置作业。



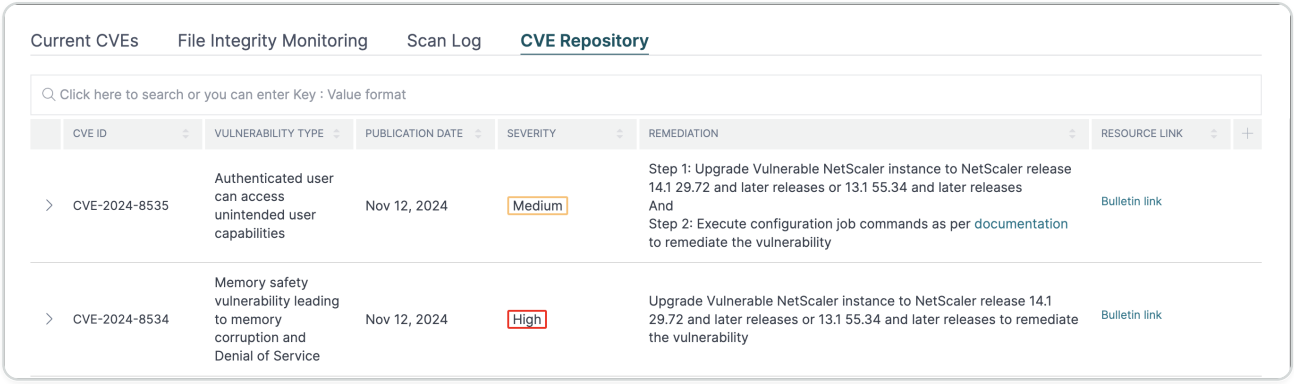
作业运行后，它会显示在“**基础结构 > 配置 > 配置作业**”下。

完成所有易受攻击的 NetScaler 实例的两个修复步骤后，您可以运行按需扫描以查看修订后的安全状况。

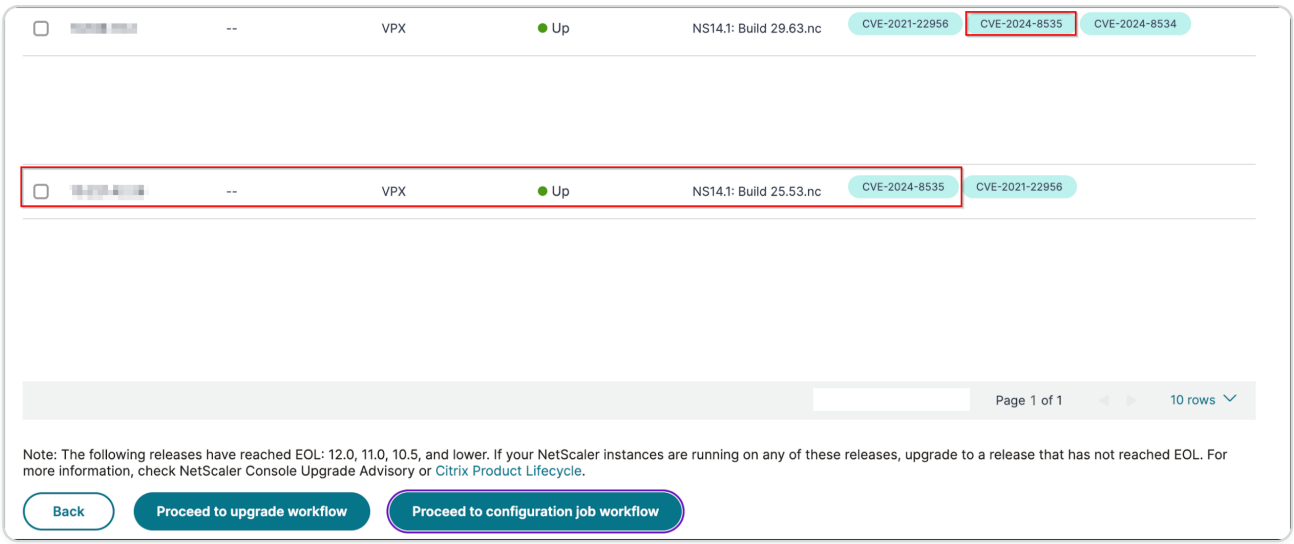
© 1997–2026 Citrix Systems, Inc. All rights reserved.

修复 CVE-2024-8535 的漏洞

在 NetScaler Console 安全通告仪表板中，在 **当前 CVE >** `<number of>` 受常见漏洞和暴露 (CVE) 影响的 NetScaler 实例下，您可以看到所有受此特定 CVE 影响的实例。要查看受 CVE-2024-8535 影响的实例的详细信息，请选择 CVE-2024-8535，然后单击 **查看受影响的实例**。



出现 `<number of>` 受 CVE 影响的 NetScaler 实例窗口。在此处，您可以看到受 CVE-2024-8535 影响的 NetScaler 实例的数量和详细信息。



有关安全通告仪表板的更多信息，请参阅 安全通告。

注意

安全通告系统扫描可能需要一些时间才能完成，并在安全通告模块中反映 CVE-2024-8535 的影响。要更快地查看影响，请单击 **立即扫描** 启动按需扫描。

修复 CVE-2024-8535

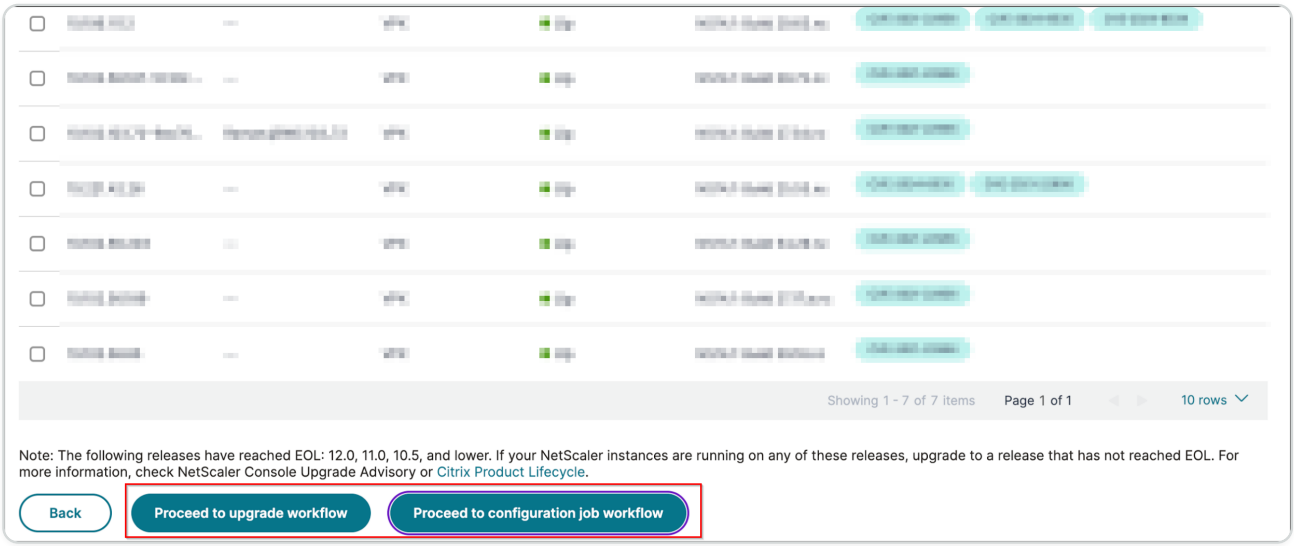
对于受 CVE-2024-8535 影响的 NetScaler 实例，修复是一个两步过程。在 GUI 中，在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您可以看到步骤 1 和 2。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

这两个步骤包括：

1. 将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。
2. 使用配置作业中可自定义的内置配置模板应用所需的配置命令。

在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您会看到此两步修复过程的两个独立工作流：分别是 **继续升级工作流** 和 **继续配置作业工作流**。



步骤 1: 升级易受攻击的 NetScaler 实例

要升级易受攻击的实例，请选择实例并单击 **继续升级工作流程**。升级工作流程将打开，其中已填充易受攻击的 NetScaler 实例。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。

注意：

此步骤可以一次性针对所有易受攻击的 NetScaler 实例完成。

步骤 2: 应用配置命令

升级受影响的实例后，在 `<number of` **> 受 CVE 影响的 NetScaler 实例** 窗口中，选择受 CVE-2024-8535 影响的实例，然后单击 **继续配置作业工作流程**。

在选择实例并单击 **继续配置作业工作流程** 之前，请记住以下几点：

- 对于受多个 CVE（例如 CVE-2020-8300、CVE-2021-22927、CVE-2021-22920 和 CVE-2021-22956）影响的 NetScaler 实例：当您选择实例并单击 **继续配置作业工作流程** 时，

© 1997–2026 Citrix Systems, Inc. All rights reserved.

内置配置模板不会在 **选择配置** 下自动填充。请手动将 **安全通告模板** 下的相应配置作业模板拖放到右侧的配置作业窗格中。

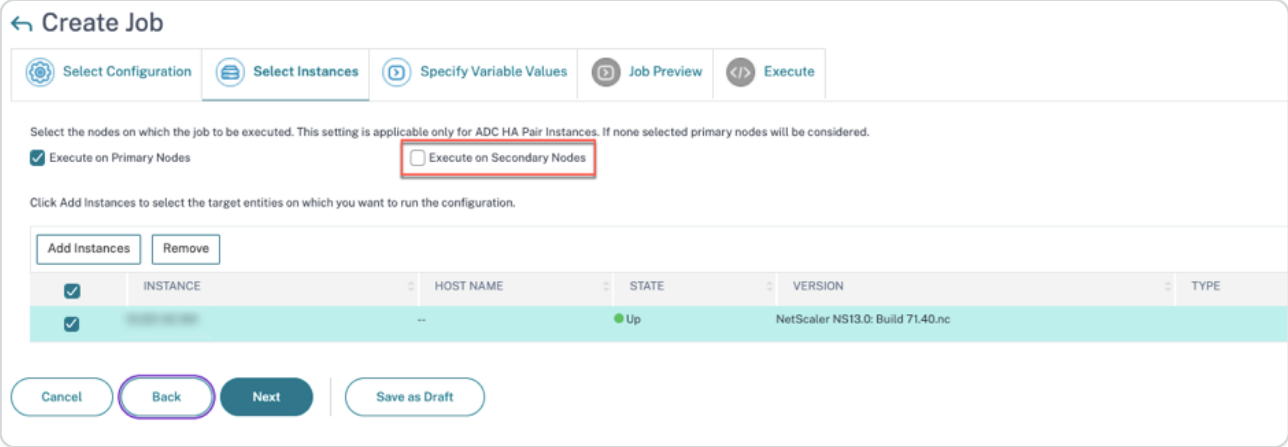
- 对于仅受 CVE-2024-8535 影响的多个 NetScaler 实例，您可以一次性在所有实例上运行配置作业。例如，您有 NetScaler 1、NetScaler 2 和 NetScaler 3，并且它们都仅受 CVE-2024-8535 影响。选择所有这些实例并单击 **继续配置作业工作流程**，内置配置模板将在 **选择配置** 下自动填充。
- 对于受 CVE-2024-8535 和一个或多个其他 CVE（例如 CVE-2020-8300、CVE-2021-22927 和 CVE-2021-22920）影响的多个 NetScaler 实例，需要一次性对每个 NetScaler 应用补救措施：当您选择这些实例并单击 **继续配置作业工作流程** 时，将出现一条错误消息，提示您一次性在每个 NetScaler 上运行配置作业。

步骤 1: 选择配置

在配置作业工作流程中，内置配置基本模板会在 **选择配置** 下自动填充。

步骤 2: 选择实例

受影响的实例会在“**选择实例**”下自动填充。选择该实例。如果此实例是 HA 对的一部分，请选择“**在辅助节点上执行**”。单击“**下一步**”。



注意：

对于处于群集模式的 NetScaler 实例，使用安全建议时，NetScaler Console 仅支持在群集配置协调器 (CCO) 节点上运行配置作业。在非 CCO 节点上单独运行命令。

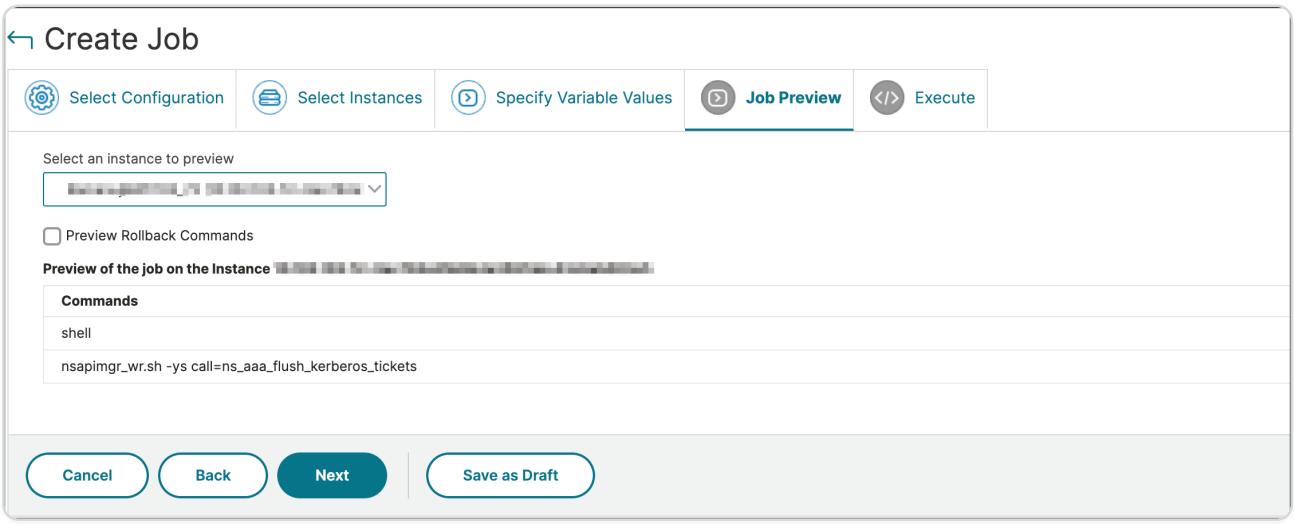
步骤 3: 指定变量值

此步骤无需指定任何变量。选择“**所有实例的通用变量值**”，然后单击“**下一步**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

步骤 4: 预览配置

预览已插入配置中的变量值，然后单击“**下一步**”。



步骤 5: 运行作业

单击“**完成**”以运行配置作业。

作业运行后，它会显示在“**基础结构 > 配置 > 配置作业**”下。

完成所有易受攻击的 NetScaler 实例的两个修复步骤后，您可以运行按需扫描以查看修订后的安全状况。

修复 CVE-2020-8300 的漏洞

在 NetScaler Console 安全通告控制板中，在“**当前 CVE > `<number of>` 受 CVE 影响的 NetScaler 实例**”下，您可以看到所有受此特定 CVE 影响的易受攻击实例。要查看受 CVE-2020-8300 影响的实例的详细信息，请选择“**CVE-2020-8300**”并单击“**查看受影响的实例**”。

CVE-2020-8300 的安全通告控制板(/en-us/netscaler-application-delivery-management-software/media/security-advisory-2020-8300.png)

注意

有关安全通告控制板的更多信息，请参阅安全通告。

出现“**`<number of>` 受 CVE 影响的 NetScaler 实例**”窗口。在此处，您可以看到受 CVE-2020-8300 影响的 NetScaler 实例的数量和详细信息。

受 CVE-2020-8300 影响的实例(/en-us/netscaler-application-delivery-management-software/media/2020-8300-impacted-instances.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

修复 CVE-2020-8300

对于受 CVE-2020-8300 影响的 NetScaler 实例，修复过程分为两步。在 GUI 中，在“**当前 CVE > 受 CVE 影响的 NetScaler 实例**”下，您可以看到步骤 1 和 2。

修复步骤(/en-us/netscaler-application-delivery-management-software/media/remediate-steps.png)

这两个步骤包括：

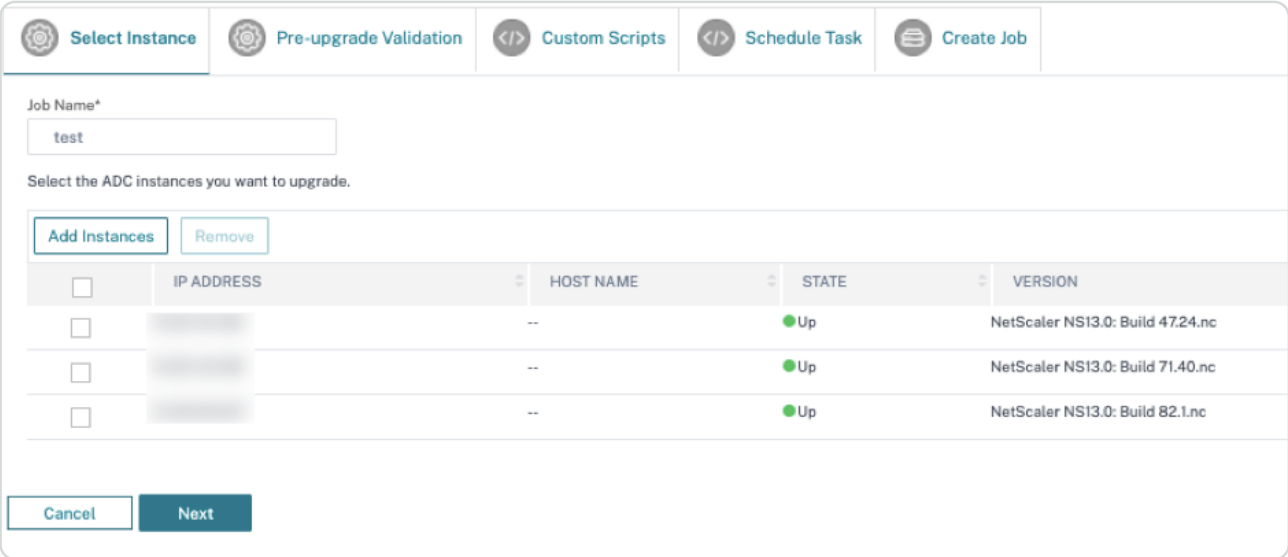
1. 将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。
2. 在配置作业中使用可自定义的内置配置模板应用所需的配置命令。针对每个易受攻击的 NetScaler 实例逐一执行此步骤，并包括该 NetScaler 的所有 SAML 操作和 SAML 配置文件。

在“**当前 CVE > 受 CVE 影响的 NetScaler 实例**”下，您会看到此两步修复过程的两个独立工作流：分别是“**继续升级工作流**”和“**继续配置作业工作流**”。

修复工作流(/en-us/netscaler-application-delivery-management-software/media/remediation-workflows.png)

步骤 1：升级易受攻击的 NetScaler 实例

要升级易受攻击的实例，请选择这些实例，然后单击“**继续升级工作流**”。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。



有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。

注意

此步骤可以一次性针对所有易受攻击的 NetScaler 实例完成。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

步骤 2：应用配置命令

升级受影响的实例后，在“`<number of` **> 受 CVE 影响的 NetScaler 实例**”窗口中，选择一个受 CVE-2020-8300 影响的实例，然后单击“**继续配置作业工作流**”。该工作流包括以下步骤。

1. 自定义配置。
2. 审查自动填充的受影响实例。
3. 为作业的变量指定输入。
4. 审查填充了变量输入的最终配置。
5. 运行作业。

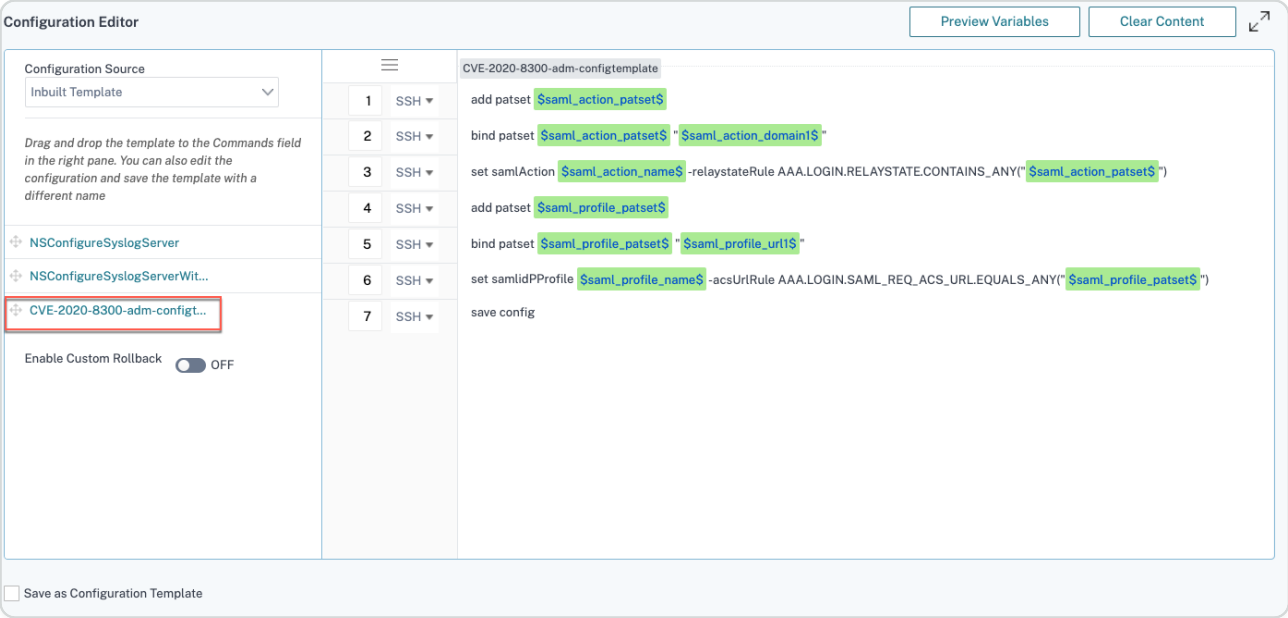
在选择实例并单击“**继续配置作业工作流**”之前，请记住以下几点：

- 对于受多个 CVE（例如 CVE-2020-8300、CVE-2021-22927、CVE-2021-22920 和 CVE-2021-22956）影响的 NetScaler 实例：当您选择实例并单击“**继续配置作业工作流**”时，内置配置模板不会在“选择配置”下自动填充。请手动将“**安全建议模板**”下相应的配置作业模板拖放到右侧的配置作业窗格中。
- 仅适用于受 CVE-2021-22956 影响的多个 NetScaler 实例：您可以一次性在所有实例上运行配置作业。例如，您有 NetScaler 1、NetScaler 2 和 NetScaler 3，并且它们都仅受 CVE-2021-22956 影响。选择所有这些实例，然后单击“**继续执行配置作业工作流**”，内置配置模板将在“**选择配置**”下自动填充。
- 对于受 CVE-2021-22956 和一个或多个其他 CVE（例如 CVE-2020-8300、CVE-2021-22927 和 CVE-2021-22920）影响的多个 NetScaler 实例，这些 CVE 需要一次对一个 NetScaler 应用修复：当您选择这些实例并单击“**继续执行配置作业工作流**”时，将出现一条错误消息，提示您一次在一个 NetScaler 上运行配置作业。

步骤 1：选择配置

在配置作业工作流中，内置配置模板将在“**选择配置**”下自动填充。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



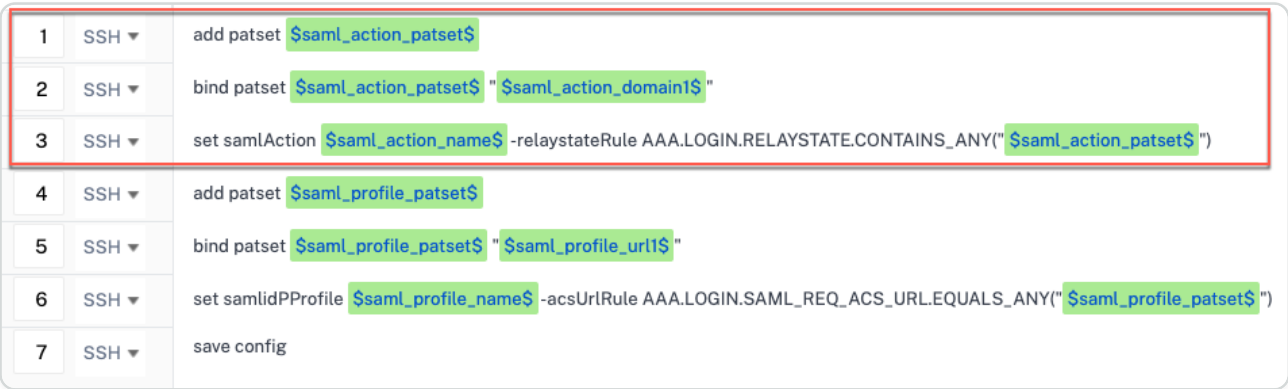
针对每个受影响的 NetScaler 实例，一次运行一个单独的配置作业，并包含该 NetScaler 的所有 SAML 操作和 SAML 配置文件。例如，如果您有两个易受攻击的 NetScaler 实例，每个实例都有两个 SAML 操作和两个 SAML 配置文件，您必须运行此配置作业两次。每个 NetScaler 运行一次，涵盖其所有 SAML 操作和 SAML 配置文件。

NETSCALER 1	NETSCALER2
作业 1：两个 SAML 操作 + 两个 SAML 配置文件	作业 2：两个 SAML 操作 + 两个 SAML 配置文件

为作业命名并根据以下规范自定义模板。内置配置模板仅为大纲或基本模板。根据您的部署自定义模板以满足以下要求：

a. **SAML 操作及其关联域**

根据您部署中的 SAML 操作数量，您必须复制第 1-3 行并为每个 SAML 操作自定义域。



例如，如果您有两个 SAML 操作，重复第 1-3 行两次，并相应地自定义每个 SAML 操作的变量定义。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

如果您有一个 SAML 操作有 N 个域，则必须手动键入 `bind patset $saml_action_patset$ “$saml_action_domain1$”` 行多次，以确保该行在该 SAML 操作中出现 N 次。并更改以下变量定义名称：

- `saml_action_patset`：是配置模板变量，它表示 SAML 操作的模式集 (patset) 名称的值。您可以在配置作业工作流的步骤 3 中指定实际值。请参阅本文档中的“步骤 3：指定变量值”部分。
- `saml_action_domain1`：是配置模板变量，它表示该特定 SAML 操作的域名。您可以在配置作业工作流的步骤 3 中指定实际值。请参阅本文档中的“步骤 3：指定变量值”部分。

要查找设备的全部 SAML 操作，请运行命令 `show samlaction`。

```
>
>
>
> show samlaction -summary
--------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------
     Name            Username field  Decryption key       Encryption key       Url to be redirected to
                   Reject unsigned assertions Issuer name          Two factor Smart Group
--------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------
1    SamlSPAct1                      idp_private_public   sp_private_public    https://<IP3>/saml/login
                   ON         http://<IP1>         OFF
2    SamlSPAct2                      idp_private_public   sp_private_public    https://[redacted]/saml/login
                   ON         http://[redacted]    OFF
Done
```

b. **SAML 配置文件及其关联的 URL**

根据部署中 SAML 配置文件的数量，复制第 4-6 行。自定义每个 SAML 配置文件的 URL。

```
1  SSH  add patset $saml_action_patset$
2  SSH  bind patset $saml_action_patset$ "$saml_action_domain1$"
3  SSH  set samlAction $saml_action_name$ -relaystateRule AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("$saml_action_patset$")
4  SSH  add patset $saml_profile_patset$
5  SSH  bind patset $saml_profile_patset$ "$saml_profile_url1$"
6  SSH  set samlidPProfile $saml_profile_name$ -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.EQUALS_ANY("$saml_profile_patset$")
7  SSH  save config
```

例如，如果您有两个 SAML 配置文件，请手动输入第 4-6 行两次，并相应地自定义每个 SAML 操作的变量定义。

如果您有一个 SAML 操作有 N 个域，则必须手动键入 `bind patset $saml_profile_patset$ “$saml_profile_url1$”` 行多次，以确保该行在该 SAML 配置文件中出现 N 次。并更改以下变量定义名称：

- `saml_profile_patset`：是配置模板变量，它表示 SAML 配置文件的模式集 (patset) 名称的值。您可以在配置作业工作流的步骤 3 中指定实际值。请参阅本文档中的“步骤 3：指定变量值”部分。
- `saml_profile_url1`：是配置模板变量，它表示该特定 SAML 配置文件的域名。您可以在配置作业工作流的步骤 3 中指定实际值。请参阅本文档中的“步骤 3：指定变量值”部分。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要查找设备的全部 SAM 配置文件，请运行命令 `show samlidpProfile`。

```
> show samlidpProfile -summary
--------------------------
      Name
--------------------------
1     samlIDPProf1
2     samlIDPProf2
 Done
>
```

步骤 2：选择实例

受影响的实例在“**选择实例**”下自动填充。选择实例，然后单击“**下一步**”。

选择实例(/en-us/netscaler-application-delivery-management-software/media/select-instance.png)

步骤 3：指定变量值

输入变量值。

- `saml_action_patset`：为 SAML 操作添加名称
- `saml_action_domain1`：输入格式为 `https://<example1.com>/` 的域
- `saml_action_name`：输入您正在为其配置作业的 SAML 操作的名称
- `saml_profile_patset`：为 SAML 配置文件添加名称
- `saml_profile_url1`：输入格式为 `https://<example2.com>/cgi/samlauth` 的 URL
- `saml_profile_name`：输入您正在为其配置作业的 SAML 配置文件的名称

注意

对于 URL，扩展名并非总是 `cgi/samlauth`。它取决于您拥有的第三方授权，因此您必须放置相应的扩展名。

指定变量(/en-us/netscaler-application-delivery-management-software/media/specify-variables.png)

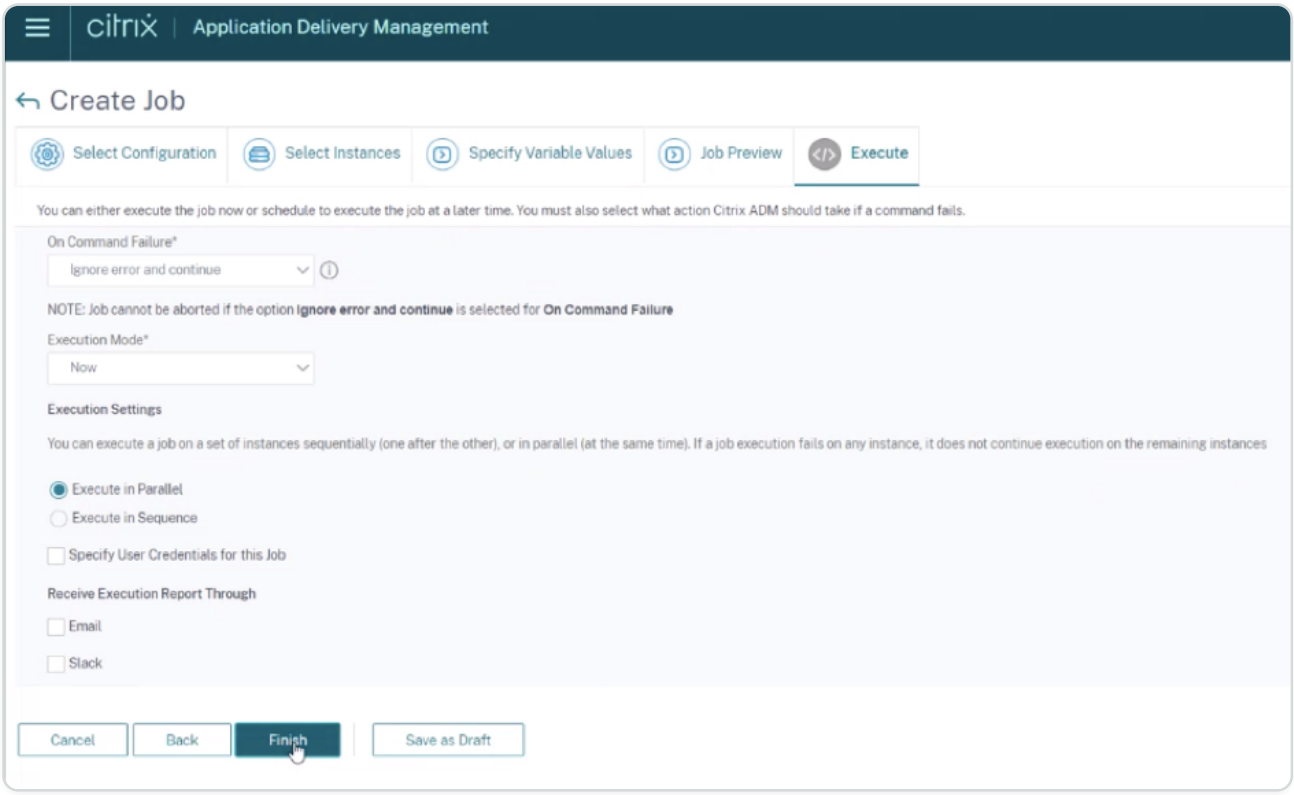
步骤 4：预览配置

预览已插入配置中的变量值，然后单击“**下一步**”。

步骤 5: 运行作业

单击 **完成** 以运行配置作业。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



作业运行后，它将显示在 **基础架构 > 配置 > 配置作业** 下。

完成针对所有易受攻击的 NetScaler 实例的这两个修复步骤后，您可以运行按需扫描以查看修订后的安全状况。

适用于 NetScaler Console Express 帐户的注意事项

NetScaler Console Express 帐户具有有限的功能，其中包括仅限两个配置作业的限制。

对于 CVE-2020-8300 修复，您必须运行与易受攻击的 NetScaler 实例数量相同的配置作业。因此，如果您有 Express 帐户并且需要运行两个以上的配置作业，请遵循此解决方法。

解决方法：为两个易受攻击的 NetScaler 实例运行两个配置作业，然后删除这两个作业，以继续为接下来的两个易受攻击的 NetScaler 实例运行接下来的两个作业。重复此操作，直到覆盖所有易受攻击的实例。在删除作业之前，您可以下载报告以供将来参考。要下载报告，请在 **网络 > 作业** 下，选择作业，然后单击 **操作** 下的 **下载**。

示例：如果您有六个易受攻击的 NetScaler 实例，请分别在两个易受攻击的实例上运行两个配置作业，然后删除这两个配置作业。再重复此步骤两次。最后，您将分别针对六个 NetScaler 实例运行了六个配置作业。在 NetScaler Console UI 的 **基础架构 > 作业** 下，您只能看到最后两个配置作业。

场景

在此场景中，三个 NetScaler 实例易受 CVE-2020-8300 攻击，您需要修复所有实例。请按照以下步骤操作：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 升级所有三个 NetScaler 实例，方法是遵循本文档中“**升级实例**”部分中给出的步骤。
2. 一次将配置修补程序应用于一个 NetScaler，使用配置作业工作流。请参阅本文档中“**应用配置命令**”部分中给出的步骤。

易受攻击的 NetScaler 1 具有以下配置：

两个 SAML 动作	两个 SAML 配置文件

启动配置作业工作流(/en-us/netscaler-application-delivery-management-software/media/scenario-config-job-workflow.png)

选择 NetScaler 1，然后单击“**继续配置作业工作流**”。内置模板会自动填充。接下来，输入作业名称并根据给定配置自定义模板。

根据给定场景自定义模板(/en-us/netscaler-application-delivery-management-software/media/scenario-customize-template.png)

下表列出了自定义参数的变量定义。

表 1. SAML 动作的变量定义

NETSCALER 配置	PATSET 的变量定义	SAML 动作名称的变量定义	域的变量定义
SAML 动作 1 有一个域	saml_action_patset1	saml_action_name1	saml_action_domain 1
SAML 操作 2 有两个域	saml_action_patset2	saml_action_name2	saml_action_domain 2, saml_action_domain 3

表 2. SAML 配置文件的变量定义

NETSCALER 配置	PATSET 的变量定义	SAML 配置文件名称的变量定义	URL 的变量定义
SAML 配置文件 1 有一个 URL	saml_profile_patset1	saml_profile_name1	saml_profile_url1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETSCALER 配置	PATSET 的变量定义	SAML 配置文件名称的变量定义	URL 的变量定义
SAML 配置文件 2 有两个 URL	saml_profile_patset2	saml_profile_name2	saml_profile_url2, saml_profile_url3

在“**选择实例**”下，选择 NetScaler 1，然后单击“**下一步**”。此时将显示“**指定变量值**”窗口。在此步骤中，您需要为上一步中定义的所有变量提供值。

指定变量场景(/en-us/netscaler-application-delivery-management-software/media/specify-variables-scenario.png)

接下来，查看变量。

单击“**下一步**”，然后单击“**完成**”以运行作业。

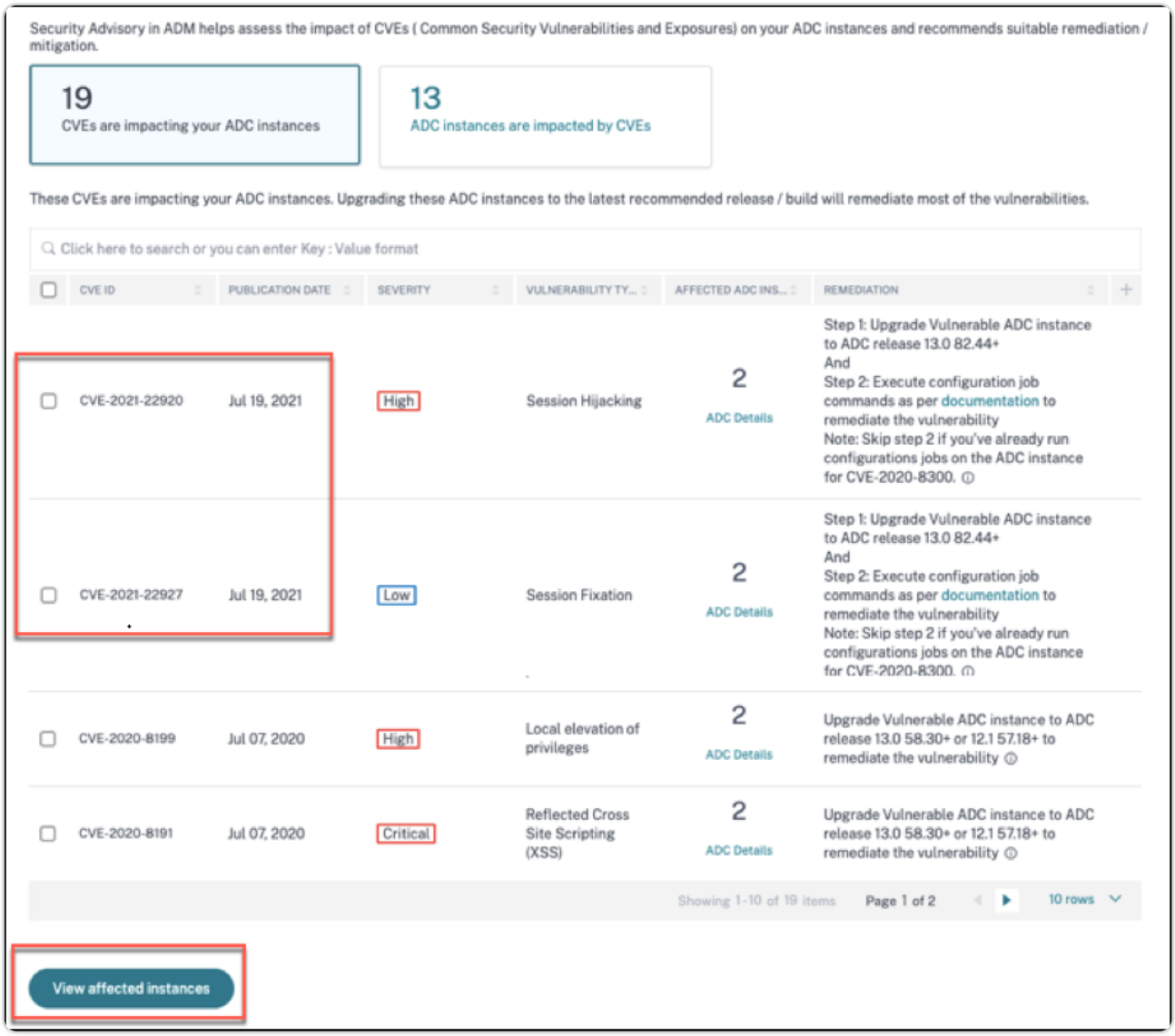
作业运行后，它将显示在“**基础架构 > 配置 > 配置作业**”下。

完成 NetScaler1 的两个修复步骤后，按照相同的步骤修复 NetScaler 2 和 NetScaler 3。修复完成后，您可以运行按需扫描以查看修订后的安全状况。

修复 CVE-2021-22927 和 CVE-2021-22920 的漏洞

在 NetScaler Console 安全通报仪表板中，在 **当前 CVE > `<number of>` 受 CVE 影响的 NetScaler 实例** 下，您可以看到所有因 CVE-2021-22927 和 CVE-2021-22920 而易受攻击的实例。要查看受这两个 CVE 影响的实例的详细信息，请选择一个或多个 CVE，然后单击 **查看受影响的实例**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意

安全通报系统扫描可能需要几个小时才能完成，并在安全通报模块中反映 CVE-2021-22927 和 CVE-2021-22920 的影响。要更快地查看影响，请单击 **立即扫描** 启动按需扫描。

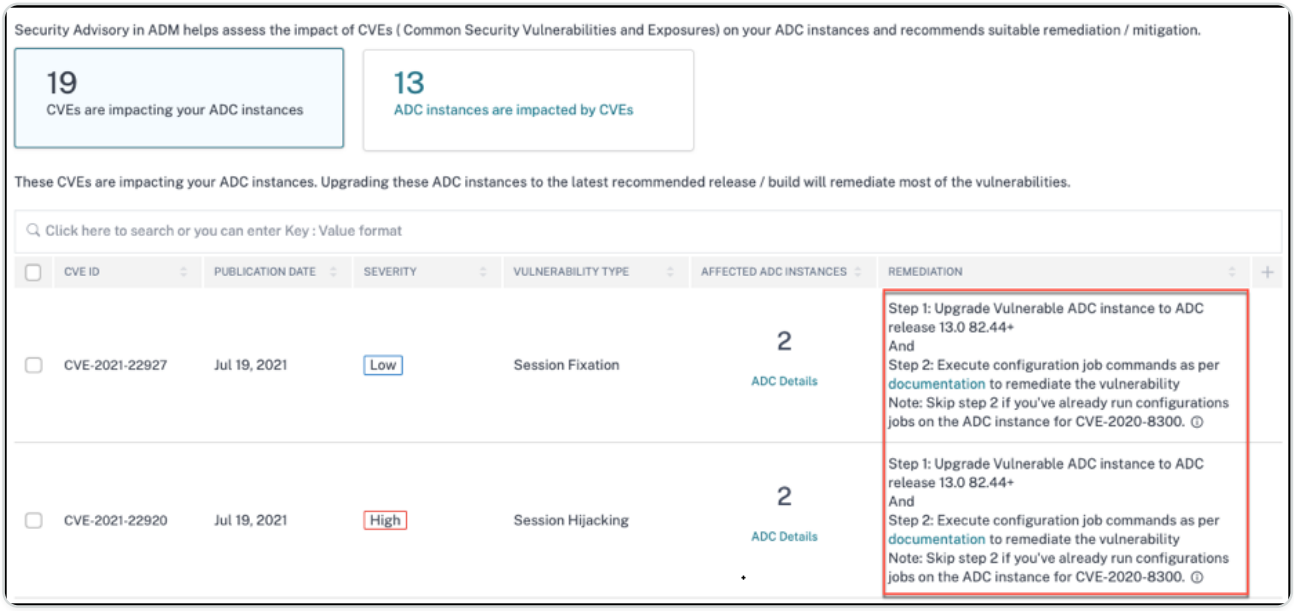
有关安全通报仪表板的更多信息，请参阅 安全通报。

出现 `<number of>` **受 CVE 影响的 NetScaler 实例** 窗口。在以下屏幕截图中，您可以看到受 CVE-2021-22927 和 CVE-2021-22920 影响的 NetScaler 实例的数量和详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

修复 CVE-2021-22927 和 CVE-2021-22920

对于受 CVE-2021-22927 和 CVE-2021-22920 影响的 NetScaler 实例，修复是一个两步过程。在 GUI 中，在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您可以看到步骤 1 和 2。



这两个步骤包括：

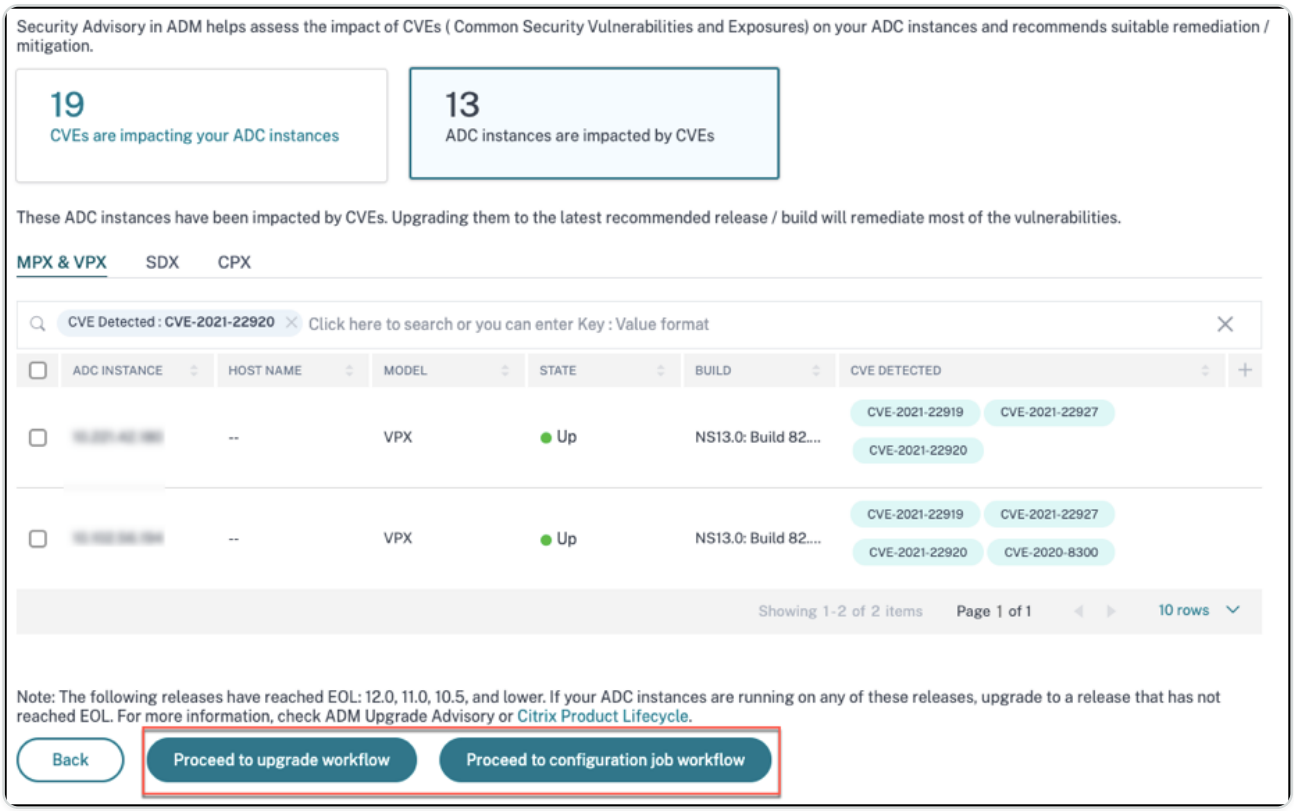
1. 将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。
2. 在配置作业中使用可自定义的内置配置模板应用所需的配置命令。针对每个易受攻击的 NetScaler 实例逐一执行此步骤，并包含该 NetScaler 的所有 SAML 操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

如果您已在 NetScaler 实例上为 CVE-2020-8300 运行了配置作业，请跳过步骤 2。

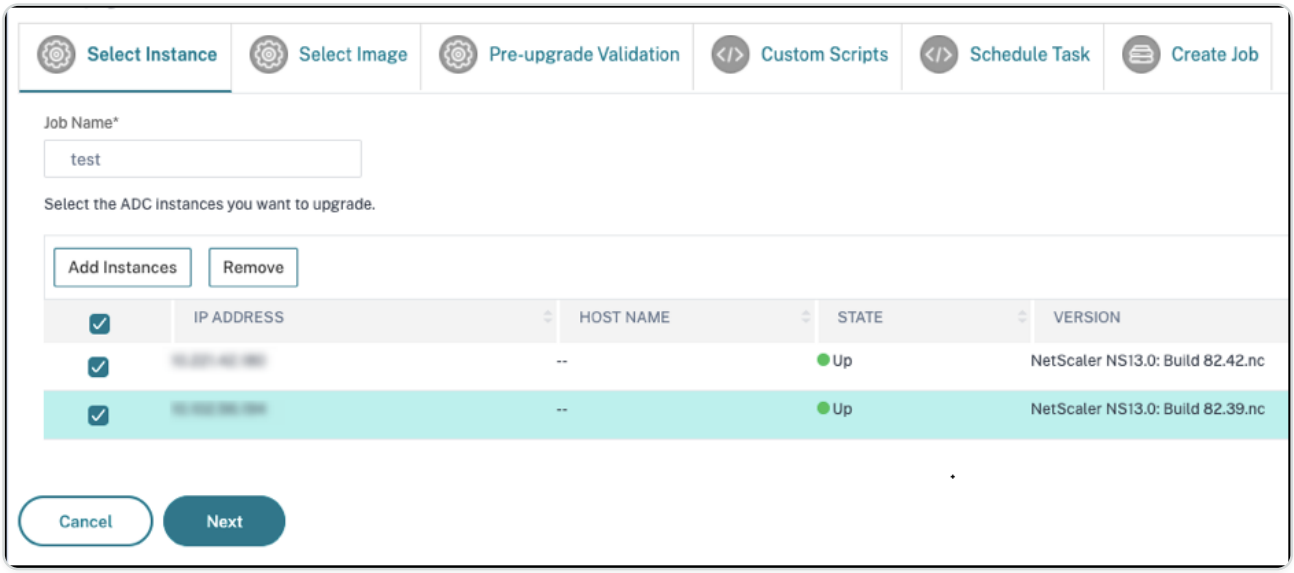
在 **Current CVEs> NetScaler instances impacted by CVEs** 下，您会看到此两步修复过程的两个独立工作流：**Proceed to upgrade workflow** 和 **Proceed to configuration job workflow**。



步骤 1：升级易受攻击的 NetScaler 实例

要升级易受攻击的实例，请选择这些实例并单击 **Proceed to upgrade workflow**。升级工作流将打开，其中已填充了易受攻击的 NetScaler 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。

注意

此步骤可以一次性完成所有易受攻击的 NetScaler 实例。 **注意**

完成所有易受 CVE-2021-22920 和 CVE-2021-22927 攻击的 NetScaler 实例的步骤 1 后，执行按需扫描。**Current CVEs** 下更新的安全状况可帮助您了解 NetScaler 实例是否仍易受这些 CVE 的攻击。根据新的状况，您还可以检查是否需要运行配置作业。 如果您已为 CVE-2020-8300 对 NetScaler 实例应用了适当的配置作业，并且现在已升级 NetScaler 实例，则在执行按需扫描后，该实例将不再显示为易受 CVE-2020-8300、CVE-2021-22920 和 CVE-2021-22927 攻击。

步骤 2：应用配置命令

升级受影响的实例后，在 `<number of` **> NetScaler instances impacted by CVEs** 窗口中，选择一个受 CVE-2021-22927 和 CVE-2021-22920 影响的实例，然后单击 **Proceed to configuration job workflow**。该工作流包括以下步骤。

1. 自定义配置。
2. 审查自动填充的受影响实例。
3. 为作业的变量指定输入。
4. 审查填充变量输入后的最终配置。
5. 运行作业。

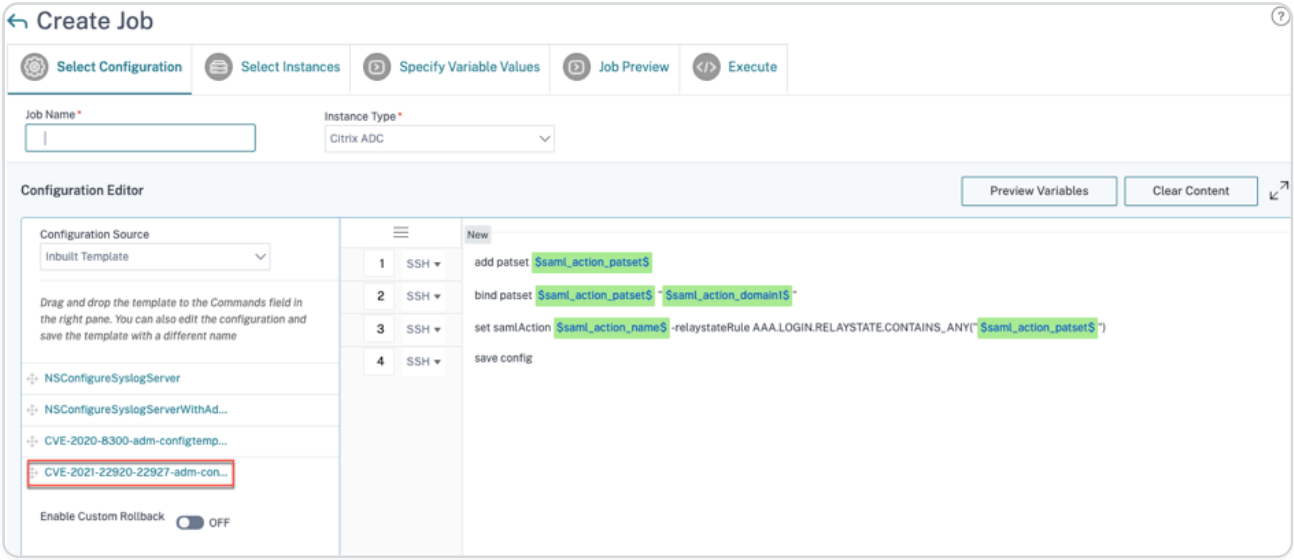
在选择实例并单击 **继续配置作业工作流** 之前，请记住以下几点：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 对于受多个 CVE（例如 CVE-2020-8300、CVE-2021-22927、CVE-2021-22920 和 CVE-2021-22956）影响的 NetScaler 实例：当您选择实例并单击 **继续配置作业工作流** 时，内置配置模板不会在“选择配置”下自动填充。请手动将 **安全公告模板** 下的相应配置作业模板拖放到右侧的配置作业窗格中。
- 对于仅受 CVE-2021-22956 影响的多个 NetScaler 实例：您可以一次性在所有实例上运行配置作业。例如，您有 NetScaler 1、NetScaler 2 和 NetScaler 3，并且它们都仅受 CVE-2021-22956 影响。选择所有这些实例并单击 **继续配置作业工作流**，内置配置模板将在 **选择配置** 下自动填充。
- 对于受 CVE-2021-22956 和一个或多个其他 CVE（例如 CVE-2020-8300、CVE-2021-22927 和 CVE-2021-22920）影响的多个 NetScaler 实例，这些实例需要一次性对每个 NetScaler 应用补救措施：当您选择这些实例并单击 **继续配置作业工作流** 时，将出现一条错误消息，提示您一次性在每个 NetScaler 上运行配置作业。

步骤 1：选择配置

在配置作业工作流中，内置配置基本模板会在 **选择配置** 下自动填充。



注意

如果在步骤 2 中选择的用于应用配置命令的 NetScaler 实例易受 CVE-2021-22927、CVE-2021-22920 以及 CVE-2020-8300 的攻击，则会自动填充 CVE-2020-8300 的基本模板。CVE-2020-8300 模板是所有三个 CVE 所需配置命令的超集。请根据您的 NetScaler 实例部署和要求自定义此基本模板。

您必须为每个受影响的 NetScaler 实例单独运行一个配置作业，一次一个，并包含该 NetScaler 的所有 SAML 操作。例如，如果您有两个易受攻击的 NetScaler 实例，每个实例都有两个 SAML 操作，则必须运行此配置作业两次。每个 NetScaler 运行一次，涵盖其所有 SAML 操作。

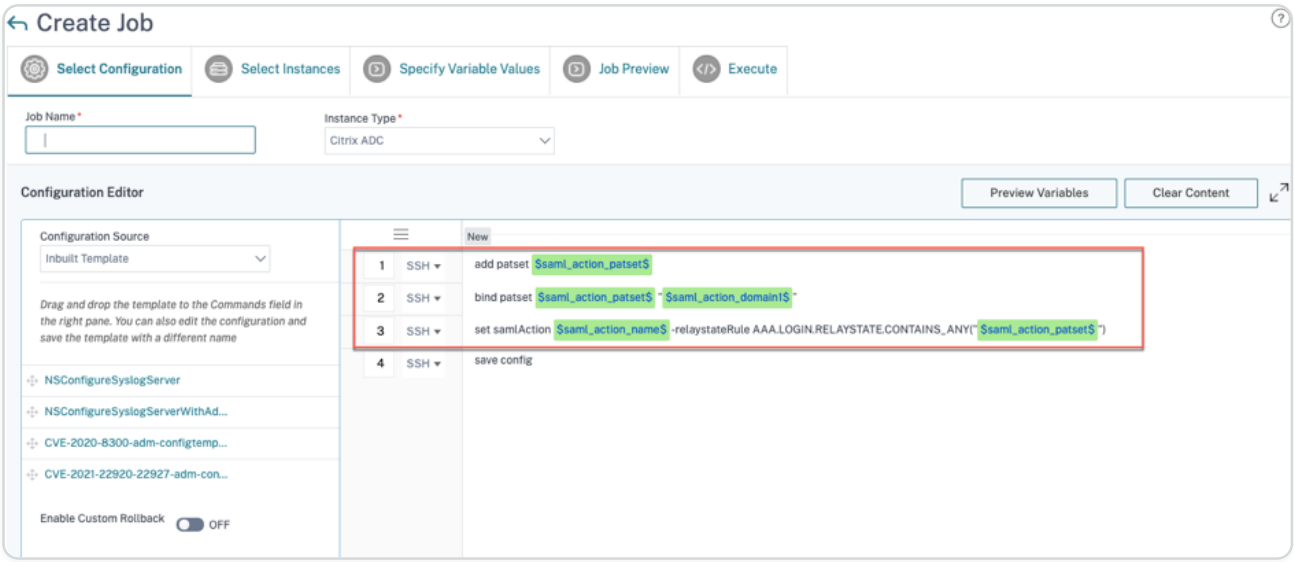
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETSCALER 1	NETSCALER 2
作业 1：两个 SAML 操作	作业 2: 两个 SAML 操作

为作业命名，并根据以下规范自定义模板。内置配置模板仅为大纲或基本模板。根据您的部署，按照以下要求自定义模板：

a. **SAML 操作及其关联域**

根据您部署中 SAML 操作的数量，您必须复制第 1-3 行并为每个 SAML 操作自定义域。



例如，如果您有两个 SAML 操作，请重复第 1-3 行两次，并相应地为每个 SAML 操作自定义变量定义。

如果一个 SAML 操作有 N 个域，您必须手动键入 `bind patset $saml_action_patset$ “$saml_action_domain1$”` 行多次，以确保该行在该 SAML 操作中出现 N 次。并更改以下变量定义名称：

- `saml_action_patset`: 是配置模板变量，它表示 SAML 操作的模式集 (patset) 名称的值。您可以在配置作业工作流的步骤 3 中指定实际值。请参阅本文档中的“步骤 3：指定变量值”部分。
- `saml_action_domain1`: 是配置模板变量，它表示该特定 SAML 操作的域名。您可以在配置作业工作流的步骤 3 中指定实际值。请参阅本文档中的“步骤 3：指定变量值”部分。

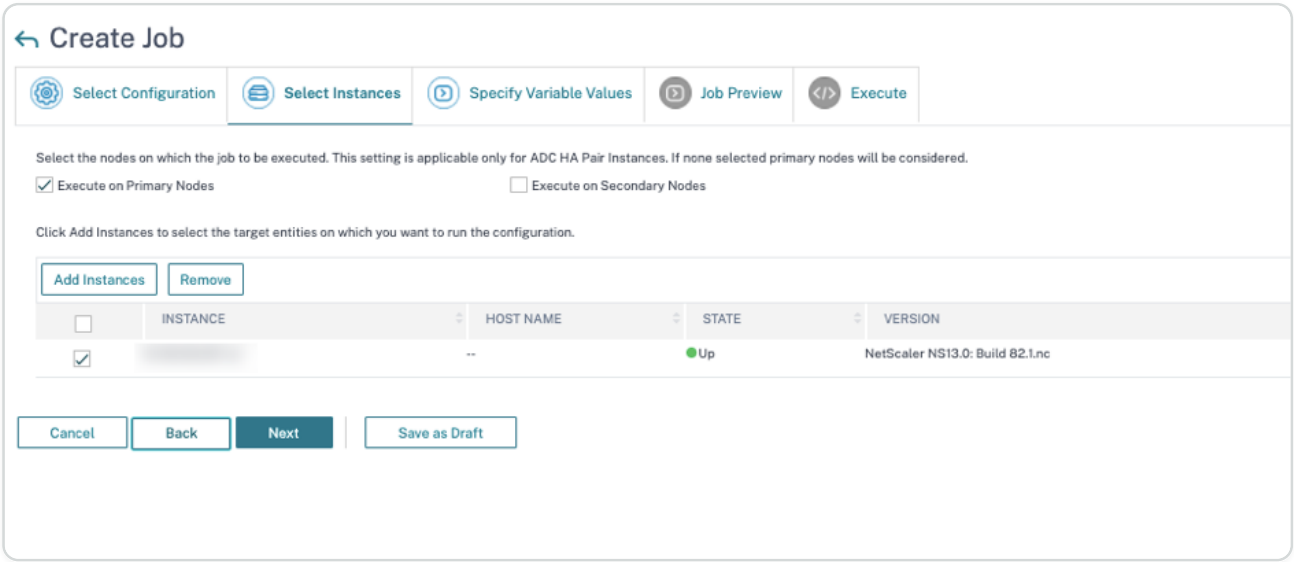
要查找设备的全部 SAML 操作，请运行命令 `show samlaction`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
>
>
>
> show samlaction -summary
--------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------
     Name            Username field  Decryption key       Encryption key       Url to be redirected to
                    Reject unsigned assertions Issuer name          Two factor Smart Group
--------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------
1    SamlSPAct1                      idp_private_public   sp_private_public    https://<IP3>/saml/login
                    ON         http://<IP1>         OFF
2    SamlSPAct2                      idp_private_public   sp_private_public    https://[redacted]/saml/login
                    ON         http://[redacted]    OFF
Done
```

步骤 2: 选择实例

受影响的实例在“**选择实例**”下自动填充。选择实例，然后单击“**下一步**”。

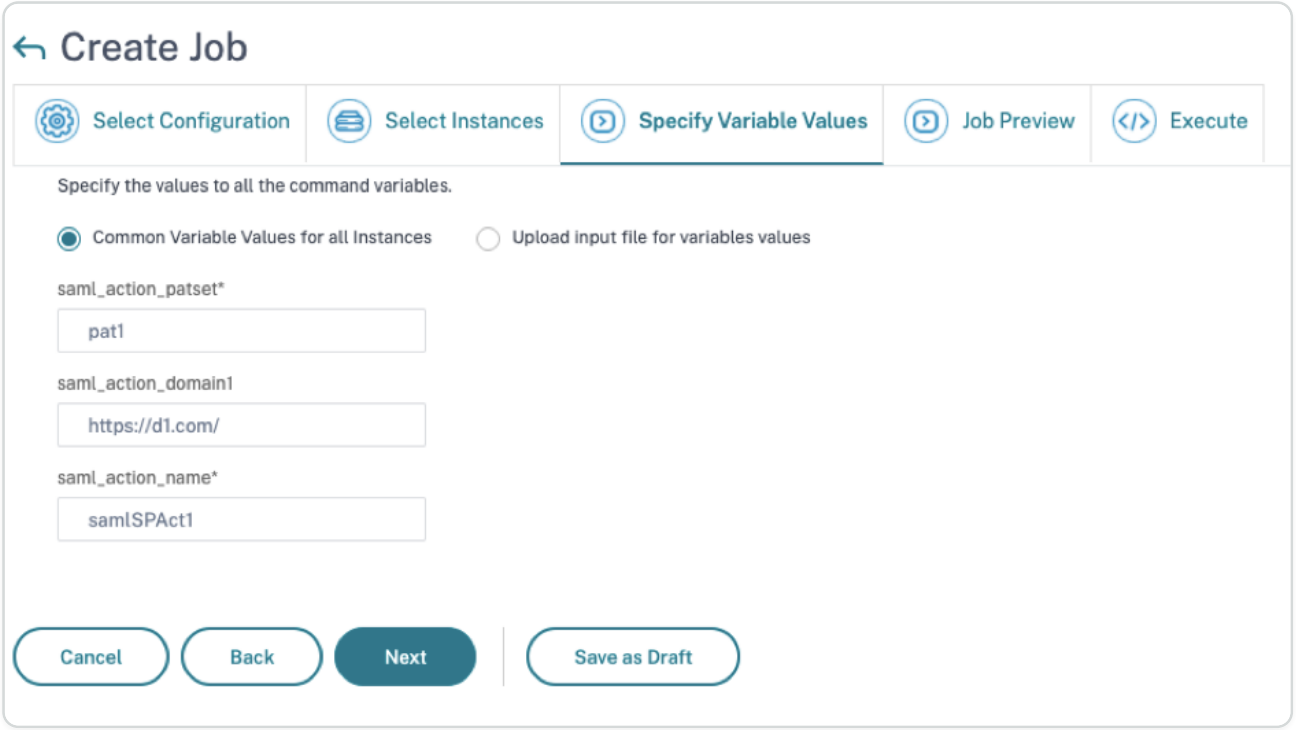


步骤 3: 指定变量值

输入变量值。

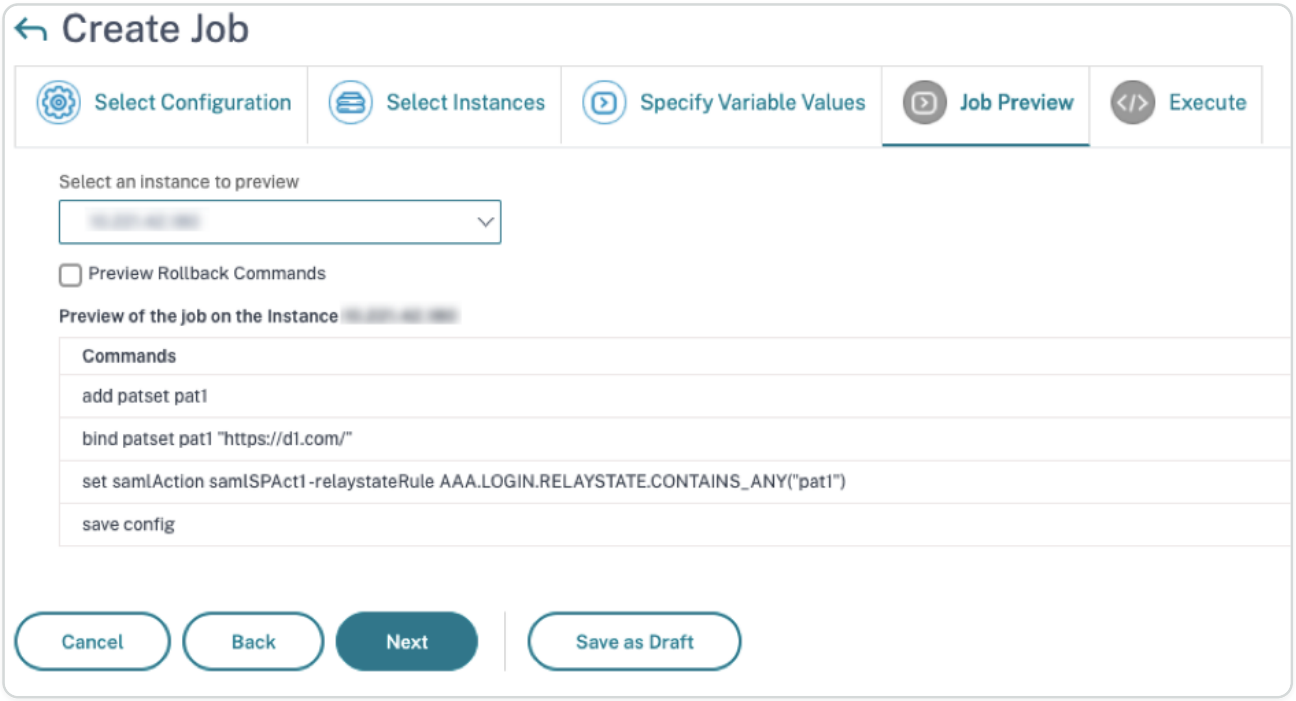
- `saml_action_patset`：为 SAML 操作添加名称
- `saml_action_domain1`：输入格式为 `https://<example1.com>/` 的域
- `saml_action_name`：输入您正在为其配置作业的 SAML 操作的名称

© 1997–2026 Citrix Systems, Inc. All rights reserved.



步骤 4：预览配置

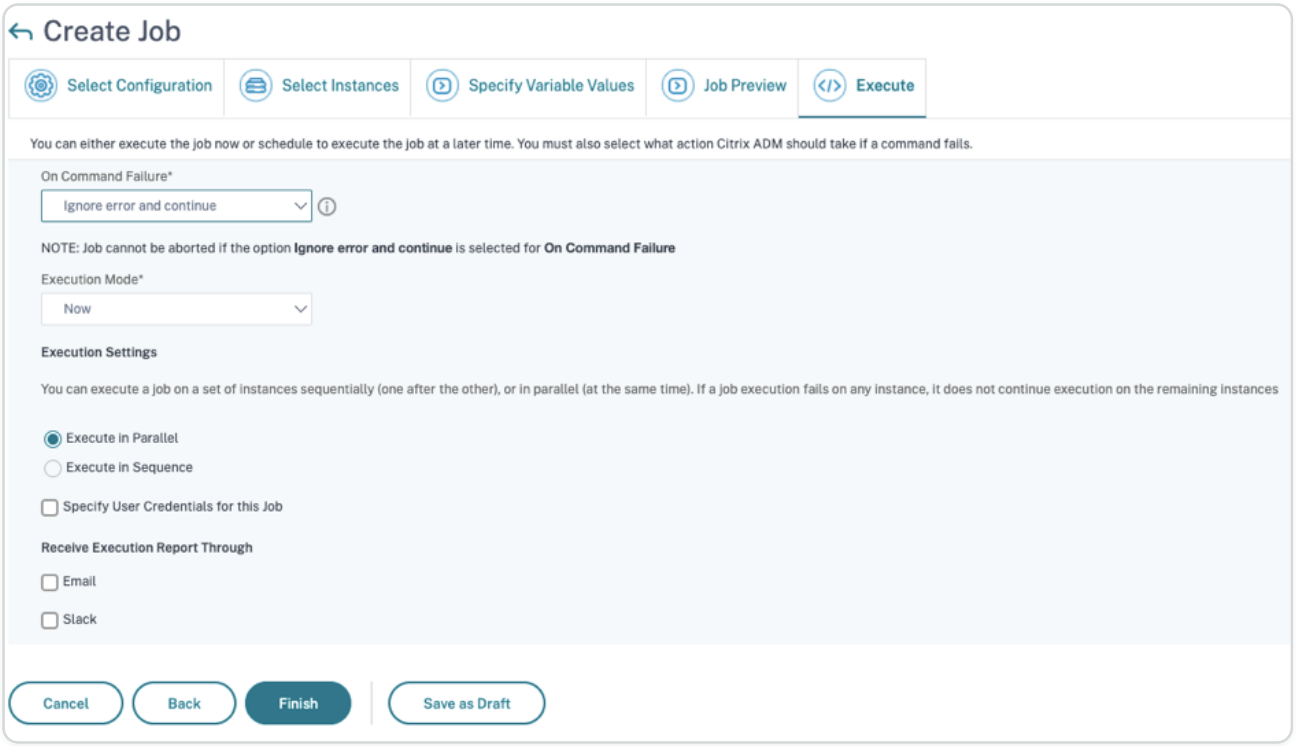
预览已插入配置中的变量值，然后单击“**下一步**”。



步骤 5：运行作业

单击“**完成**”以运行配置作业。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



作业运行后，它将显示在“**基础结构 > 配置 > 配置作业**”下。

完成所有易受攻击的 NetScaler 实例的两个修复步骤后，您可以运行按需扫描以查看修订后的安全状况。

场景

在此场景中，两个 NetScaler 实例易受 CVE-2021-22920 攻击，您需要修复所有实例。请按照以下步骤操作：

1. 按照本文档中“升级实例”部分提供的步骤，升级所有三个 NetScaler 实例。
2. 使用配置作业工作流，一次将配置补丁应用于一个 NetScaler。请参阅本文档中“应用配置命令”部分提供的步骤。

易受攻击的 NetScaler 1 有两个 SAML 操作：

- SAML 操作 1 有一个域
- SAML 操作 2 有两个域

启动配置作业工作流(/en-us/netscaler-application-delivery-management-software/media/scenario-config-job-workflow-cve-2021-22927-2021-22920.png)

选择 NetScaler 1，然后单击“**继续执行配置作业工作流**”。内置基本模板会自动填充。接下来，输入作业名称并根据给定配置自定义模板。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

为给定场景自定义模板(/en-us/netscaler-application-delivery-management-software/media/scenario-customize-template-cve-2021-22927-2021-22920.png)

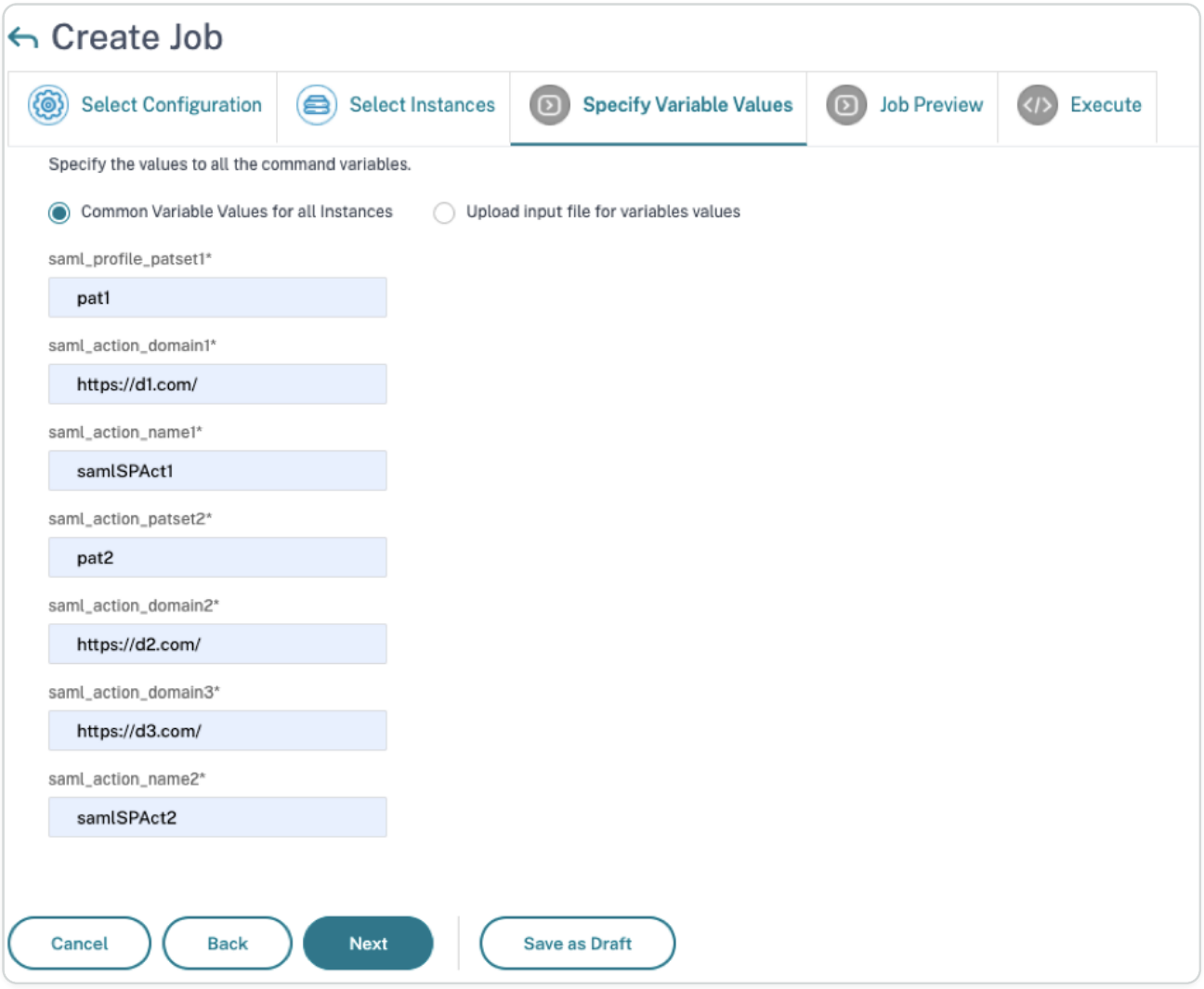
下表列出了自定义参数的变量定义。

表。SAML 操作的变量定义

NETSCALER 配置	PATSET 的变量定义	SAML 操作名称的变量定义	域的变量定义
SAML 操作 1 有一个域	saml_action_patset1	saml_action_name1	saml_action_domain1
SAML 操作 2 有两个域	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

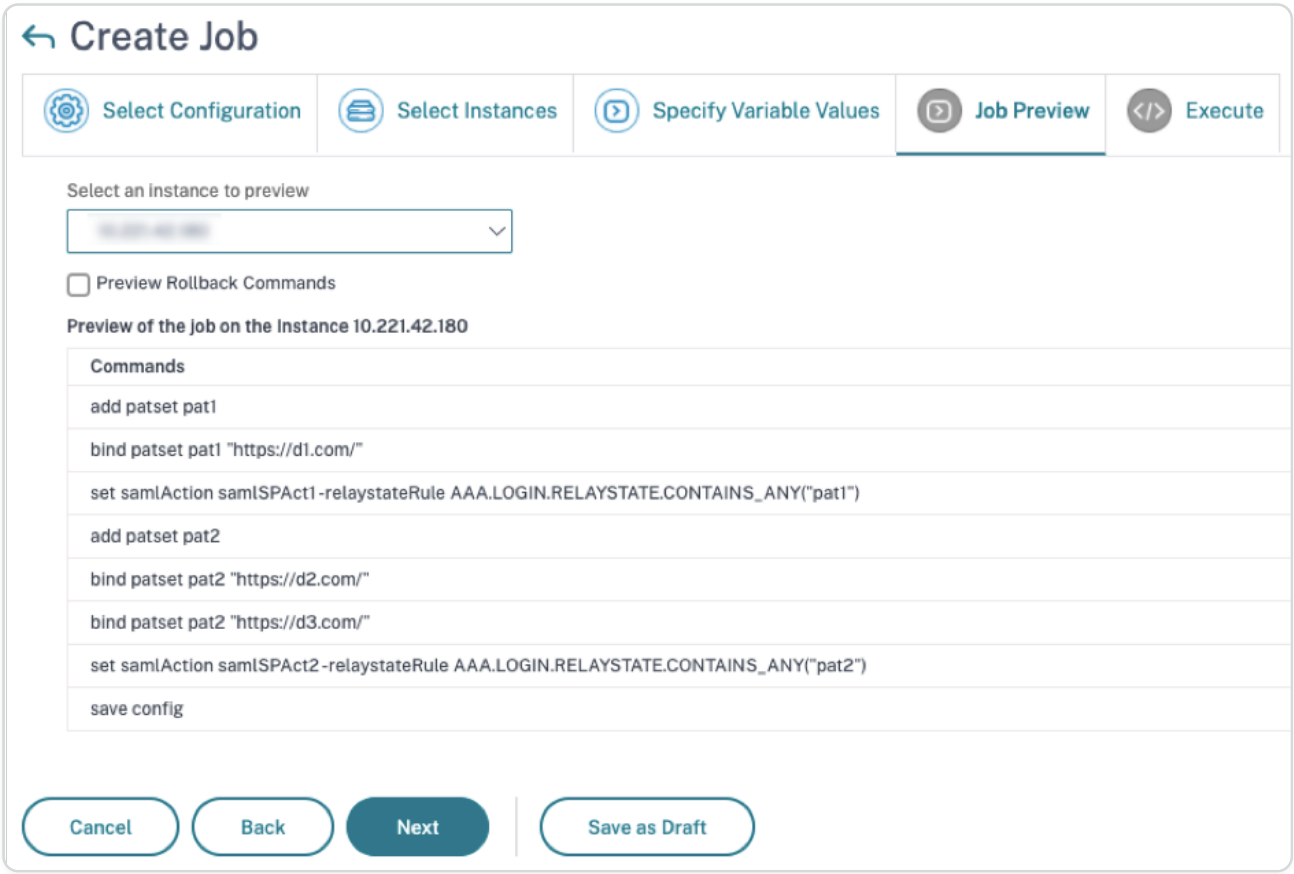
在“**选择实例**”下，选择 NetScaler 1，然后单击“**下一步**”。“**指定变量值**”窗口随即出现。在此步骤中，您需要为上一步中定义的所有变量提供值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



接下来，查看变量。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



单击“**下一步**”，然后单击“**完成**”以运行作业。

作业运行后，它将显示在“**基础架构 > 配置 > 配置作业**”下。

完成 NetScaler1 的两个修复步骤后，请按照相同的步骤修复 NetScaler 2 和 NetScaler 3。修复完成后，您可以运行按需扫描以查看修订后的安全状况。

识别并修复 CVE-2021-22956 漏洞

在 NetScaler Console 安全通报仪表板中，在“**当前 CVE >** `<number of>` NetScaler 实例受常见漏洞和披露 (CVE) 影响”下，您可以看到所有受此特定 CVE 影响的实例。要查看受 CVE-2021-22956 影响的实例的详细信息，请选择 CVE-2021-22956，然后单击“**查看受影响的实例**”。

针对 CVE-2021-22927 和 CVE-2021-22920 的安全通报仪表板(/en-us/netscaler-application-delivery-management-software/media/security-advisory-cve-2021-22956.png)

“`<number of>` 受 CVE 影响的 NetScaler 实例”窗口随即出现。在此处，您可以看到受 CVE-2021-22956 影响的 NetScaler 实例的数量和详细信息。

受 CVE-2020-8300 影响的实例(/en-us/netscaler-application-delivery-management-software/media/cve-2021-22956-impacted-instance.png)

有关安全通报仪表板的更多信息，请参阅安全通报。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

安全通报系统扫描可能需要一些时间才能完成并在安全通报模块中反映 CVE-2021-22956 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

识别受 CVE-2021-22956 影响的实例

CVE-2021-22956 需要自定义扫描，其中 NetScaler Console 服务连接到托管的 NetScaler 实例，并将脚本推送到该实例。该脚本在 NetScaler 实例上运行，并检查 Apache 配置文件 (`httpd.conf file`) 和最大客户端连接 (`maxclient`) 参数，以确定实例是否存在漏洞。脚本与 NetScaler Console 服务共享的信息是布尔值（true 或 false）的漏洞状态。脚本还会向 NetScaler Console 服务返回不同网络接口（例如本地主机、NSIP 和具有管理访问权限的 SNIP）的 max_clients 计数列表。

每次运行计划扫描或按需扫描时，此脚本都会运行。扫描完成后，脚本将从 NetScaler 实例中删除。

修复 CVE-2021-22956

对于受 CVE-2021-22956 影响的 NetScaler 实例，修复是一个两步过程。在 GUI 中，在“**当前 CVE > NetScaler 实例受 CVE 影响**”下，您可以看到步骤 1 和 2。

针对 CVE-2021-22927 和 CVE-2021-22920 的修复步骤(/en-us/netscaler-application-delivery-management-software/media/remediate-steps-cve-2021-22956.png)

这两个步骤包括：

1. 将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。
2. 在配置作业中使用可自定义的内置配置模板应用所需的配置命令。

在“当前 CVE > 受 CVE 影响的 NetScaler 实例”下，您会看到此两步修复过程的两个独立工作流：分别是“继续升级工作流”和“继续配置作业工作流”。

修复工作流(/en-us/netscaler-application-delivery-management-software/media/remediation-workflows-cve-2021-22956.png)

步骤 1：升级易受攻击的 NetScaler 实例

要升级易受攻击的实例，请选择实例并单击“**继续升级工作流**”。升级工作流将打开，其中已填充易受攻击的 NetScaler 实例。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅创建 NetScaler 升级作业。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

此步骤可以一次性针对所有易受攻击的 NetScaler 实例完成。

步骤 2：应用配置命令

升级受影响的实例后，在“`<number of` **> 受 CVE 影响的 NetScaler 实例**”窗口中，选择受 CVE-2021-2295 影响的实例，然后单击“**继续配置作业工作流**”。该工作流包括以下步骤。

1. 自定义配置。
2. 审查自动填充的受影响实例。
3. 为作业指定变量输入。
4. 审查已填充变量输入的最终配置。
5. 运行作业。

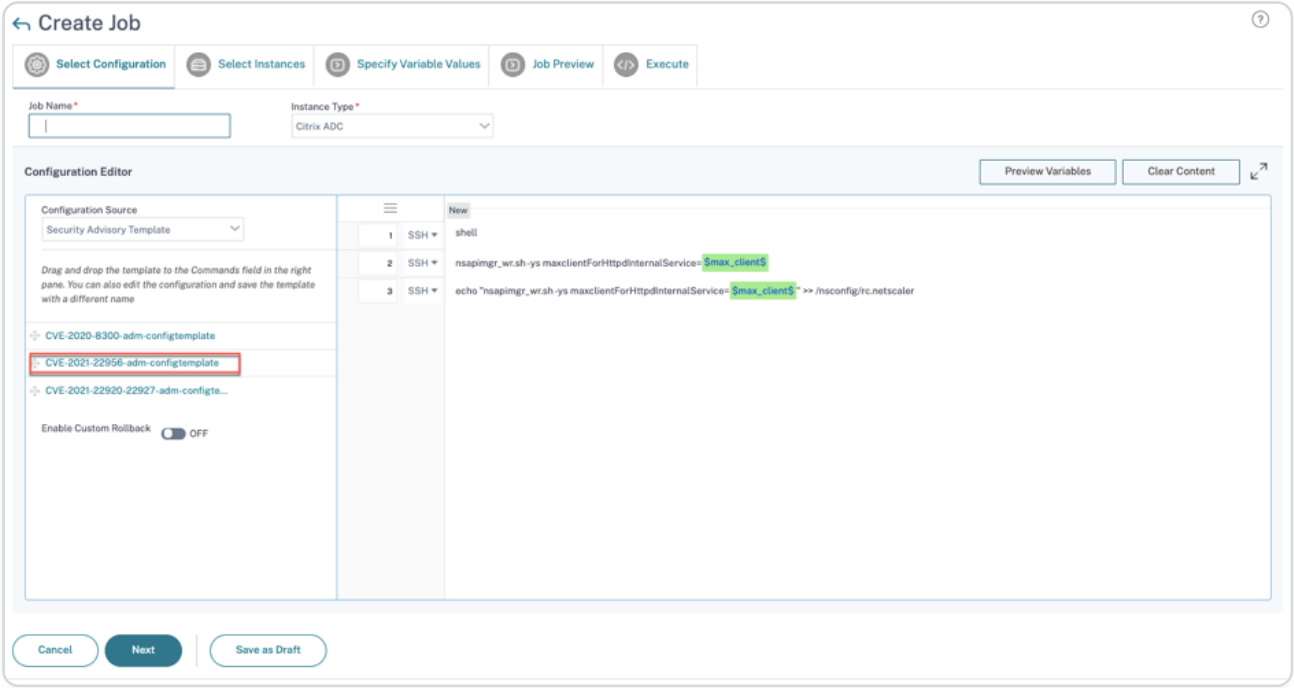
在选择实例并单击“**继续配置作业工作流**”之前，请记住以下几点：

- 对于受多个 CVE（例如 CVE-2020-8300、CVE-2021-22927、CVE-2021-22920 和 CVE-2021-22956）影响的 NetScaler 实例：当您选择实例并单击“**继续配置作业工作流**”时，内置配置模板不会在“选择配置”下自动填充。请手动将“**安全通告模板**”下相应的配置作业模板拖放到右侧的配置作业窗格中。
- 对于仅受 CVE-2021-22956 影响的多个 NetScaler 实例：您可以一次性在所有实例上运行配置作业。例如，您有 NetScaler 1、NetScaler 2 和 NetScaler 3，并且它们都仅受 CVE-2021-22956 影响。选择所有这些实例并单击“**继续配置作业工作流**”，内置配置模板将在“**选择配置**”下自动填充。
- 对于受 CVE-2021-22956 和一个或多个其他 CVE（例如 CVE-2020-8300、CVE-2021-22927 和 CVE-2021-22920）影响的多个 NetScaler 实例，需要一次对一个 NetScaler 应用修复：当您选择这些实例并单击“**继续配置作业工作流**”时，将出现一条错误消息，提示您一次在一个 NetScaler 上运行配置作业。

步骤 1：选择配置

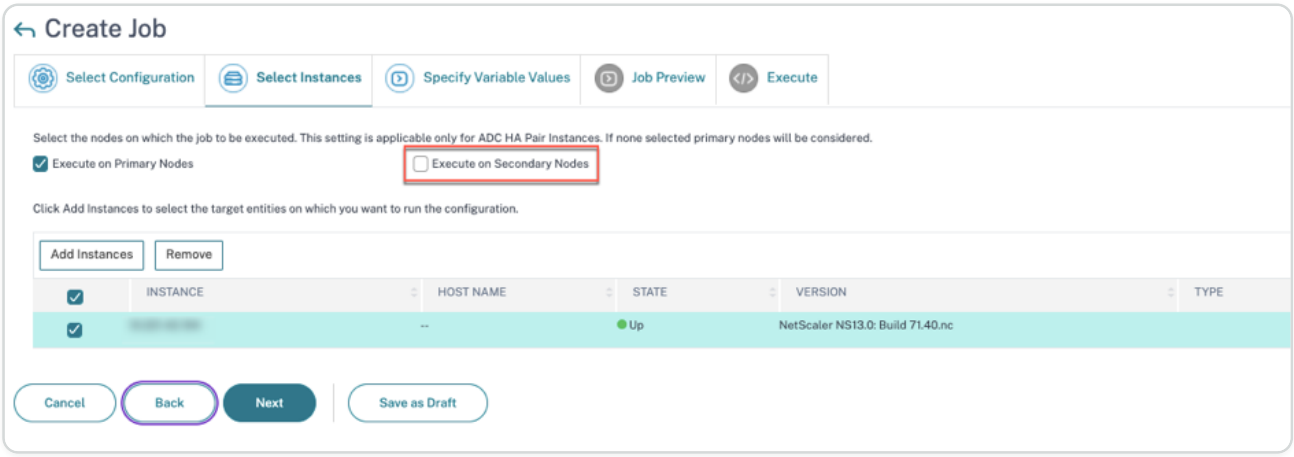
在配置作业工作流中，内置配置基本模板会在“**选择配置**”下自动填充。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



步骤 2：选择实例

受影响的实例会在“**选择实例**”下自动填充。选择该实例。如果此实例是 HA 对的一部分，请选择“**在辅助节点上执行**”。单击“**下一步**”。



注意

对于群集模式下的 NetScaler 实例，使用 NetScaler Console 安全通告，NetScaler Console 仅支持在群集配置协调器 (CCO) 节点上运行配置作业。请在非 CCO 节点上单独运行命令。

`rc.netscaler` 会在所有 HA 和群集节点之间同步，从而使修复在每次重新启动后都保持持久。

步骤 3：指定变量值

输入变量值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

指定变量(/en-us/netscaler-application-delivery-management-software/media/specify-variables-cve-2021-22956.png)

选择以下选项之一，为您的实例指定变量：

所有实例的通用变量值：为变量 `max_client` 输入一个通用值。

上传变量值的输入文件：单击**下载输入密钥文件**以下载输入文件。在输入文件中，输入变量 `max_client` 的值，然后将文件上传到 NetScaler Console 服务器。

> **注意**
>
> 对于上述两个选项，建议的 `max_client` 值为 30。您可以根据当前值设置该值。但是，它不应为零，并且应小于或等于 `/etc/httpd.conf` 文件中设置的 max_client。您可以通过在 NetScaler 实例中搜索字符串 `MaxClients` 来检查 Apache HTTP Server 配置文件 `/etc/httpd.conf` 中设置的当前值。

步骤 4：预览配置

预览已插入配置中的变量值，然后单击**下一步**。

预览作业(/en-us/netscaler-application-delivery-management-software/media/preview-job-cve-2021-22956.png)

步骤 5：运行作业

单击**完成**以运行配置作业。

运行配置作业(/en-us/netscaler-application-delivery-management-software/media/run-job-cve-2021-22956.png)

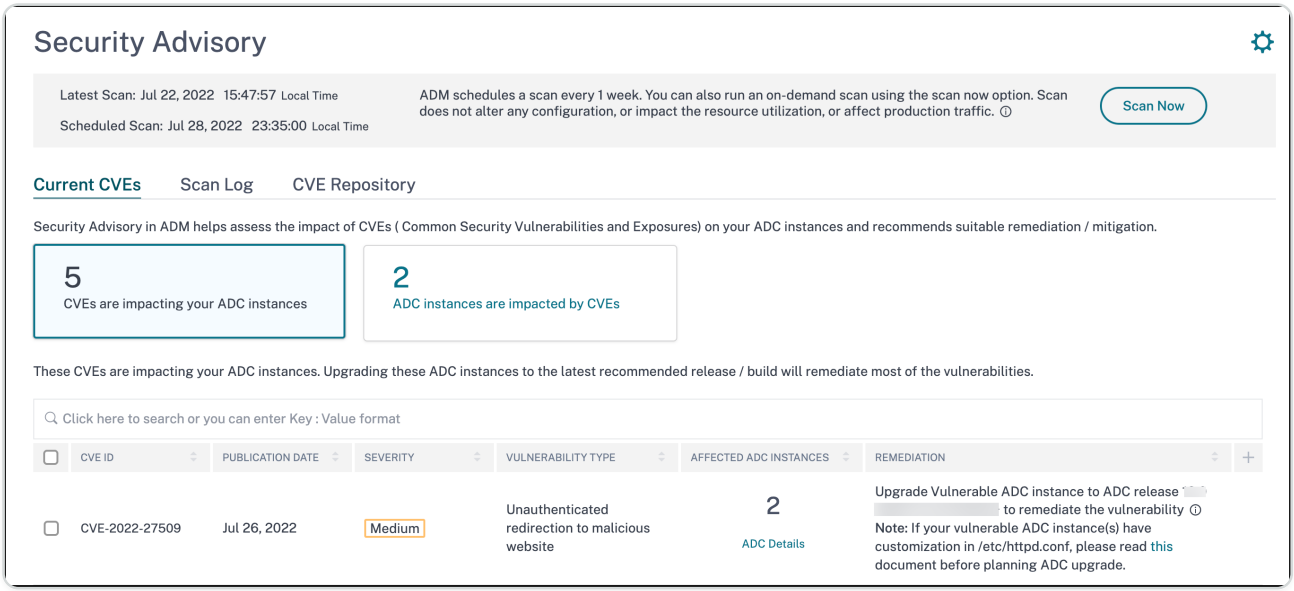
作业运行后，它会显示在**基础架构 > 配置 > 配置作业**下。

完成所有易受攻击的 NetScaler 实例的两个修复步骤后，您可以运行按需扫描以查看修订后的安全状况。

识别并修复 CVE-2022-27509 漏洞

在 NetScaler Console 安全通告仪表板中，在“**当前 CVE `<number of>` 受 CVE 影响的 NetScaler 实例**”下，您可以查看所有因 CVE-2022-27509 而易受攻击的实例。要查看受 CVE 影响的实例的详细信息，请选择 CVE-2022-27509，然后单击“**查看受影响的实例**”。

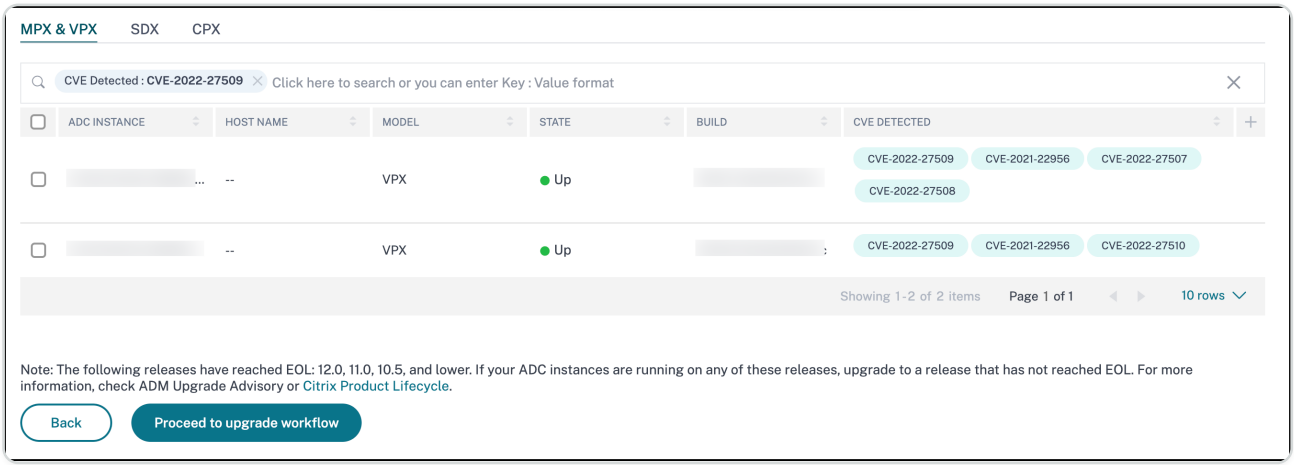
© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意

要了解 NetScaler 漏洞的原因，请在安全通告的“扫描日志”选项卡中下载 CSV 报告。

出现“`<number of>` **受 CVE 影响的 NetScaler 实例**”窗口。在以下屏幕截图中，您可以看到受 CVE-2022-27509 影响的 NetScaler 实例的数量和详细信息。



有关安全通告仪表板的更多信息，请参阅安全通告。

注意

安全通告系统扫描可能需要几个小时才能完成并在安全通告模块中反映 CVE-2022-27509 的影响。要更快地查看影响，请单击“**立即扫描**”启动按需扫描。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

识别受 CVE-2022-27509 影响的实例

CVE-2022-27509 需要自定义扫描和版本扫描的组合。作为自定义扫描的一部分，NetScaler Console 服务连接到受管 NetScaler 实例并将脚本推送到该实例。该脚本在 NetScaler 实例上运行，并确定该实例是否易受攻击。此脚本在每次计划扫描或按需扫描运行时都会运行。

扫描完成后，脚本将从 NetScaler 实例中删除。

您也可以选择退出这些安全通告自定义扫描。有关自定义扫描设置以及如何选择退出自定义扫描的更多信息，请参阅“**安全通告**”页面上的“**配置自定义扫描设置**”部分。

修复 CVE-2022-27509

对于受 CVE-2022-27509 影响的 NetScaler 实例，补救措施是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到包含修复程序的版本和内部版本。在 GUI 中，在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您可以看到补救步骤。

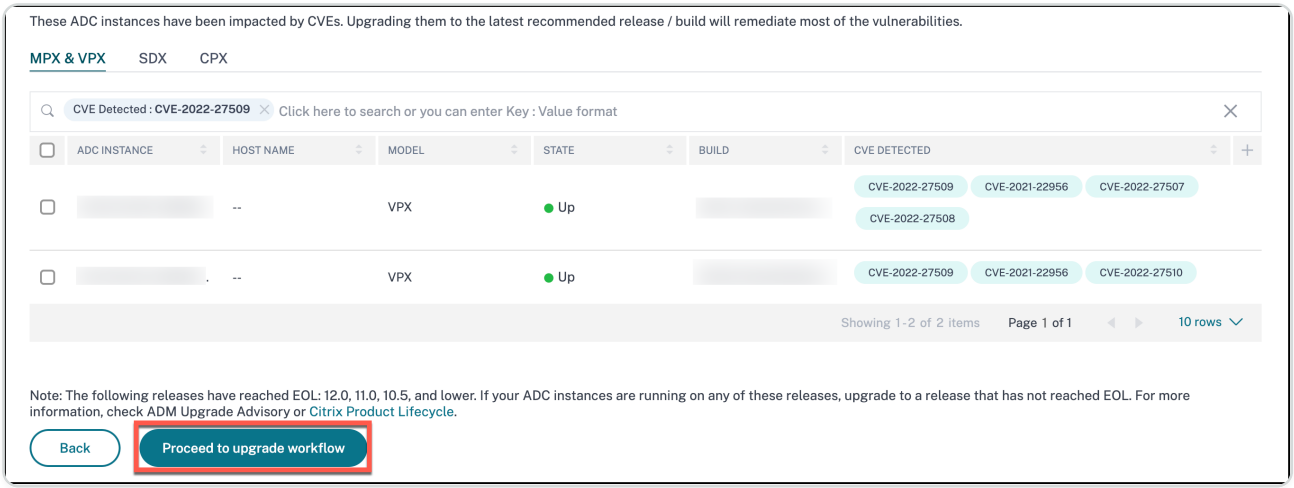
在 **当前 CVE > 受 CVE 影响的 NetScaler 实例** 下，您会看到此单步补救过程的以下工作流，即 **继续升级工作流**。

要升级易受攻击的实例，请选择实例并单击 **继续升级工作流**。升级工作流将打开，其中已填充了易受攻击的 NetScaler 实例。

重要

如果您的易受攻击的 NetScaler 实例已将 /etc/httpd.conf 文件复制到 /nsconfig 目录，请在计划 NetScaler 升级之前参阅 自定义 NetScaler 配置的升级注意事项。

有关如何使用 NetScaler Console 升级 NetScaler 实例的更多信息，请参阅 创建 NetScaler 升级作业。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

安全通报中不支持的 CVE

NetScaler Console 安全通报跟踪所有新的通用漏洞披露 (CVE)，并评估 CVE 对基础设施的影响。您可以查看建议并采取适当的措施。但是，有一些 CVE 不受支持，并且这些漏洞的检测和修复超出了 NetScaler Console 安全通报的范围。

- **CVE-2022-21827：**

  CVE-2022-21827 影响适用于 Windows 的 NetScaler Gateway 插件 21.9.1.2 之前的受支持版本。

  影响适用于 Windows 的 NetScaler Gateway 插件的漏洞的检测和修复不受 NetScaler Console 支持。此外，无法通过在 NetScaler 侧执行任何检查、验证 NetScaler 版本或检查 NetScaler 配置来评估 NetScaler Gateway 插件漏洞。此 CVE 的检测和修复只能根据部署在客户端上的适用于 Windows 的 NetScaler Gateway 插件的版本进行评估。

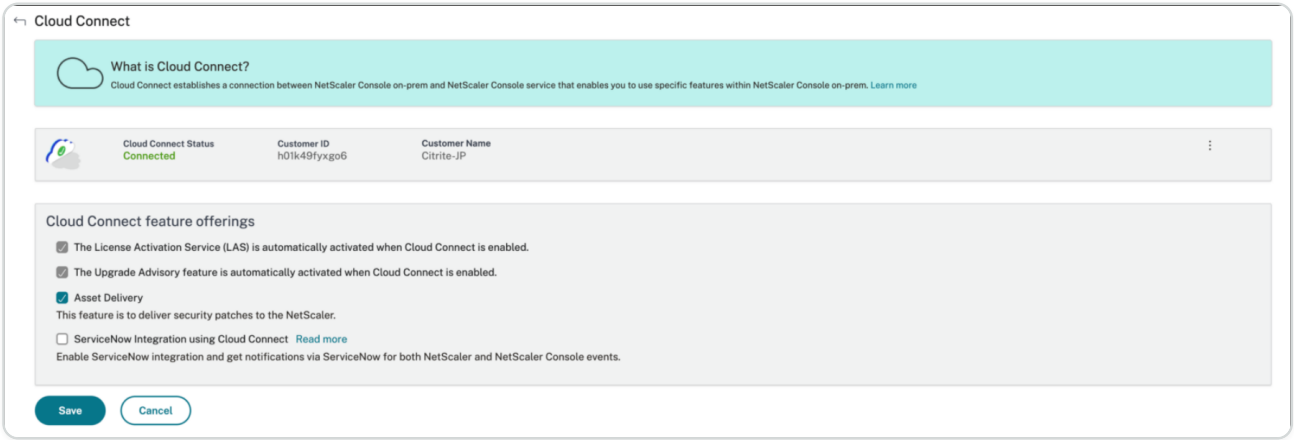
  因此，此漏洞的检测和修复超出了 NetScaler Console 安全通报的范围。

升级建议

从 NetScaler Console 14.1 版本 build 66.x 开始，升级建议功能得到全面支持。您可以通过启用 Cloud Connect 来访问和使用此功能。成功建立 Cloud Connect 后，升级建议将自动启用。

重要

确保 Cloud Connect 已完全启用且所有先决条件均已完成。Cloud Connect 连接的任何问题都将导致升级建议不可用。



作为网络管理员，您可能在 NetScaler Console 中管理运行不同 NetScaler 版本的许多 NetScaler 实例。监控每个 NetScaler 实例的生命周期可能是一项繁琐的任务。您必须访问 NetScaler 产品矩阵

© 1997–2026 Citrix Systems, Inc. All rights reserved.

，识别即将达到或已达到生命周期结束 (EOL) 或维护结束 (EOM) 的 NetScaler 实例。然后，规划它们的升级。

为了简化此过程，NetScaler Console 升级建议通过以下方式帮助您监控 NetScaler 实例的生命周期：

- 识别即将达到或已达到 EOL 或 EOM 的实例。因此，您可以在 EOL 或 EOM 日期之前规划 NetScaler 升级。
- 突出显示未运行最新版本或内部版本的实例。您可以将这些实例升级到最新版本或内部版本。通过此升级，您将收到有关新功能和已修复问题的更新。
- 突出显示未运行首选 NetScaler 内部版本的实例。某些组织可能为其实例设置了首选 NetScaler 内部版本。在 NetScaler Console 中，您可以根据内部版本稳定性、功能和其他考虑因素为您的组织设置首选内部版本。然后，审查并升级未运行首选内部版本的实例。运行首选内部版本的实例将用星形图标表示。
- 突出显示运行最流行版本或内部版本的实例。运行流行内部版本的实例将用功能区图标表示。

升级建议提供指向相应发行说明的链接。借助此信息，您可以审查并决定用于升级的 NetScaler 内部版本。您可以从“升级建议”页面继续创建维护作业以升级 NetScaler 实例。

重要：

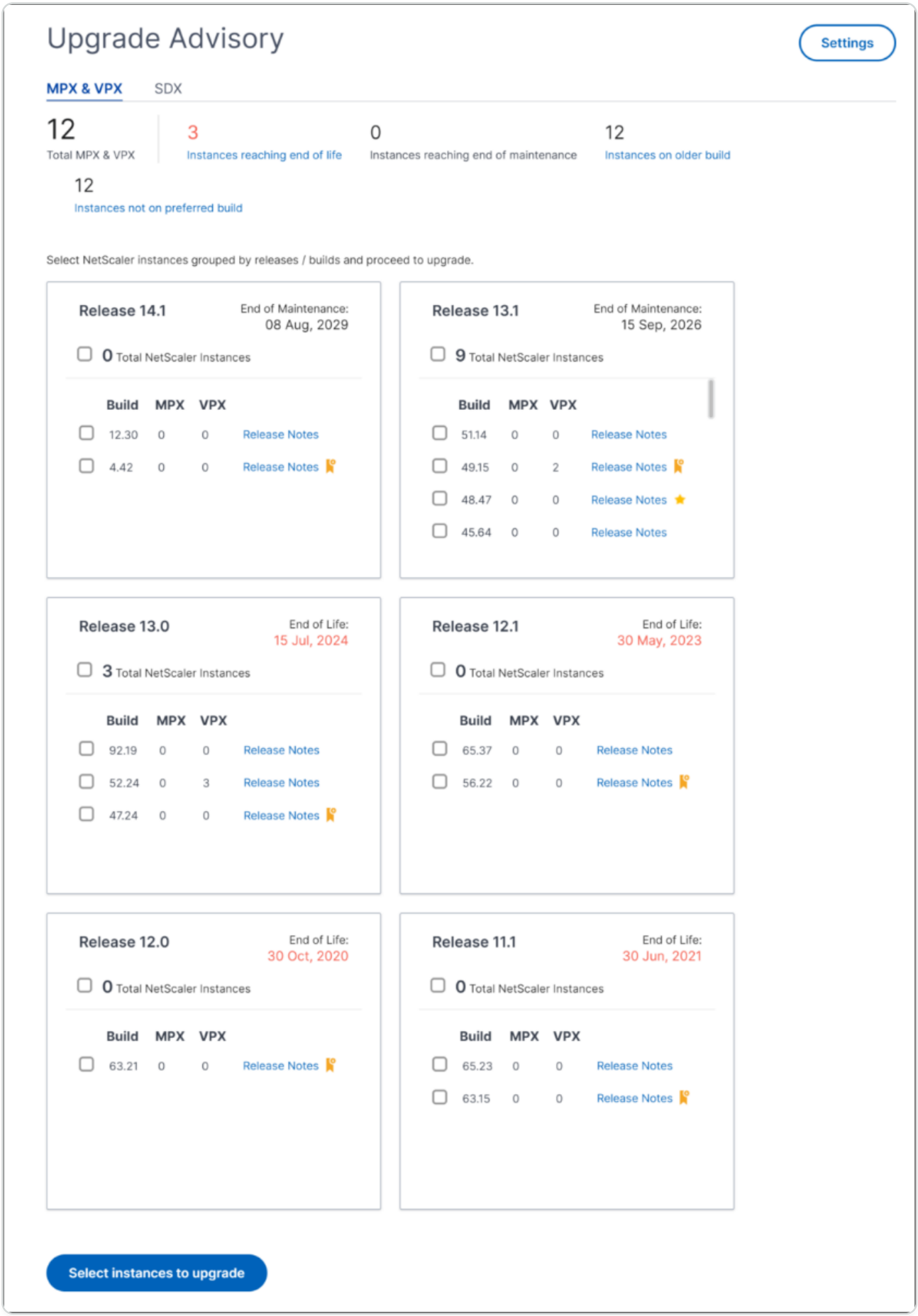
升级建议仅监控 NetScaler 软件版本的 EOL。它不检查 NetScaler 设备的 EOL。

查看升级建议

导航到 **基础架构 > 实例建议 > 升级建议** 并查看以下信息：

- NetScaler 实例总数。
- 即将终止生命周期的实例。
- 即将终止维护的实例。
- 旧版本中的实例。
- 不在首选版本中的实例。
- 各种 NetScaler 版本的生命周期终止和维护终止日期。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



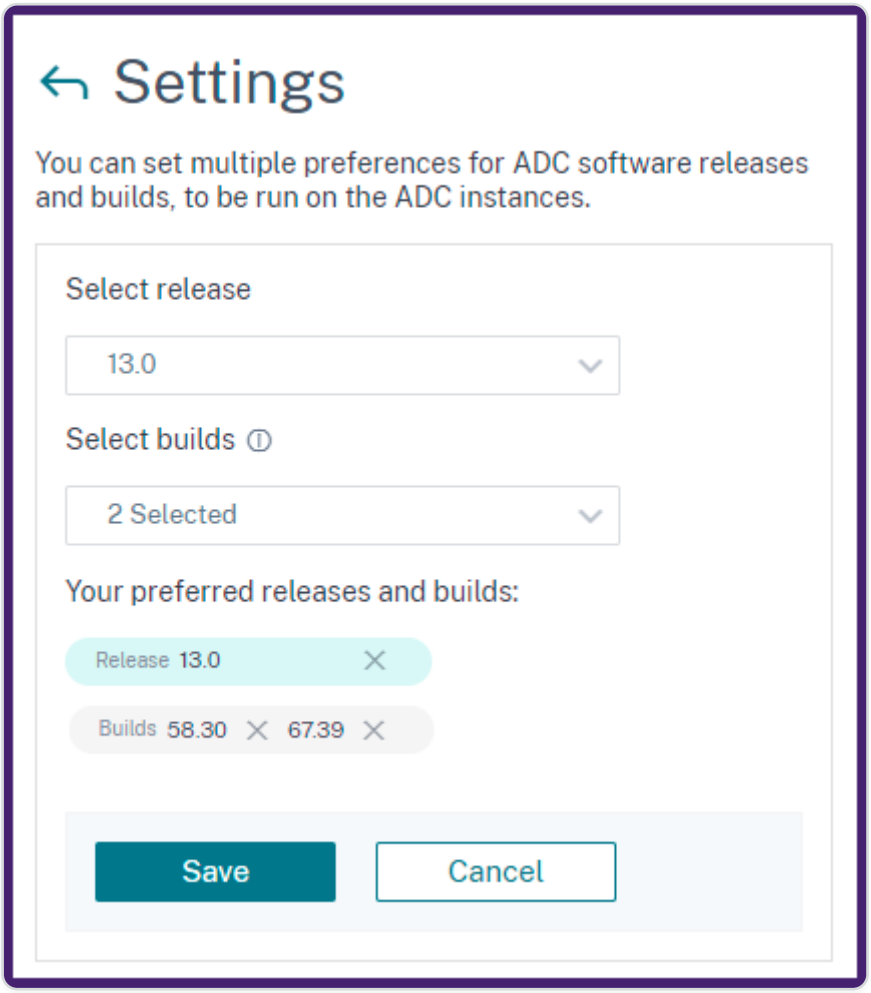
© 1997–2026 Citrix Systems, Inc. All rights reserved.

升级建议页面按版本对 NetScaler 实例进行分组。**发行说明**链接将引导您查看特定的 NetScaler 发行说明。在决定升级之前，请查看新功能、已修复问题和已知问题。您可以一次选择不同版本中的多个 NetScaler 实例进行升级。当您继续升级时，它会创建一个升级作业。请参阅，升级 NetScaler 实例。

设置首选版本

作为管理员，您可以为组织定义首选的 NetScaler 版本。执行以下操作以设置首选版本：

1. 在 **基础架构 > 实例建议 > 升级建议** 中，单击**设置**。
2. 选择首选版本和内部版本。



在此示例中，首选版本是 `13.0-58.30` 和 `13.0-67.39`。

3. 点击 **保存**。

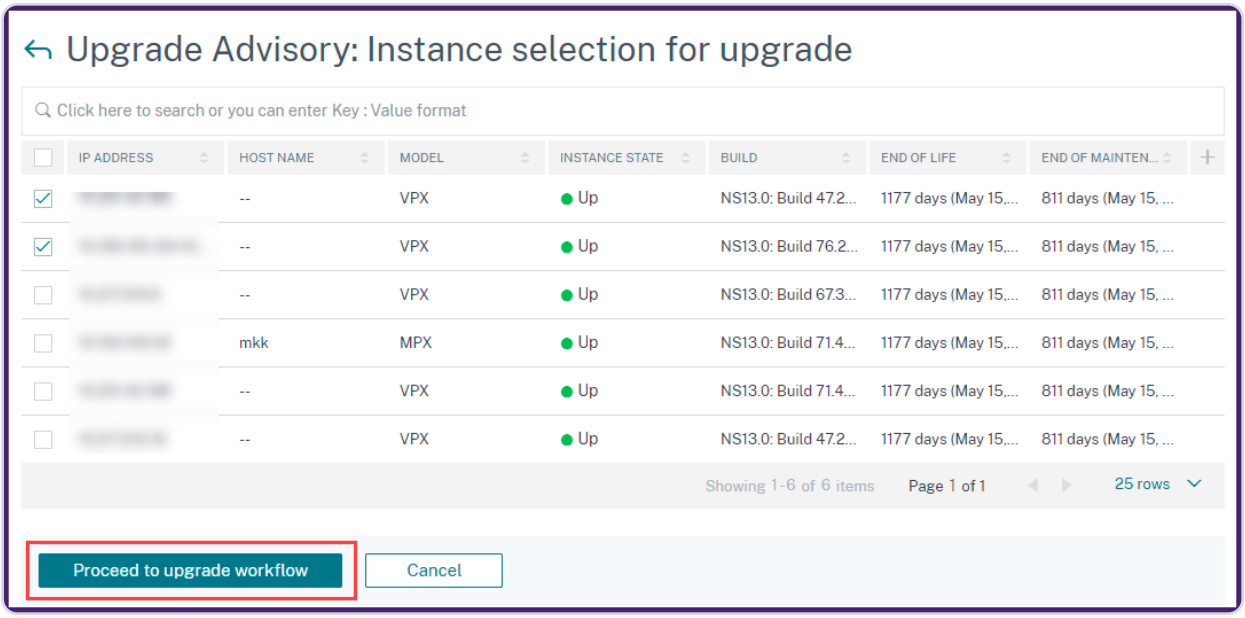
升级 NetScaler 实例

在 **升级建议** 页面中，审阅后，执行以下步骤以升级所需的 NetScaler 实例：

1. 选择要升级的实例版本，然后点击 **选择要升级的实例**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 选择要升级的 NetScaler 实例，然后点击 **继续升级工作流**。



此工作流创建一个升级作业。

3. 在 **选择实例** 选项卡中，

   a. 为升级作业指定名称。

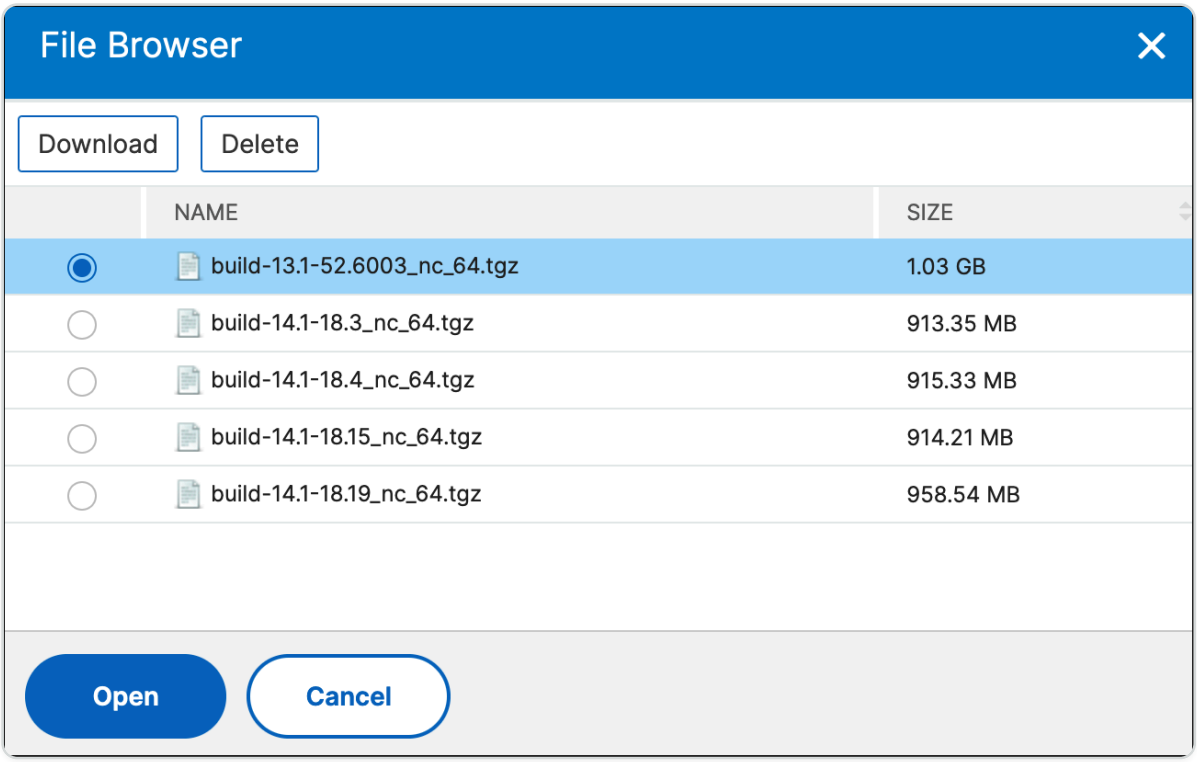
   b. （可选）如果要添加其他实例，点击 **添加实例**。

   c. 点击 **下一步**。

4. 在 **选择映像** 选项卡中，从映像库、本地或设备中选择一个 NetScaler 映像。

   - **从映像库中选择**：从列表中选择一个 NetScaler 映像。此选项列出了 NetScaler 下载网站中所有可用的 NetScaler 映像。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler 软件映像显示带有星形图标的首选版本，以及带有书签图标的下载次数最多的版本。

- **从本地或设备中选择**：您可以从本地计算机或 NetScaler 设备上传映像。当您选择 NetScaler 设备时，NetScaler Console GUI 会显示 `/var/mps/mps_images` 中存在的实例文件。从 NetScaler Console GUI 中选择映像。
- **如果所选映像已可用，则跳过将映像上传到 NetScaler** - 此选项检查所选映像在 NetScaler 中是否可用。升级作业会跳过上传新映像，并使用 NetScaler 中可用的映像。
- **成功升级后从 NetScaler 清理软件映像** - 此选项会在实例升级后清除 NetScaler 实例中上传的映像。

单击“**下一步**”以开始对所选实例进行升级前验证。

5. “**升级前验证**”选项卡显示失败的实例。您可以删除失败的实例，然后单击“**下一步**”。

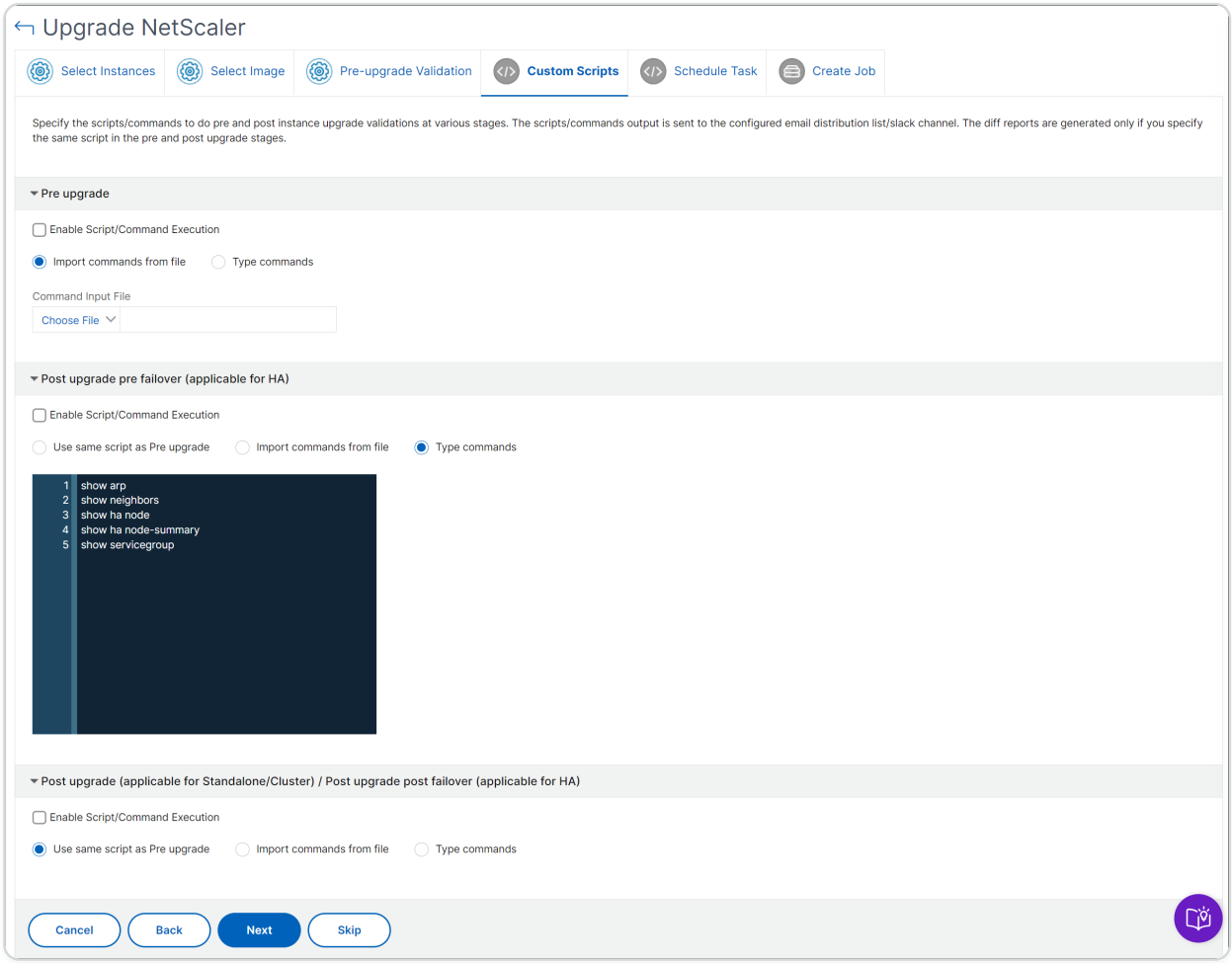
- **磁盘空间检查**：如果实例上磁盘空间不足，您可以检查并清理磁盘空间。请参阅清理 NetScaler 磁盘空间。
- **策略检查**：如果 NetScaler Console 发现不支持的经典策略，您可以删除此类策略以创建升级作业。

注意：

如果您指定群集 IP 地址，NetScaler Console 仅对指定的实例执行升级前验证，而不对其他群集节点执行验证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. （可选）在“**自定义脚本**”选项卡中，指定要在实例升级前后运行的脚本。



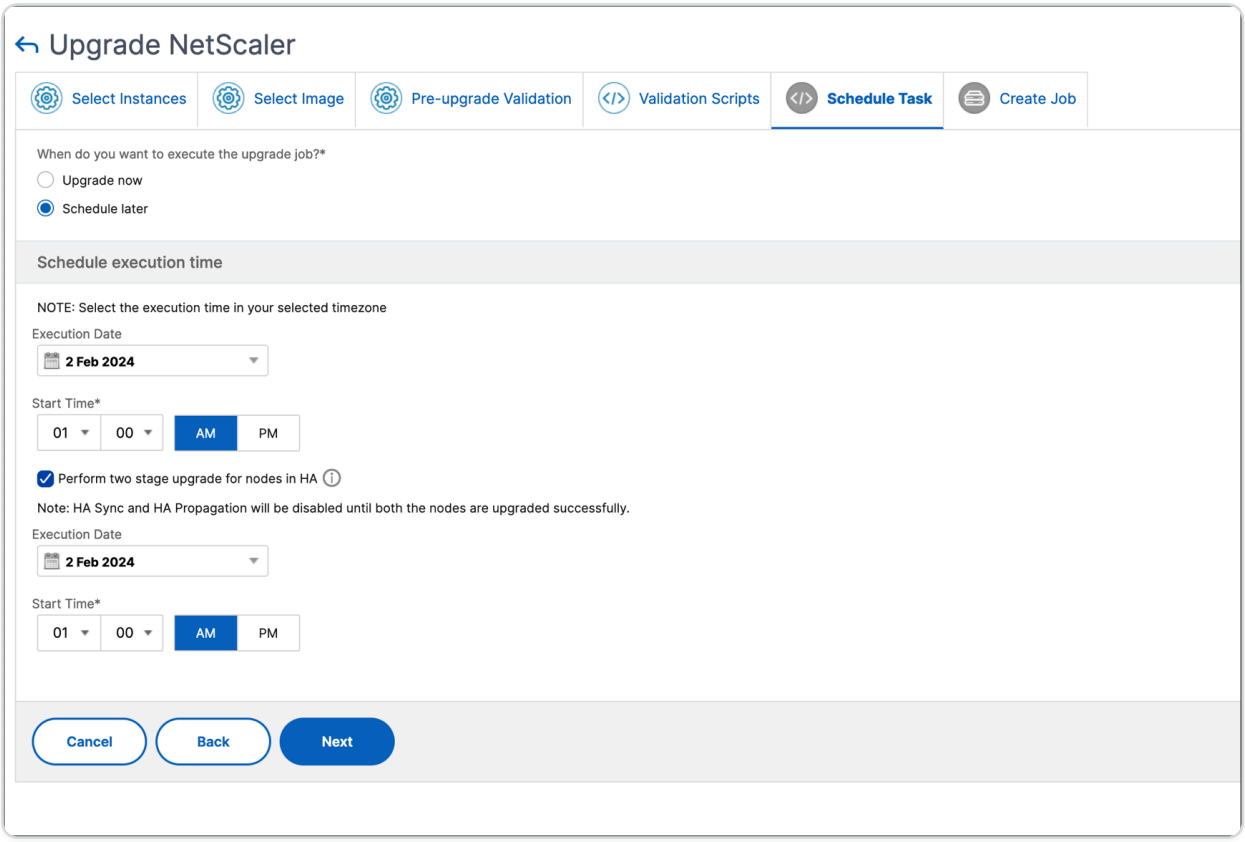
有关详细信息，请参阅使用自定义脚本。

7. 在“**计划任务**”中，选择以下选项之一：

   - **立即升级** - 升级作业会立即运行。
   - **稍后计划** - 选择此选项可稍后运行此升级作业。指定您要升级实例的“**执行日期**”和“**开始时间**”。

   如果您想分两个阶段升级 NetScaler 高可用性对，请选择“对 HA 中的节点执行两阶段升级”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



有关更多信息，请参阅升级 NetScaler 高可用性对。

8. 在“**创建作业**”选项卡中，指定以下详细信息：

   如果您计划升级作业，可以指定何时将映像上传到实例：

   - **立即上传**：选择此选项可立即上传映像。但是，升级作业将在计划的时间运行。
   - **在执行时上传**：选择此选项可在升级作业执行时上传映像。

有关其他选项的更多信息，请参阅NetScaler 升级选项。

编排

在软件定义网络 (SDN) 中，软件应用程序控制器管理网络及其活动，而不是支持网络的硬件。也就是说，SDN 允许网络管理员将物理网络连接虚拟化为逻辑网络连接，并使用基于软件的集中管理工具管理网络服务。SDN 允许网络工程师和管理员响应快速变化的业务需求。

尽管 SDN 更广为人知的优势是流量可编程性、更高的敏捷性、创建策略驱动的网络监管的能力以及实现网络自动化，但 SDN 的一些具体优势如下：

- 集中式网络调配
- 提高粒度级别的网络安全性
- 降低运营成本

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 提高云抽象级别
- 保证内容交付
- 减少网络停机时间

NetScaler Console 通过与不同供应商的 SDN 控制器集成来支持企业网络中的 SDN。NetScaler Console 同时支持 VMware NSX Manager 和 Cisco Application Policy Infrastructure Controller (APIC)。

VMware NSX 管理器

NetScaler Console 与 VMware 网络虚拟化平台集成，以自动化 NetScaler 服务的部署、配置和管理。这种集成抽象了与物理网络拓扑相关的传统复杂性，使 vSphere/vCenter 管理员能够更快地以编程方式部署 NetScaler 服务。

VMware NSX Manager 暴露逻辑防火墙、交换机、路由器、端口和其他网络元素，以允许在不同的虚拟机管理程序、云管理系统和相关网络硬件之间进行虚拟网络连接。它还支持外部网络和安全服务。

NetScaler Console 的云编排功能实现了 NetScaler 产品与 VMware NSX 的集成，并提供以下功能：

- 能够按需分配预配置的 VPX，作为服务插入的一部分，分配给特定的边缘网关。
- 能够在 NSX 环境中运行的实例上，通过应用程序模板配置 NetScaler 的高级功能（如 SSL 和 CS）以及基本的负载均衡。
- 能够在服务删除时从某个 Edge 网关解除分配 VPX，并为另一个 Edge 网关重新分配相同的 VPX。
- 能够作为应用程序所需所有基础设施部署工作流的一部分，从 vCenter 控制台快速部署 NetScaler 功能。

优势：

- 作为应用程序部署工作流的一部分，自动按需分配新的 NetScaler 服务
- 通过应用程序模板简化应用程序特定的高级 NetScaler 功能配置
- 多租户职责分离和自助服务消费模型，同时为云管理员提供单一控制点
- 更轻松地与 NetScaler Console API 集成，有助于支持未来不可预见的使用。

有关如何在 NetScaler Console 上配置 VMware NSX Manager 的更多信息，请参阅将 NetScaler 设备与 VMware NSX Manager 集成。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OpenStack: 集成 NetScaler 实例

NetScaler Console 的云编排功能支持 NetScaler 产品与 OpenStack 平台的集成。通过在 OpenStack 平台中使用此功能，OpenStack 用户可以利用 NetScaler 的负载均衡功能 (LBaaS)。之后，OpenStack 用户可以将他们的负载均衡器配置从 OpenStack 部署到 NetScaler 实例中。

以下部分简要介绍了 NetScaler Console 和 OpenStack 集成工作流中的功能。

适用于 OpenStack Neutron LBaaS 的 NetScaler 驱动程序

OpenStack Neutron LBaaS 插件包含一个 NetScaler 驱动程序，该驱动程序使 OpenStack 能够与 NetScaler Console 通信。OpenStack 使用此驱动程序将通过 LBaaS API 完成的任何负载均衡配置转发到 NetScaler Console，后者在所需的 NetScaler 实例上创建负载均衡器配置。OpenStack 还使用该驱动程序定期调用 NetScaler Console，以从 NetScaler 检索所有负载均衡配置的不同实体（例如 VIP 和池）的状态。适用于 OpenStack 平台的 NetScaler 驱动程序软件与 NetScaler Console 捆绑在一起。要下载并安装驱动程序，您必须首先安装 NetScaler Console 并启动应用程序。

NetScaler Console 和 OpenStack 相互注册

您必须首先在 NetScaler Console 上注册 OpenStack 信息。指定 OpenStack 控制器 IP 地址和云管理员用户凭据，以及 OpenStack NetScaler 驱动程序用户凭据。您稍后可以在 Neutron 配置文件 (neutron.conf) 的 NetScaler_driver 部分中指定相同的登录凭据，以便 OpenStack 中的 NetScaler 驱动程序在 LB 配置期间可以连接到 NetScaler Console。

OpenStack 和 NetScaler Console 相互注册后，两者可以相互通信。此外，OpenStack 用户可以使用他们在 OpenStack 中的现有凭据登录到 NetScaler Console 用户界面，以检查他们的 LB 配置在 NetScaler 中的运行情况。

OpenStack 中的租户

在 OpenStack 中，租户也称为项目。租户是一组用户；租户或项目也可以定义为分配给一组独立用户的资源（计算、网络、存储等）的集合。

放置策略

放置策略提供了灵活性，可以决定在用户创建的每个负载均衡器配置中使用哪个 NetScaler 实例。此外，NetScaler Console 还提供了一个选项，可以根据 OpenStack 租户分配 NetScaler 实例。

服务包

服务包是将策略/SLA、设备或自动配置规范以及租户/放置策略捆绑在一起的集合。服务包通常根据提供给租户的隔离策略来定义。

以下是与服务包相关的一些要点：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 租户不能属于多个服务包。
- 多个租户可以与同一个服务包关联。
- 在设置为自动预配的服务包中，虚拟 NetScaler 实例只能从一种平台类型（在 SDX 平台或 OpenStack Compute 平台）创建。

LBaaS V1 和 LBaaS V2 支持的功能

尽管 OpenStack 中的 LBaaS V1 驱动程序支持从 OpenStack Horizon 用户界面进行操作，但 LBaaS V2 驱动程序仅支持命令行操作。

以下列表显示了 OpenStack 上 LBaaS V1 和 LBaaS V2 都支持的功能：

- LBaaS V1
  - 负载均衡
- LBaaS V2
  - 负载均衡
  - 使用由 OpenStack 中的密钥管理器 **Barbican** 管理的证书进行 SSL 卸载
  - 证书捆绑包（包括中间证书颁发机构）
  - SNI 支持

本文档提供有关以下内容的信息：

- 用例场景
- NetScaler Console 与 OpenStack 工作流集成
- 先决条件
- NetScaler Console 和 OpenStack 中的预配置任务
- 使用 Horizon 配置 LBaaS V1 的步骤
- 使用命令行配置 LBaaS V2 的步骤
- 在 OpenStack 上手动预配 NetScaler VPX 实例
- 将 NetScaler Console 与 OpenStack Heat 服务集成
- 在 NetScaler Console 中监控 OpenStack 应用程序

用例场景

以下用例场景解释了 NetScaler Console 与 OpenStack 平台集成的流程：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

一家名为 Example-Cloud-Provider 的企业已使用 OpenStack 组件搭建了一个云，为其租户提供基础设施。Steve 是该云提供商的管理员，而 Tom 是 Example-Cloud-Provider 云基础设施的租户。Tom 的组织 Example-SportsOnline.com 需要两台服务器 S1 和 S1，Tom 还需要一个专用的 NetScaler 设备来在 OpenStack 平台上对服务器 S1 和 S2 之间的流量进行负载均衡。

为满足此要求，Steve 必须安装和配置 OpenStack 和 NetScaler Console，并使它们相互兼容。Steve 必须在 OpenStack 中创建一个名为 Example-SportsOnline 的租户帐户，然后为该租户帐户分配资源。Steve 还必须为 Example-SportsOnline 创建不同的登录凭据（用户），以管理其资源和配置。Tom 现在可以在 OpenStack 上创建两台服务器 S1 和 S2，以管理其组织中的流量。

Steve 必须向 NetScaler Console 注册 OpenStack 详细信息，并在 OpenStack 网络组件 Neutron 中配置 NetScaler LBaaS 驱动程序。注册完成后，NetScaler Console 会显示 OpenStack 中所有租户的详细信息。Steve 可以从列表中选择需要 NetScaler LBaaS 功能的 Example-SportsOnline，并配置 Tom 以便在 NetScaler Console 中为其负载均衡器配置分配一个专用的 NetScaler。

为此，Steve 可以使用 NetScaler Console 用户界面在 OpenStack 的计算层 (Nova) 上预配 NetScaler VPX 实例，或者在 Tom 在 OpenStack 中进行 LB 配置时，启用 MAS 按需自动预配 NetScaler VPX 实例。无论哪种情况，NetScaler Console 都会管理 VPX 实例。为实现此目的，Steve 在 NetScaler Console 中创建了一个服务包，并定义了与 Tom 在 SLA 中商定的服务包条件。例如，Steve 选择“专用”隔离策略，为 Tom 提供一个专用实例来提供负载均衡器配置。也就是说，Steve 在服务包中为 Tom 选择了一个非共享实例。然后，他将许多 NetScaler VPX 实例分配给该服务包，并将 Example-SportsOnline 以及其他需要专用 NetScaler 的租户与该服务包关联起来。因此，当 Tom 执行其第一个负载均衡器配置时，NetScaler Console 会将服务包中的一个 NetScaler VPX 实例分配给 Example-SportsOnline，并将其配置部署到该 NetScaler 中。

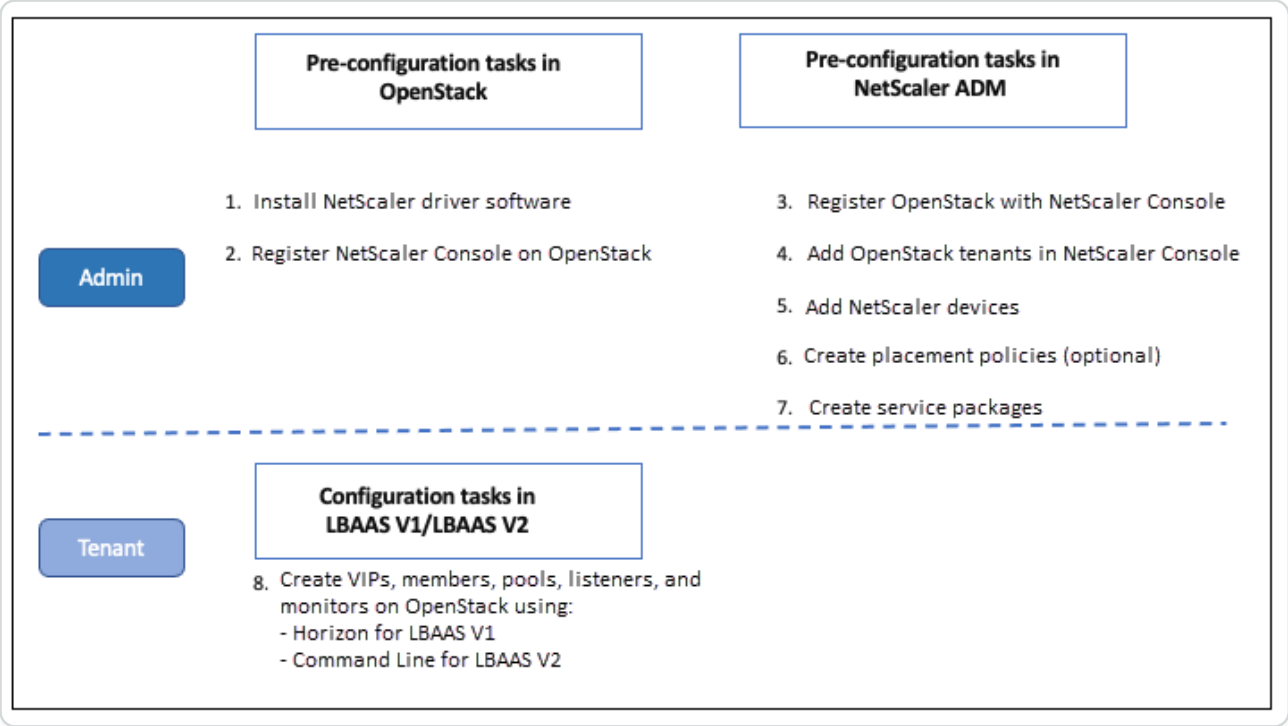
Tom 现在可以使用 OpenStack LBaaS/UI 创建负载均衡配置，包括创建池、虚拟 IP (VIP) 和健康监视器。OpenStack 中的池和 VIP 将作为服务组和虚拟服务器部署在 NetScaler 实例上。Tom 还可以创建健康监视器来监控服务器，并将应用程序流量仅发送到在任何时间点都处于 UP 状态且可从 NetScaler 访问的服务器。

在 OpenStack 中创建的负载均衡配置现在已在 NetScaler 实例上实施。完全配置后，NetScaler VPX 实例将接管负载均衡功能，并开始接受应用程序流量，并在 Tom 创建的服务器 S1 和 S2 之间进行流量负载均衡。

NetScaler Console 与 OpenStack 工作流集成

以下流程图描述了您在配置 LBaaS V1 和 LBaaS V2 时需要遵循的工作流。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



OpenStack: 集成 NetScaler 实例

NetScaler Console 的云编排功能支持 NetScaler 产品与 OpenStack 平台的集成。通过在 OpenStack 平台中使用此功能，OpenStack 用户可以利用 NetScaler 的负载均衡功能 (LBaaS)。之后，OpenStack 用户可以将他们的负载均衡器配置从 OpenStack 部署到 NetScaler 实例中。

以下部分简要介绍了 NetScaler Console 和 OpenStack 集成工作流中的功能。

适用于 OpenStack Neutron LBaaS 的 NetScaler 驱动程序

OpenStack Neutron LBaaS 插件包含一个 NetScaler 驱动程序，该驱动程序使 OpenStack 能够与 NetScaler Console 通信。OpenStack 使用此驱动程序将通过 LBaaS API 完成的任何负载均衡配置转发到 NetScaler Console，后者在所需的 NetScaler 实例上创建负载均衡器配置。OpenStack 还使用该驱动程序定期调用 NetScaler Console，以从 NetScaler 检索所有负载均衡配置的不同实体（例如 VIP 和池）的状态。适用于 OpenStack 平台的 NetScaler 驱动程序软件与 NetScaler Console 捆绑在一起。要下载并安装驱动程序，您必须首先安装 NetScaler Console 并启动应用程序。

NetScaler Console 和 OpenStack 相互注册

您必须首先在 NetScaler Console 上注册 OpenStack 信息。指定 OpenStack 控制器 IP 地址和云管理员用户凭据，以及 OpenStack NetScaler 驱动程序用户凭据。您稍后可以在 Neutron 配置文件 (neutron.conf) 的 NetScaler_driver 部分中指定相同的登录凭据，以便 OpenStack 中的 NetScaler 驱动程序在 LB 配置期间可以连接到 NetScaler Console。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OpenStack 和 NetScaler Console 相互注册后，两者可以相互通信。此外，OpenStack 用户可以使用他们在 OpenStack 中的现有凭据登录到 NetScaler Console 用户界面，以检查他们的 LB 配置在 NetScaler 中的运行情况。

OpenStack 中的租户

在 OpenStack 中，租户也称为项目。租户是一组用户；租户或项目也可以定义为分配给一组独立用户的资源（计算、网络、存储等）的集合。

放置策略

放置策略提供了灵活性，可以决定在用户创建的每个负载均衡器配置中使用哪个 NetScaler 实例。此外，NetScaler Console 还提供了一个选项，可以根据 OpenStack 租户分配 NetScaler 实例。

服务包

服务包是将策略/SLA、设备或自动配置规范以及租户/放置策略捆绑在一起的集合。服务包通常根据提供给租户的隔离策略来定义。

以下是与服务包相关的一些要点：

- 租户不能属于多个服务包。
- 多个租户可以与同一个服务包关联。
- 在设置为自动预配的服务包中，虚拟 NetScaler 实例只能从一种平台类型（在 SDX 平台或 OpenStack Compute 平台）创建。

LBaaS V1 和 LBaaS V2 支持的功能

尽管 OpenStack 中的 LBaaS V1 驱动程序支持从 OpenStack Horizon 用户界面进行操作，但 LBaaS V2 驱动程序仅支持命令行操作。

以下列表显示了 OpenStack 上 LBaaS V1 和 LBaaS V2 都支持的功能：

- LBaaS V1
  - 负载均衡
- LBaaS V2
  - 负载均衡
  - 使用由 OpenStack 中的密钥管理器 **Barbican** 管理的证书进行 SSL 卸载
  - 证书捆绑包（包括中间证书颁发机构）
  - SNI 支持

© 1997–2026 Citrix Systems, Inc. All rights reserved.

本文档提供有关以下内容的信息：

- 用例场景
- NetScaler Console 与 OpenStack 工作流集成
- 先决条件
- NetScaler Console 和 OpenStack 中的预配置任务
- 使用 Horizon 配置 LBaaS V1 的步骤
- 使用命令行配置 LBaaS V2 的步骤
- 在 OpenStack 上手动预配 NetScaler VPX 实例
- 将 NetScaler Console 与 OpenStack Heat 服务集成
- 在 NetScaler Console 中监控 OpenStack 应用程序

用例场景

以下用例场景解释了 NetScaler Console 与 OpenStack 平台集成的流程：

一家名为 Example-Cloud-Provider 的企业已使用 OpenStack 组件搭建了一个云，为其租户提供基础设施。Steve 是该云提供商的管理员，而 Tom 是 Example-Cloud-Provider 云基础设施的租户。Tom 的组织 Example-SportsOnline.com 需要两台服务器 S1 和 S1，Tom 还需要一个专用的 NetScaler 设备来在 OpenStack 平台上对服务器 S1 和 S2 之间的流量进行负载均衡。

为满足此要求，Steve 必须安装和配置 OpenStack 和 NetScaler Console，并使它们相互兼容。Steve 必须在 OpenStack 中创建一个名为 Example-SportsOnline 的租户帐户，然后为该租户帐户分配资源。Steve 还必须为 Example-SportsOnline 创建不同的登录凭据（用户），以管理其资源和配置。Tom 现在可以在 OpenStack 上创建两台服务器 S1 和 S2，以管理其组织中的流量。

Steve 必须向 NetScaler Console 注册 OpenStack 详细信息，并在 OpenStack 网络组件 Neutron 中配置 NetScaler LBaaS 驱动程序。注册完成后，NetScaler Console 会显示 OpenStack 中所有租户的详细信息。Steve 可以从列表中选择需要 NetScaler LBaaS 功能的 Example-SportsOnline，并配置 Tom 以便在 NetScaler Console 中为其负载均衡器配置分配一个专用的 NetScaler。

为此，Steve 可以使用 NetScaler Console 用户界面在 OpenStack 的计算层 (Nova) 上预配 NetScaler VPX 实例，或者在 Tom 在 OpenStack 中进行 LB 配置时，启用 MAS 按需自动预配 NetScaler VPX 实例。无论哪种情况，NetScaler Console 都会管理 VPX 实例。为实现此目的，Steve 在 NetScaler Console 中创建了一个服务包，并定义了与 Tom 在 SLA 中商定的服务包条件。例如，Steve 选择“专用”隔离策略，为 Tom 提供一个专用实例来提供负载均衡器配置。也就是说，Steve 在服务包中为 Tom 选择了一个非共享实例。然后，他将许多 NetScaler VPX 实例分配给该服务包，并将 Example-SportsOnline 以及其他需要专用 NetScaler 的租户与该服务包关联起来。因

© 1997–2026 Citrix Systems, Inc. All rights reserved.

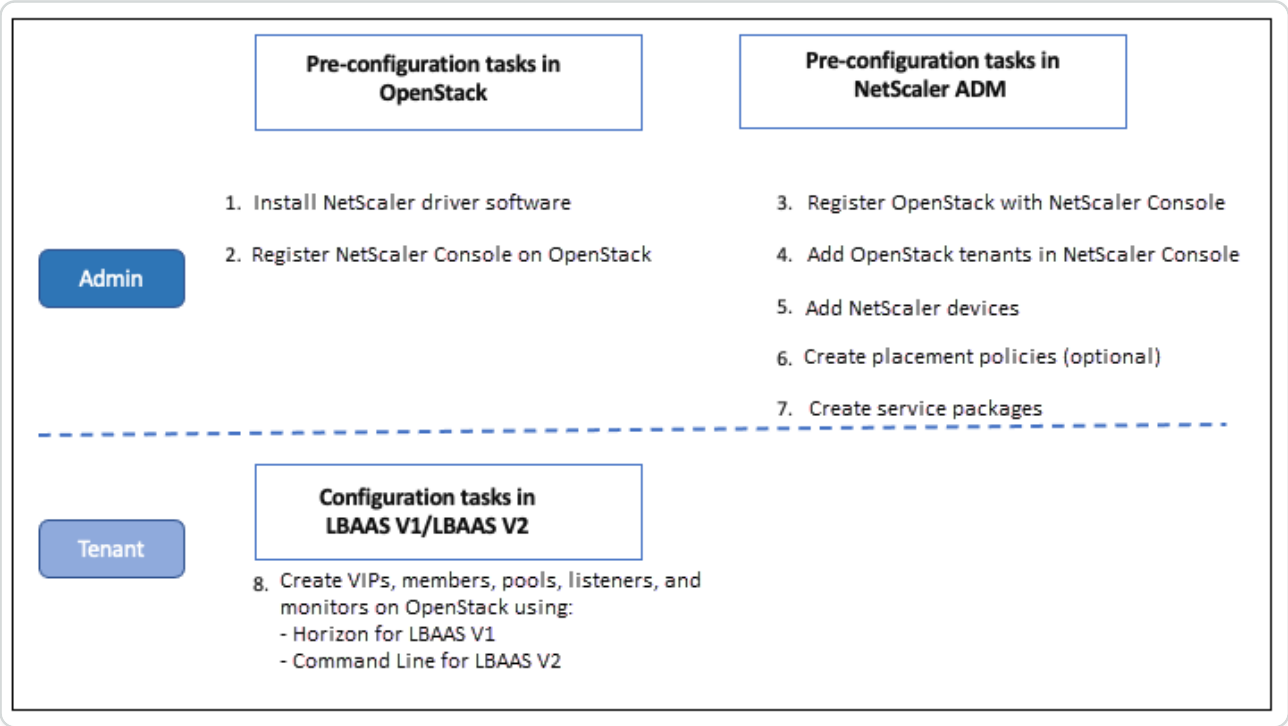
此，当 Tom 执行其第一个负载均衡器配置时，NetScaler Console 会将服务包中的一个 NetScaler VPX 实例分配给 Example-SportsOnline，并将其配置部署到该 NetScaler 中。

Tom 现在可以使用 OpenStack LBaaS/UI 创建负载均衡配置，包括创建池、虚拟 IP (VIP) 和健康监视器。OpenStack 中的池和 VIP 将作为服务组和虚拟服务器部署在 NetScaler 实例上。Tom 还可以创建健康监视器来监控服务器，并将应用程序流量仅发送到在任何时间点都处于 UP 状态且可从 NetScaler 访问的服务器。

在 OpenStack 中创建的负载均衡配置现在已在 NetScaler 实例上实施。完全配置后，NetScaler VPX 实例将接管负载均衡功能，并开始接受应用程序流量，并在 Tom 创建的服务器 S1 和 S2 之间进行流量负载均衡。

NetScaler Console 与 OpenStack 工作流集成

以下流程图描述了您在配置 LBaaS V1 和 LBaaS V2 时需要遵循的工作流。



先决条件

在将 NetScaler 虚拟实例与 OpenStack 平台集成之前，请确保满足以下要求：

NetScaler Console 和 OpenStack 软件要求

- NetScaler Console 13.1 已安装在满足最低硬件要求的受支持虚拟机管理程序工作站上。
- OpenStack 组件已安装并正在运行。
- NetScaler Console 13.1 支持以下 OpenStack 版本 - **Newton**、**Ocata**、**Pike** 和 **Queens**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console 硬件要求

确保您的 OpenStack 服务器上具有以下虚拟计算资源，以便安装 NetScaler 虚拟实例：

组件	要求
内存	8 GB
虚拟 CPU	8
存储空间	500 GB
虚拟网络接口	1
吞吐量	1 吉比特/秒 或 100 兆比特/秒

注意

此处指定的内存和硬盘要求适用于在 OpenStack 平台上部署 NetScaler Console，前提是主机上没有运行其他虚拟机。OpenStack 的硬件要求取决于其上运行的虚拟机数量。

NetScaler Console 和 OpenStack 中的预配置任务

本节将帮助您在配置 NetScaler Console 和 OpenStack 之前执行预配置任务。

安装 NetScaler Console

在受支持的管理程序上安装 NetScaler Console。有关如何下载和安装 NetScaler Console 的更多信息，请参阅 部署 NetScaler Console。

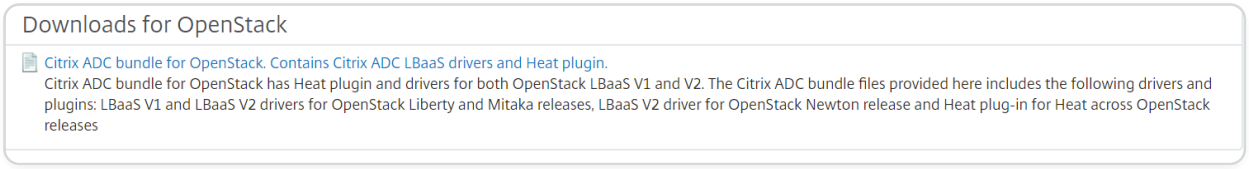
安装 NetScaler 驱动程序软件并在 OpenStack 上注册 NetScaler Console

从 NetScaler Console 下载页面下载适用于 OpenStack 的 NetScaler 捆绑包。

使用 NetScaler Console GUI 在 OpenStack 平台上安装 NetScaler 驱动程序：

1. 在 NetScaler Console 中，单击**下载**。NetScaler Console 中的**下载**页面提供了下载 **NetScaler bundle for OpenStack** 软件的链接，该软件是 **Newton**、**Ocata** 和 **Pike** OpenStack 版本所需的。
2. 将最新的 NetScaler 捆绑包 tar 文件下载到 OpenStack 控制器中的临时目录（例如，/tmp）。此捆绑包包括所有 OpenStack 版本的 LBaaS V2 驱动程序和 Heat 插件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 运行以下命令从 NetScaler 驱动程序 tar 文件中提取文件：`tar -xvzf <name_of_tar_file>`
4. 如果您有 OpenStack \<Release Name\> 设置，请在提示符下键入以下命令：

   `cd <Release Name>`

   示例：

   `cd Newton`

5. 运行以下命令以安装驱动程序，并指定 NetScaler Console IP 地址、在将 OpenStack 注册到 NetScaler Console 时配置的 NetScaler 驱动程序密码以及协议：

   `./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>`

   单节点 OpenStack 设置示例：

   `./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/opt/stack/neutron-lbaas`

   多节点 OpenStack 设置示例：

   `./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/usr/lib/python2.7/site-packages`

   > **注意**
   >
   > 提供系统 `neutron-lbaas` 目录的路径是可选的。提供该路径可能有助于脚本查找驱动程序。

   在 OpenStack 上成功注册 NetScaler Console 后，您也可以使用 OpenStack 用户凭据登录 NetScaler Console。
   在 OpenStack 上成功注册 NetScaler Console 后，请重新启动 OpenStack Neutron 服务。

将 OpenStack 注册到 NetScaler Console

使用 NetScaler Console GUI 将 OpenStack 注册到 NetScaler Console：

1. 在 NetScaler Console 中，导航到 **编排** \> **云编排** \> **OpenStack**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 单击“**配置 OpenStack 设置**”。
3. 在“**配置 OpenStack 设置**”页面中，您可以设置参数以在 NetScaler Console 中配置 OpenStack。您有两个选项：默认和自定义。

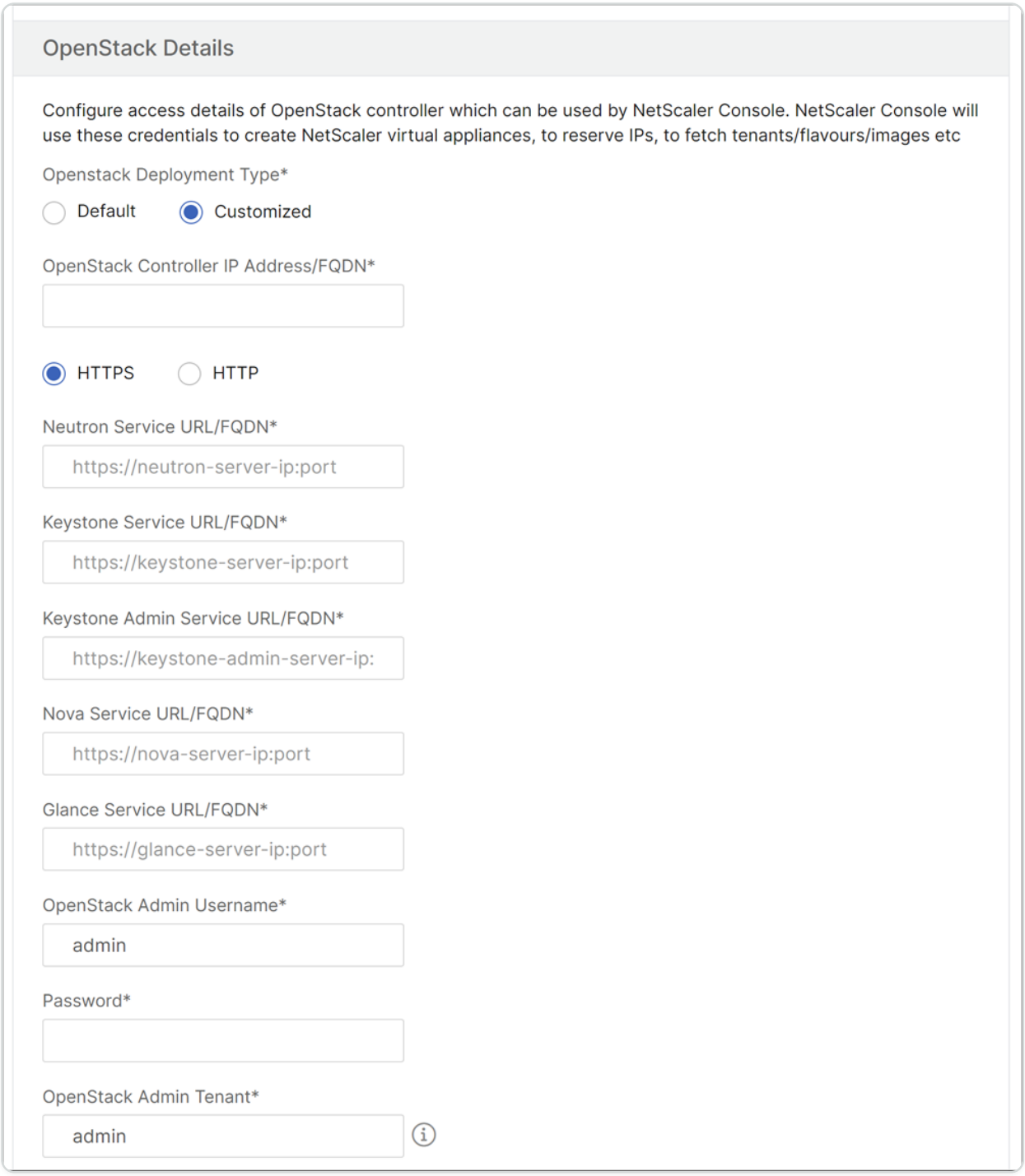
   对于 OpenStack 的 Newton 和 **Ocata** 版本，您可以使用默认或自定义部署类型。但对于 Pike 版本，您必须使用自定义部署类型才能将 OpenStack 注册到 NetScaler Console。

- **默认部署类型**

  如果 OpenStack 服务在默认端口上运行，请选择**默认**。例如，Neutron 服务的默认端口是 9696，Keystone 服务的默认端口是 5000。

1. OpenStack 控制器 IP 地址 - OpenStack 控制器的 IP 地址（**KeyStone** 服务和 **Neutron** 服务都应可通过此 IP 地址访问）。例如，输入 IP 地址 10.102.205.23。
2. OpenStack 管理员用户名 - OpenStack 控制器的管理用户名。例如，输入 admin1。
3. 密码 - OpenStack 控制器的管理用户的密码。
4. OpenStack 管理员租户 - OpenStack 上管理租户的名称。例如，输入 admin。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **自定义部署类型**

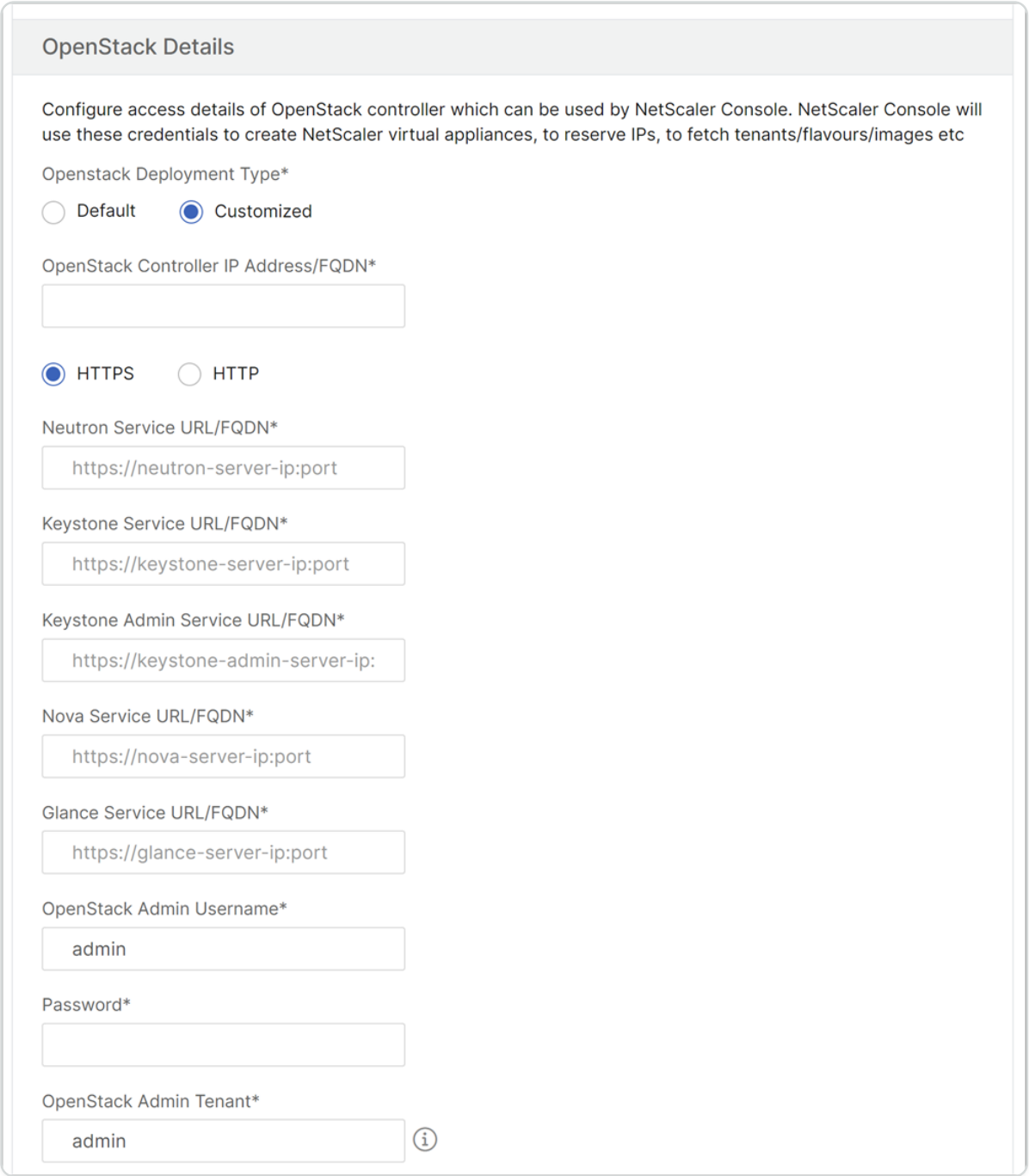
  如果 OpenStack 服务在非默认端口上运行，请选择**自定义**部署类型。如果这些服务在不同端口上运行，请在此处指定。将 OpenStack Newton 和 **Ocata** 版本注册到 NetScaler Console 与注册 OpenStack Pike 版本不同。

  OpenStack 的 Newton 和 Ocata 版本：

  a. 如果您正在注册 OpenStack 的 Newton 版本，请指定各种 OpenStack 服务的端口号。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. 指定 OpenStack 管理员用户名、密码和 OpenStack 管理员租户用户名，与您之前在**默认**设置中指定的一致。



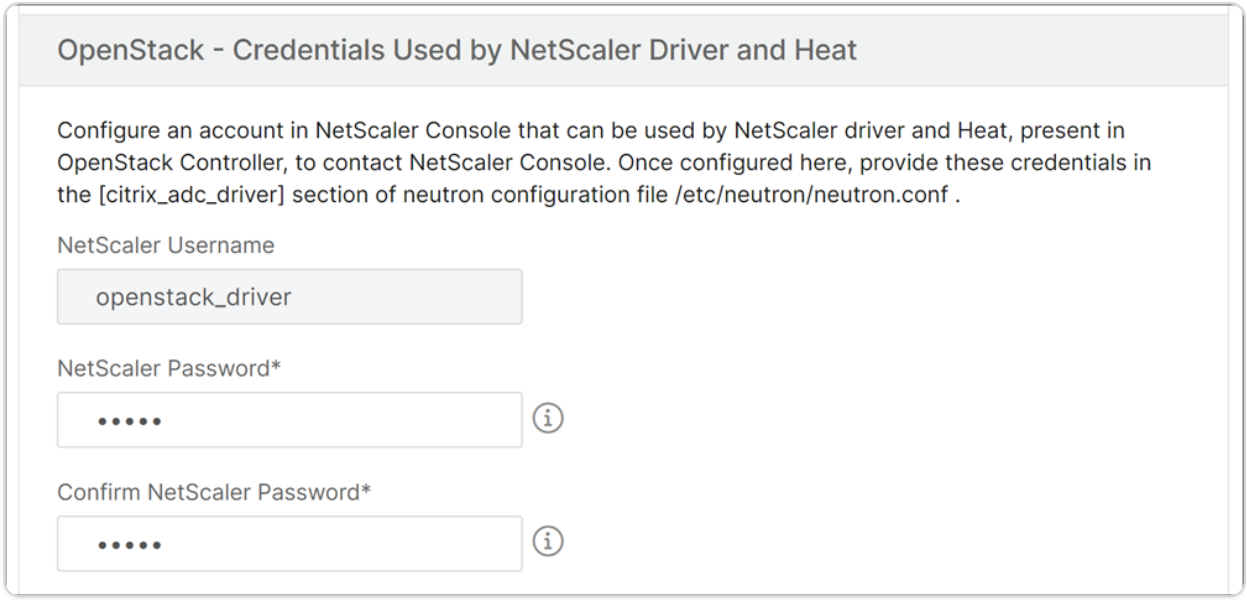
OpenStack 的 Pike 版本：

如果您正在注册 OpenStack 的 Pike 版本，请输入 OpenStack 服务的详细信息，如以下图像所示。您还必须指定 OpenStack 管理员用户名、密码和 OpenStack 管理员租户用户名，如默认设置中所示。

OpenStack 详细信息(/en-us/netscaler-application-delivery-management-software/media/orchestration-openstack-pike.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 在“**OpenStack Neutron LBaaS - NetScaler 驱动程序使用的凭据**”部分中，为 OpenStack NetScaler 驱动程序用户帐户设置 NetScaler 驱动程序密码。NetScaler Console 使用这些凭据对来自 OpenStack NetScaler 驱动程序的调用进行身份验证。在 OpenStack 控制器中运行 NetScaler 驱动程序安装脚本时，必须指定相同的密码。



2. 单击“**确定**”。

在 OpenStack 上创建租户

在 OpenStack 上创建项目或租户，将用户添加到项目或租户，并为所有用户分配角色。OpenStack 中的身份服务 **KeyStone** 为每个 OpenStack 服务提供身份验证服务。身份验证服务使用域、项目（租户）、用户和角色的组合。

有关如何创建项目以及在 OpenStack 中执行其他任务的更多信息，请参阅 `<http://docs.openstack.org/>` 处的 OpenStack 文档。

添加 OpenStack 租户

1. 在 NetScaler Console 中，导航到 **编排** \> **云编排** \> **OpenStack** \> **OpenStack 租户**，然后单击**添加**。
2. 在“**添加 OpenStack 租户**”页面中，单击“**+添加**”，然后选择 OpenStack 租户。
3. 单击“**确定**”。

根据您在集成 OpenStack 时是使用预置实例还是自动置备实例，请执行以下两项任务之一：

- 预置 NetScaler 设备
- 在 OpenStack 上自动置备 NetScaler VPX 设备

© 1997–2026 Citrix Systems, Inc. All rights reserved.

置备 NetScaler 设备

根据您在集成 OpenStack 时是使用预置实例还是自动置备实例，请执行以下两项任务之一：

- 预置 NetScaler 设备
- 在 OpenStack 上自动置备 NetScaler VPX 设备

预置 NETSCALER 设备

在 Citrix Hypervisor、KVM 或 ESX 等任何管理程序平台上安装 NetScaler 设备，并将实例添加到 NetScaler Console。NetScaler Console 随后管理此设备，该设备负责对服务器中的流量进行负载平衡。

将现有 NetScaler VPX 实例添加到 NetScaler Console 中：

1. 在 NetScaler Console 中，导航到 **Infrastructure** \> **Instances** \> **NetScaler VPX**，然后单击 **Add**。
2. 在 **Add NetScaler VPX** 页面上，指定 NetScaler VPX 实例的 IP 地址，并从 **Profile Name** 列表中选择一个实例配置文件。实例配置文件包含用于登录 NetScaler VPX 的凭据。您也可以通过单击 + 图标创建新的实例配置文件。单击 **OK**。

自动置备 NETSCALER 设备

从 NetScaler 下载页面下载所需的 NetScaler 实例映像，并将其上传到 OpenStack 映像服务 Glance 上。在 Glance 上提供映像后，您可以在将实例分配给租户时按需配置 NetScaler 实例。

在 OpenStack 上自动置备 NetScaler VPX 设备：

1. 在 NetScaler Console 中，导航到 **编排** \> **云编排** \> **OpenStack**。
2. 单击 **部署设置**。
3. 设置以下参数：
   a. 管理网络 - 选择 OpenStack 上的管理网络，自动预配的 NetScaler VPX 将连接到该网络。
   b. 配置文件名称 - 从下拉列表中选择配置文件。NetScaler Console 使用此配置文件中包含的密码来配置新的自动预配的 NetScaler VPX 实例。
   c. 许可证 - 提供用于许可新的自动预配的 NetScaler 实例的 NetScaler Console 许可证访问代码。NetScaler Console 在管理网络中的 OpenStack 计算上预配 NetScaler 实例，然后使用指定的许可证代码触发在其上安装许可证。然后，NetScaler 实例使用此处指定的许可证访问代码从 Citrix 网站下载许可证文件。
   d. Glance 中的 NetScaler VPX 映像 - 选择 OpenStack Glance 中可用的 NetScaler VPX 映像，该映像用于创建 NetScaler VPX 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. 代理设置 - 提供用于安装许可证的 NetScaler 代理服务器详细信息。当 NetScaler 无法通过管理网络直接访问 Internet 时，可能需要此设置。

4. 单击 **确定**。

部署设置(/en-us/netscaler-application-delivery-management-software/media/openstack-configure-deployment-settings.png)

在 NetScaler Console 中创建服务包

在 NetScaler Console 中为租户创建服务包：

1. 在 NetScaler Console 中，导航到 **编排** \> **云编排** \> **OpenStack** \> **服务包**，然后单击 **添加**。
2. 在 **Service Package** 页面上指定以下参数：

   a. 名称 - 服务包的名称。例如，输入 SVC-PKG-GOLD。

   b. NetScaler 实例分配 - 服务包中定义的实例分配类型，基于此类型将 NetScaler 实例资源分配给租户。选择 **Dedicated**。有关策略的更多信息，请参阅 服务包隔离策略。

   c. NetScaler 实例预配 - 选择 **Existing Instance** 以将现有 NetScaler 实例分配给租户。如果要在配置过程中创建 NetScaler 实例，请选择 **Create Instance OnDemand**。

   d. NetScaler 实例类型 - 选择 **NetScaler VPX**。

   > **注意**
   >
   > 选择 NetScaler VPX 以分配托管在 SDX 平台上的预配置 NetScaler 实例。

3. 单击“**继续**”以将租户与服务包关联。

   > **注意**
   >
   > 如果您正在以高可用性模式部署 NetScaler 实例，请启用“**为高可用性预配一对 NetScaler 实例**”。

4. 在“**分配实例**”部分中，单击“**添加**”，然后选择要分配给租户的 NetScaler 实例，并单击“**继续**”。
5. 在“**分配 OpenStack 租户/放置策略**”部分中，在“**OpenStack 租户**”下，单击“**添加**”，然后选择租户。
6. 单击“**继续**”，然后单击“**完成**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

如果未找到策略，则会恢复回退机制，NetScaler Console 会根据租户分配 NetScaler 实例。如果租户不属于任何服务包，NetScaler Console 会显示一条错误消息，指出：“租户 \<admin\> 不属于任何服务包，并且没有默认服务包。”

创建放置策略（可选）

隔离策略并非仅基于租户。您可以创建灵活的放置策略，其中策略不仅基于租户名称或 ID，还基于其他自定义属性。

要在 NetScaler Console 中为租户创建放置策略，请执行以下操作：

1. 在 NetScaler Console 中，导航到“**编排**” \> “**云编排**” \> “**OpenStack**” \> “**放置策略**”，然后单击“**添加**”。
2. 在“**添加放置策略**”页面上，设置以下参数：
   a. 名称 - 输入放置策略的名称
   b. 示例表达式 - 从列表中选择一个示例表达式。这些示例有助于构建放置策略。
   c. 表达式 - 此字段中会根据您在前面字段中选择的示例表达式填充布尔表达式。根据需要编辑字段名称。
3. 单击 **确定**。

通过客户端网络启用从 NetScaler 实例到后端服务器的流量

默认情况下，在 OpenStack 编排工作流中，NetScaler 实例动态绑定到负载均衡器或客户端网络以及成员或服务器网络。

在某些部署中，服务器也可以通过客户端网络访问，并且可以通过客户端网关进行路由。在这种情况下，NetScaler 实例无需绑定到服务器网络，而只需绑定到客户端网络。

执行以下设置以通过客户端网关配置流量。

导航到 **编排** > **云编排** > **OpenStack** > **部署设置**，然后选择 **仅预配 VIP 网络并通过 VIP 网络路由池流量** 选项。

NetScaler Console 然后通过在该网络中添加 SNIP 将 NetScaler 实例配置到客户端网络，并将进一步向客户端网络网关添加默认路由。这使得实例能够通过客户端网关访问服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

自动预配部署在 NetScaler SDX 平台上的 NetScaler VPX 设备

在 NetScaler Console 中添加 NetScaler SDX 平台，以便 NetScaler Console 按需在该平台上预配实例。

要自动预配部署在 NetScaler SDX 平台上的 NetScaler 实例：

1. 在 NetScaler Console GUI 中，导航到 **基础架构 > 实例** \> **NetScaler SDX**，然后单击 **添加** 以添加 NetScaler SDX 平台。
2. 导航到 **编排** \> **云编排** \> **OpenStack** \> **部署设置。**
3. 在“**管理网络**”部分，选择 OpenStack 上自动预配的 NetScaler SDX 所连接的管理网络。
   a. 在“**配置文件名称**”中，从下拉列表中选择配置文件。NetScaler Console 使用此配置文件中包含的密码来配置新的自动预配的 NetScaler VPX 实例。
   b. 单击“**确定**”。
4. 要在 OpenStack 中预配 NetScaler SDX 平台，请导航到 **编排** \> **云编排** \> **OpenStack** \> **服务包**。
   a. 单击“**添加**”以创建新的服务包。
   b. 输入服务包的名称。
   c. 在“**NetScaler 实例分配**”字段中，选择“**专用**”。
   d. 在“**NetScaler 实例预配**”字段中，选择“**按需创建实例**”，并在“**自动预配平台**”字段中，选择“**NetScaler SDX**”。
   e. 默认情况下，仅在 NetScaler SDX 平台上预配 NetScaler VPX 实例。
   f. 单击“**继续**”。
   g. 在“**自动预配设置**”部分中，设置“**资源**”属性。
      i. “**吞吐量**”字段。输入 1000 Mbps。
      ii. “**NetScaler 版本**”字段。从列表中选择 NetScaler SDX 平台 上存在的 NetScaler VPX 映像的正确版本。
   h. 在“**NetScaler SDX 平台**”部分中，单击“**添加**”以将 SDX 平台添加到服务包。
   i. 单击“**继续**”。
   j. 在“**配置 OpenStack 租户**”部分，单击“**添加**”以添加租户。您也可以通过单击“**新建**”来添加新租户。
   k. 单击“**完成**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. LBaaS V2 API 实现通过 Neutron LBaaS 命令执行。连接到任何 Neutron 客户端并运行配置任务。有关如何运行配置命令的更多信息，请参阅使用命令行配置 LBaaS V2。

使用 Horizon 配置 LBaaS V1

您可以登录 OpenStack Horizon 门户以创建 LBaaS 池并选择一个子网。此池的所有成员都在该子网中。要配置：

- 添加一个虚拟 IP (VIP) 地址，并将此 VIP 分配给已创建的池。
- 您也可以在命令行或通过 API 执行此操作。
- 您的服务器的外部客户端可以连接到分配的 NetScaler 上托管的此 VIP 地址。
- NetScaler 将所有请求分发到配置端口上的池成员。
- LBaaS 池成员是添加到所选池中的负载均衡服务器。
- 为每个成员分配一个权重和一个端口。

运行状况监视器用于监视池中所有成员的运行状况和良好运行情况。您可以在 OpenStack 中通过定义延迟、超时、重试限制、方法、URL 路径和预期 HTTP 成功代码等参数来创建运行状况监视模板。创建监视器后，您必须将该监视器与之前创建的池关联。

有关如何在 OpenStack 中创建池以及其他 LBaaS 配置任务的更多信息，请参阅 OpenStack 文档。

重要

OpenStack 的 Liberty 版本不支持 LBaaS V1。有关更多信息，请参阅 OpenStack 发行说明。

使用命令行配置 LBaaS V2

LBaaS V2 支持 SSL 卸载，其证书由 **Barbican** 管理，还支持证书捆绑包（包括中间证书颁发机构）、SNI 以及常规负载均衡功能。LBaaS V2 仅支持命令行界面来运行配置任务。LBaaS V2 API 实现通过 Neutron LBaaS 命令执行。

注意

当您需要 SSL 卸载功能时，请将证书和密钥上传到 **Barbican** 服务。如果支持 SSL 卸载，请执行步骤 1、2 和 3，否则从 步骤 4 继续，以创建负载均衡器、侦听器、池和成员。

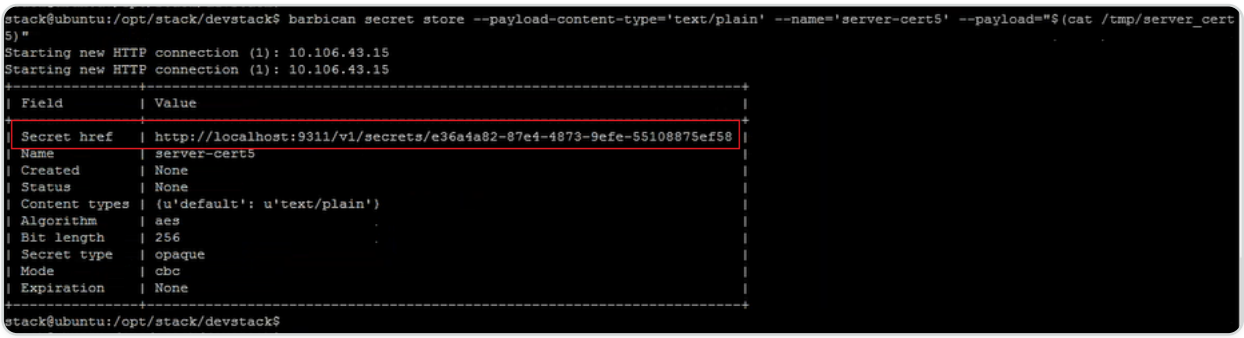
1. 使用以下命令将证书上传到 **Barbican** 服务：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
barbican secret store --payload-content-type <content_type> --name
<certificate_name> --payload<certificate_location>
```

示例：

```
barbican secret store --payload-content-type='text/plain' --
name='hp_server_certificate' --payload=" hp_server/tmp/
server_certificate"
```



2. 使用以下命令将密钥上传到 **Barbican** 服务：

```
barbican secret store --payload-content-type <content_type> --name
<key_name> --payload<key_location>
```

示例：

```
barbican secret store -- payload-content-type='text/plain' --
name='shp_server_key' --payload="hp-server/tmp/server_key"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

当您运行这两个 **Barbican** 命令来加载证书和密钥时，Secret href 字段会提供一个位置或 URL。这是证书和密钥存储在安装了 OpenStack 的系统上的位置。复制这些链接，并在步骤 3 中在 **Barbican** 服务上创建容器时将这些链接作为参数提供。

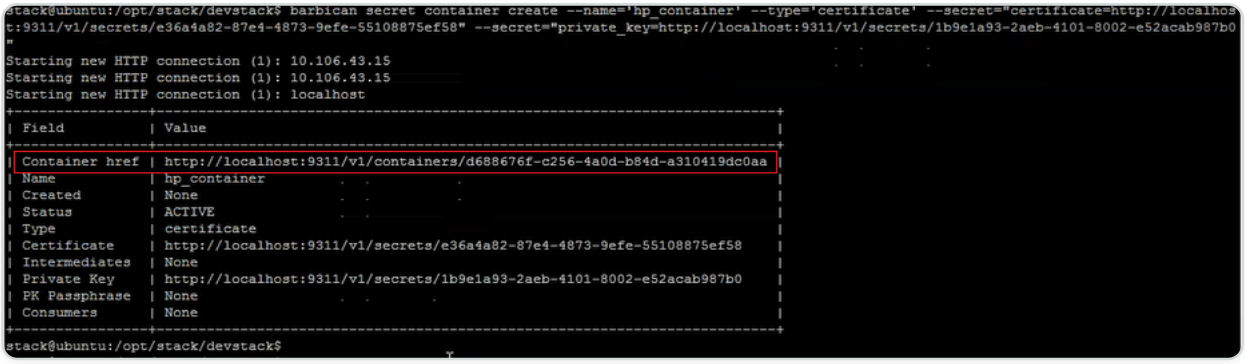
3. 使用以下命令在 **Barbican** 服务中创建容器以存储证书和密钥：

   在命令中，将 <certificate_url> 替换为您上传证书时从 Secret href 字段获取的 URL。同样，将 <key_url> 替换为您上传密钥时从 Secret href 字段获取的 URL。

```
barbican secret container create --name<container_name> --
type<container_type> --secret<certificate_url> --secret<key_url>
```

   示例：

```
barbican secret container create --name='hp_container' --
type='certificate' --secret="`certificate=http://localhost:9311/v1/
secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --
secret="private_key=http://localhost:9311/v1/secrets/
1b9e1a93-2aeb-4101-8002-e52acab987b0`"
```



   复制容器的 href 值。在步骤 6 中创建侦听器时，您必须提供容器的链接。

4. 在 OpenStack 中设置环境变量。这些变量使 OpenStack 客户端命令能够与 OpenStack 服务通信。

   示例:

   导出 OS_PASSWORD-hp

   导出 OS_AUTH_URL=`http://10.106.43.15:35357/v2.0/`

   导出 OS_USERNAME=hp_user

© 1997–2026 Citrix Systems, Inc. All rights reserved.

导出 OS_TENANT_NAME=hp

导出 OS_IDENTITY_API_VERSION=2.0

导出 BARBICAN_ENDPOINT="`http://10.106.43.15:9311/`"

```
stack@ubuntu:/opt/stack/devstack$ export OS_PASSWORD=hp
stack@ubuntu:/opt/stack/devstack$ export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/
stack@ubuntu:/opt/stack/devstack$ export OS_USERNAME=hp_user
stack@ubuntu:/opt/stack/devstack$ export OS_TENANT_NAME=hp
stack@ubuntu:/opt/stack/devstack$ export OS_IDENTITY_API_VERSION=2.0
stack@ubuntu:/opt/stack/devstack$ export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"
stack@ubuntu:/opt/stack/devstack$
```

注意

在运行其他命令之前，为每个 SSH 会话设置这些变量。有关 OpenStack 环境变量的更多信息，请参阅 OpenStack 环境变量。

5. 使用以下命令创建负载均衡器：

```
neutron lbaas-loadbalancer-create --name <loadbalancer-name>  <subnet-name> --provider <netscaler>
```

示例:

```
neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler
```

创建负载均衡器(/en-us/netscaler-application-delivery-management-software/media/neutron-lbaas-lb-create.png)

负载均衡器成功创建后，状态从 PENDING_CREATE 变为 ACTIVE。

负载均衡器状态变更(/en-us/netscaler-application-delivery-management-software/media/neutron-lbaas-lb-create-status.png)

6. 使用以下命令创建侦听器：

```
neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol_type> --protocol-port <port_number> --default-tls-container-id<container_url>
```

示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
neutron lbaas-listener-create --name hp-lb-test-list  --loadbalancer
hp-lb-test --protocol TERMINATED_HTTPS --protocol-port 443 --default-
tls-container-id `http://10.106.43.15:9311/v1/containers/d688676f-
c256-4a0d-b84d-a310419dc0aa`
```

注意

如果您要创建不支持 SSL 卸载的侦听器，请运行以下命令，而无需向容器提供位置：

`neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol_type> --protocol-port <port_number>`

创建不支持 SSL 卸载的侦听器(/en-us/netscaler-application-delivery-management-software/media/neutron-lbaas-listener-create.png)

7. 使用以下命令创建池：

```
neutron lbaas-pool-create --lb-algorithm <algorithm_type> --listener
<listener-name> --protocol <protocol_type> --name <pool-name>
```

示例：

```
neutron lbaas-pool-create --lb-algorithm LEAST_CONNECTIONS --listener
demolistener --protocol http --name demopool
```

创建池(/en-us/netscaler-application-delivery-management-software/media/neutron-lbaas-pool-create.png)

8. 使用以下命令创建成员：

```
neutron lbaas-member-create  --subnet <subnet-name> --address <ip-
address of the web server> --protocol-port <port_number>  <pool-name>
```

示例：

```
neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --
protocol-port 80 hp-lb-test-pool
```

创建成员(/en-us/netscaler-application-delivery-management-software/media/neutron-lbaas-member-create.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 NetScaler Console 中监控 OpenStack 应用程序

您的租户可以使用其 OpenStack 凭据登录到 NetScaler Console，以便从任何浏览器监控从 OpenStack 创建的 VIP 和池。URL 必须采用以下格式：

`http://<mas_ip>/<admin_ui>/mas/ent/html/cc_tenant_main.html`

其中，`mas-ip-address` 是在 OpenStack 中注册的 NetScaler Console IP 地址。

注意

- OpenStack VIP 对应于 NetScaler Console 中的虚拟服务器。
- OpenStack 池对应于 NetScaler Console 中的服务组。
- OpenStack 池成员对应于 NetScaler Console 中的服务组成员。

配置七层内容切换

NetScaler Console 与 OpenStack 协同工作，以在 NetScaler 实例上配置七层 (L7) 交换或基于内容的交换功能。内容交换与简单的负载均衡不同，它能够将特定类型的请求定向到特定服务器。当在 OpenStack 中以 NetScaler 实例作为提供者创建 L7 配置时，NetScaler Console 会分配一个 NetScaler 实例，并部署与 L7 配置相对应的内容交换和响应器配置。然后，NetScaler 实例可以根据请求的应用层特性分发和负载均衡用户请求。

OpenStack 七层 (L7) 负载均衡功能结合了负载均衡和内容交换，以提供特定类型内容的优化交付。这通过仅运行适用于内容的策略来提高负载均衡器的性能。七层负载均衡还有助于提高应用程序基础设施的效率。根据类型、URI 或数据分离内容的能力，可以更好地分配应用程序基础设施中的物理资源。例如，浏览到 `http://example-sports.com/about-us` 的最终用户由托管公司和服务的相关内容的服务器池提供服务，而浏览到 `http://example-sports.com/shopping-cart-football` 的用户则由另一个服务器池提供服务，该服务器池允许用户进行在线购买。

在 L7 交换中，负载均衡器作为内容交换虚拟服务器实现，接收来自用户的 HTTP 请求并将这些请求分发到应用程序服务器。L7 交换或内容交换允许您拥有一个单点入口来访问各种后端服务（例如，不仅是 Web 应用程序、Web 服务门户、Web 邮件，还包括移动管理、不同语言的内容等）。也就是说，您可以为向用户提供的所有服务提供一个公共 IP 地址。

与低层负载均衡不同，七层交换不要求池中的所有服务器都具有相同的内容。使用 L7 交换的负载均衡器配置期望来自不同池的应用程序或后端服务器具有不同的内容。L7 交换机可以根据 URI、主机、HTTP 标头或应用程序消息中的任何其他内容来定向请求。应用程序服务器本质上是提供特定类型的内容。例如，一个服务器只能提供图像，另一个可能运行服务器端脚本语言，如 PHP 和 ASP，而另一个可以提供静态内容，如 HTML、CSS 和 JavaScript。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L7 规则

以下属性在规则中定义，用于评估流量，并与规则中定义的值进行比较：

- 主机名：HTTP 请求中的主机名与规则中的值参数进行比较。例如，“www.example-sports.com.”
- 路径：HTTP URI 的路径部分与规则中的值参数进行比较。例如，“www.example-sports.com/shopping-cart/football_pump.html”
- 文件_类型: URI 的最后一部分与规则中的值参数进行比较。例如，txt、html、jpg、PNG、xls 等。
- 标头：键参数中定义的标头与规则中的值参数进行比较。
- Cookie：键参数命名的 Cookie 与规则中的值参数进行比较。Cookie 请求头字段值包含为该 URL 存储的名称和值对信息；一般语法如下 - Cookie: name=value。例如，查找名为“stores”且值以“football-”开头的 Cookie 的规则将如下所示：type = Cookie, compare_type=StartsWith, key = stores value = football-。

比较类型

在评估流量时，L7 策略会将以下表达式与规则中定义的属性进行比较。

- 正则表达式：Perl 类型正则表达式匹配
- starts_with: 字符串开头是
- ends_with: 字符串结尾是
- contains: 字符串包含
- equal_to: 字符串等于

注意

主机名、路径、标头和 Cookie 属性支持所有比较类型，但 file_type 属性仅支持正则表达式和 equal_to。

L7 策略

L7 策略处理传入的 HTTP 流量，并在策略中定义的所有规则都匹配时返回“true”值。

在任何 L7 策略中，所有规则都通过 AND 运算符逻辑连接。请求必须匹配所有规则，策略才能返回“true”值。负载均衡器采取的操作基于策略返回的值。您可以创建具有相同操作的第二个策略，以在规则之间实现逻辑 OR 操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

例如，您可以创建一个策略，其中传入的 HTTP 请求可以包含“EXAMPLE-SPORTS”、“SPORTS-FOOTBALL”或“EXAMPLE-FOOTBALL”等词，以便负载均衡器采取适当的操作，将这些请求转发到 Example-sports 电子商务公司的服务器池以提供请求的内容。您可以创建另一个策略，该策略执行相同的操作，但匹配“example-sports”、“example-sports-football”或“example-football”。当用户发送包含这六个关键字中任何一个的 HTTP 请求时，负载均衡器会将请求转发到 Example-Sports 服务器。

根据策略中定义的规则，L7 策略可以执行以下任何操作：

- 重定向到池 - 将请求转发到由与 L7 策略关联的规则标识的应用程序服务器池。也就是说，您可以创建应用程序规则，根据域名将请求定向到特定的负载均衡器池。例如，您可以创建一个规则，将一些请求定向到 example-football.com 到 pool_1，将其他请求定向到 example-sports-online_purchase.com 到 pool_2。
- 重定向到 URL - 向客户端发送重定向 HTTP 响应，其中位置响应标头包含新位置。浏览器将使用新位置更新地址栏并发出新请求。用例很多。例如，如果网站地址已更改，您可以将请求重定向到新地址而不是丢弃。或者，在网站维护期间，您可以将用户重定向到只读站点。
- 拒绝 - 拒绝请求，不采取进一步行动。例如，您可以返回 401 未授权响应，以拒绝用户访问受限网页。

内容切换配置包括内容切换虚拟服务器、由负载均衡虚拟服务器和服务组成的负载均衡设置以及内容切换策略。创建内容切换虚拟服务器和策略后，将每个策略绑定到内容切换虚拟服务器。将策略绑定到内容切换虚拟服务器时，需要指定目标负载均衡虚拟服务器。当请求到达内容切换虚拟服务器时，虚拟服务器会将关联的内容切换策略应用于该请求。策略的优先级定义了绑定到内容切换虚拟服务器的策略的评估顺序。

任何具有侦听器 ID 的池都可以被指定为虚拟服务器的默认池，流量将重定向到该池。池与侦听器松散绑定，并且仅通过实施 L7 策略才能与侦听器关联。池也可以直接在负载均衡器下创建，而不必与侦听器绑定。在这种情况下，池将以“pending_create”状态创建。由于 L7 策略与侦听器紧密绑定，因此必须创建并实施包含池 ID 的 L7 策略，才能使池变为“active”状态并开始接收流量请求。

一个池可以由多个 L7 策略提供服务，但如果至少有一个策略附加到它，它将保持“active”状态。当最后一个策略被移除时，池将返回到“pending_create”状态，直到创建并关联另一个策略。如果池本身被移除，所有它本应接收到的 HTTP 请求都将被重定向到默认池。

OPENSTACK L7 策略与 NETSCALER 实体之间的映射

OpenStack	NetScaler 实体	描述

© 1997–2026 Citrix Systems, Inc. All rights reserved.

具有 REDIRECT_TO_POOL 操作的 L7 策略	内容切换策略 > 内容切换操作	NetScaler Console 创建一个内容切换策略，该策略绑定到内容切换虚拟服务器，并与一个内容切换操作相关联，该操作指定用于内容检索和向用户呈现的应用程序服务器目标池。
具有 REDIRECT_TO_URL 操作的 L7 策略	响应器策略 > 响应器操作	NetScaler Console 创建一个响应器策略，该策略绑定到内容切换虚拟服务器，并与一个响应器操作相关联，该操作指定要呈现给用户的目标 URL。
具有 REJECT 操作的 L7 策略	响应器策略 > 丢弃请求	NetScaler Console 创建一个响应器策略，该策略绑定到内容切换虚拟服务器，并与一个丢弃请求的响应器操作相关联。

如果 L7 策略的操作评估为“true”并将流量重定向到处于“create_pending”状态的池，NetScaler Console 将实现指定的池以及负载均衡虚拟服务器。NetScaler Console 从 L7 策略创建内容切换策略，并使用相应的内容切换操作将请求重定向到与该池关联的负载均衡虚拟服务器。如果第二个 L7 策略重定向到同一个池，NetScaler Console 将创建内容切换策略和内容切换操作，以将流量重定向到与该池关联的现有负载均衡虚拟服务器。

策略定位

OpenStack 中 L7 策略的评估由其优先级决定。在 OpenStack 中，默认情况下，策略按照创建顺序分配优先级。首先创建的策略编号为“1”，随后创建的策略按顺序编号。但您可以更改策略的优先级并为其分配不同的优先级。策略始终按照其优先级的顺序进行评估。第一个匹配特定请求的策略总是最先运行。

创建策略时，请注意以下几点：

- 如果您为新策略分配与现有策略相同的优先级，则新策略将获得该优先级。现有策略的优先级会降低。如有必要，其他策略的优先级也会降低，以保持策略的评估顺序。
- 如果您创建新策略时未指定位置，则新策略将直接附加到列表中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 如果您创建新策略并为其分配一个大于列表中现有策略数量的位置，则新策略将附加到列表末尾，也就是说，新策略总是获得下一个可用的优先级。例如，如果存在优先级分别为 1、2 和 3 的三个策略 A、B 和 C，并且您创建了一个策略并为其分配优先级 8，则新策略的优先级将变为 4。
- 如果您向列表中添加策略或从列表中删除策略，策略位置值将从 1 开始重新排序，不跳过任何数字。例如，如果策略 A、B、C 和 D 的位置值分别为 1、2、3 和 4，并且您从列表中删除了策略 B，则策略 C 现在将占据第二个位置，策略 D 将占据第三个位置。

在 NetScaler Console 中，始终存在一个与 `csvserver` 关联的默认策略，其优先级为 1。此默认策略指定 `lbvserver` 在任何给定时间处理的 TCP 连接数。因此，当在 NetScaler 中创建相应的响应器策略和内容切换策略时，它们的优先级总是比相应的 L7 策略的优先级高 1。例如，当评估优先级为 1 的 L7 策略时，会创建一个优先级为 2 的内容切换策略。同样，当评估优先级为 2 的 L7 策略时，会创建一个优先级为 3 的响应器策略。

在 OpenStack 中，首先评估“reject”或“redirect_to_url”策略，然后评估“redirect_to_pool”策略。在 NetScaler 实例中，响应器策略总是最先评估，以丢弃请求或向用户呈现重定向的网址，而内容切换策略最后评估。如果内容切换策略和响应器策略是互斥的，这种评估顺序通常不会引起任何冲突。也就是说，两个 L7 策略不能具有相同的表达式。在响应器和内容切换策略中添加派生表达式以避免此类冲突。例如，编写一个表达式来拒绝所有对“sports-football.com”的请求，并编写另一个表达式来允许对“example-sports-football.com”的请求。创建 L7 策略时，应将所有拒绝请求的响应器策略排在评估列表的顶部，然后是用于 Web 直接的响应器策略，最后是内容切换策略。

在 NetScaler Console 中，始终存在一个与 `csvserver` 关联的默认策略，其优先级为 1。此默认策略指定 `lbvserver` 在任何给定时间处理的 TCP 连接数。因此，当在 NetScaler 中创建相应的响应器策略和内容切换策略时，它们的优先级总是比相应的 L7 策略的优先级高 1。例如，当评估优先级为 1 的 L7 策略时，会创建一个优先级为 2 的内容切换策略。同样，当评估优先级为 2 的 L7 策略时，会创建一个优先级为 3 的响应器策略。

在 OpenStack 中，首先评估“reject”或“redirect_to_url”策略，然后评估“redirect_to_pool”策略。在 NetScaler 中，响应器策略总是最先评估，以丢弃请求或向用户呈现重定向的网址，而内容切换策略最后评估。如果内容切换策略和响应器策略是互斥的，这种评估顺序通常不会引起任何冲突。也就是说，没有两个 L7 策略具有相似的表达式。在响应器和内容切换策略中添加相似的派生表达式以避免此类冲突。例如，编写一个表达式来拒绝所有对“sports-football.com”的请求，并编写另一个表达式来允许对“example-sports-football.com”的请求。创建 L7 策略时，应将所有拒绝请求的响应器策略排在评估列表的顶部，然后是用于 Web 直接的响应器策略，最后是内容切换策略。

配置任务

L7 策略和操作的实现通过 Neutron LBaaS 命令执行。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 OpenStack 中设置环境变量并创建负载均衡器（例如，LB1）。成功创建负载均衡器后，创建侦听器和池（例如，L1、P1 和 P2），并向池中添加成员和监视器。例如，P1 是 L1 的默认池，而 P2 是与 LB1 绑定并管理应用服务器的池。

有关如何使用命令行配置 LBaaS V2 的更多信息，请参阅 使用命令行配置 LBaaS V2。

以下命令创建策略并定义特定操作：
创建用于丢弃请求的 L7 策略

```
neutron lbaas-l7policy-create --name &lt;L7 policy name> --listener
&lt;listener name> --action&lt;action-name>
```

示例：

neutron lbaas-l7policy-create --name policy11 --action REJECT --listener L1

上述命令创建并将 policy11（一个响应器策略）绑定到内容交换服务器以拒绝请求。由于未为此策略创建任何规则，因此该策略评估为“false”，并且请求被拒绝。
创建用于将请求重定向到特定 URL 的 L7 策略

```
neutron lbaas-l7policy-create --name &lt;L7 policy name> --listener
&lt;listener name> --action &lt;action-name> --redirect-url &lt;redirect-
url>
```

示例：

neutron lbaas-l7policy-create --name policy12 --action REDIRECT_TO_URL --listener admin-list1 --redirect-url `http://example-sports/about-us.html`

上述命令创建一个响应器操作以将请求重定向到 URL，创建一个带操作的响应器策略，并将此策略绑定到内容交换虚拟服务器。

```
neutron lbaas-l7rule-create --type HOST_NAME --compare-type CONTAINS --
value &lt;value-string> &lt;L7 policy name>



neutron lbaas-l7rule-create --type PATH --compare-type CONTAINS --value
&lt;value-string> &lt;L7 policy name>
```

上述两条规则可以通过 AND 运算符连接起来，以导出响应器策略的表达式。
创建用于将请求重定向到池的 L7 策略

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
neutron lbaas-l7policy-create --name &lt;L7 policy name> --listener
&lt;listener name> --action &lt;action-name> --redirect-pool &lt;redirect-
pool>
```

示例：

neutron lbaas-l7policy-create --名称 policy13 --操作 REDIRECT_TO_POOL --监听器 admin-list1 --重定向池 admin-pool2

如果这是第一个 L7 策略，则上述命令将 P2 与 LB1 一起实施，创建内容交换重定向操作并将请求重定向到 LB1。如果 P2 已存在，则该命令创建内容交换重定向操作并将请求重定向到 LB1。

在 OpenStack 上手动预配 NetScaler VPX 实例

在一些企业网络中，出于安全原因，NetScaler VPX 实例无法连接到 NetScaler 许可证服务器以自动下载许可证。在这种情况下，您需要在 OpenStack 平台上手动部署 NetScaler VPX 实例。使用您从 Citrix 收到的许可证访问代码，下载相应的 NetScaler VPX 许可证并将其保存到您的本地系统。

在 OpenStack 上手动预配 NetScaler VPX 实例：

1. 在 OpenStack 上安装 NetScaler 驱动程序软件并注册 NetScaler Console
   a. 在 NetScaler Console 中，导航到 **编排** \> **云编排** \> **OpenStack**。
   b. 单击**配置 OpenStack 设置**。在**配置 OpenStack 设置**页面中，您可以设置参数以在 NetScaler Console 中配置 OpenStack。您有两个选项：**默认**和**自定义**。
   c. 如果 OpenStack 服务在默认端口上运行，请选择**默认**。
2. 导航到 **Orchestration** \> **Cloud Orchestration** \> **OpenStack**，然后单击**部署设置**。
   a. **管理网络** - 选择 OpenStack 上的管理网络，自动预配的 NetScaler VPX 将连接到该网络。
   b. **配置文件名称** - 从下拉列表中选择配置文件。NetScaler Console 使用此配置文件中包含的密码来配置新的自动预配 NetScaler VPX 实例。
   c. Glance 中的 NetScaler VPX 映像 - 选择 OpenStack Glance 中可用的 NetScaler VPX 映像，用于创建 NetScaler VPX 实例。下拉列表将仅显示 OpenStack Glance 中存在的映像。
3. 在 NetScaler Console 中，导航到 **Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Service Packages**，然后单击**添加**。
4. 在**服务包**页面上指定以下参数：
   a. **名称** - 服务包的名称。例如，输入 SVC-PKG-GOLD。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **NetScaler 实例分配** - 选择**专用**或**分区**作为服务包中定义的实例分配类型。

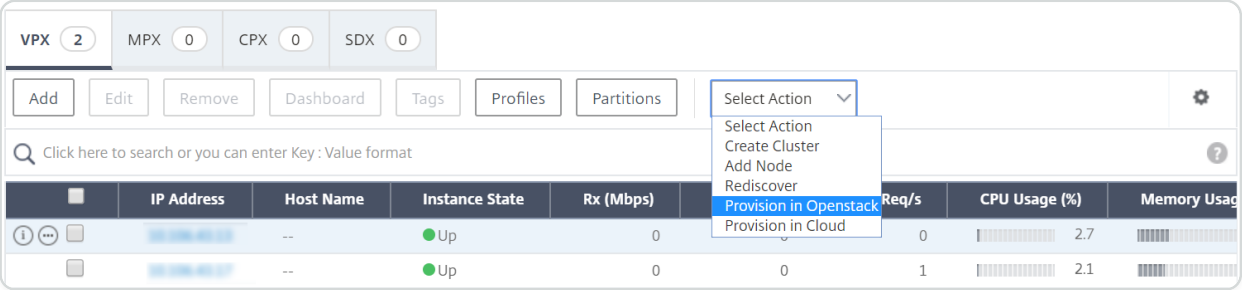
c. **NetScaler 实例预配** - 选择 **按需创建实例** 以便在配置过程中创建 NetScaler 实例。

d. **自动预配平台** - 选择 **OpenStack Compute**。默认情况下，NetScaler VPX 将被选为实例类型。

e. **分配 OpenStack 租户/放置策略** 部分，在 OpenStack 租户下，单击 **添加**，然后选择租户。

f. 单击 **继续**，然后单击 **完成**。

5. 导航到 **系统** \> **系统管理** \> **更改系统设置** 并从下拉列表中选择 **http**。
6. 导航到 **基础架构 > 实例 > NetScaler VPX**。
7. 在 **NetScaler VPX** 页面中，单击 **管理员** 下拉列表并选择 **预配设备**。

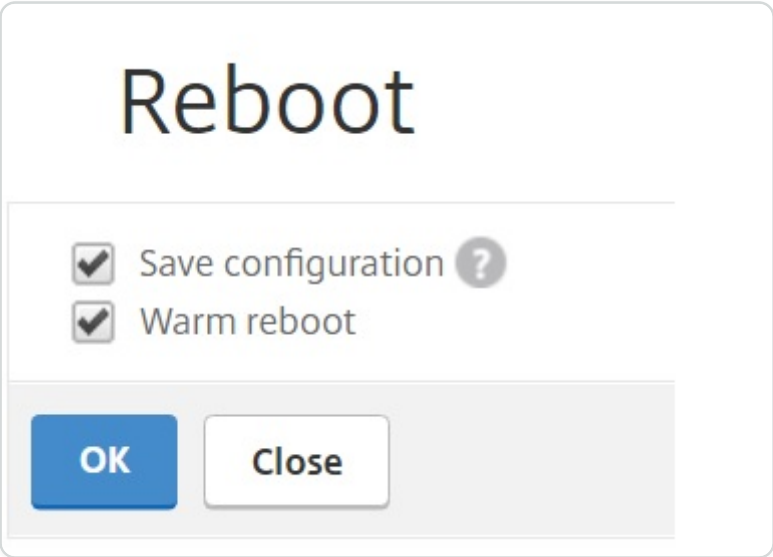


a. 在 **设备预配** 页面上，输入设备的名称，并选择您在上一步中创建的服务包。

b. 单击 **确定**。

8. 导航到 **编排** \> **云编排** \> **OpenStack** \> **请求** 选项卡。选择请求并单击 **任务** 以查看任务。当任务状态变为 **已完成** 时，表示 NetScaler VPX 已在 NetScaler Console 中预配。
9. 导航到 **基础架构 > 实例** \> **NetScaler VPX** 以检查 NetScaler VPX 实例是否显示在 NetScaler VPX 页面中。
10. 单击 NetScaler VPX 实例。当 NetScaler VPX 实例在浏览器窗口中打开时，登录到该实例。导航到 **配置** \> **系统** \> **许可证**，然后手动添加新许可证。有关如何添加新许可证的更多信息，请参阅 NetScaler 许可概述。
11. 重新启动 NetScaler VPX 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



12. 几分钟后，您可以登录 OpenStack 并在 **System** \> **Instances** 中，您可以看到 NetScaler VPX 实例已部署在 OpenStack 上。
13. LBaaS V2 API 实现通过 Neutron LBaaS 命令执行。连接到任何 Neutron 客户端并运行配置任务。有关如何运行配置命令的更多信息，请参阅 使用命令行配置 LBaaS V2。

使用 StyleBook 在 OpenStack 上预置 NetScaler VPX 实例

在 OpenStack 编排工作流中，NetScaler Console 现在使用 `os-cs-lb-mon` StyleBook 在分配给 OpenStack 租户的 NetScaler 实例上部署 LBaaS 配置。OpenStack 用户创建的每个负载均衡器都会创建一个配置包。

在 OpenStack 工作流中使用 StyleBook 进行配置可提供以下优势：

- 通过查看所有配置对象获得更好的可视化效果。
- 通过回滚实现可靠性。
- 支持各种 NetScaler 实例类型（NetScaler HA、分区、VPX、CPX、MPX 等）。
- 通过使用您自己的 StyleBook 为 OpenStack 租户部署配置来实现自定义。

作为 NetScaler Console 管理员，导航到 **应用程序** > **配置** 以查看部署在 NetScaler 实例上的配置包。 您可以执行以下任务：

- 滚动以查看为负载均衡器部署的 `os-cs-lb-mon` 配置包。
- 单击 `os-cs-lb-mon` StyleBook 面板上的 **查看定义** 以检查部署在实例上的配置。
- 单击 **查看对象** 以查看部署在实例上的 NetScaler 对象或实体列表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 StyleBook 预置实例前需要注意的事项

从 NetScaler Console 12.1 build 49.23 开始，OpenStack 编排工作流的架构已更新。该工作流现在使用 NetScaler Console StyleBook 来配置 NetScaler 实例。如果您从 12.0 版或 12.1 build 48.18 版升级到 NetScaler Console 12.1 build 49.23，则必须运行以下迁移脚本：

```
/mps/scripts/migration_scripts/migrate_configurations.py
```

- 运行迁移脚本会创建与现有 OpenStack 配置对应的 `os-cs-lb-mon` StyleBook 配置包。
- 如果您从这些早期版本部署了 OpenStack 配置，则必须运行此迁移脚本。
- 只有在运行了版本 12.1 build 49.23 的迁移脚本之后，您才能使用 `os-cs-lb-mon` StyleBook 在实例上部署新配置。
- 在运行迁移脚本之前，所有从 OpenStack 尝试的配置都将失败。

注意

- 运行迁移脚本后，您无法降级到 NetScaler Console 的先前版本。
- 确保您已将 OpenStack LBaaS V2 的 NetScaler 驱动程序升级到最新版本。使用随最新 NetScaler Console 13.0 版本提供的 NetScaler 捆绑文件。

LBaaS V2 API 实现通过 Neutron LBaaS 命令执行。连接到任何 Neutron 客户端并运行配置任务。有关如何运行配置命令的更多信息，请参阅使用命令行配置 LBaaS V2。

OpenStack 环境的 VPX 签入和签出许可证以及池化许可证支持

在 OpenStack 编排工作流中，当您选择包含 **OpenStack Compute** 的服务包时，NetScaler Console 会按需创建 NetScaler VPX 实例。现在，NetScaler Console 中编排功能的服务包页面已得到增强，以提供按需创建的 NetScaler VPX 实例所需的许可证。提供的许可证可以是 VPX 签入和签出许可证或池化许可证。

要使用此功能，您必须首先将许可证上传到 NetScaler Console，然后创建使用 OpenStack 计算的服务包。

- 如果是签入和签出许可证，那么您可以从各种可用许可证中选择要安装的许可证。

  服务包签入和签出许可证(/en-us/netscaler-application-delivery-management-software/media/orchestration-openstack-vpx-pooled-licenses-1.jpg)

- 如果是池化许可证，那么您可以选择要安装的带宽和许可证版本类型。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

服务包池化许可证(/en-us/netscaler-application-delivery-management-software/media/orchestration-openstack-vpx-pooled-licenses-2.jpg)

每当您使用 NetScaler Console 作为提供程序部署第一个负载均衡器时，NetScaler Console 会创建 NetScaler VPX 实例，并将服务包中指定的许可证安装到新创建的实例。

此外，当您删除现有负载均衡实例时，该实例将不再需要。该实例将被停用，并且许可证将返回到 NetScaler Console。这有助于优化利用 NetScaler Console 中可用的许可证。

注意

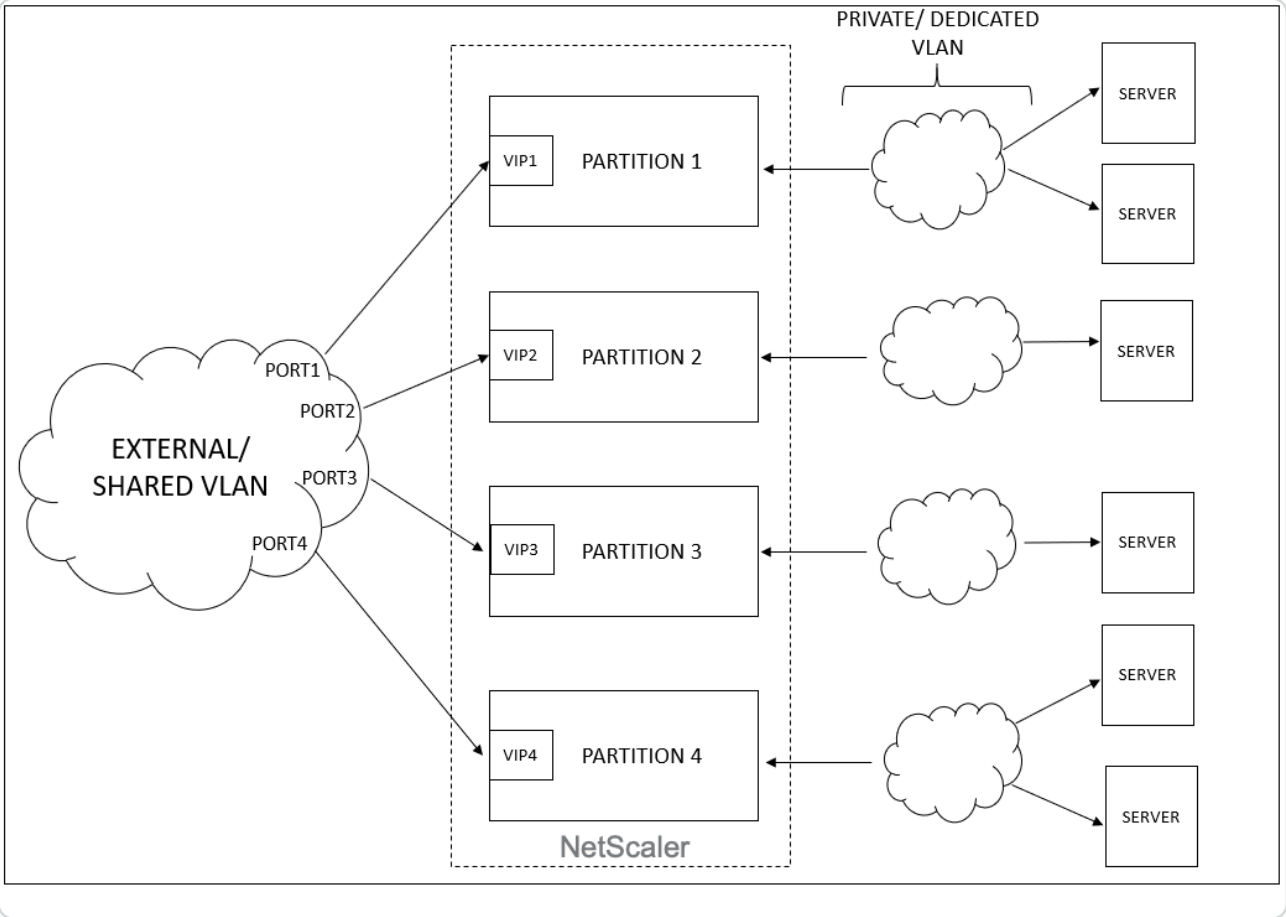
当 NetScaler Console 以高可用性模式部署时，请考虑将许可证上传到当前活动或主 NetScaler Console (MAS-HA-1)。当您部署第一个请求并且 NetScaler Console 创建 NetScaler VPX 实例时，该实例会从 MAS-HA-1 签出所需的许可证。在稍后的时间点，假设没有许可证的辅助 NetScaler Console (MAS-HA-2) 现在处于活动状态。NetScaler VPX 实例现在无法从 MAS-HA-2 签出许可证，因此无法为新用户创建实例。

在这种情况下，请确保 MAS-HA-1 处于 UP 状态并且是当前主节点。也就是说，手动将 NetScaler Console 从 MAS-HA-2 故障转移到 MAS-HA-1。此后，您必须从 OpenStack 重新尝试配置，并且实例将使用正确的许可证重新创建。有关 NetScaler Console 高可用性部署中许可证支持的更多信息，请参阅 高可用性。

管理员分区共享 VLAN 支持

对于从私有网络连接的租户，NetScaler Console 支持隔离策略，以便每个租户都有自己的专用分区、专用 VLAN 和专用服务器。对于从公共网络连接的租户，专用 VLAN 将需要使用过多的 IP 地址。共享 VLAN 通过在每个分区上创建一个虚拟 IP 地址来规避此问题，从而创建一个单一的 IP 子网。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



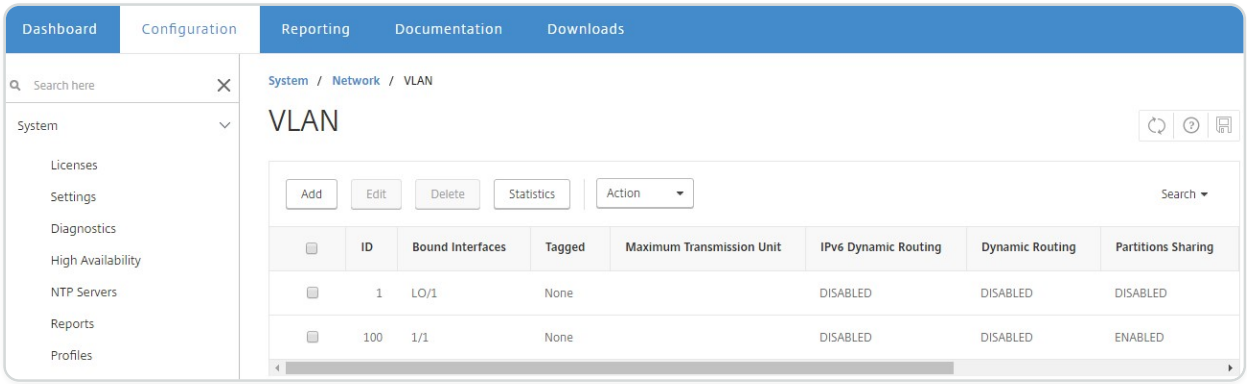
当租户配置 VIP 或侦听器时，会在 NetScaler 设备中为该租户创建一个管理员分区。所有负载均衡器配置都会推送到已创建的管理员分区。如果租户使用共享网络或外部网络创建负载均衡器，则会添加该网络的 VLAN 并启用共享功能。当不同的租户使用相同的共享网络创建其负载均衡器时，VLAN 不会再次添加到 NetScaler，但 VLAN 也会绑定到第二个分区。因此，任何使用相同共享网络的租户都会获得一个绑定到相同 VLAN 的分区。

NetScaler Console 支持虚拟目标 MAC 地址。当租户共享 VLAN 时，NetScaler Console 会为 NetScaler 设备上的分区分配不同的 MAC 地址。这允许 VLAN 跨分区或跨所有租户和所有流量域共享。

从 NetScaler 实例配置共享 VLAN

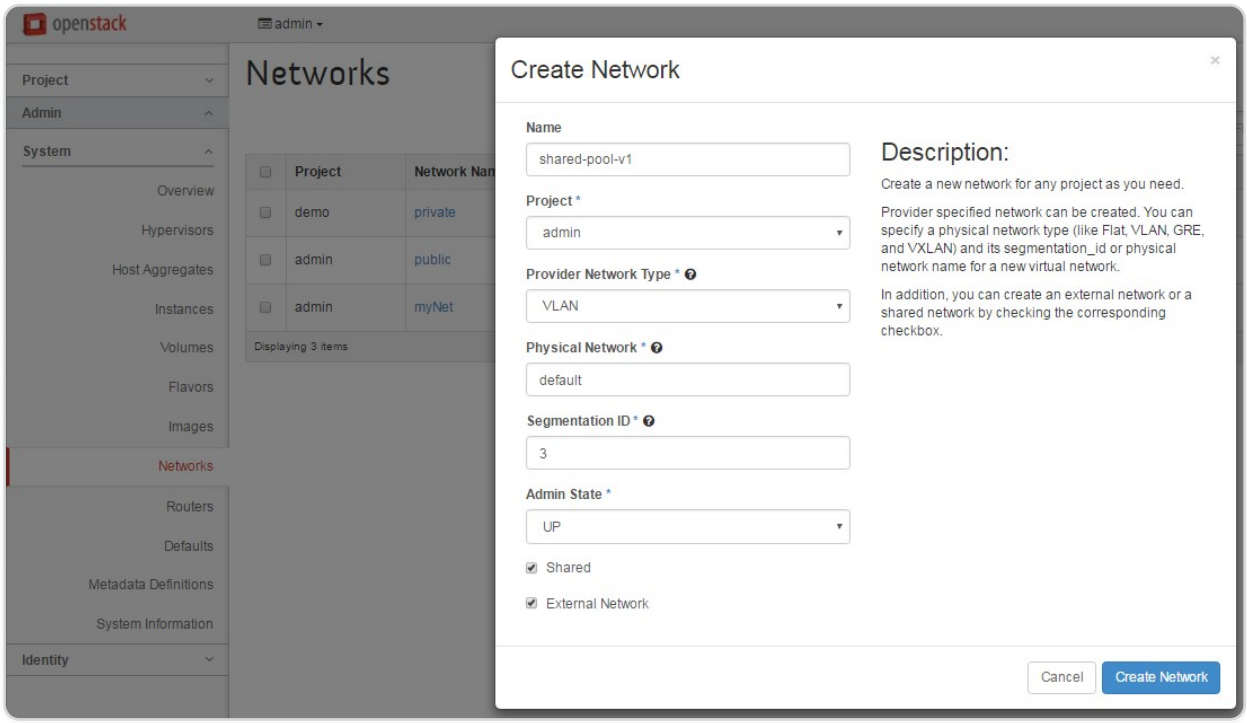
1. 在 NetScaler 实例中，导航到 **Configuration** \> **System** \> **Network** \> **VLANs**，选择一个 VLAN 配置文件，然后单击 **Edit** 以设置分区共享参数。
2. 在 **Configure VLAN** 页面上，选中 **Partitions Sharing** 复选框。
3. 单击 **OK**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



从 OpenStack 编排配置共享 VLAN

1. 在 OpenStack 中，导航到 **Admin** \> **System** \> **Networks**，然后单击 **Create Network**。
2. 在 **Create Network** 中，设置以下参数：
   a. Name - 输入网络名称
   b. Project - 从下拉列表中选择一个项目
   c. 提供商网络类型 - 从下拉列表中选择 **VLAN**。这表示虚拟网络已建立为 VLAN。
   d. 物理网络 - 此处已选择默认物理网络。您可以编辑此项。
   e. 管理状态 - 默认情况下，网络的管理状态为 UP
   f. 选择 **共享** 和 **外部** 网络以定义 VLAN 是共享的并正在使用外部网络。
3. 单击 **创建网络**。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

试用许可工作流程

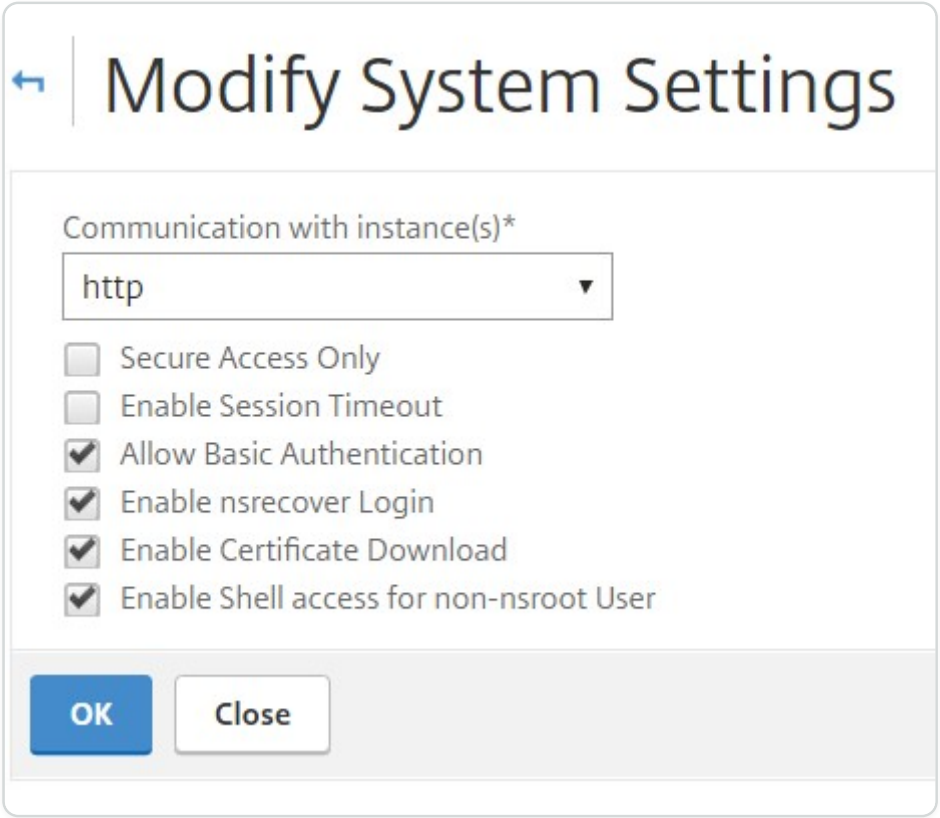
在使用 OpenStack 编排自动预配 NetScaler VPX 实例期间，NetScaler Console 使用 OpenStack Compute 启动 NetScaler VPX 实例。新预配的 NetScaler VPX 实例在设置过程中会联系 Citrix 许可门户，并使用许可证访问代码自动下载并安装许可证文件。

试用许可证

技术支持人员在现场安装 NetScaler Console 和 NetScaler VPX 设备时使用试用许可证。NetScaler VPX 的试用或评估许可证有效期为 90 天。如果需要评估多个 NetScaler 或在 90 天后延长测试，则需要申请新的评估许可证。NetScaler Console 为您提供了一种替代解决方案，而不是自动安装试用许可证文件。您可以手动下载许可证文件并将其安装到 NetScaler VPX 上，以完成实例的安装。

如果 NetScaler VPX 无法连接到互联网，请将 NetScaler Console 配置为 Citrix 许可门户的代理服务器并安装许可证文件。

具有试用许可证的 NetScaler VPX 实例只能通过 HTTP 与 NetScaler Console 通信。要在 NetScaler Console 中配置 HTTP 通信，请导航到 **System** \> **System Administration**，然后单击 **Change System Settings**。从下拉列表中选择 **http** 以设置通信方法，然后单击 **OK**。



与 OpenStack Heat 服务集成

OpenStack Neutron LBaaS 为应用程序提供核心负载平衡服务，例如负载平衡、SSL 卸载和内容切换。LBaaS 通过 REST API 进行管理，该 API 允许租户发出 REST 调用来创建、更新和删除

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LBaaS 对象。由于 LBaaS 提供负载平衡服务，因此在编排过程中不允许使用更高级的 NetScaler 功能。NetScaler Heat 插件克服了这一限制。

Heat 编排服务

OpenStack Heat 编排服务允许基于模板部署复杂的云应用程序。Heat 编排模板 (HOT) 以人类可读写且可通过版本控制工具管理的文本文件形式描述云应用程序的基础设施。YAML 是一种结构化语言，用于编写这些模板。HOT 模板允许您创建大多数 OpenStack 资源类型，并指定其中定义的资源之间的关系。NetScaler Heat 插件允许您在任何 NetScaler 实例上配置高级 NetScaler 功能。

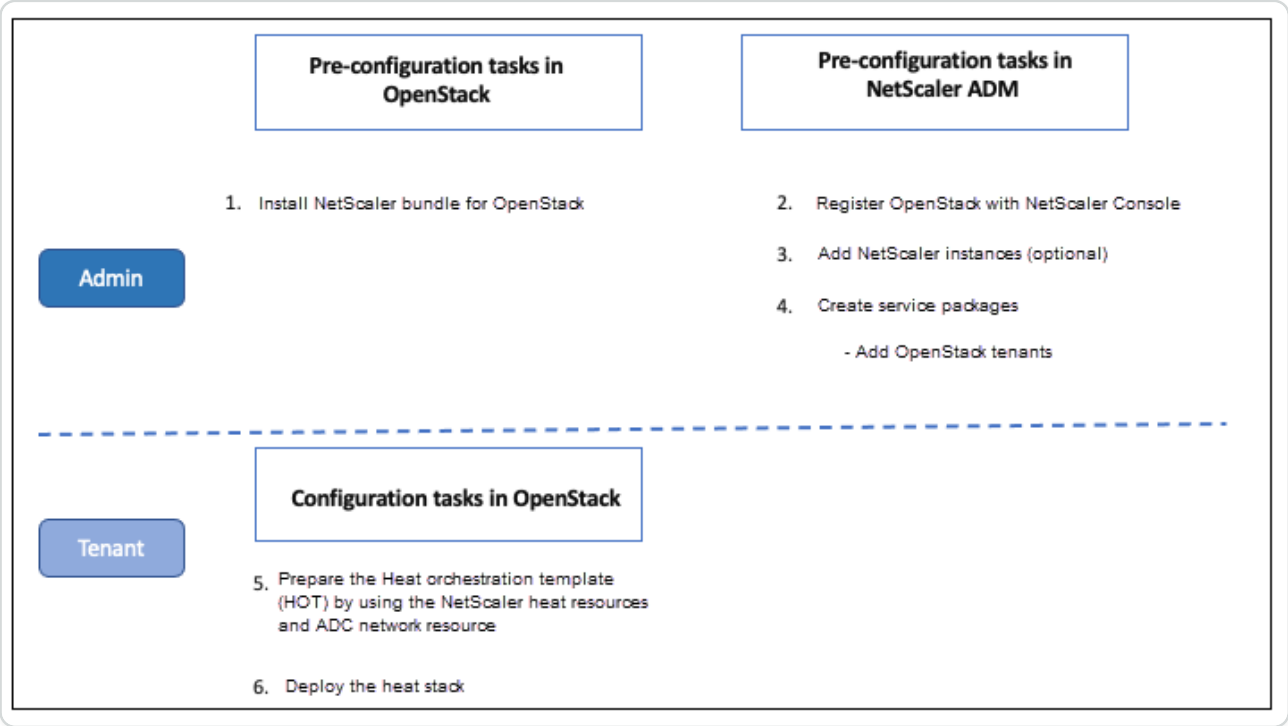
NetScaler StyleBooks

NetScaler Console StyleBooks 可用于创建和配置 NetScaler 功能。与 Heat 模板一样，StyleBooks 也采用 YAML 编写。可以为每个功能创建单独的 StyleBooks，并且可以使用单个 StyleBooks 在多个 NetScaler 实例上部署配置。

在 NetScaler 与 OpenStack 集成期间，NetScaler Console 会将所有 NetScaler Console StyleBooks 作为资源发布到 Heat 服务中。这包括 NetScaler Console 随附的 StyleBooks 以及用户稍后创建的 StyleBooks。Heat 模板允许您使用这些 StyleBooks 资源配置 NetScaler 的高级功能。

使用 Heat 配置 NetScaler 实例的工作流程

以下流程图说明了部署 Heat 堆栈的工作流程：



作为云管理员，执行以下任务：

在 OpenStack 中配置 Heat 服务：

1. 下载适用于 OpenStack 的 NetScaler 捆绑包

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 OpenStack 中安装 NetScaler 捆绑包。在 NetScaler Console 中，导航到 **Downloads** 并下载 NetScaler 驱动程序捆绑包，解压捆绑包，然后将捆绑包中 Heat 文件夹的内容复制到 OpenStack 中的 Heat 引擎资源目录。目录路径如下： /opt/stack/heat/heat/engine/resources/netscaler_resources

2. 在 heat.conf 文件中创建“netscaler_plugin”部分，并更新该部分中的以下参数：

   a. 当通信方式为 HTTP 时，参数更新如下：

   NMAS_BASE_URI=< `http://10.146.103.45:80` >

   NMAS_USERNAME=<openstack_driver_username>

   NMAS_PASSWORD=<openstack_driver_password>

   b. 当通信方式为 HTTPS 时，参数更新如下：

   NMAS_BASE_URI= `https://common_name_used_in_certificate`

   NMAS_USERNAME=\<openstack_driver_username

   NMAS_PASSWORD=\<openstack_driver_password\>

   SSL_CERT_VERIFY=\<True_or_False\>

   CERT_FILE_PATH=\<path_of_the_certificate_file\>

   如果用户将 ssl_cert_verify 设置为“False”，NetScaler Console 会在请求调用中发送 verify=False，这将禁用 SSL 证书验证。如果 ssl_cert_verify 设置为“True”且 cert_file_path 条目存在，NetScaler Console 会在请求的 verify 参数中发送此路径，否则 NetScaler Console 会发送 verify=True。

   注意

   要在“高可用性”模式下部署 NetScaler Console，请更新 heat.conf 文件中的以下参数：

   NMAS_BASE_URI=\<前端虚拟服务器的IP地址\>

3. 重新启动 OpenStack 中的 Heat 服务。

   当您重新启动 OpenStack 中的 NetScaler Heat 服务时，所有已定义的 NetScaler Console StyleBook 都将作为资源导入到 Heat 中。此外，NetScaler 网络资源和证书资源也将作为 NetScaler Heat 资源导入到 OpenStack 中。

4. 将 NetScaler Console 注册到 OpenStack。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 在 NetScaler Console 中，导航到 **编排** \> **云编排** \> **OpenStack**，然后单击 **配置 OpenStack 设置**。

b. 在 **Configure OpenStack Settings** 页面中，您可以设置参数来配置 OpenStack。您有两个选项：Default 和 Customized。

c. 如果 OpenStack 服务在默认端口上运行，请选择 **Default**。输入以下参数：

   i. OpenStack 控制器 IP 地址

   ii. 管理员用户名

   iii. 密码

   iv. OpenStack 管理租户

   v. NetScaler 驱动程序和 Heat 密码

> **注意**
>
> 这是您在 heat.conf 文件中输入的相同密码 (NMAS_PASSWORD)。

5. 创建服务包并与您的租户定义 SLA。

   在 OpenStack 注册期间，NetScaler Console 中会为每个用户创建一个租户，租户信息由 LBaaS 驱动程序和 Heat 插件使用。Heat 插件使用此信息联系 NetScaler Console，将 StyleBook 作为 Heat 资源导入到 OpenStack 中。

> **注意**
>
> 有关在 NetScaler Console 和 OpenStack 中创建服务包和其他预配置任务的更多信息，请参阅 将 NetScaler Console 与 OpenStack 平台集成。

6. 请注意，NetScaler Console 中的所有相关 StyleBook 都已作为资源导入 OpenStack Heat。此外，请注意 NetScaler 网络资源和 NetScaler 证书资源已作为资源导入 OpenStack Heat。

> **注意**
>
> 目前，您只能使用 NetScaler Console 附带的 StyleBook。

   您的租户现在可以在 OpenStack 中创建 Heat 模板，输入所需的 Heat 参数值，并部署 Heat 堆栈。部署 Heat 堆栈后，配置将推送到 NetScaler Console，并配置所需的 NetScaler 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

准备 Heat 模板并启动 Heat 堆栈：

1. 在 OpenStack 中，租户可以使用 Heat 资源创建 Heat 编排模板 (HOT)。
2. 在 OpenStack Horizon 中，租户管理员可以导航到 **Project** \> **Orchestration** \> **Stacks** 以创建 Heat 模板并启动 Heat 堆栈。创建 HOT 的方法有两种：

   - **文件** - 从本地目录中选择更新的模板
   - **直接输入** - 从窗口中的模板复制并粘贴 YAML 内容

   > **注意**
   >
   > 成功部署堆栈后，租户可以使用“更改堆栈模板”来更新堆栈。但是，在创建堆栈时最初提供的子网信息和虚拟 IP 地址 (VIP) 无法修改。

   租户部署堆栈后，导航到 NetScaler Console 中的 **Orchestration** \> **Cloud Orchestration** \> **OpenStack** \> **Requests** 以查看任务列表。此外，导航到 NetScaler Console 中的 **Applications** \> **Configuration** 以查看 NetScaler 实例是否已成功配置为 StyleBook 配置包的形式。

NetScaler Console StyleBook 示例：

下图展示了 NetScaler Console StyleBooks 的构建示例，并简要解释了其组件。有关 NetScaler Console StyleBooks 以及如何使用随附 StyleBooks 的更多信息，请参阅 StyleBooks。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```yaml
name: lb-vserver
description: "This stylebook defines a load balancing virtual server configuration."
display-name: "Load Balancing Virtual Server (HTTP)"
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
    -
    name: name
    type: string
    required: true
    -
    name: ip
    type: ipaddress
    required: true
   -
    name: lb-alg
    type: string
    allowed-values:
      - ROUNDROBIN
      - LEASTCONNECTION
    default: ROUNDROBIN
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
        name: $parameters.name
        servicetype: HTTP
        ipv46: $parameters.ip
        port: 80
        lbmethod: $parameters.lb-alg
```

header

StyleBooks imported

parameters

components

Heat 模板示例：

下图显示了 YAML 中定义的 Heat 模板结构，并指向作为 Heat 资源导入的 StyleBooks 资源和 NetScaler 网络资源。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
heat_template_version: '2015-10-15'
parameter_groups:
- description: servers
  label: servers
  parameters: [server_ips, server_port]
- description: vip ip
  label: VIP IP
  parameters: [lb-virtual-ip, lb-virtual-port, lb-service-type]
- description: lb-appname
  parameters: [lb-appname]
parameters:
  lb-appname: {description: This is the lb-name, label: LB-NAME, type: string}
  lb-service-type:
    constraints:
    - allowed_values: [HTTP, SSL, TCP, UDP, ANY]
    default: HTTP
    description: This is lb-service-type
    label: Service-type
    type: string
  lb-virtual-ip: {description: This is LB vip, label: VIP, type: string}
  lb-virtual-port: {description: This is virtual port, label: Virtual-port, type: string}
  server_ips: {description: Ip address of servers, label: IP of server, type: comma_delimited_list}
  server_port: {description: Port of server, label: Server port, type: string}
resources:
  sb_config:
    properties:
      lb-appname: {get_param: lb-appname}
      lb-service-type: {get_param: lb-service-type}
      lb-virtual-ip: {get_param: lb-virtual-ip}
      lb-virtual-port: {get_param: lb-virtual-port}
      mas_device_handle:
        get_attr: [network_resource_NS, mas_device_handle]
      svc-servers:
        repeat:
          for_each:
            ipvar%: {get_param: server_ips}
          template:
            ip: ipvar%
            port: {get_param: server_port}
    type: Citrix::NetScaler::Stylebook_com_citrix_adc_stylebooks_1_0_lb
  network_resource_NS:
    properties:
      subnets: [c07d727c-37a6-493a-ab4e-b96d9ddab560]
    type: Citrix::NetScaler::NetscalerNetworkConfigurator
```

version of the Heat template

parameter groups - declares the input parameter groups and order

parameter groups - declares the input parameters

resources - declares template resources; in this example declares the StyleBook resources

resources - declares template resources; in this example declares the NetScaler network resources

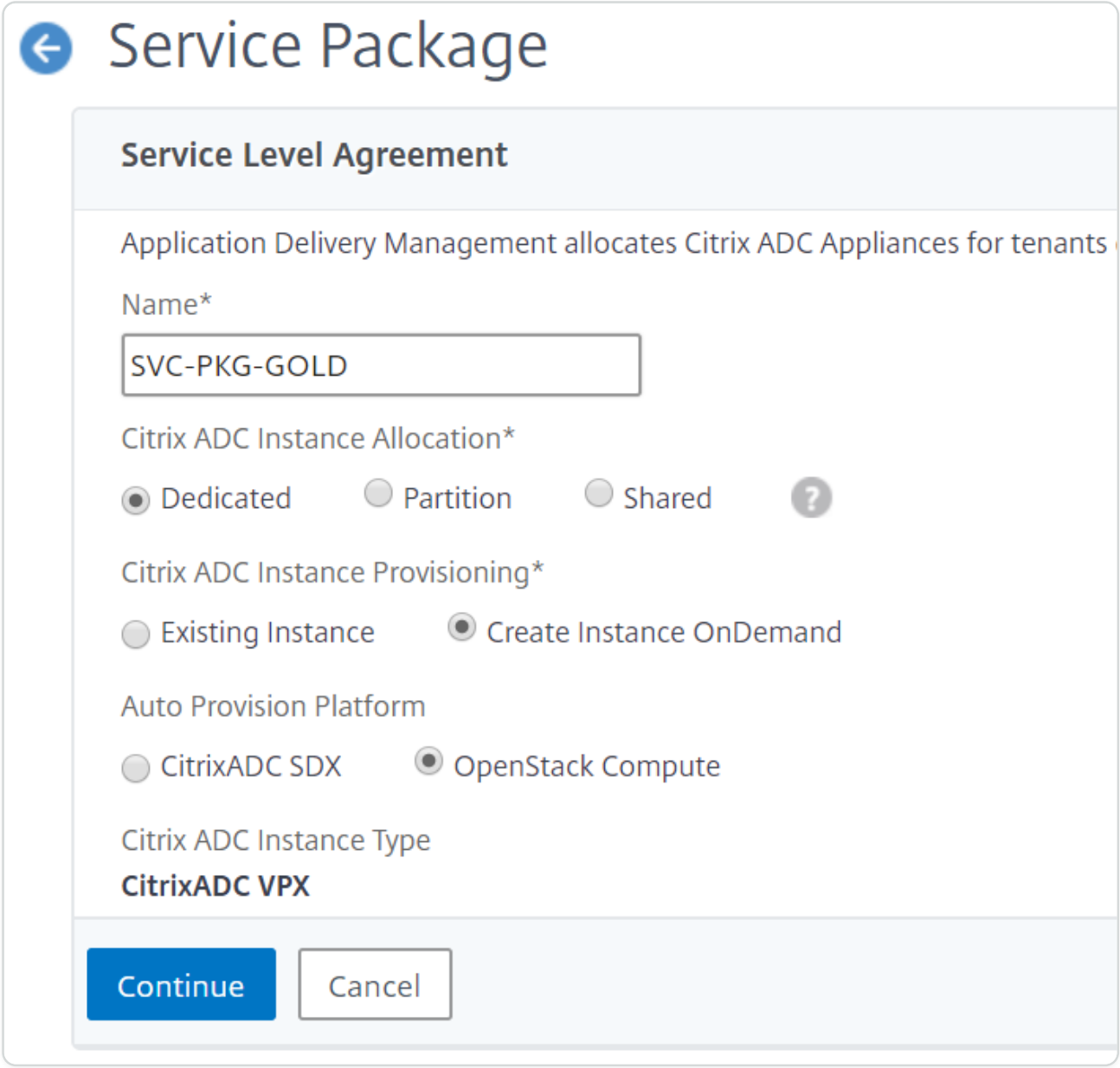
有关 Heat 服务以及如何创建模板的更多信息，请参阅 OpenStack Heat documentation。

服务包隔离策略

专用隔离策略

与专用策略的 NetScaler Console 服务包关联的每个租户都会从属于此服务包的实例中分配一个 NetScaler 实例。此分配的 NetScaler 实例不与其他租户共享。

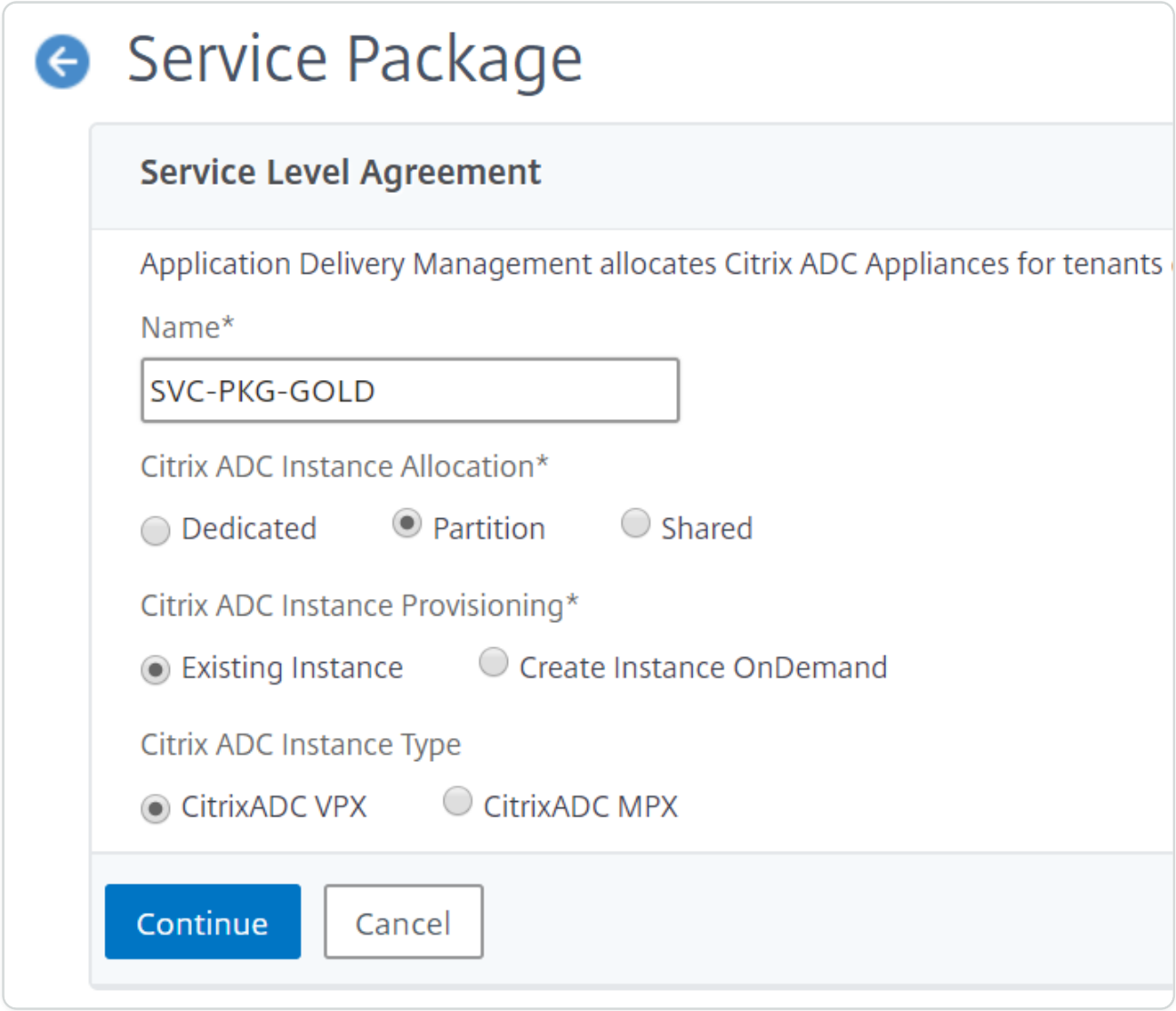
© 1997–2026 Citrix Systems, Inc. All rights reserved.



分区隔离策略

与分区策略的服务包关联的每个租户都会被分配一个属于该服务包的 NetScaler 实例的专用逻辑管理分区。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



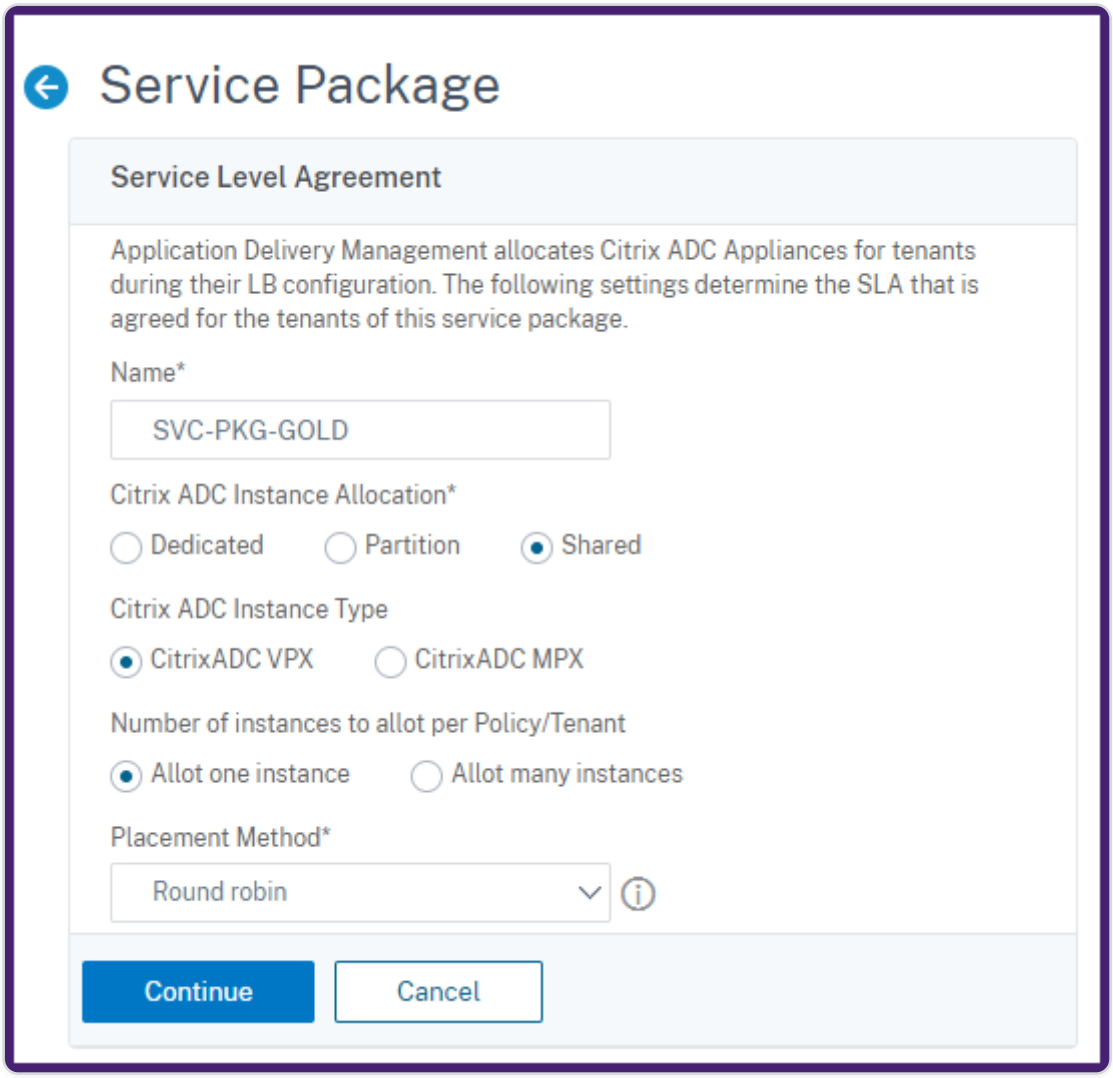
共享隔离策略

与服务包关联的租户共享属于该服务包的 NetScaler 实例。租户的所有配置都分配给一个 NetScaler 实例。在此模式下，来自多个租户的配置可以托管在同一个 NetScaler 实例上。您可以选择 **NetScaler VPX** 或 **NetScaler MPX** 作为设备类型。您可以选择只为服务包分配一个 NetScaler 实例或多个实例。也就是说，多个租户可以共享 NetScaler 设备的一个或多个虚拟实例。

注意

在服务包中仅将 NetScaler SDX 实例添加为 NetScaler VPX 实例，因为 NetScaler SDX 上已预置 NetScaler VPX。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意

您还可以创建灵活的放置策略，其中策略不仅基于租户名称或 ID，还基于其他自定义属性。有关灵活放置策略的更多信息，请参阅 基于策略的灵活设备分配。

灵活的基于策略的设备分配

NetScaler Console 根据与租户商定的 SLA，将 NetScaler 虚拟实例分配给租户。将虚拟实例分配给租户会在实例和租户之间创建一对一关系，其中一个租户只能分配到数据中心中的一个服务包。

在某些情况下，租户可能需要多个实例，或者实例的分配可能不是基于租户作为标准，而是基于其他因素，例如网络 ID 或应用程序。在这种情况下，NetScaler Console 允许您根据用户定义的表达式精确定义放置策略，以便将负载均衡器配置分配给其中一个托管实例。

放置策略提供了灵活性，可以决定在用户创建的每个负载均衡器配置中使用哪个 NetScaler 实例。NetScaler Console 中的灵活放置策略为基于租户分配 NetScaler 实例的现有方法提供了额外的选项。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

您可以手动将实例分配给租户，也可以使用放置策略根据创建的表达式分配实例。您不能在单个服务包上同时使用这两种方法。

放置策略基于在主要 LBaaS 配置对象（例如池和负载均衡器）的属性上定义的布尔表达式。NetScaler Console 中的放置策略用户界面提供了预定义的表达式，您可以从中选择以定义自定义策略。您可以为不同的表达式创建多个放置策略。因此，每个租户可以拥有由租户要求定义的多个设备。

您必须首先选择一个表达式来匹配稍后需要配置的根对象。根对象可以是 LBaaS V1 中的池对象，也可以是 LBaaS V2 中的负载均衡器对象。因此，NetScaler Console 基于策略的放置支持 LBaaS V1 和 V2 API。然后，这些放置策略与服务包关联。一旦根对象放置在实例中，模型中的后续对象也会添加到该实例中。

例如，池配置对象可以具有以下属性：

- tenant_id
- 名称
- 描述
- 协议
- lb_method
- subnet_id
- subname_name
- admin_state_up
- 状态
- network_id
- network_type
- segmentation_id
- subnet_cidr
- subnet_gateway_ip

以下示例展示了使用池属性为策略定义表达式的一些表达式：

1. 基于池名称的策略表达式

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
config["pools"]["name"] =="high-end-pool"
```

2. 基于池子网名称的策略表达式

```
config ["pools"]["subnet_name"] == "us-west-payment-subnet1"
```

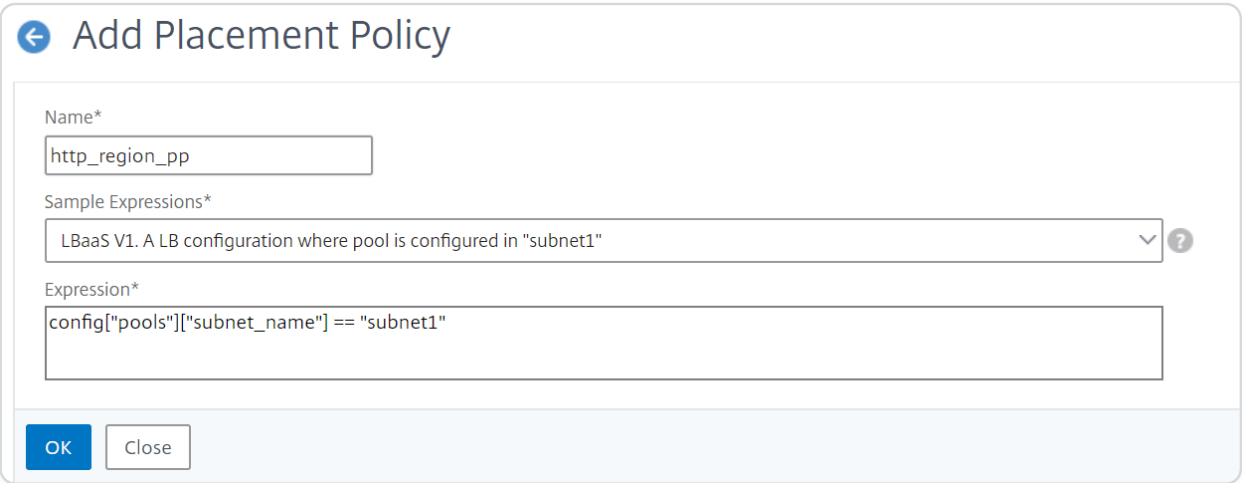
3. 基于负载均衡器子网名称的策略表达式

```
config["loadbalancers"]["subnet_name"] == "mas-subnet"
```

添加放置策略

1. 在 NetScaler Console 主页上，导航到 **编排** > **云编排** > **放置策略**，然后单击**添加**。
2. 在**添加放置策略**页面上，设置以下参数：
   a. 名称 - 输入放置策略的名称
   b. 常用表达式 - 从下拉列表中选择一个表达式。
   c. 表达式 - 此字段中会根据您在前面字段中选择的表达式填充逻辑（布尔）表达式。根据需要编辑字段名称。

> **注意**
>
> 创建多个策略时，请确保这些策略是相互排斥的。



3. 单击 **OK**。
4. 导航到 **编排** > **云编排** > **OpenStack** > **服务包**，然后单击 **添加**。
5. 在 **Service Package** 页面上，设置以下参数：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 名称 - 输入服务包的名称

b. 隔离策略 - 选择 **Shared** 策略

   在共享隔离策略中，租户的负载均衡器配置与分配给该租户的设备中其他租户的负载均衡器配置共存。

c. 设备类型 - 选择预置的 **NetScaler VPX** 或 **NetScaler MPX**

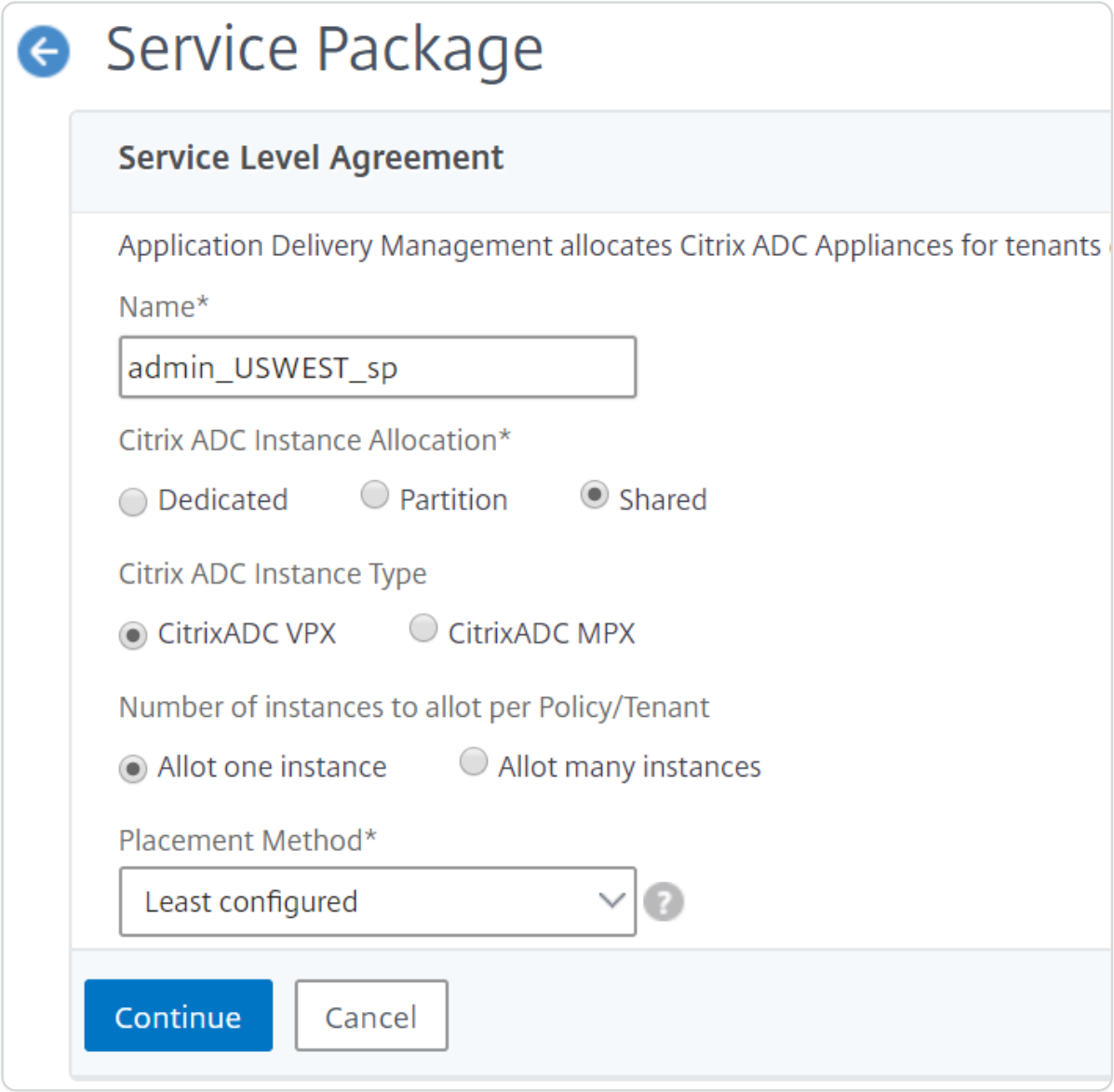
   如果您希望租户的所有负载均衡器配置都绑定到一个设备，请选择 **Allot one device**。如果您希望租户的每个负载均衡器配置都根据放置策略分布在多个设备上，请选择 **Allot many devices**。

   > **注意**
   >
   > NetScaler SDX 必须作为 NetScaler VPX 实例添加到服务包中，因为 NetScaler SDX 上已预置 NetScaler VPX。

d. 放置方法 - 选择 **最少配置**

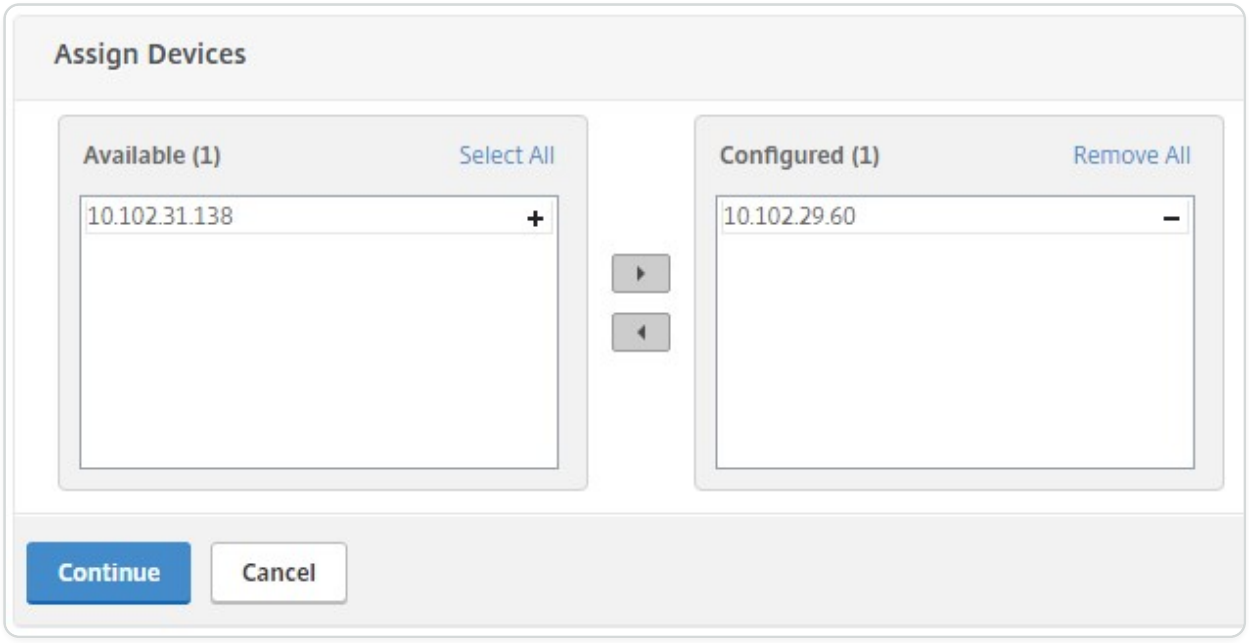
   选择“最少配置”时，将选择当时配置的池成员数量最少的 NetScaler 实例作为租户的设备。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

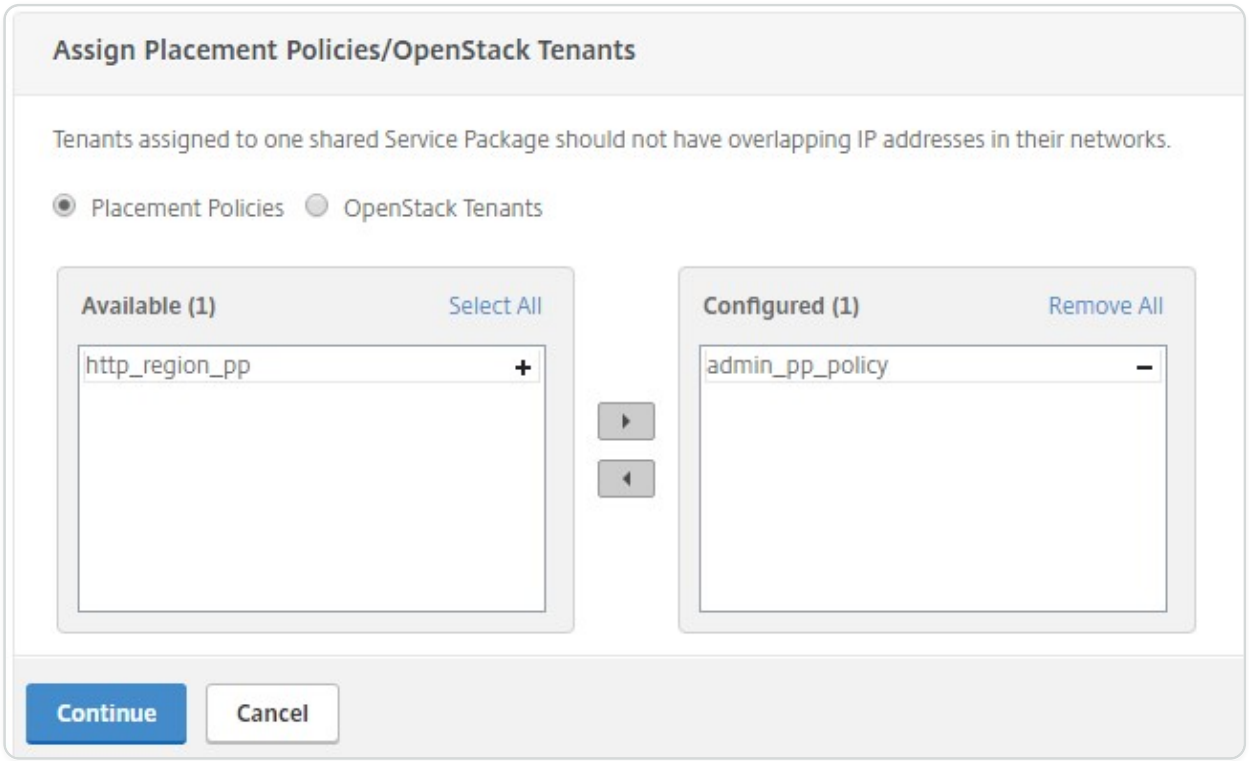


6. 单击 **继续**。
7. 在 **分配设备** 部分，将可用的 NetScaler 设备添加到已配置设备列表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. 单击 **继续**。
9. 在 **分配放置策略/OpenStack 租户** 部分，添加您之前创建的放置策略。



注意

如果找不到策略，则会恢复回退机制，NetScaler Console 会根据租户分配 NetScaler 实例。如果租户不属于任何服务包，NetScaler Console 将显示一条错误消息，内容如下：

“租户 `admin` 不属于任何服务包，并且没有默认服务包。”.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. 单击 **继续**，然后单击 **完成**。

NSX Manager: NetScaler 实例的手动预配

NetScaler Console 与 VMware 网络虚拟化平台集成，以自动化 NetScaler 服务的部署、配置和管理。这种集成消除了与物理网络拓扑相关的传统复杂性，使 vSphere/vCenter 管理员能够更快地以编程方式部署 NetScaler 服务。

本文提供了您必须在 VMware NSX Manager 和 NetScaler Console 上执行的任务列表。

注意

确保已安装并配置 VMware NSX for vSphere 6.2 及更高版本，并且已创建需要进行负载均衡的边缘网关、DLR 和虚拟机。

先决条件

- 安装 VMware ESXi 4.1 或更高版本，并确保硬件满足最低要求。
- 在满足最低系统要求的管理工作站上安装 VMware Client。
- 在满足最低系统要求的管理工作站上安装 VMware OVF Tool（VMware ESXi 4.1 版必需）。
- 在任何受支持的虚拟机管理程序上安装 NetScaler Console。

  有关在任何受支持的虚拟机管理程序上安装 NetScaler Console 13.1 版本的任务，请参阅部署 NetScaler Console。

VMware ESXi 硬件要求

下表列出了在 VMware ESXi 服务器上安装 NetScaler Console 虚拟设备所需的虚拟计算资源。

组件	要求
内存	8 GB
虚拟 CPU	8
存储空间	500 GB
虚拟网络接口	1
吞吐量	1 千兆位/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

上述内存和硬盘要求适用于在 VMware ESXi 服务器上部署 NetScaler Console，前提是主机上没有运行其他虚拟机。VMware ESXi 服务器的硬件要求取决于其上运行的虚拟机数量。

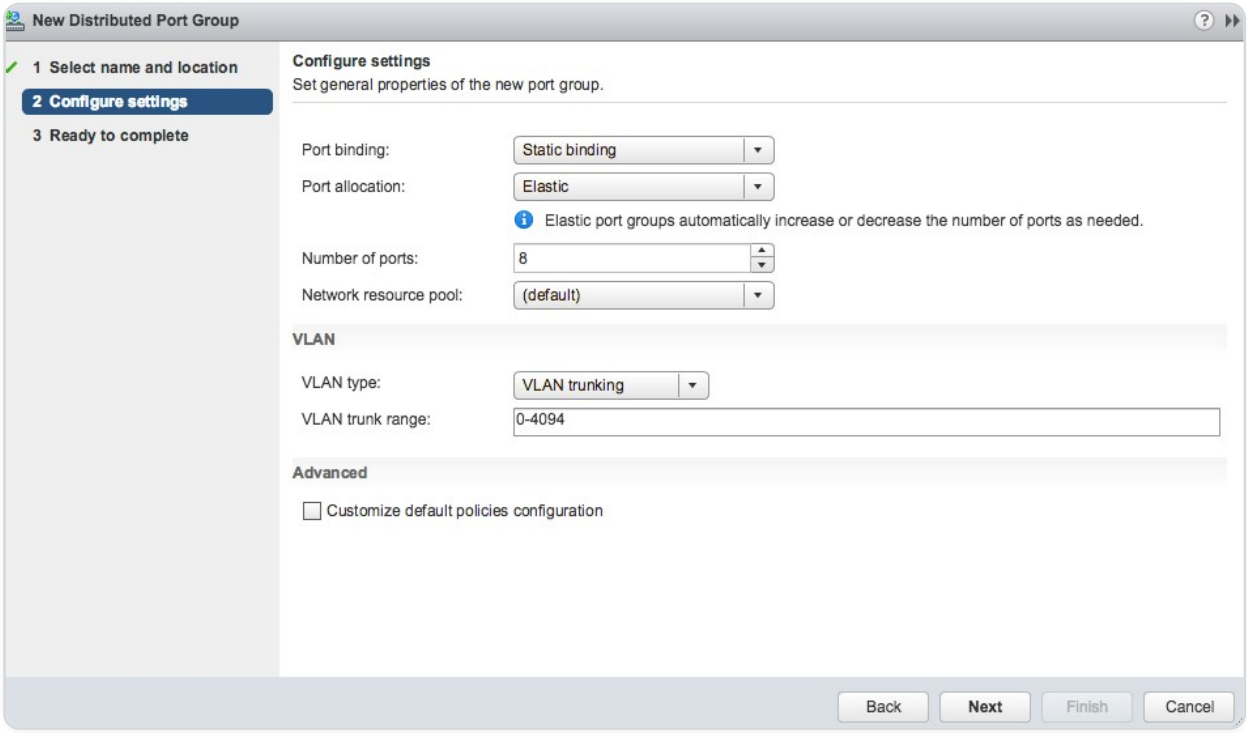
配置 VMware NSX

- 创建不同容量的 NetScaler VPX 实例池，这些实例将添加到不同的服务包中。

例如：

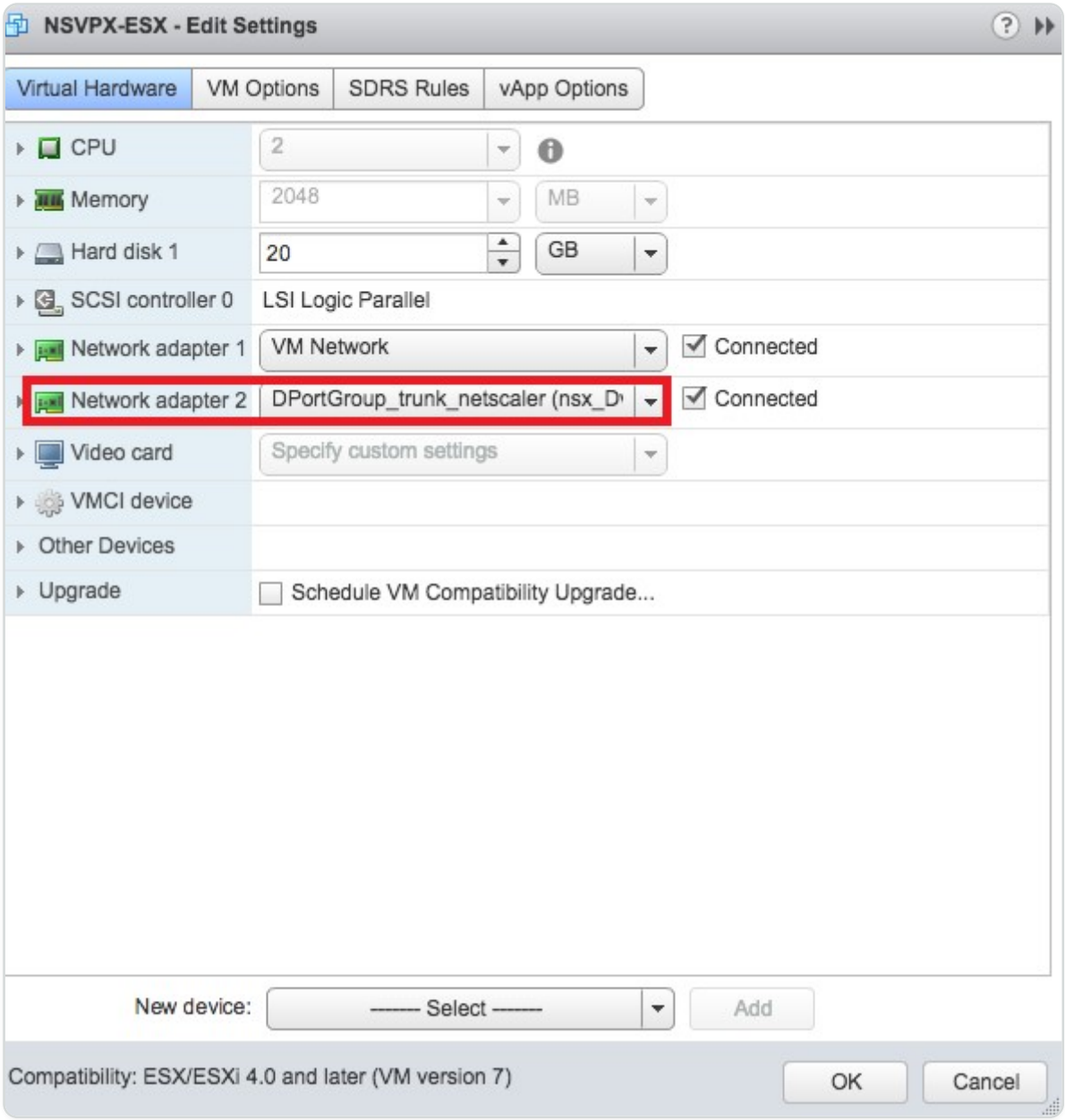
- 创建五个 VPX1000 (1 Gbps) 的 NetScaler VPX 实例。这些实例将添加到 Gold 服务包中。
- 创建五个 VPX10 (10 Mbps) 的 NetScaler VPX 实例。这些实例将添加到 Bronze 服务包中。

1. 在 vSphere 客户端中，导航到 **Networking**，并创建一个类型为 VLAN trunking 的端口组，例如，范围为 101-105（您甚至可以提供完整范围，但仅为所需的 VLAN 创建类型为 VLAN 的端口组）。



2. 为每个 NetScaler VPX 实例创建一个新接口，并将其附加到上面创建的 VLAN 范围中继端口组。

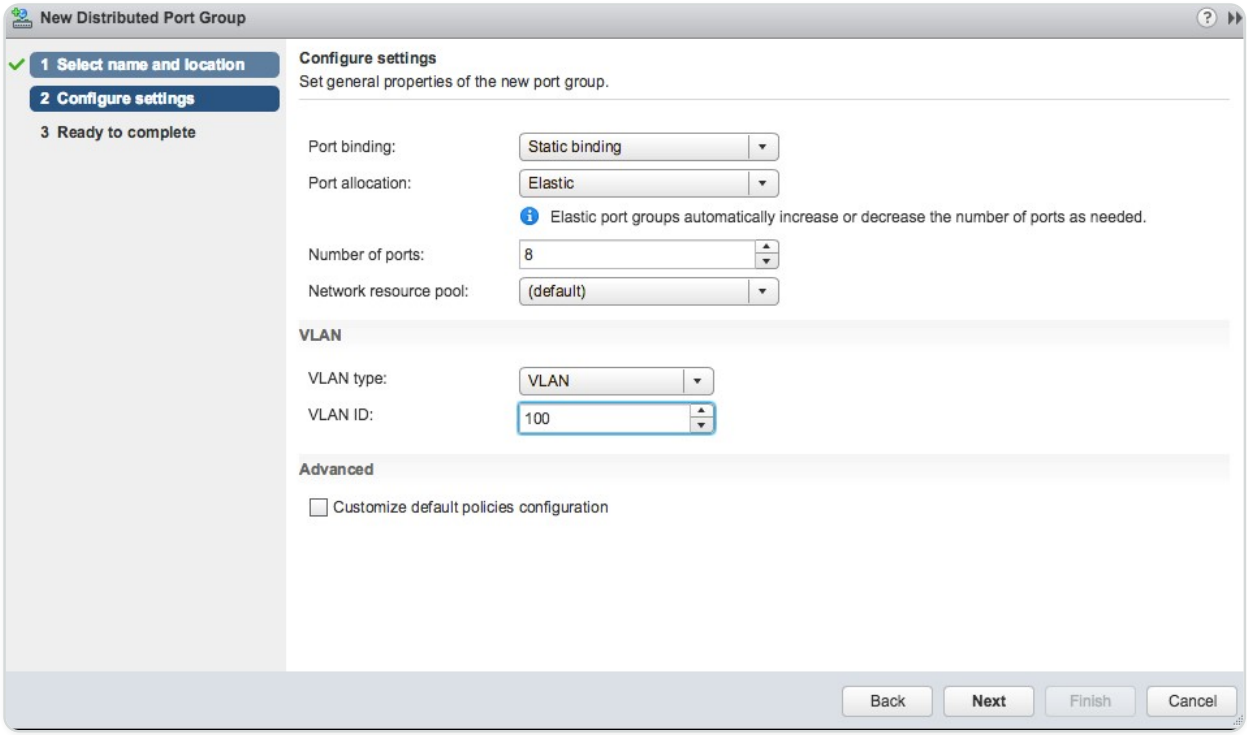
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 在 vSphere 客户端中，导航到 **Networking**，并创建一个类型为 VLAN 的端口组。

   例如，如果最初的中继端口组是使用范围 101-105 创建的，则为每个 VLAN 创建一个 VLAN 端口组，即一个带有 VLAN 101 的端口组，另一个带有 VLAN 102 的端口组，依此类推，直到 VLAN 105。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

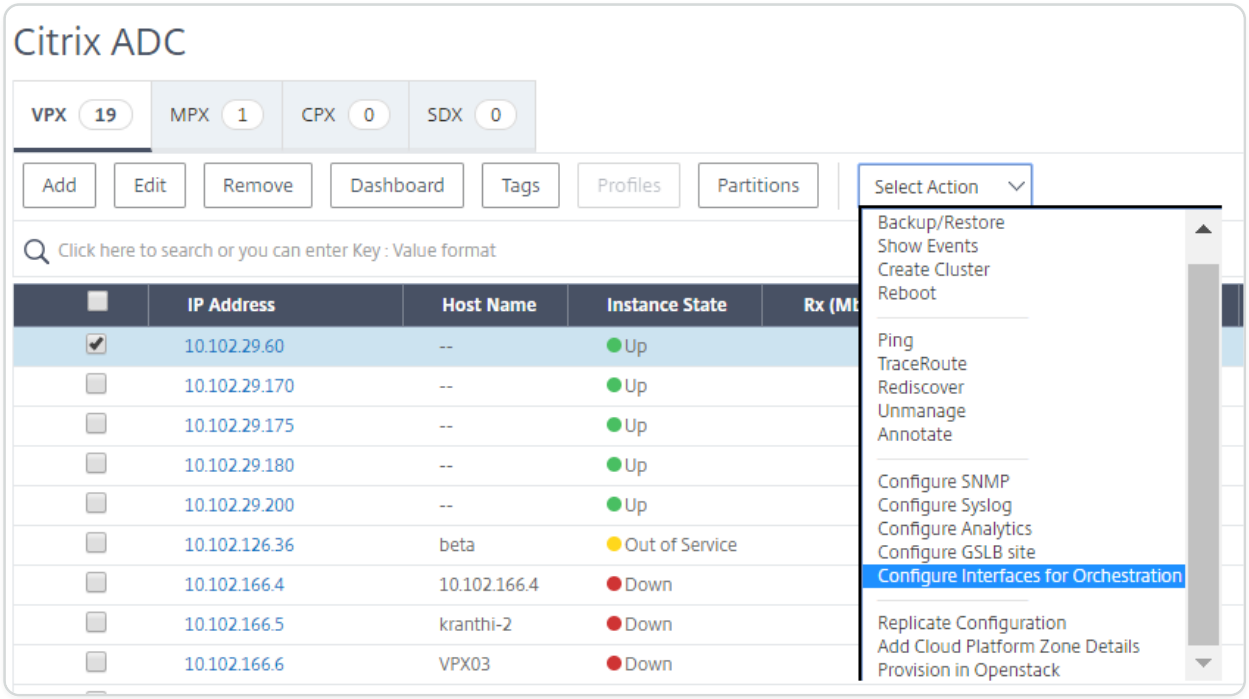


在 NetScaler Console 中添加 NetScaler VPX 实例

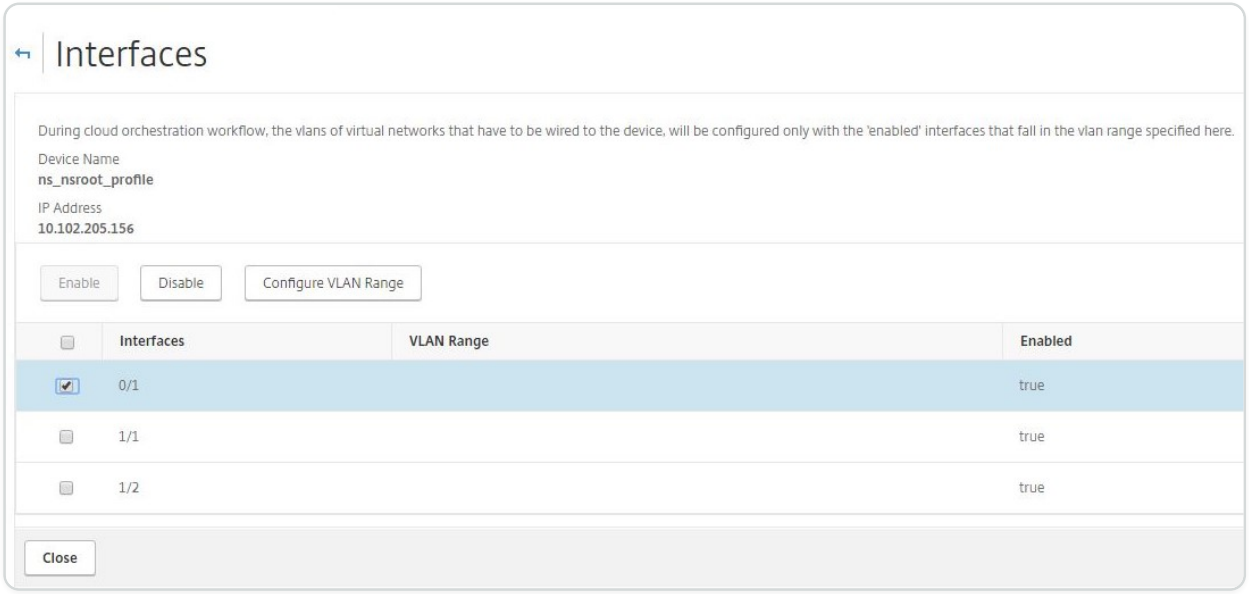
在 NetScaler Console 中添加 NetScaler VPX 实例，并为每个设备指定中继组的 VLAN 范围。

1. 在 NetScaler Console 中，导航到 **Infrastructure** \> **Instances** \> **NetScaler VPX**，然后单击 **Add**。
2. 在 **Add NetScaler VPX** 页面上，指定实例的主机名、每个实例的 IP 地址或 IP 地址范围，然后从 **Profile Name** 列表中选择一个实例配置文件。您也可以通过单击 + 图标创建新的实例配置文件。
3. 单击 **OK**。
4. 在 **NetScaler VPX** 页面上的列表中选择新添加的 NetScaler VPX 实例，然后单击 **Action** 字段中的向下箭头按钮。选择 **Configure Interfaces for Orchestration**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

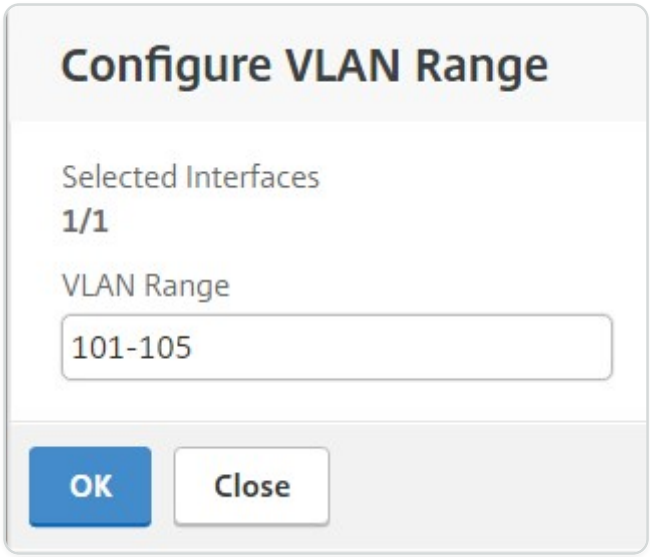


5. 在“**接口**”页面上，选择管理接口，然后单击“**禁用**”以禁用 VLAN 绑定到管理接口。



6. 在“**接口**”页面上，选择所需的接口，然后单击“**配置 VLAN 范围**”。
7. 输入在 NSX Manager 中配置的 VLAN 范围，单击“**确定**”，然后单击“**关闭**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

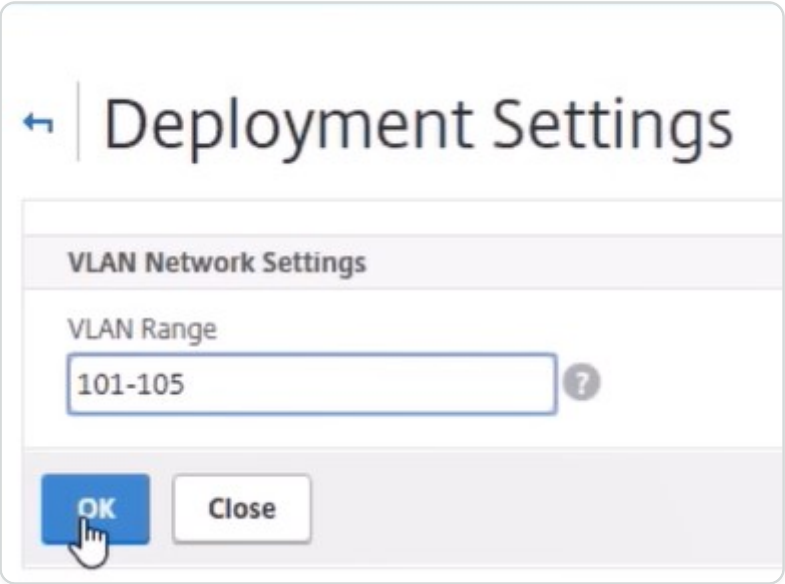


将 VMware NSX Manager 注册到 NetScaler Console

将 VMware NSX Manager 注册到 NetScaler Console，以在它们之间创建通信通道。

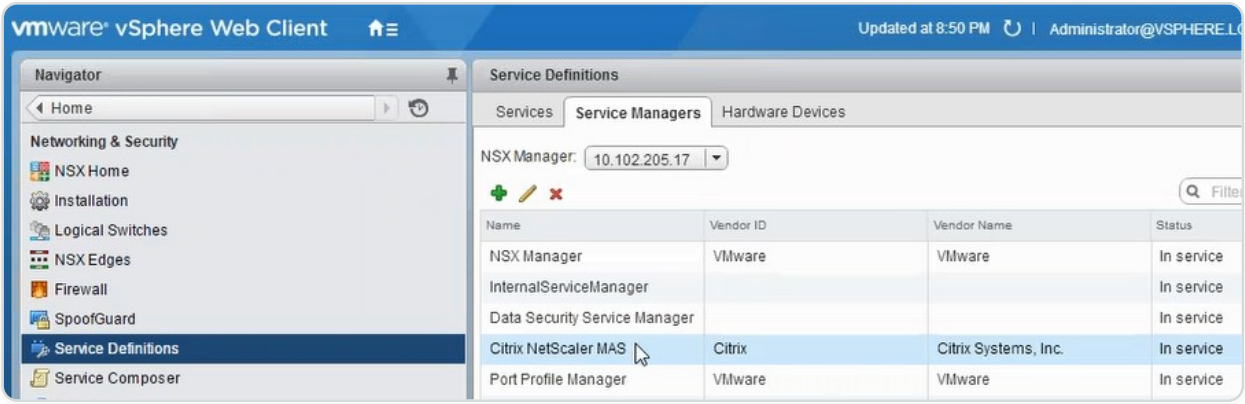
1. 在 NetScaler Console 中，从下拉列表中导航到“**编排**”\>“**SDN 编排**”\>“**VMware NSX Manager**”，然后单击“**配置 NSX Manager 设置**”。
2. 在“**配置 NSX Manager 设置**”页面上，设置以下参数：
   a. NSX Manager IP 地址 - NSX Manager 的 IP 地址。
   b. NSX Manager 用户名 - NSX Manager 的管理用户名。
   c. 密码 - NSX Manager 管理用户的密码。
3. 在“**NSX Manager 使用的 NetScaler Console 帐户**”部分中，设置 NSX Manager 的 NetScaler 驱动程序用户名和密码。NetScaler Console 使用这些登录凭据对来自 NSX Manager 的负载平衡器配置请求进行身份验证。
4. 单击“**确定**”。
5. 导航到 **编排** \> **系统** \> **部署设置**。提供在中继端口组中配置的 VLAN 范围。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 登录到 vSphere Web Client 上的 NSX Manager，然后导航到 **服务定义** \> **服务管理器**。

   您可以将 Citrix NetScaler Console 视为其中一个服务管理器。这表明注册成功，并且 NSX Manager 与 NetScaler Console 之间已建立通信通道。



在 NetScaler Console 中创建服务包

1. 在 NetScaler Console 中，导航到 **编排** \> **SDN 编排** \> **VMware NSX Manager** \> **服务包**，然后单击“**添加**”以添加新的服务包。
2. 在“**服务包**”页面上的“**基本设置**”部分中，设置以下参数：

   a. 名称 – 键入服务包的名称

   b. 隔离策略 – 默认情况下，隔离策略设置为“专用”

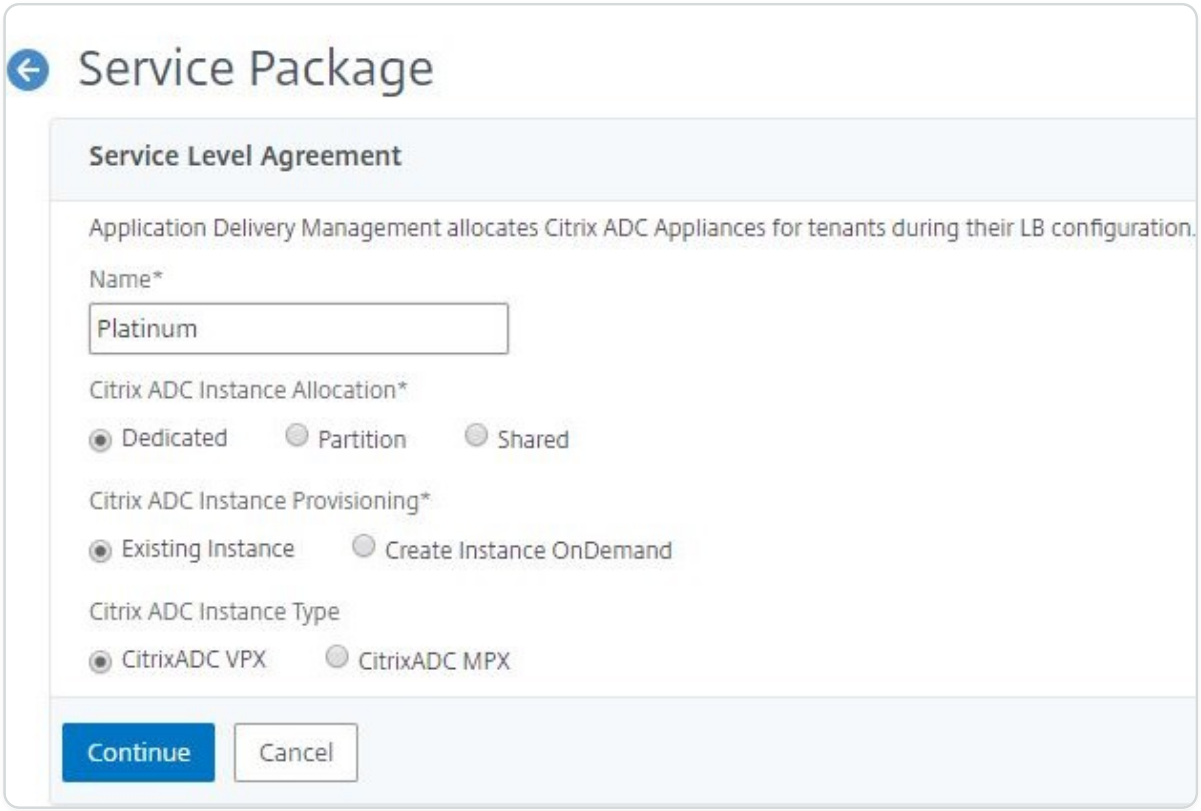
   c. 设备类型 – 默认情况下，设备类型设置为 NetScaler VPX

   注意

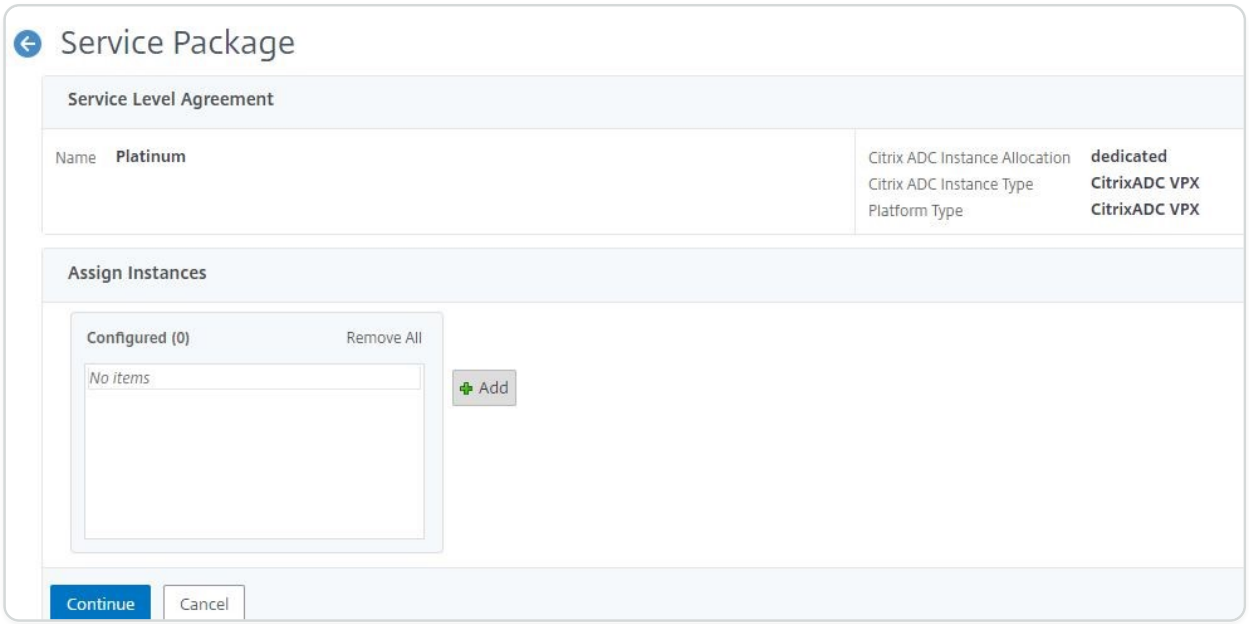
   这些值在此版本中默认设置，并且您无法修改它们。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

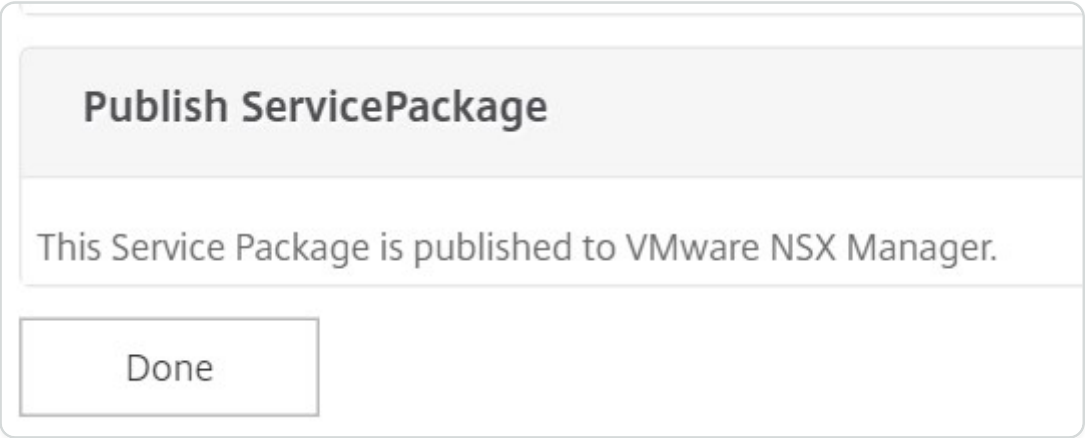
d. 单击“**继续**”。



3. 在“**分配设备**”部分，选择此软件包的预配置 VPX，然后单击“**继续**”。
4. 在“**发布服务软件包**”部分，单击“**继续**”将服务软件包发布到 VMware NSX，然后单击“**完成**”。



© 1997–2026 Citrix Systems, Inc. All rights reserved.



此过程在 NSX Manager 中配置服务软件包。一个服务可以添加多个设备，并且多个边缘可以使用相同的服务软件包将 NetScaler VPX 实例卸载到 NetScaler Console。

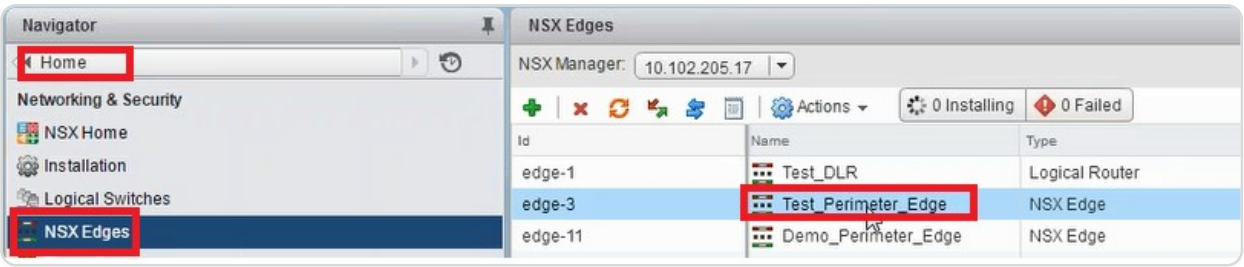
5. 登录到 vSphere Web Client 上的 NSX Manager，然后导航到 **服务定义** \> **服务**。

   您可以看到 NetScaler Console 服务软件包已注册。

为边缘执行负载平衡器服务插入

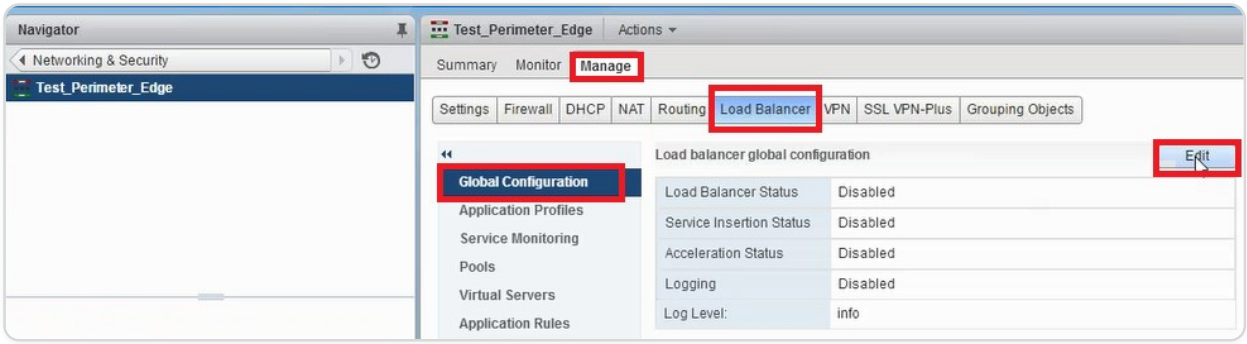
在之前创建的 NSX Edge 网关上执行负载平衡器服务插入（将负载平衡功能从 NSX LB 卸载到 NetScaler）。

1. 在 NSX Manager 中，导航到 **主页** \> **NSX 边缘**，然后选择您已配置的边缘网关。



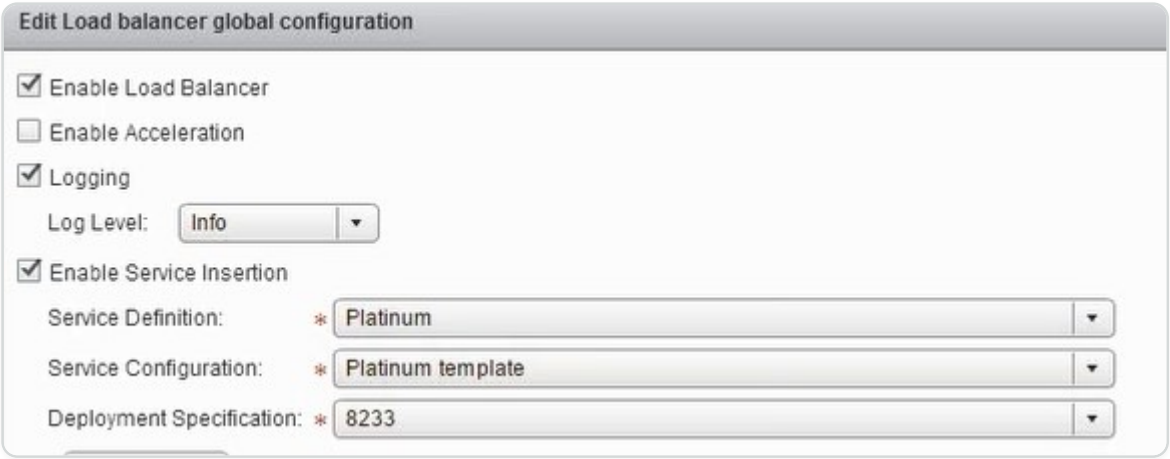
2. 单击“**管理**”，然后在“**负载平衡器**”选项卡上，选择“**全局配置**”，然后单击“**编辑**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

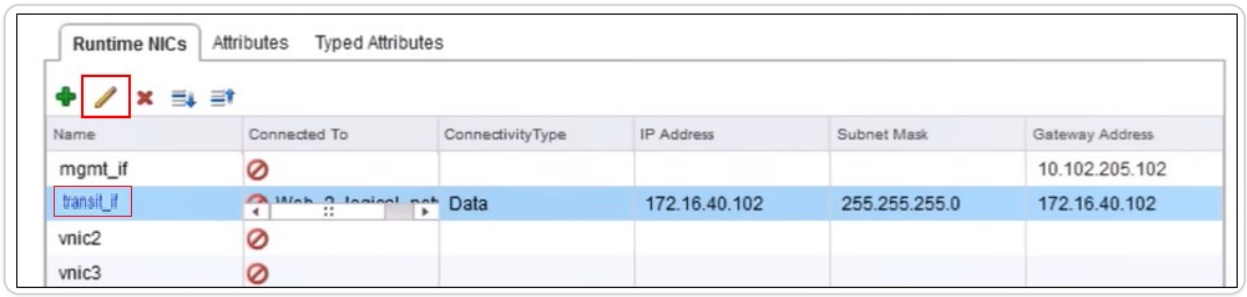


3. 选择“**启用负载平衡器**”、“**日志记录**”、“**启用服务插入**”以启用它们。

   a. 在**服务定义**中，选择在 NetScaler Console 中创建并发布到 NSX Manager 的服务包。

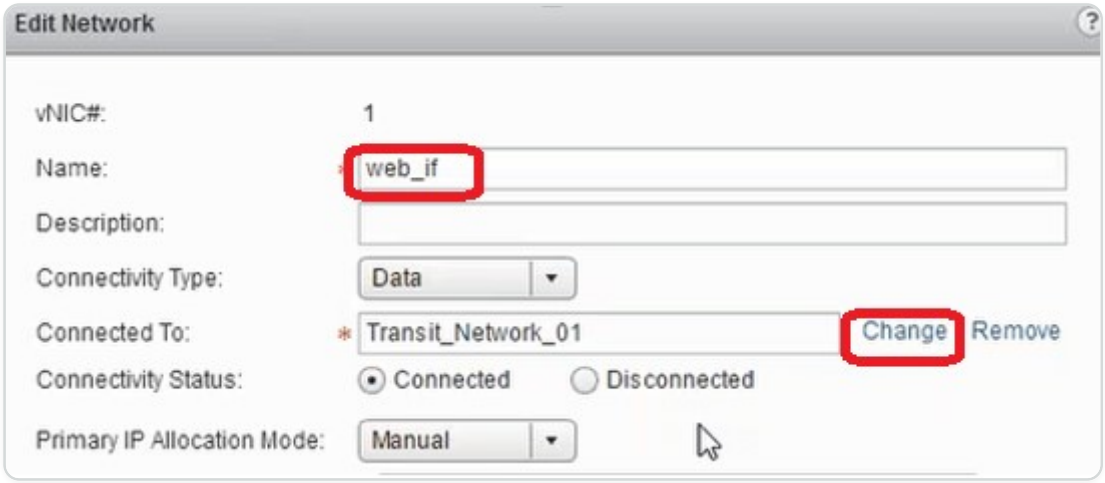


4. 选择现有的运行时 NIC，然后单击“编辑”图标以编辑在分配 NetScaler VPX 时必须连接的运行时 NIC。

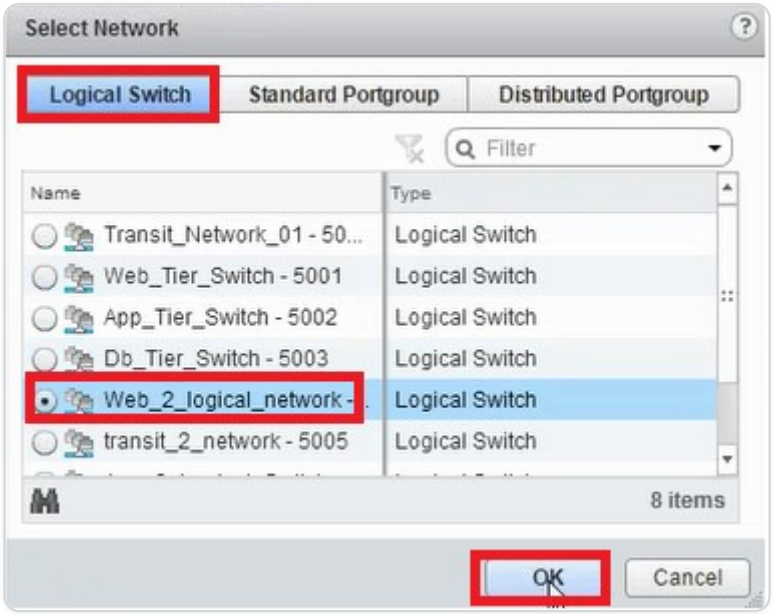


5. 编辑 NIC 的名称，将连接类型指定为**数据**，然后单击**更改**。

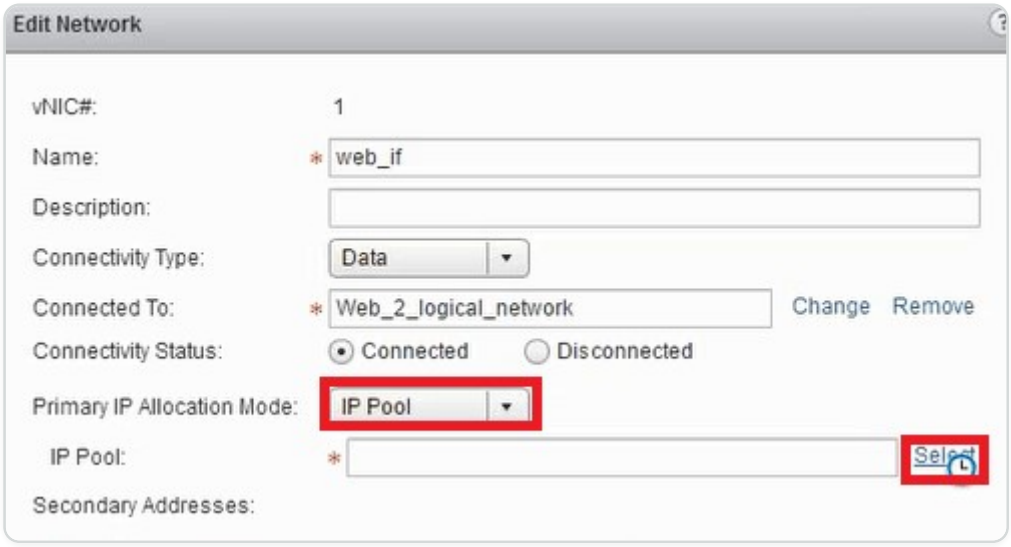
© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. 选择相应的 Web 逻辑交换机。

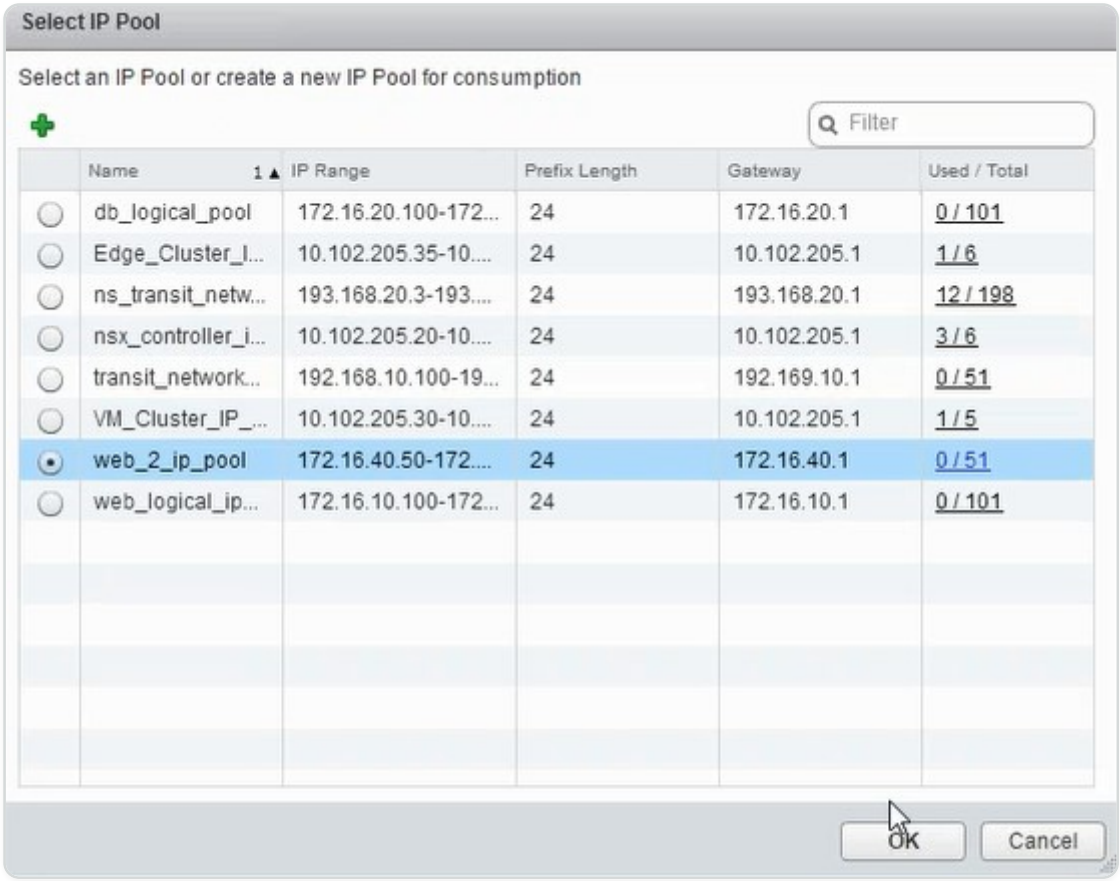


7. 在**主 IP 分配模式**中，从下拉列表中选择“IP 池”，然后单击 IP 池字段上的向下箭头按钮。



8. 在**选择 IP 池**窗口中，选择相应的 IP 池，然后单击**确定**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



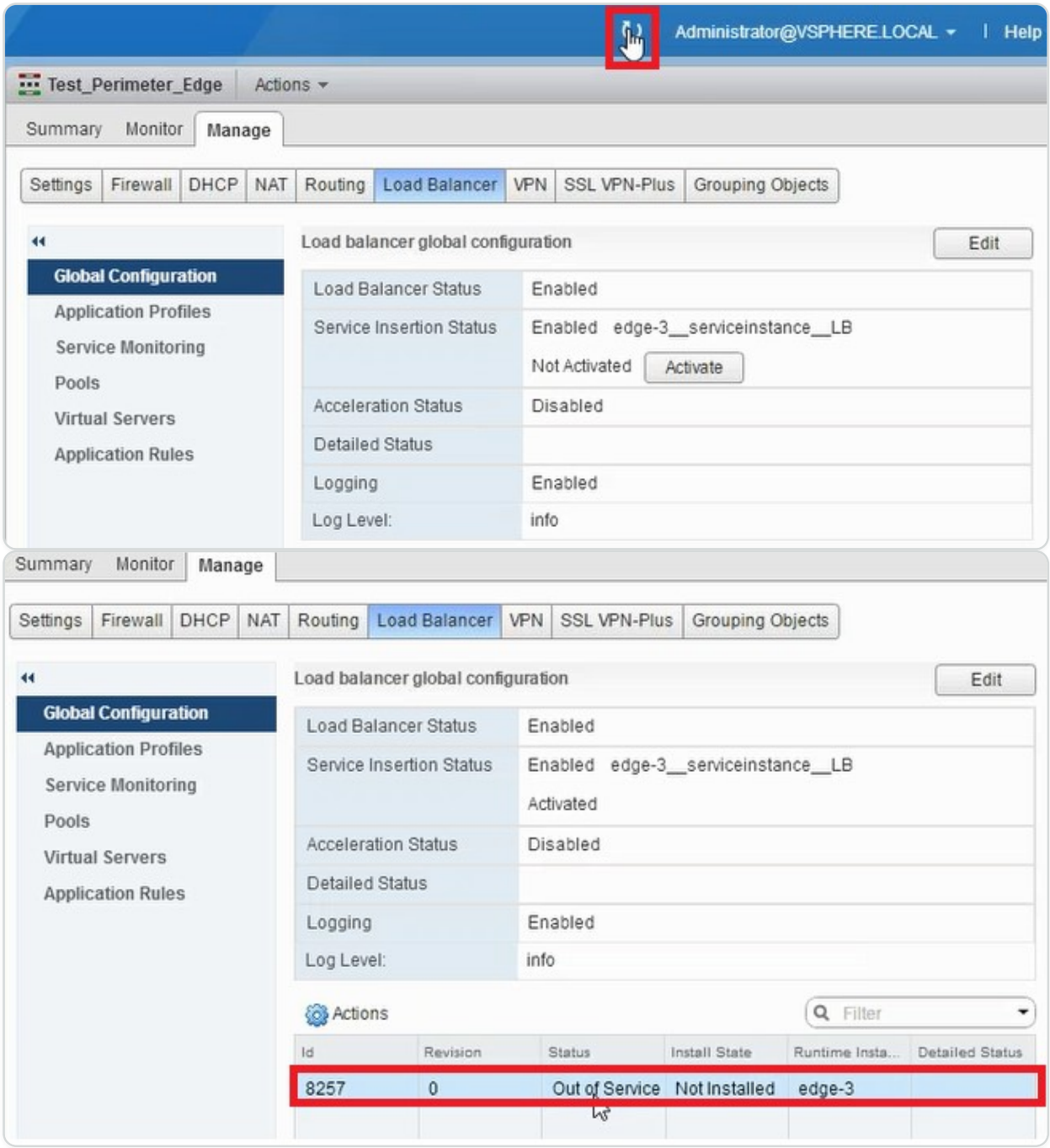
获取 IP 地址并将其设置为 NetScaler VPX 设备中的源网络 IP 地址。在 NSX Manager 中创建 L2 网关以将 VXLAN 映射到 VLAN。

注意

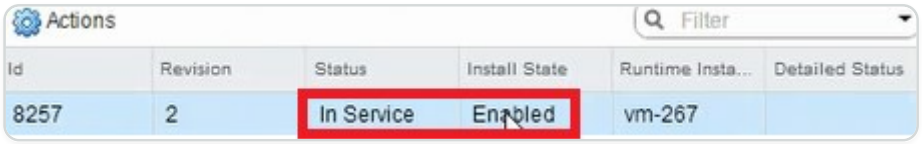
所有数据接口都作为运行时 NIC 连接，并且它们是 DLR 接口的一部分。

9. 刷新视图以查看运行时的创建。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. 虚拟机启动后，Status 的值变为 **In Service**，Install State 的值变为 **Enabled**。



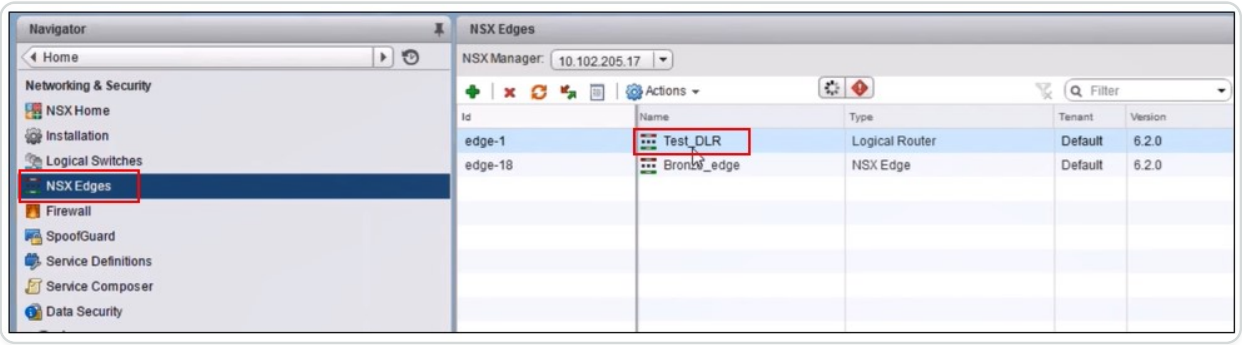
注意

在 NetScaler Console 中，导航到 **Orchestration** \> **Requests** 以查看 LB 服务插入完成的进度详细信息。

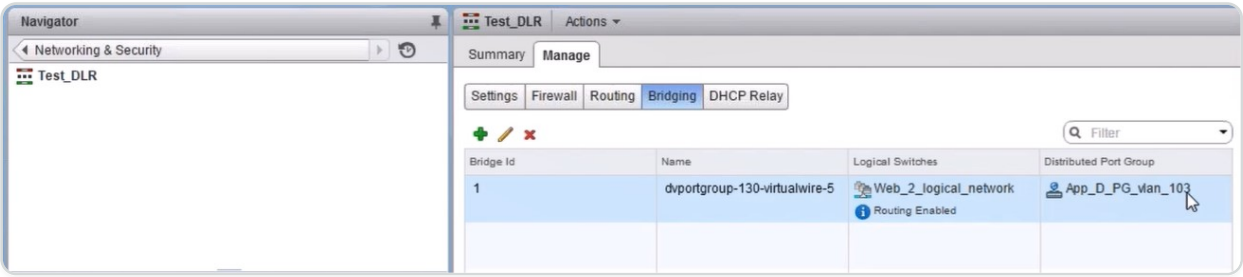
© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 NSX Manager 上查看 L2 网关

1. 登录到 vSphere Web Client 上的 NSX Manager，导航到 **NSX Edges**，然后选择已创建的 DLR。



2. 在 DLR 页面中，导航到 **Manage** \> **Bridging**。您可以在列表中看到 L2 网关。



注意

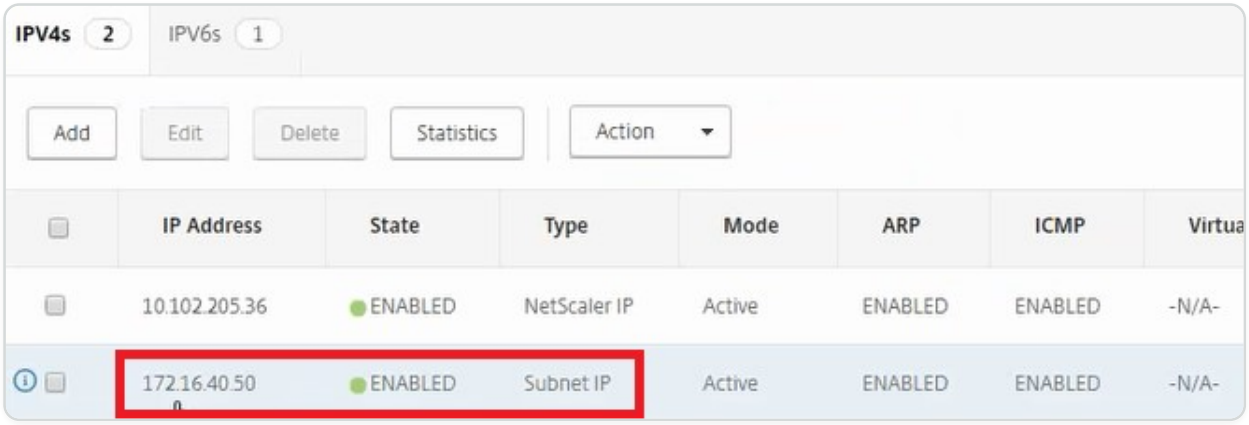
每个数据接口都会创建一个 L2 网关。

查看已分配的 NetScaler

1. 使用 NetScaler Console 中显示的 IP 地址登录到 NetScaler VPX 实例。然后，导航到 **Configuration** \> **System** \> **Networking**。在右侧窗格中，您可以看到已添加了两个 IP 地址。单击 IP 地址超链接以查看详细信息。

子网 IP 地址与 NSX 中添加的 Web 界面 IP 地址相同。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 导航到 **Configuration** \> **System** \> **Licenses** 以查看应用于此实例的许可证。

使用 StyleBook 配置 NetScaler VPX 实例

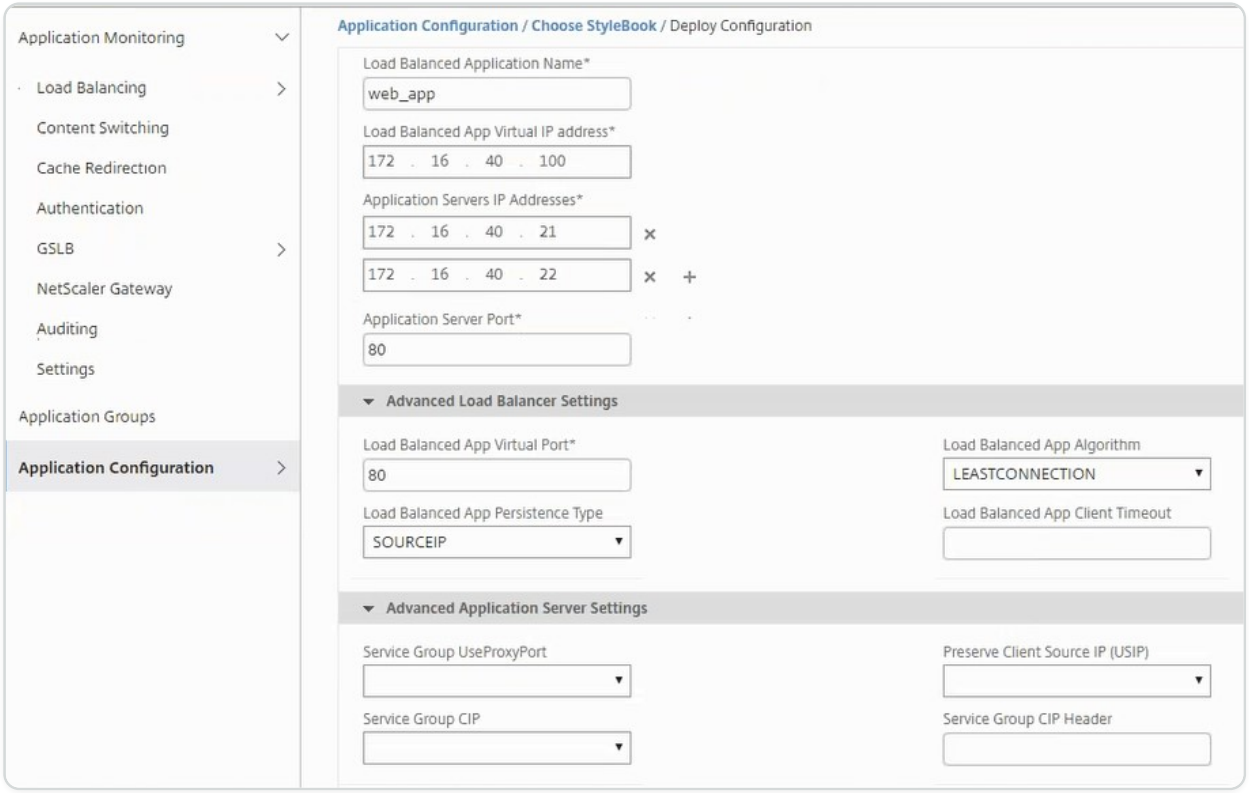
1. 在 NetScaler Console 中，导航到 **编排** > **SDN 编排** > **配置 NSX Manager** > **边缘网关**。

   记下分配给相应 Edge Gateway 的 NetScaler 实例 IP，该 Edge Gateway 将应用通过 StyleBooks 进行的负载平衡配置。

2. 创建一个新的 StyleBook。导航到 **Applications** \> **Configuration**，导入 StyleBook，然后从列表中选择 StyleBook。

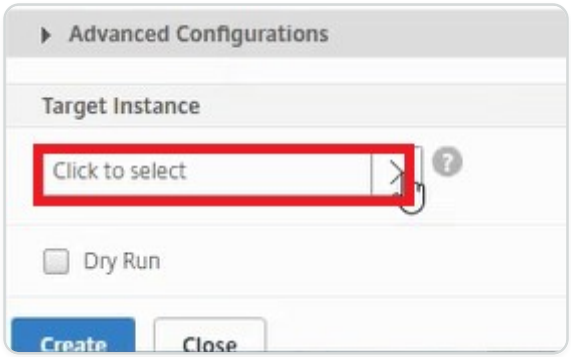
   要创建新的 StyleBook，请参阅 创建您自己的 StyleBook。

3. 为所有必需参数指定值。



4. 指定要运行这些配置设置的 NetScaler VPX 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 选择之前记下的 IP 实例，然后单击 **Select**。

   指定 IP 实例(/en-us/netscaler-application-delivery-management-software/media/nmas-stylebook-config-3.jpg)

6. 单击“**创建**”以将配置应用于所选设备。

   创建配置包(/en-us/netscaler-application-delivery-management-software/media/nmas-stylebook-config-4.jpg)

查看负载均衡器配置

1. 登录到 NetScaler VPX 实例，导航到“**配置**” \> “**流量管理**” \> “**负载均衡**”以查看已创建的负载均衡虚拟服务器。

   查看负载均衡器配置(/en-us/netscaler-application-delivery-management-software/media/nmas-view-lb-config-view.jpg)

   您还可以查看已创建的服务组。

   查看服务组(/en-us/netscaler-application-delivery-management-software/media/nmas-view-sg-config-view.jpg)

2. 选择服务组，然后单击“**管理成员**”。“**配置服务组成员**”页面显示与服务组关联的成员。

   配置服务组成员(/en-us/netscaler-application-delivery-management-software/media/nmas-view-sg-members.jpg)

删除负载均衡器服务

1. 在 NetScaler Console 中，导航到“**应用程序**” \> “**配置**”，然后单击 **X** 图标以删除应用程序配置。
2. 登录到 vSphere Web Client 上的 NSX Manager，然后导航到 NetScaler VPX 实例所连接的边缘网关。
3. 导航到“**管理**” \> “**负载均衡器**” \> “**全局配置**”，右键单击运行时条目，然后单击“**取消预配**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注意**
>
> NetScaler Console 中的边缘网关对应于 NSX Manager 中的运行时条目。

取消配置(/en-us/netscaler-application-delivery-management-software/media/nmas-delete-lb-service-2.jpg)

NetScaler VPX 实例已停止服务。

4. 在 NetScaler Console 中，导航到 **编排** \> **SDN 编排** \> **配置 NSX Manager** \> **边缘网关**。验证边缘网关与已删除实例的相应映射不存在。

NSX Manager：NetScaler 实例的自动预配

概述

NetScaler Console 与 VMware 网络虚拟化平台集成，以自动化 NetScaler 服务的部署、配置和管理。这种集成消除了与物理网络拓扑相关的传统复杂性，使 vSphere/vCenter 管理员能够更快地以编程方式部署 NetScaler 服务。

在 VMware NSX Manager 上插入和删除负载平衡服务期间，NetScaler Console 会动态预配和销毁 NetScaler 实例。这种动态预配要求在 NetScaler Console 中自动分配 NetScaler VPX 许可证。当 NetScaler 许可证上传到 NetScaler Console 时，NetScaler Console 将充当许可证服务器。

先决条件

> **注意**
>
> 此集成仅支持 **VMware NSX for vSphere 6.1 或更早版本**。

- NetScaler Console 13.0 版，以高可用性模式设置并安装在 ESX 上。
- NetScaler VPX 13.0 版
- NetScaler VPX 实例的 NetScaler VPX 许可证 13.0 版
- 安装 VMware ESXi 4.1 版或更高版本，硬件需满足最低要求。
- 在满足最低系统要求的管理工作站上安装 VMware Client。
- 在满足最低系统要求的管理工作站上安装 VMware OVF Tool（VMware ESXi 4.1 版必需）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console 和 NetScaler 实例的高可用性部署

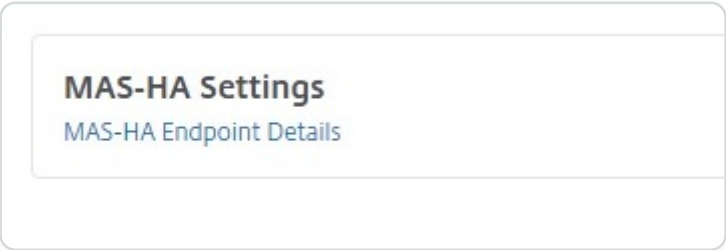
要预配 NetScaler Console HA 设置，请安装您从 NetScaler 站点下载的 NetScaler Console 映像文件。有关如何预配 NetScaler Console HA 设置的更多信息，请参阅 在高可用性模式下部署 NetScaler Console。

设置 NetScaler Console HA 端点详细信息

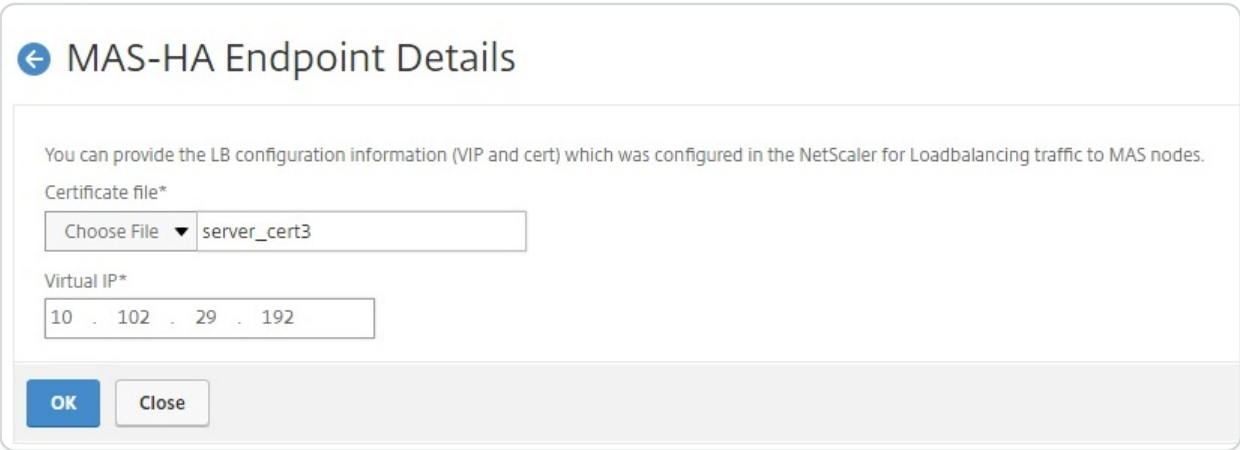
要将以 HA 模式部署的 VMware NSX Manager 与 NetScaler Console 集成，您必须首先输入负载平衡 NetScaler 实例的虚拟 IP 地址。您还必须将 NetScaler 负载平衡虚拟服务器上存在的证书文件上传到 NetScaler Console 文件系统。

在 NetScaler Console 中提供负载平衡配置信息：

1. 在 NetScaler Console HA 节点中，导航到 **系统** \> **部署**。
2. 单击右上角的 **HA 设置**，然后在 **MAS-HA 设置** 页面中，单击 **MAS-HA 端点详细信息**。



3. 在 **MAS-HA 端点详细信息** 页面上，上传已存在于负载平衡 NetScaler 实例上的相同证书。
4. 输入负载平衡 NetScaler 实例的虚拟 IP 地址，然后单击 **确定**。



将 VMware NSX Manager 注册到 NetScaler Console

当您设置两个高可用性 NetScaler Console 服务器时，这两个服务器节点处于主动-被动模式。登录到主 NetScaler Console 服务器节点，以 HA 模式将 VMware NSX Manager 注册到 NetScaler Console，从而在它们之间创建通信通道。

以 HA 模式将 VMware NSX Manager 注册到 NetScaler Console：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 在主 NetScaler Console 服务器节点中，导航到 **编排** \> **SDN 编排** \> **VMware NSX Manager**。
2. 单击 **配置 NSX Manager 设置**。
3. 在 **配置 NSX Manager 设置** 页面上，设置以下参数：
   a. NSX Manager IP 地址 - NSX Manager 的 IP 地址。
   b. NSX Manager 用户名 - NSX Manager 的管理用户名。
   c. 密码 - NSX Manager 的管理用户的密码。
4. 在 NSX Manager 使用的 NetScaler Console 帐户部分中，设置 NSX Manager 的 NetScaler 驱动程序密码。
5. 单击 **确定**。

在 NetScaler Console 中上传许可证

将 NetScaler VPX 许可证上传到 NetScaler Console，以便 NetScaler Console 可以在与 NSX 进行编排时自动将许可证分配给实例。

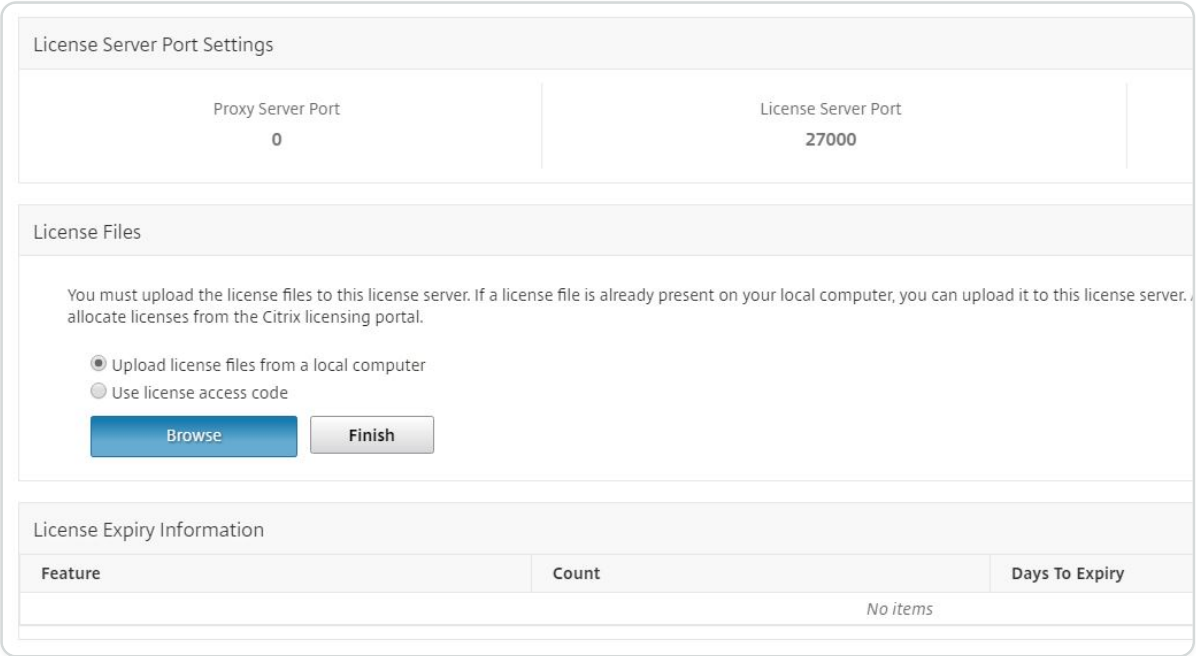
在 NetScaler Console 上安装许可证文件：

1. 在 NetScaler Console 中，导航到 **基础架构 > 池化许可**。
2. 在 **License Files** 部分中，选择以下选项之一：
   a. **从本地计算机上传许可证文件** - 如果许可证文件已存在于您的本地计算机上，您可以将其上传到 NetScaler Console。要添加许可证文件，请单击 **Browse** 并选择要添加的许可证文件 (.lic)。然后单击 **Finish**。
   b. **使用许可证访问代码** - Citrix 会通过电子邮件发送您购买的许可证的许可证访问代码。要添加许可证文件，请在文本框中输入许可证访问代码，然后单击 **Get Licenses**。

   注意

   您可以随时从许可证设置中向 NetScaler Console 添加更多许可证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在 NetScaler Console 中上传 NetScaler VPX 映像

将 NetScaler 映像添加到 NetScaler Console，以便 NetScaler Console 使用服务包中定义的这些映像。

在 NetScaler Console 中上传 NetScaler VPX 映像：

1. 在 NetScaler Console 中，导航到 **编排** \> **SDN 编排** \> **VMware NSX Manager** \> **ESX NSVPX 镜像**。
2. 单击“**Upload**”，然后从本地存储文件夹中选择 NetScaler VPX zip 包。

在 NetScaler Console 中创建服务包

在 NetScaler Console 中创建服务包以定义 SLA 集，其中说明了如何分配 NetScaler 资源。

在 NetScaler Console 中创建服务包：

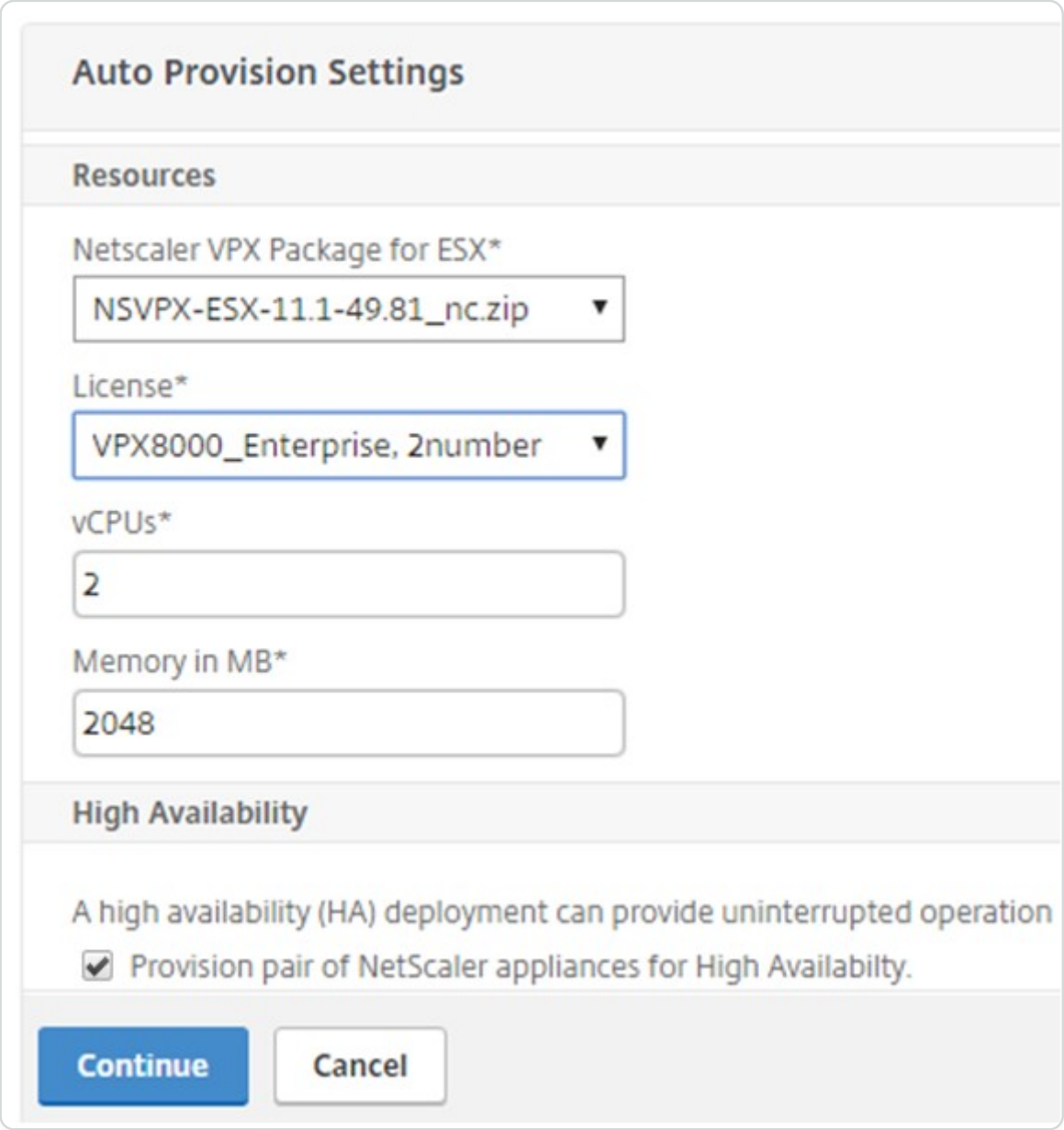
1. 在 NetScaler Console 中，导航到 **Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager** \> **Service Packages**，然后单击“**Add**”以添加新的服务包。
2. 在“**Service Package**”页面上的“**Basic Settings**”部分中，设置以下参数：
   a. 名称 - 服务包的名称
   b. 隔离策略 - 选择“**Dedicated**”
   c. NetScaler 实例预配 - 选择“**Create Instance OnDemand**”
   d. 自动预配平台 - 选择“**CitrixNetScaler SDX**”
   e. 单击“**Continue**”

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在“**自动预配设置**”部分中，选择最近上传的 NetScaler VPX zip 包以将其部署在 NSX 平台上，选择相应的许可证，然后单击“**继续**”。

注意

在“**高可用性**”部分中，选中该复选框以预配用于 HA 的 NetScaler 实例。



注意

上图中列表框中显示的许可证名称 VPX8000_Advanced, 2 number 是一个示例，解释如下：

- VPX - 此许可证用于部署 NetScaler VPX 实例

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 8000 - 可用带宽为 8GB
- Advanced - NetScaler® 提供三种类型的许可证：Standard、Advanced 和 Premium
- 2 number - 可以使用此许可证部署两个 NetScaler VPX 实例

“**许可证**”列表框中显示的许可证名称取决于您从 Citrix 购买的许可证。

4. 单击“**继续**”。
5. 服务包已发布到 NSX Manager。在 NSX Manager 中，导航到“**服务定义**” \> “**服务管理器**”。您可以将 NetScaler Console 视为其中一个服务管理器。这表明注册成功，并且 NSX Manager 与 NetScaler Console 之间建立了双向通信。

> **注意**
>
> 对于高可用性部署中的 NetScaler Console，许可证仅上传到 NetScaler Console 许可证服务器节点。NetScaler Console 节点处于主动-被动模式。

为 Edge 执行负载均衡器服务插入

在现有 NSX Edge Gateway 上执行负载均衡器服务插入，即将负载均衡功能从 NSX 负载均衡器卸载到 NetScaler。

在 NSX Edge Gateway 上插入负载均衡服务：

1. 在 NSX Manager 中，导航到 **主页** \> **网络和安全** \> **NSX Edge**，然后双击选择您已配置的边缘网关。
2. 单击**管理**，然后在**负载均衡器**选项卡上，选择**全局配置**，然后单击**编辑**。
3. 选择**启用负载均衡器**和**启用服务插入**以启用它们。
4. 在**服务定义**中，选择已发布到 NSX Manager 的服务包。
5. 为管理接口配置一个虚拟 NIC，为数据接口配置一个或多个虚拟 NIC。相应地选择管理和数据网络。

> **注意**
>
> 在主 IP 分配模式中选择 IP 池选项。NetScaler Console 不支持手动或 DHCP 分配 IP 地址。

6. 单击刷新图标以查看运行时的创建。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注意**
>
> 由于您在 HA 部署中部署了两个 NetScaler VPX 实例，因此在 NSX Manager 中会创建两个运行时。

您可能需要刷新屏幕才能查看屏幕上显示的运行时。

7. 选择运行时，单击**操作**，然后从弹出菜单中选择**安装**。对于 HA，也对另一个运行时重复此操作。
8. 当两台虚拟机都启动时，Status 的值变为“In Service”，Install State 的值变为“Enabled。”

> **注意**
>
> 您可能需要刷新屏幕才能查看状态更改。

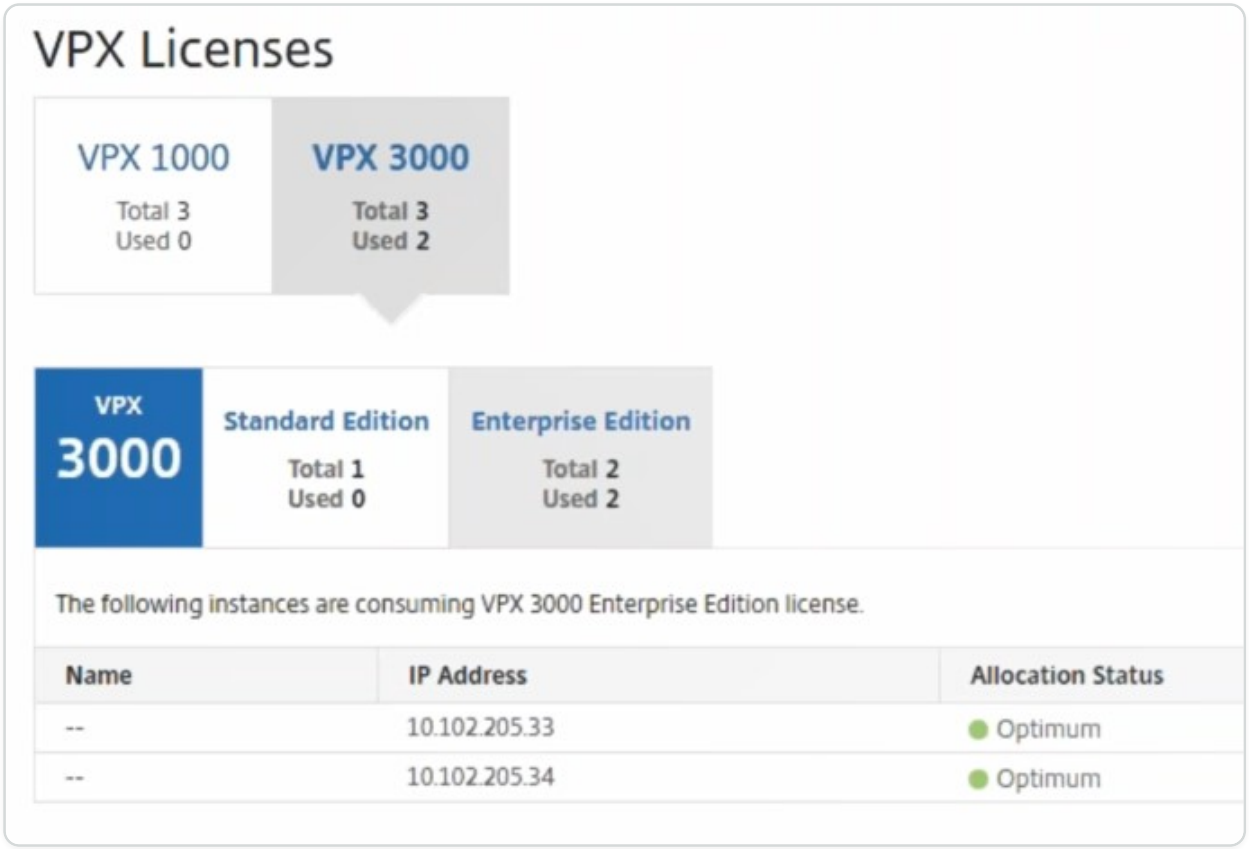
9. 在 NetScaler Console 中，导航到 **Orchestration** \> **Requests** 以查看服务插入完成的进度详细信息。您可以看到一个创建和更新运行时的请求已进入 NetScaler Console。运行时更新后，选择该请求并单击 **Tasks** 按钮，以查看 NetScaler Console 已添加到 NSX Manager 中。

   对于 HA，NetScaler Console 中将有两个请求用于创建和更新两个运行时。当两个运行时都已更新时，选择这两个请求并单击 **Tasks** 按钮，以查看两个 NetScaler Console HA 节点已添加到 NSX Manager 中。
10. 在 NetScaler Console 中，导航到 **Orchestration** \> **SDN Orchestration** \> **VMware NSX Manager** \> **Edge Gateways**。在右侧面板中，您可以看到 NetScaler VPX 已添加到 NSX Edge Gateway。

    对于 HA，您可以看到两个处于 HA 模式的 NetScaler VPX 实例已添加到 NSX Edge Gateway。
11. 在 NetScaler Console 中，导航到 **Infrastructure > Pooled Licensing > VPX Licenses**。选择您已安装的 NetScaler VPX 许可证和版本。

    处于 HA 模式的 NetScaler VPX 实例会消耗两个许可证，状态如下所示显示在屏幕上。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



服务插入完成后，您可以使用 StyleBooks 通过以下两种方法之一配置 NetScaler 实例：

- 在 VMware NSX Manager GUI 中配置 NetScaler VPX 上的负载平衡服务
- 在 NetScaler Console GUI 中配置 NetScaler VPX 上的负载平衡服务

在 VMware NSX Manager GUI 中配置 NetScaler VPX 上的负载平衡服务

执行以下任务，以使用内置 StyleBooks 在 NSX Edge 网关设备上启用负载平衡服务的配置。

在 NSX Manager 中，导航到 **主页** \> **网络和安全** \> **NSX Edge**，然后双击选择您已配置的边缘网关。

创建池和池成员

创建具有不同容量的服务器池和成员。

1. 单击 **管理**，然后在 **负载均衡器** 选项卡上，选择 **池**，然后单击“**+**”图标以添加新池，并设置以下参数：

   a. 名称 - 新池的名称

   b. 算法 - 从下拉列表中选择一个算法，池将根据该算法进行选择。

   c. 监视器 - 确保服务监视器设置为 default_http_monitor

   d. 成员 - 单击“+”将成员添加到池中，并在“新建成员”窗口中输入所需参数。

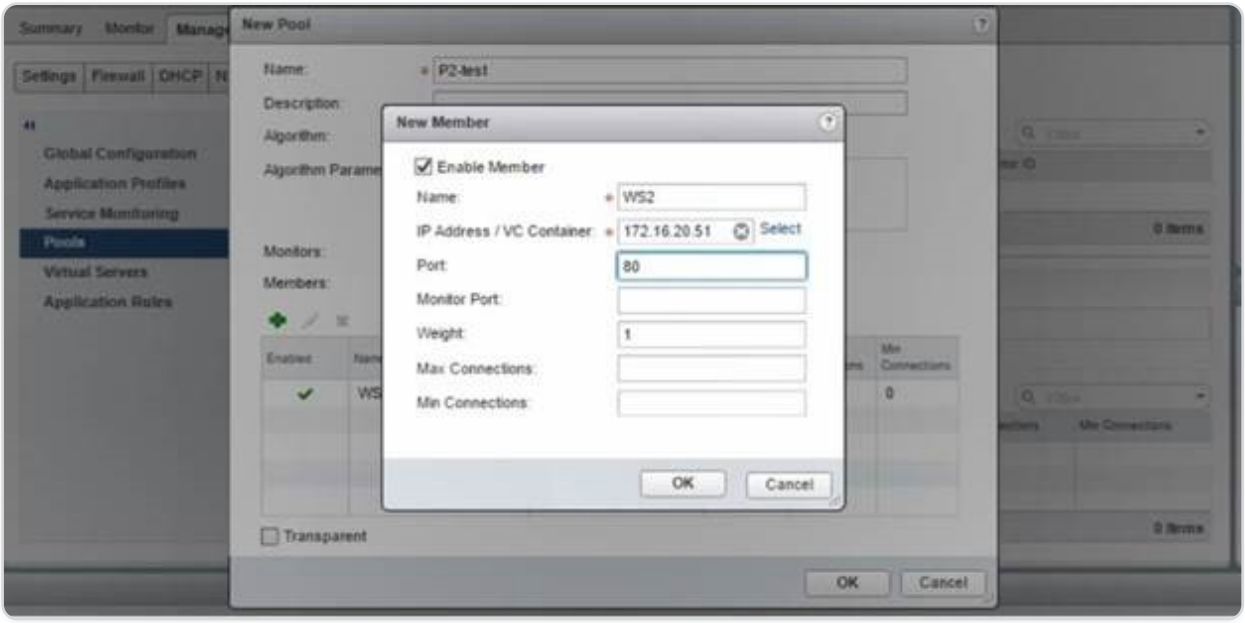
© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. 名称 - 成员的名称

ii. IP 地址/VC 容器 - 单击“选择”从可用列表中选择对象，或输入对象的 IP 地址。

2. 单击 **确定**。

根据需要添加任意数量的成员。



创建虚拟服务器

创建一组虚拟服务器，并为每个虚拟服务器分配一个池。

1. 单击 **管理**，然后在“负载均衡器”选项卡上，选择 **虚拟服务器**，然后单击“**+**”图标以添加虚拟服务器，并设置以下参数：

   a. 应用程序配置文件 - 默认情况下，将显示您在 NetScaler Console 中创建的服务配置文件。

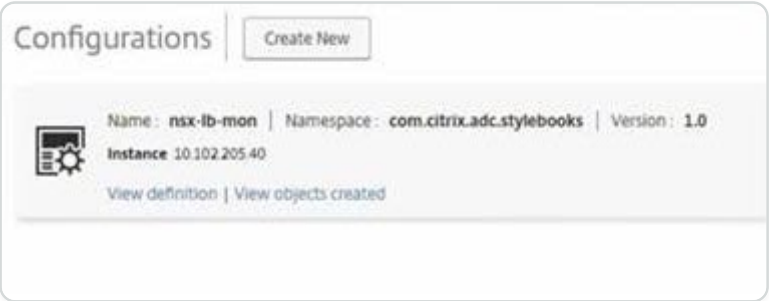
   b. 名称 - 虚拟服务器的名称。

   c. IP 地址 - 单击“选择”以选择现有 IP 地址池或创建新的 IP 地址池。

   d. 默认池 - 从下拉列表中选择默认池。

2. 单击 **确定**。
3. 在 NetScaler Console 中，导航到 **编排** \> **请求** 以查看在一个或多个选定 NetScaler 实例上完成服务创建的进度详细信息。
4. 在 NetScaler Console 中，导航到 **应用程序** \> **配置**，并检查是否已创建 `nsx-lb-mon` 配置包。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在 NetScaler Console GUI 中配置 NetScaler VPX 上的负载均衡服务

使用 NetScaler Console StyleBooks 在 NetScaler 实例上部署负载均衡器配置。对于 HA，配置将部署在处于 HA 模式的两个 NetScaler 实例上。

通过 StyleBooks 创建配置包：

1. 在 NetScaler Console 中，导航到 **应用程序** \> **配置** \> **新建**，然后从列表中选择 **HTTP/SSL 负载均衡（带监视器）StyleBook**。StyleBook 将作为用户界面页面打开，您可以在其中输入此 StyleBook 中定义的所有参数的值。
2. 指定所有必需参数的值。
3. 选择在 NSX 环境中预置的目标 NetScaler VPX 实例，然后单击 **创建** 以将配置应用于所选设备。对于 HA 部署，请选择处于 HA 模式的实例。

验证 NetScaler VPX 实例中虚拟服务器和服务组的创建

您可以登录 NetScaler VPX 实例，查看服务组和虚拟服务器是否已创建。

查看服务组和虚拟服务器：

1. 登录 NetScaler VPX 实例。对于 HA 部署，您必须登录处于 HA 状态的两个 NetScaler 实例。
2. 导航到 **Configuration** \> **System** \> **Networking**。在右侧窗格中，您可以查看已添加的 IP 地址。单击 IP 地址超链接以查看详细信息。您可以看到子网 IP 地址与 NSX 中添加的 Web 界面 IP 地址相同。
3. 接下来，导航到 **Traffic Management** \> **Load Balancing** \> **Virtual Servers** 并查看虚拟服务器详细信息。
4. 接下来，导航到 **Service Groups** 并查看服务组详细信息。
5. 最后，导航到 **Configuration** \> **System** \> **Licenses** 以查看应用于此实例的许可证。

删除负载平衡服务

当 NSX Manager 上部署的 NetScaler VPX 实例不再需要负载平衡服务时，您可以删除之前执行的服务插入。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

删除配置和服务插入：

1. 在 NetScaler Console 中，导航到 **Applications** \> **Configuration**，选择已创建的应用程序配置，然后单击“X”图标删除该配置。
2. 在 NSX Manager 中，导航到 NetScaler VPX 实例连接到的边缘网关。导航到 **Manage** \> **Load Balancer** \> **Global Configuration**，右键单击运行时条目，然后单击 **Unprovision**。虚拟机将停止服务。
3. 在 NetScaler Console 中，导航到 **Orchestration** \> **Cloud Orchestration** \> **Edge Gateways**。确保没有边缘网关到已删除实例的相应映射。

在 NetScaler Console 中管理 Kubernetes Ingress 配置

Kubernetes (K8s) 是一个开源容器编排平台，可自动执行云原生应用程序的部署、扩展和管理。

Kubernetes 提供了 Ingress 功能，允许集群外部的客户端流量访问在 Kubernetes 集群内部运行的应用程序的微服务。NetScaler 实例可以充当在 Kubernetes 集群内部运行的应用程序的 Ingress。NetScaler 实例可以将客户端的南北向流量负载均衡并内容路由到 Kubernetes 集群内部的任何微服务。

注意

- NetScaler Console 支持 Kubernetes 1.14–1.21 版本的集群上的 Ingress 功能。
- NetScaler Console 支持 NetScaler VPX 和 MPX 设备作为 Ingress 设备。
- 在 Kubernetes 环境中，NetScaler 实例仅对“NodePort”服务类型进行负载均衡。

您可以配置多个 NetScaler 实例，使其在同一集群或不同集群或命名空间上充当 Ingress 设备。配置实例后，您可以根据 Ingress 策略将每个实例分配给不同的应用程序。

您可以使用 Kubernetes `kubectl` 或 API 创建和部署 Ingress 配置。您也可以从 NetScaler Console 配置和部署 Ingress。

您可以在 NetScaler Console 中指定 Kubernetes 集成的以下方面：

- **集群** – 您可以注册或注销 NetScaler Console 可以部署 Ingress 配置的 Kubernetes 集群。在 NetScaler Console 中注册集群时，请指定 Kubernetes API 服务器信息。然后，选择一个可以访问 Kubernetes 集群并部署 Ingress 配置的代理。
- **策略** – Ingress 策略用于根据集群或命名空间选择 NetScaler 实例以部署 Ingress 配置。添加策略时，请指定集群、站点和实例信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

开始之前

要将 NetScaler 实例用作 Kubernetes 集群上的 Ingress 设备，请确保您已具备：

- 已部署 Kubernetes 集群。
- 在 NetScaler Console 中注册的 Kubernetes 集群。

使用秘密令牌配置 NetScaler Console 以管理 Kubernetes 集群

为了让 NetScaler Console 能够从 Kubernetes 接收事件，您需要在 Kubernetes 中为 NetScaler Console 创建一个服务帐户。并且，在集群中为该服务帐户配置必要的 RBAC 权限。

1. 为 NetScaler Console 创建一个服务帐户。例如，服务帐户名称可以是 `citrixadm-sa`。要创建服务帐户，请参阅 使用多个服务帐户。
2. 使用 `cluster-admin` 角色绑定 NetScaler Console 服务帐户。此绑定将 `ClusterRole` 授予集群中的服务帐户。以下是将 `cluster-admin` 角色绑定到服务帐户的示例命令。

   ```
   kubectl create clusterrolebinding citrixadm-sa-admin --
   clusterrole=cluster-admin --serviceaccount=default:citrixadm-sa
   ```

   将 NetScaler Console 服务帐户绑定到 `cluster-admin` 角色后，该服务帐户将具有集群范围的访问权限。有关更多信息，请参阅 `kubectl` 创建 `clusterrolebinding`。
3. 从创建的服务帐户中获取令牌。

   例如，运行以下命令查看 `citrixadm-sa` 服务帐户的令牌：

   ```
   kubectl describe sa citrixadm-sa
   ```

4. 运行以下命令获取令牌的秘密字符串：

   ```
   kubectl describe secret <token-name>
   ```

在 NetScaler Console 中添加 Kubernetes 集群

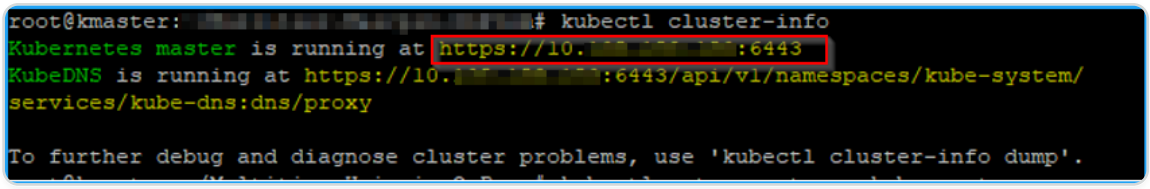
配置 NetScaler 代理并配置静态路由后，您必须在 NetScaler Console 中注册 Kubernetes 集群。

要注册 Kubernetes 集群：

1. 使用管理员凭据登录 NetScaler Console。
2. 导航到 **Orchestration** > **Kubernetes** > **Cluster**。 将显示“集群”页面。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 单击 **Add**。
4. 在“**添加集群**”页面中，指定以下参数：
   a. **名称** - 指定一个您选择的名称。
   b. **API 服务器 URL** - 您可以从 Kubernetes 主节点获取 API 服务器 URL 详细信息。
      i. 在 Kubernetes 主节点上，运行命令 `kubectl cluster-info`。



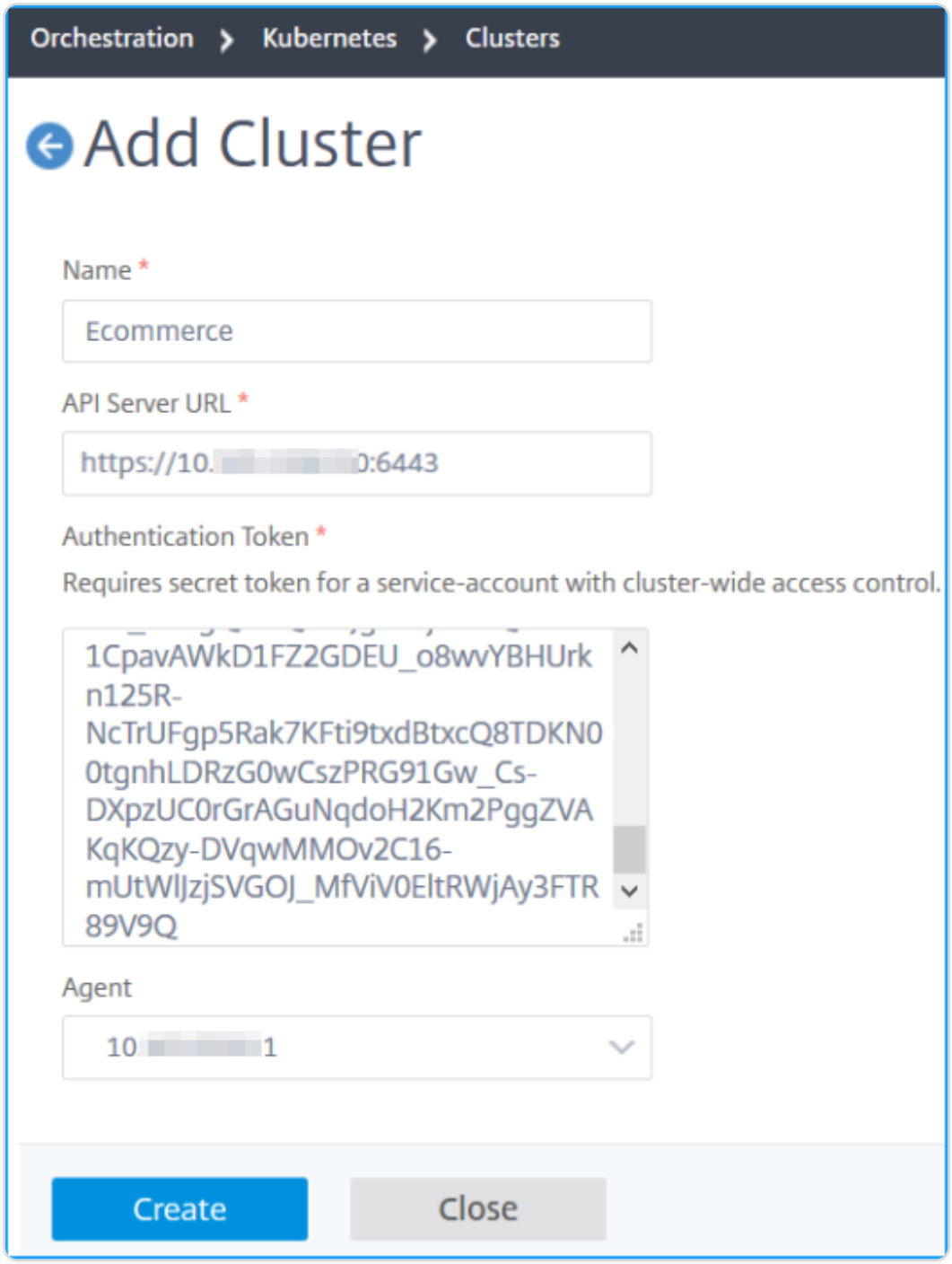
      ii. 输入显示为 **“Kubernetes master 正在运行于。”** 的 URL。
   c. **身份验证令牌** - 指定在您配置 NetScaler Console 以管理 Kubernetes 集群时获得的身份验证令牌字符串。身份验证令牌是验证 Kubernetes 集群与 NetScaler Console 之间通信访问所需的。要生成身份验证令牌：
      i. 在 Kubernetes 主节点上，运行以下命令：

```
kubectl describe secret <token-name>
```

      ii. 复制生成的令牌并将其粘贴为身份验证令牌

      有关更多信息，请参阅 Kubernetes 文档。
   d. 从列表中选择代理。
   e. 单击“**创建**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

设置

NetScaler Console 提供了一些设置，可帮助您配置和集成部署以满足您的基础架构需求。以下主题可帮助您配置这些设置：

- 配置 IPAM
- 配置操作策略
- 可观测性集成
- 配置访问控制列表
- 使用 NetScaler Console 日志消息管理和监控您的基础架构

配置 IP 地址管理 (IPAM)

NetScaler Console IPAM 允许您在 NetScaler Console 管理的配置中自动分配和释放 IP 地址。您可以从使用以下 IP 提供程序定义的网络或 IP 范围分配 IP：

- NetScaler Console 内置 IPAM 提供程序。
- Infoblox IPAM 解决方案。

您可以在以下场景中使用 NetScaler Console IPAM：

- **StyleBooks**：在创建配置时自动分配 IP 到虚拟服务器。
- **API 网关**：自动分配 IP 地址到 API 代理。

您还可以跟踪 NetScaler Console 管理的每个网络或 IP 范围中的 IP 地址。

添加外部 IP 地址提供程序

NetScaler Console 具有内置 IPAM 提供程序，用于管理 IP 和 IP 范围。您还可以将外部 IP 地址提供程序集成到 NetScaler Console。

重要提示：

在开始之前，请确保在外部 IP 地址提供程序中启用了以下权限：

- 查询提供程序中存在的网络的能力。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在网络中保留 IP 地址。
- 从网络中释放 IP 地址。
- 从网络中检索已使用的 IP 地址。
- 从网络中检索可用的 IP 地址。

在 NetScaler Console 中执行以下步骤以添加外部 IPAM 提供程序解决方案：

1. 导航到 **设置 > IPAM**。
2. 在 **提供程序** 中，单击 **添加**。
3. 指定以下详细信息以添加 IPAM 提供程序：
   - **名称** - 指定要在 NetScaler Console 中使用的 IP 提供程序名称。
   - **供应商** - 从列表中选择一个 IPAM 供应商。
   - **URL** - 指定在 NetScaler Console 环境中分配 IP 地址的 IPAM 解决方案的 URL。请确保以以下格式指定 URL：

     ```
     https://<host name>
     ```

     示例：`https://myinfoblox.example.com`
   - **是否为私有端点？** - 如果 Infoblox DDI 是私有托管的，请选中此复选框，然后选择一个代理。
   - **用户名** - 指定用于登录 IPAM 解决方案的用户名。
   - **密码** - 指定用于登录 IPAM 解决方案的密码。
4. 单击 **添加**。

将 Infoblox DDI 作为外部提供程序

目前，NetScaler® Console 支持 Infoblox DDI 作为外部提供商。Infoblox DDI 可以公开访问，也可以私有托管，仅在企业内部网络中可访问。对于私有托管的 Infoblox DDI，您必须在配置过程中选择一个 NetScaler 代理。NetScaler 代理充当代理，用于访问位于企业内网中的提供商。

您可以将 NetScaler Console IPAM 与 Infoblox 提供商结合使用，执行以下操作：

- 列出 IPAM 网络
- 创建、更新和删除 IPAM 网络
- 从 IPAM 网络中预留和释放 IP 地址

© 1997–2026 Citrix Systems, Inc. All rights reserved.

创建 IPAM 网络

要使用 Infoblox 提供商创建 NetScaler Console IPAM 网络，Infoblox 上必须存在具有相同 CIDR IP 范围的网络。

当您在 NetScaler Console 中创建 IPAM 网络时，您只是在 Console 中注册 Infoblox 网络的使用。然后，NetScaler Console 与 Infoblox 协同工作，管理从该网络分配的 IP 地址。Infoblox 网络可以继续在 NetScaler Console 之外使用。

同样，如果您删除 NetScaler Console IPAM 网络，NetScaler Console 将取消注册 Infoblox 网络。这意味着 NetScaler Console 不再与 Infoblox 交互以管理该网络中的 IP 地址。

Infoblox DDI 应用程序接口

NetScaler Console IPAM 使用以下 Infoblox API 执行相应的操作：

- (/network) - 列出所有可用的 Infoblox 网络
- (/network?network={id}) - 检索特定 Infoblox 网络的详细信息
- (/ipv4address) - 列出 Infoblox 网络上的所有 IP
- (/record:host) - 检索特定 IP 地址的详细信息
- (/{IP}) - 在 Infoblox 网络上预留和释放 IP

有关 Infoblox API 的更多信息，请参阅 Infoblox DDI 提供的 Infoblox REST API 参考指南。

添加网络

添加网络以将 IPAM 与 NetScaler Console 管理的配置结合使用。

1. 导航到 **设置 > IPAM**。
2. 在 **网络** 下，单击 **添加**。
3. 指定以下详细信息：
   - **网络名称** - 指定网络名称以在 NetScaler Console 中识别网络。
   - **提供商** - 从列表中选择提供商。

     此列表显示在 NetScaler Console 中添加的提供商。
   - **网络类型** - 根据您的要求从列表中选择 **IP 范围** 或 **CIDR**。
   - **网络值** - 指定网络值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **注意：**
>
> NetScaler Console IPAM 仅支持 IPv4 地址。

对于 **IP 范围**，请按以下格式指定网络值：

```
<first-IP-address>-<last-IP-address>
```

示例：

```
10.0.0.20-10.0.0.100
```

CIDR，请按以下格式指定网络值：

```
<IP-address>/<subnet-mask>
```

示例：

```
10.70.124.0/24
```

4. 点击 **创建**。

查看已分配的 IP 地址

要查看来自 IPAM 网络的已分配 IP 地址的更多详细信息，请执行以下步骤：

1. 导航到 **设置 > IPAM**。
2. 在 **网络** 选项卡下，点击 **查看所有已分配的 IP**。

   此窗格显示 IP 地址、提供商名称、提供商供应商和描述。它还显示保留此 IP 地址的资源详细信息：

   - **模块**：显示保留 IP 地址的 NetScaler Console 模块。例如，如果 StyleBooks 保留了 IP 地址，则此列将 StyleBooks 显示为模块。
   - **资源类型**：显示该模块中的资源类型。对于 StyleBooks 模块，只有配置资源类型使用 IPAM 网络。因此，它在此列下显示“配置”。
   - **资源 ID**：显示带有链接的确切资源 ID。点击此链接可访问正在使用 IP 地址的资源。对于配置资源类型，它将配置包 ID 显示为资源 ID。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

如果要释放 IP 地址，请选择要释放的 IP 地址，然后点击 **释放已分配的 IP**。

配置操作策略以接收应用程序事件通知

除了现有的应用程序事件分析视图之外，您还可以配置操作策略，通过 Slack、电子邮件、PagerDuty 或 ServiceNow 接收应用程序事件通知。应用程序事件包括性能问题、机器人和 WAF 违规以及服务图违规。作为管理员，您可以使用操作策略实时获取事件通知。

使用操作策略，您可以：

- 为应用程序事件预定义特定条件。
- 通过 Slack、电子邮件、PagerDuty 和 ServiceNow 接收以下事件的通知：

事件类别	事件子类别	事件
安全违规	所有安全违规	所有机器人违规（有关机器人违规列表的更多信息，请参阅 违规类别）。
		所有 WAF 违规（WAF SQL 违规、WAF XSS 违规和 WAF 推断 XML 违规）
	每个客户端的所有安全违规	每个客户端的机器人违规
		每个客户端的 WAF 违规
		注意： 要接收 WAF 违规通知，最低违规事务数必须为 20%。例如，在 100 个事务中，至少 20 个必须是违规事务。
应用程序性能		应用程序分数违规
		客户端网络延迟
		服务器网络延迟
		服务器处理时间

© 1997–2026 Citrix Systems, Inc. All rights reserved.

事件类别	事件子类别	事件
		响应时间
		请求
		带宽
		服务图违规
应用程序使用情况		每秒请求数
		吞吐量
		数据量

配置操作策略

1. 导航到 **设置 > 操作 > 操作策略**。
2. 单击 **添加**。
3. 在 **创建操作策略** 页面中：
   a. **策略名称** – 提供您选择的策略名称。
   b. **已启用** – 此选项默认处于选中状态。
   c. 如果 **发生以下事件** – 从列表中选择一个事件。
   d. **并且满足以下条件** – 从列表中选择以定义您希望收到通知的条件。您可以单击 **+** 添加更多条件。要删除条件，请单击 **–**。

   您可以使用以下运算符配置操作策略。运算符根据您选择的条件显示。

运算符	描述
等于	等于定义的值
不等于	不等于定义的值
大于	大于定义值
大于或等于	大于或等于定义值
小于	小于定义值

© 1997–2026 Citrix Systems, Inc. All rights reserved.

运算符	描述
小于或等于	小于或等于定义值
包含	包含定义的术语或值
开头是	开头是定义的术语或值
结尾是	结尾是定义的术语或值
属于	允许选择多个值

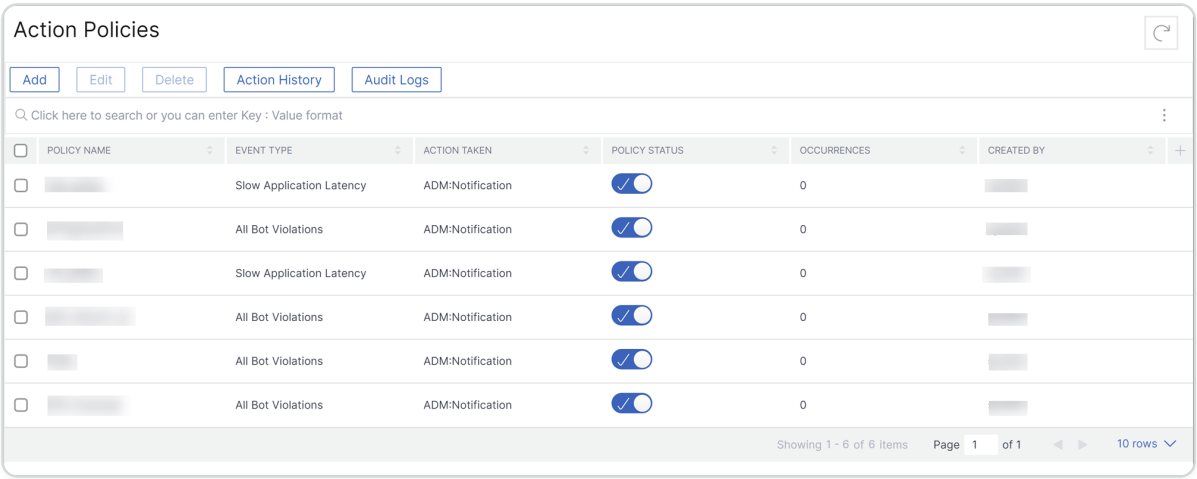
e. **然后执行以下操作** – 选择 **通知**。选择 **通知** 后，将显示“通知类型”选项。

f. **通知类型** – 选择通知类型：电子邮件、Slack、PagerDuty 或 ServiceNow。根据您选择的通知类型，将显示相应的选项（分发列表、Slack 配置文件、PagerDuty 配置文件或 ServiceNow 配置文件）。从列表中选择一个配置文件。

   如果要创建新配置文件，请单击 **添加**。

g. 单击 **创建策略**。

   策略已配置。您可以查看已配置的策略详细信息。



   配置策略后，您可以选择该策略并单击：

   - **编辑** 以更新或更改操作策略。更新后，单击“更新策略”。
   - **删除** 以删除操作策略。您可以选择多个策略，然后单击 **删除** 以将其删除。
   - **操作历史记录** 以查看时间、采取的操作、策略名称、警报类型和警报消息等详细信息。

下表描述了操作策略配置的详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

违规名称	条件	描述
所有安全违规	实例 IP	NetScaler 实例的 IP 地址。从列表中选择 IP 地址。
	违规计数	您希望收到通知的违规计数。例如，如果您将违规计数配置为小于或等于 10，则当收到 10 个或更少的机器人违规事务时，您将收到通知。
	违规比率	此值表示特定事务的总违规数，该值必须介于 0 和 1 之间。例如，在 100 个事务中，有 20 个是违规，如果您希望收到此类情况的通知，则必须输入 0.2。
所有机器人违规	机器人配置文件	用于在 NetScaler 实例上配置机器人管理的机器人配置文件名称。
	实例 IP	NetScaler 实例的 IP 地址。从列表中选择 IP 地址。
	违规计数	您希望收到通知的违规计数。例如，如果您将违规计数配置为小于或等于 10，则当收到 10 个或更少的机器人违规事务时，您将收到通知。
	违规比率	此值表示特定事务的总违规数，该值必须介于 0 和 1 之间。例如，在 100 个事务中，有 20 个是违规，如果您希望收到此类情况的通知，则必须输入 0.2。
所有 WAF 违规、WAF SQL 违规、WAF XSS 违规、WAF 推断 XML 违规	WAF 配置文件	用于在 NetScaler 实例上配置 WAF 安全设置的 WAF 配置文件名称。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

违规名称	条件	描述
	实例 IP	NetScaler 实例的 IP 地址。从列表中选择 IP 地址。
	违规计数	您希望收到通知的违规计数。WAF 违规收到通知的最低要求是 20%。
	违规比率	此值表示特定事务中的总违规数，该值必须介于 0 和 1 之间。例如，在 100 个事务中，有 20 个是 WAF SQL 违规事务，如果您希望收到此类情况的通知，则必须输入 0.2。
每个客户端的所有安全违规	应用程序名称	自定义应用程序名称。从列表中选择应用程序。如果您不添加此条件，则会考虑 NetScaler 实例中的所有应用程序。
	实例 IP	NetScaler 实例的 IP 地址。从列表中选择 IP 地址。
	客户端 IP	Bot 的来源。指定 IP 地址。
	总攻击次数	您希望收到通知的总攻击次数。
	请求 URL	您要配置为阻止的 URL。指定 URL。
	虚拟服务器名称	为自定义应用程序配置的关联应用程序。从列表中选择应用程序。如果您不添加此条件，则会考虑 NetScaler 实例中的所有应用程序。
每个客户端的 Bot 违规	应用程序名称	自定义应用程序名称。从列表中选择应用程序。如果您不添加此条件，则会考虑

© 1997–2026 Citrix Systems, Inc. All rights reserved.

违规名称	条件	描述
		NetScaler 实例中的所有应用程序。
	实例 IP	NetScaler 实例的 IP 地址。从列表中选择 IP 地址。
	客户端 IP	Bot 的来源。指定 IP 地址。
	总攻击次数	您希望收到通知的攻击总数。
	违规类型	从列表中选择机器人违规。
	请求 URL	您要配置为阻止的 URL。指定 URL。
	虚拟服务器名称	为自定义应用程序配置的关联应用程序。从列表中选择应用程序。如果您不添加此条件，则会考虑 NetScaler 实例中的所有应用程序。
每个客户端的 WAF 违规	应用程序名称	自定义应用程序名称。从列表中选择应用程序。如果您不添加此条件，则会考虑 NetScaler 实例中的所有应用程序。
	实例 IP	NetScaler 实例的 IP 地址。从列表中选择 IP 地址。
	客户端 IP	机器人来源。指定 IP 地址。
	攻击总数	您希望收到通知的总攻击次数。
	违规类型	从列表中选择 WAF 违规。
	请求 URL	您要配置以阻止的 URL。指定该 URL。
	虚拟服务器名称	为自定义应用程序配置的关联应用程序。从列表中选择应用

© 1997–2026 Citrix Systems, Inc. All rights reserved.

违规名称	条件	描述
		程序。如果您不添加此条件，则会考虑 NetScaler 实例中的所有应用程序。
应用程序评分违规	性能指标	应用程序评分组件及其阈值。从列表中选择应用程序评分组件。有关详细信息，请参阅选择应用程序评分组件并设置阈值。
	违规计数	您希望收到通知的违规计数。例如，如果您将响应时间的违规计数配置为等于 5，则当响应时间阈值被突破 5 次时，您将收到通知。
	应用程序名称	单击**选择应用程序**以选择您希望收到违规通知的应用程序。
客户端网络延迟	客户端网络平均延迟	指定您希望收到通知的客户端延迟（客户端到 NetScaler）值（以毫秒为单位）。
	客户端网络延迟异常	指定您希望收到通知的网络延迟异常计数。
	应用程序名称	单击 **选择应用程序** 以选择您希望收到违规通知的应用程序。
服务器网络延迟	服务器网络平均延迟	指定您希望收到通知的服务器延迟（服务器到 NetScaler）值（以毫秒为单位）。
	服务器网络延迟异常	指定您希望收到通知的网络延迟异常计数。
	应用程序名称	单击 **选择应用程序** 以选择您希望收到违规通知的应用程序。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

违规名称	条件	描述
响应时间	平均响应时间	指定您希望收到通知的值（以毫秒为单位）。
	响应平均时间异常	指定您希望收到通知的异常计数。
	应用程序名称	单击 **选择应用程序** 以选择您希望收到通知的应用程序。如果您未选择任何应用程序，则此设置将应用于所有应用程序。
请求	总请求数	指定您希望收到通知的总请求数。
	应用程序名称	单击 **选择应用程序** 以选择您希望收到通知的应用程序。如果您未选择任何应用程序，则此设置将应用于所有应用程序。
带宽	总带宽	指定您希望收到通知的带宽（MB）。
	应用程序名称	单击 **选择应用程序** 以选择您希望收到通知的应用程序。如果您未选择任何应用程序，则此设置将应用于所有应用程序。
服务器处理时间	服务器平均处理时间	指定您希望收到通知的服务器处理（服务器到 NetScaler）毫秒值。
	服务器处理时间异常	指定您希望收到通知的服务器处理时间异常计数。
	应用程序名称	单击 **选择应用程序** 以选择您希望收到违规通知的应用程序。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

违规名称	条件	描述
服务图违规		违反已配置阈值的微服务。有关详细信息，请参阅在服务图中配置阈值。
每秒请求数	每秒请求数平均值	应用程序每秒收到的请求数。指定平均值以接收通知。
	每秒请求数平均异常	指定您希望收到通知的平均异常计数。
		注意： 如果您正在为此事件使用 AND 条件，则可以配置“每秒请求数平均值”和“应用程序名称”，或者配置“每秒请求数异常平均值”和“应用程序名称”。
	应用程序名称	单击 **选择应用程序** 以选择您希望收到违规通知的应用程序。
吞吐量	平均吞吐量	特定时期内传输的总数据。指定平均值（以 MB 为单位）以接收通知。
	平均吞吐量异常	指定您希望收到通知的平均异常计数。
		注意： 如果您为此事件使用 AND 条件，则可以配置平均吞吐量和应用程序名称，或者平均吞吐量异常和应用程序名称。
	应用程序名称	单击 **选择应用程序** 以选择您希望收到违规通知的应用程序。
数据量	总数据量	在特定持续时间内要传输的总数据。指定值（以 MB 为单位）以接收通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

违规名称	条件	描述
	数据量异常	指定您希望收到通知的异常计数。
		注意： 如果此事件使用 AND 条件，您可以配置“总数据量和应用程序名称”或“数据量异常和应用程序名称”。
	应用程序名称	单击 **选择应用程序** 以选择您希望收到违规通知的应用程序。

使用搜索栏

搜索栏可让您筛选结果。单击搜索栏时，它会为您提供搜索建议列表。您可以选择组件并根据您的要求筛选结果。

使用审计日志选项

单击 **审计日志** 并从列表中选择持续时间，以查看在所选持续时间内创建、修改和删除的操作策略，然后单击 **搜索**。

注意

数据存储策略预计将在即将发布的版本中发生变化。随着这些变化，数据超出存储限制后将无法存储历史数据。目前，建议增加存储空间或将存储空间保持在许可证授权限制内。

可观测性集成

由于现代应用程序日益增长的复杂性，管理员面临以下挑战：

- 监控和故障排除应用程序。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 深入了解基础架构和应用程序的行为。

可观测性通过提供对整个基础架构的这些洞察来弥合这一差距。使用 NetScaler Console 中的可观测性集成功能，您可以：

- 将 NetScaler Console 与 Splunk 集成。
- 将 NetScaler Console 与 New Relic 集成。
- 配置 NetScaler 实例以使用默认架构将洞察导出到 Prometheus。

与 Splunk 集成

您现在可以将 NetScaler Console 与 Splunk 集成，以查看以下分析数据：

- WAF 违规
- Bot 违规
- SSL 证书洞察
- 网关洞察
- 事件和指标
- HDX™ 洞察
- NetScaler® Console 审计日志

Splunk 附加组件使您能够：

- 组合所有其他外部数据源。
- 在一个集中位置提供更清晰的分析可见性。

NetScaler Console 定期收集 Bot、WAF、SSL 事件，并将其发送到 Splunk。Splunk 通用信息模型 (CIM) 附加组件将事件转换为 CIM 兼容数据。作为管理员，您可以使用 CIM 兼容数据在 Splunk 控制面板中查看事件。

要成功集成，您必须：

- 配置 Splunk 以接收来自 NetScaler Console 的数据
- 配置 NetScaler Console 以将数据导出到 Splunk
- 在 Splunk 中查看仪表板

配置 Splunk 以从本地 NetScaler Console 接收数据

在 Splunk 中，您必须：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

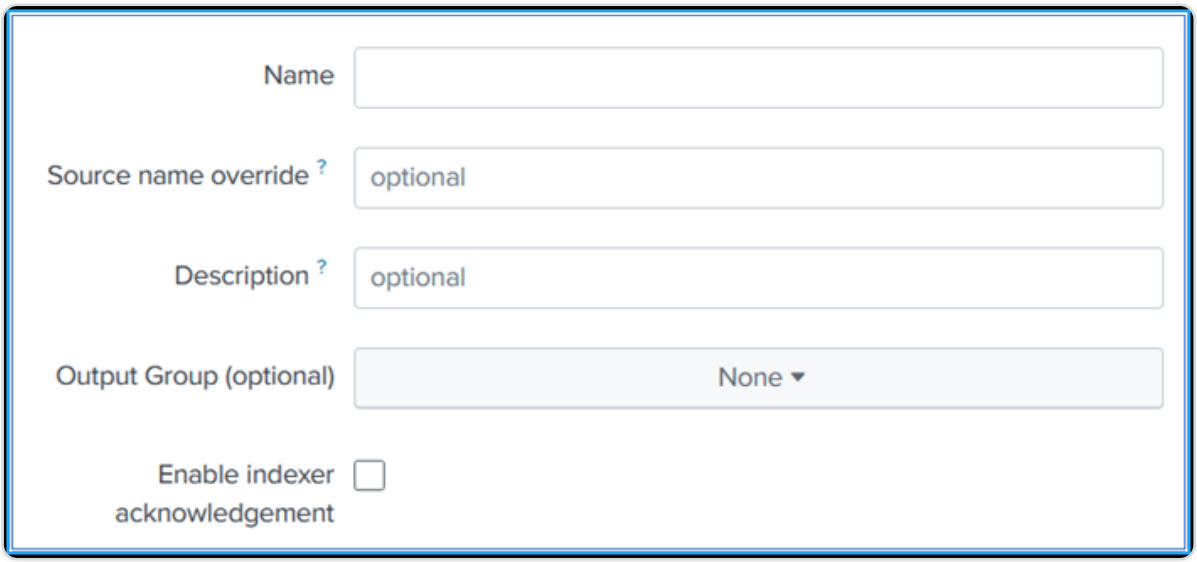
1. 设置 Splunk HTTP 事件收集器端点并生成令牌
2. 安装 Splunk 通用信息模型 (CIM) 附加组件
3. 安装 CIM 规范化器（仅适用于 WAF 和机器人洞察）
4. 在 Splunk 中准备一个示例仪表板

设置 Splunk HTTP 事件收集器端点并生成令牌

您必须首先在 Splunk 中设置 HTTP 事件收集器。此设置可实现 NetScaler Console 和 Splunk 之间的数据发送集成。接下来，您必须在 Splunk 中生成一个令牌，以便：

- 启用 NetScaler Console 和 Splunk 之间的身份验证。
- 通过事件收集器端点接收数据。

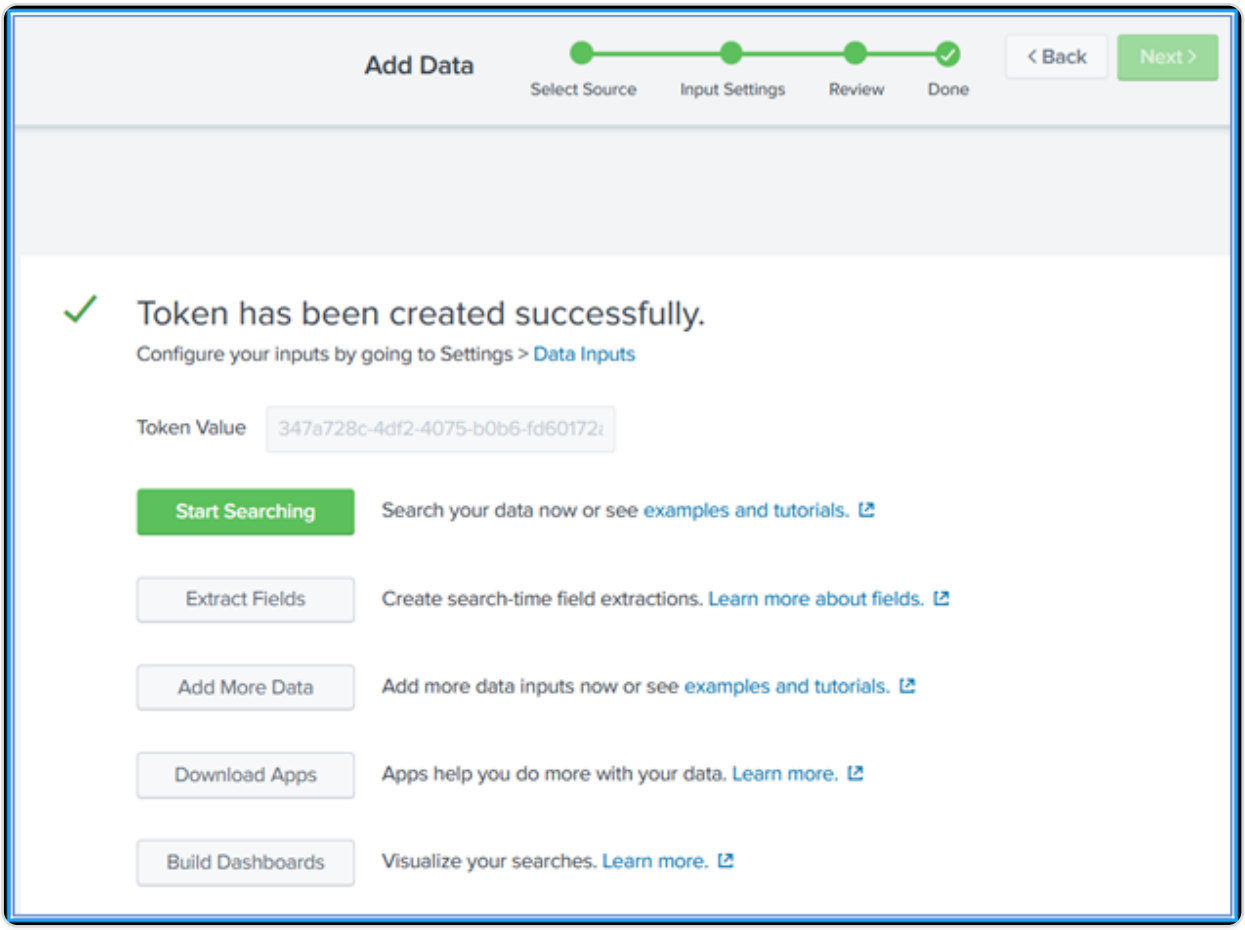
1. 登录 Splunk。
2. 导航到 **Settings > Data Inputs > HTTP event collector**，然后单击 **Add new**。
3. 指定以下参数：
   a. **名称**：指定一个您选择的名称。
   b. **源名称覆盖（可选）**：如果您设置了一个值，它将覆盖 HTTP 事件收集器的源值。
   c. **描述（可选）**：指定一个描述。
   d. **输出组（可选）**：默认情况下，此选项选择为“无”。
   e. **启用索引器确认**：NetScaler Console 不支持此选项。我们建议不要选择此选项。



4. 单击 **下一步**。
5. 您可以选择在 **输入设置** 页面中设置其他输入参数。
6. 单击 **审查** 以验证条目，然后单击 **提交**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

将生成一个令牌。在 NetScaler Console 中添加详细信息时，您必须使用此令牌。



安装 Splunk 通用信息模型

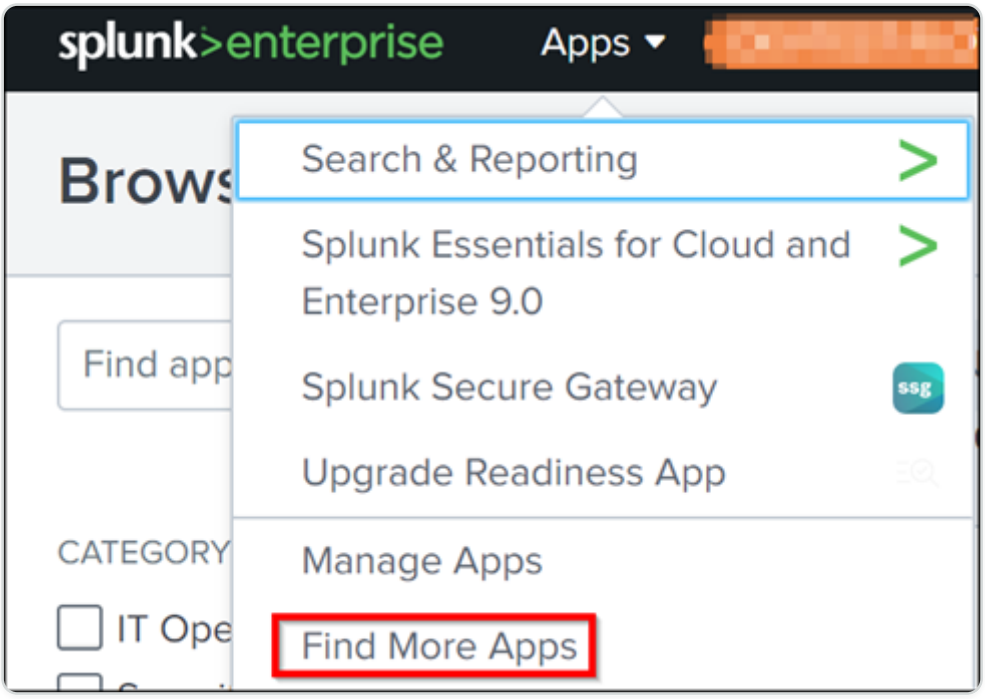
在 Splunk 中，您必须安装 Splunk CIM 附加组件。此附加组件可确保从 NetScaler Console 接收的数据能够规范化摄取的数据，并使用相同的字段名称和事件标签来匹配等效事件的通用标准。

注意

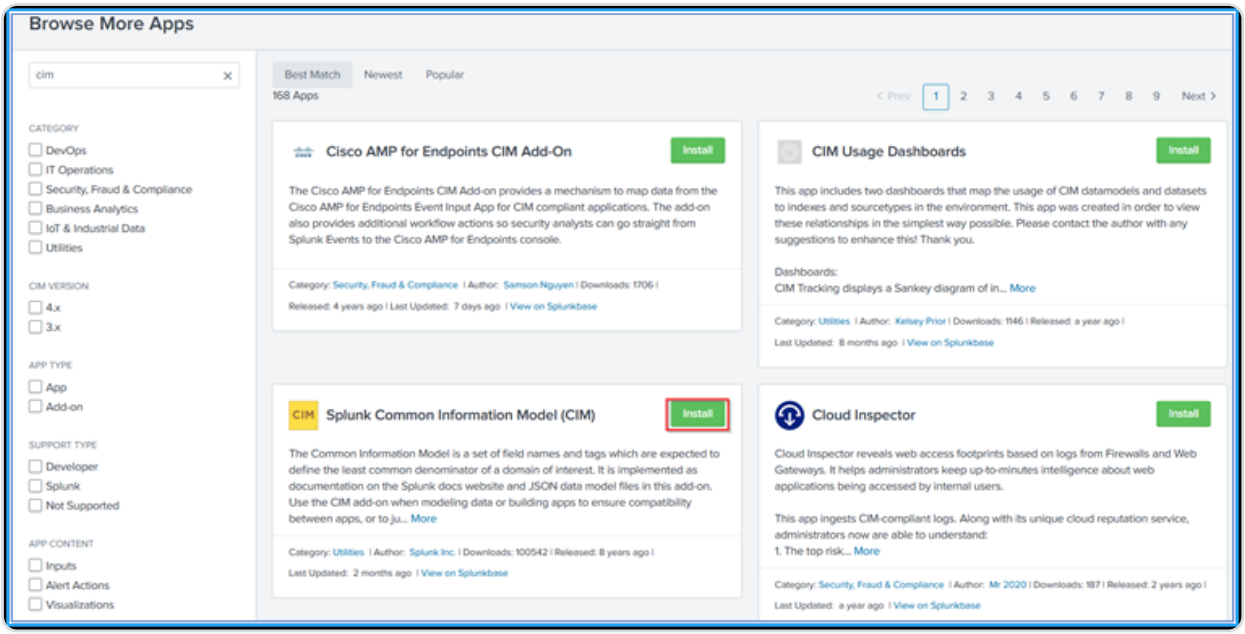
如果您已安装 Splunk CIM 附加组件，则可以忽略此步骤。

1. 登录 Splunk。
2. 导航到 **Apps > Find More Apps**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 在搜索栏中键入 **CIM**，然后按 **Enter** 获取 **Splunk Common Information Model (CIM)** 附加组件，然后单击 **Install**。

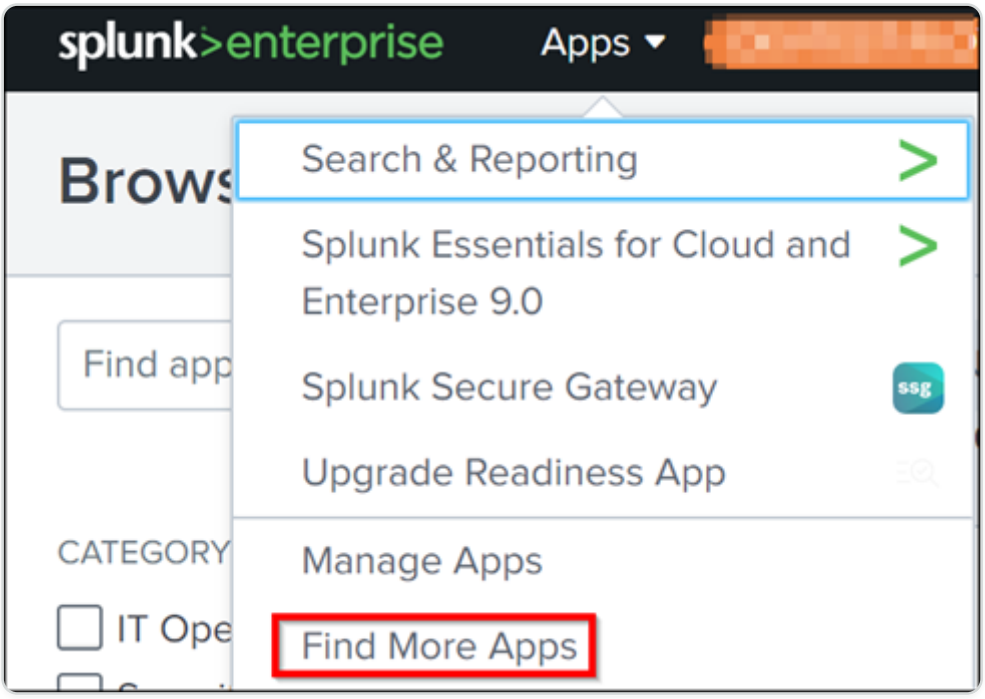


安装 CIM 规范器

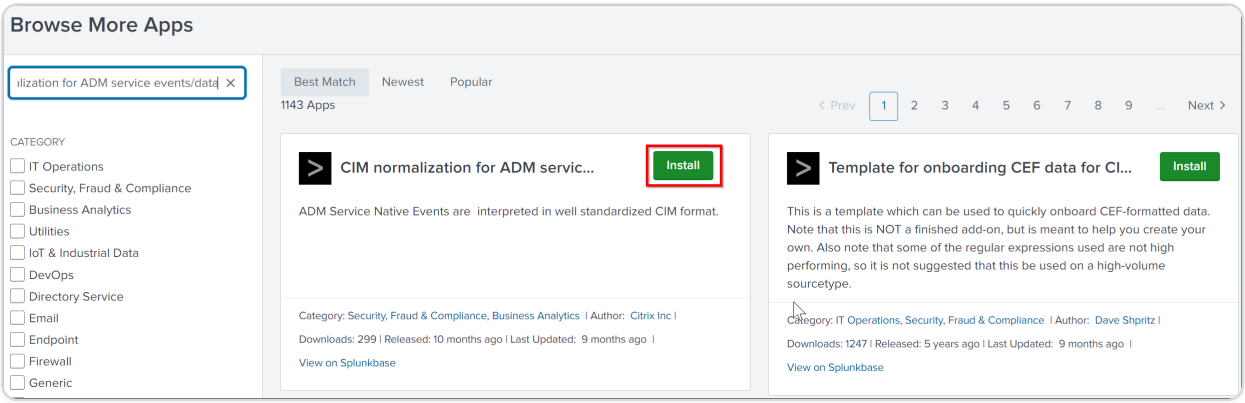
CIM 规范器是一个附加插件，您必须安装它才能在 Splunk 中查看 WAF 和机器人洞察。

1. 在 Splunk 门户中，导航到 **Apps > Find More Apps**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. 在搜索栏中键入 **CIM normalization for NetScaler Console service events/data**，然后按 **Enter** 获取附加组件，然后单击 **Install**。



在 Splunk 中准备一个示例仪表板

安装 Splunk CIM 后，您必须使用 WAF 和 Bot、SSL 证书洞察以及事件和指标的模板准备一个示例仪表板。您可以下载仪表板模板 (`.tgz`) 文件，使用任何编辑器（例如记事本）复制其内容，然后通过将数据粘贴到 Splunk 中来创建仪表板。

注意：

以下创建示例仪表板的步骤适用于所有用例。您必须使用所需的 `json` 文件。

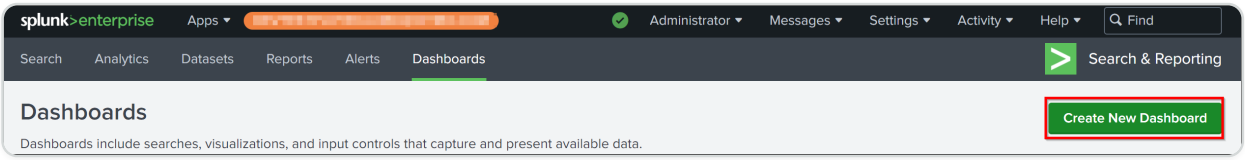
1. 登录 Citrix 下载页面，下载 Sample Dashboards for 3rd party Endpoints 下提供的示例仪表板。
2. 解压文件，使用任意编辑器打开 `json` 文件，并从文件中复制数据。

   解压后，您将获得三个 `json` 文件。使用：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `adm_splunk_security_violations.json` 文件创建 WAF 和 Bot 示例仪表板。
- `adm_splunk_ssl_certificate.json` 文件创建 SSL 证书洞察示例仪表板。
- `adm_splunk_events_and_metrics_history.json` 文件创建 NetScaler Console 事件和指标仪表板。

3. 在 Splunk 门户中，导航到 **Search & Reporting > Dashboards**，然后单击 **Create New Dashboard**。



4. 在 **Create New Dashboard** 页面中，指定以下参数：

   a. **仪表板标题** - 提供您选择的标题。

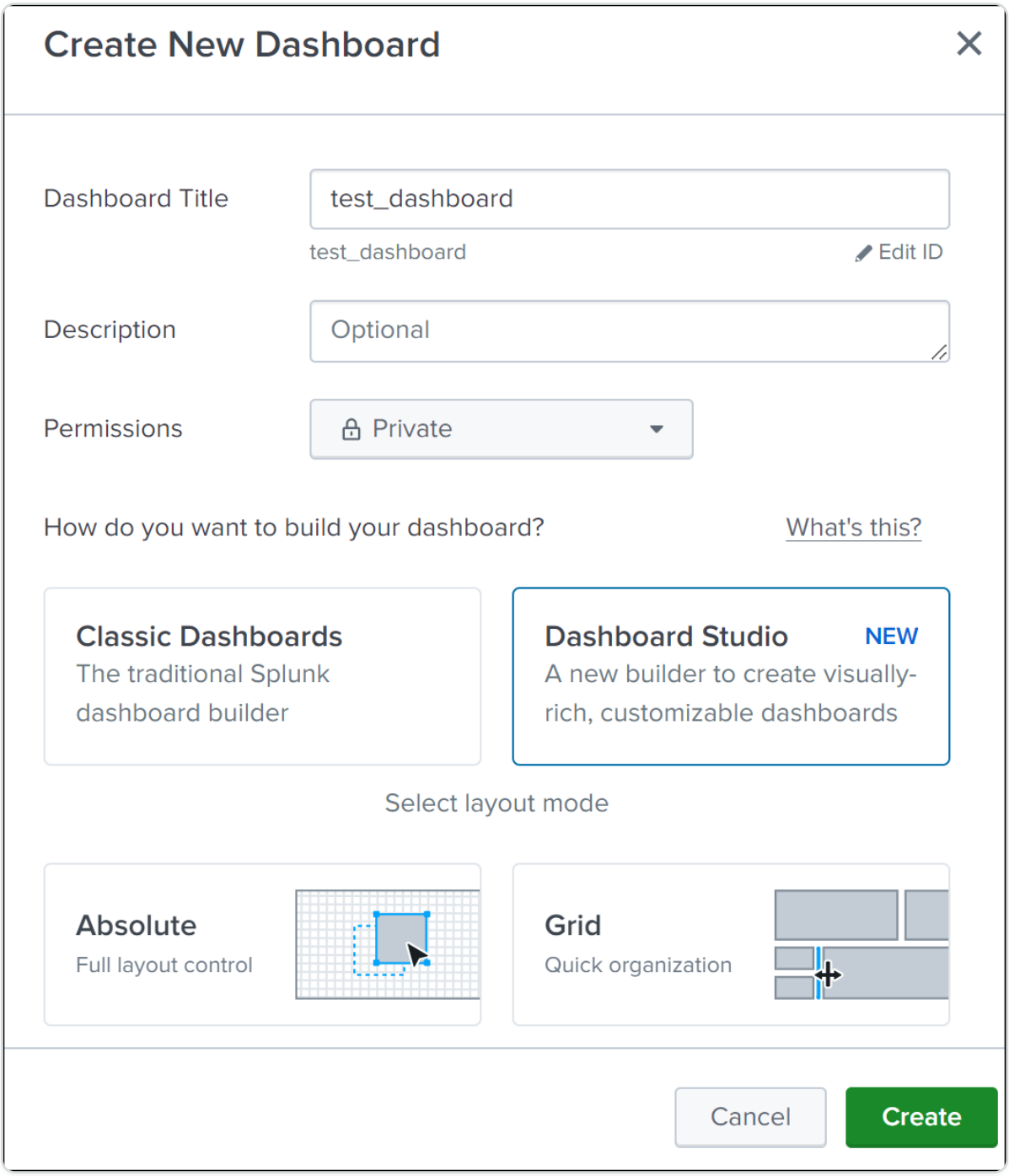
   b. **描述** - （可选）您可以提供描述以供参考。

   c. **权限** - 根据您的要求选择 **Private** 或 **Shared in App**。

   d. 选择 **仪表板工作室**。

   e. 选择任意一种布局（**Absolute** 或 **Grid**），然后单击 **Create**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



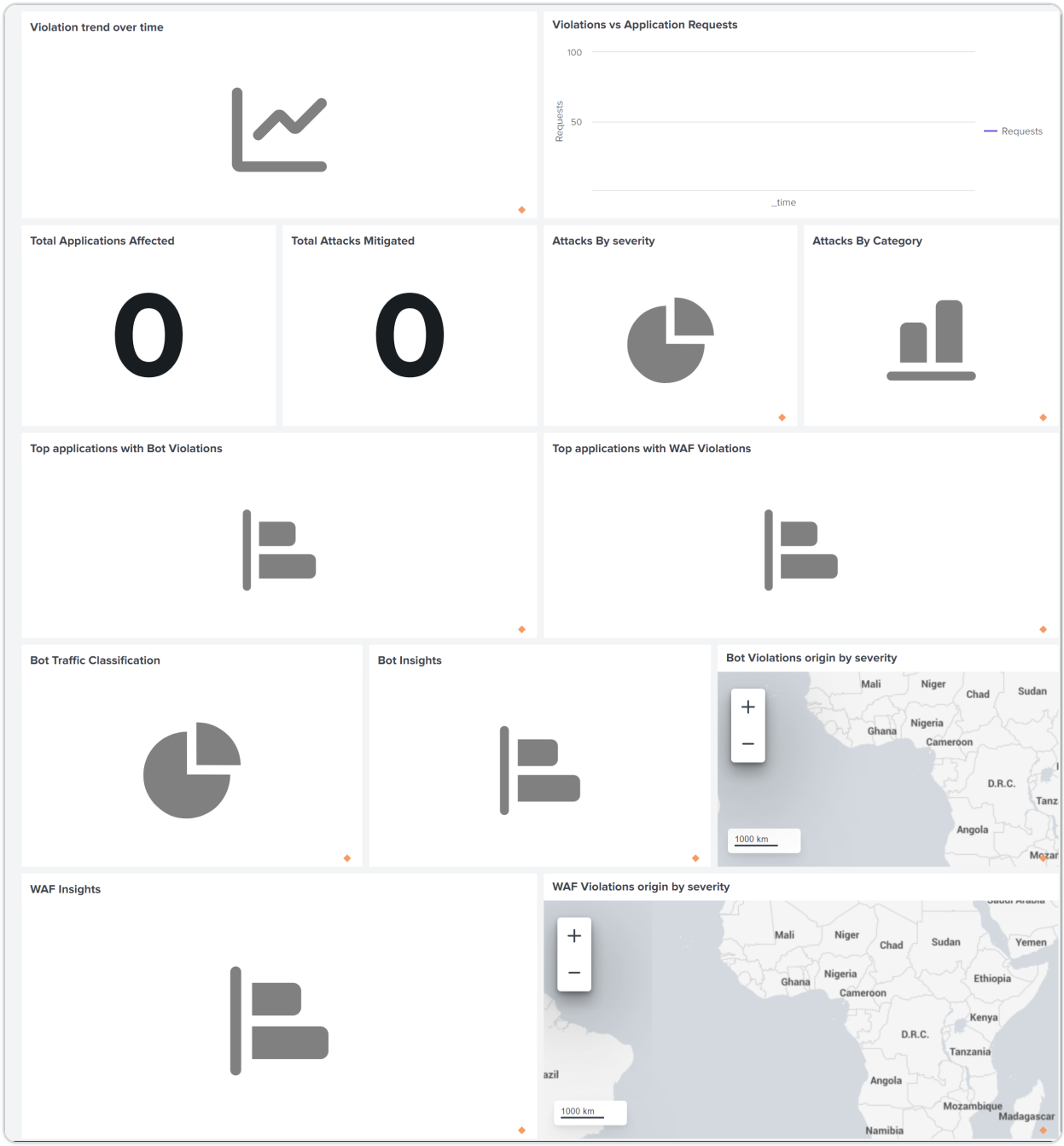
在单击 **Create** 后，从布局中选择 **Source** 图标。

5. 删除现有数据，粘贴在步骤 2 中复制的数据，然后单击 **Back**。
6. 单击 **Save**。

   您可以查看示例仪表板。

   以下是 WAF 和 bot 的示例仪表板。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



配置本地 NetScaler Console 以将数据导出到 Splunk

您现在已在 Splunk 中准备好一切。最后一步是通过创建订阅和添加令牌来配置 NetScaler Console。

完成以下过程后，您可以在 Splunk 中查看当前在 NetScaler Console 中可用的更新仪表板：

1. 登录到 NetScaler Console。
2. 导航到 **设置 > 可观测性集成**。
3. 在 **Integrations** 页面中，单击 **Add**。
4. 在 **Create Subscription** 页面中，指定以下详细信息：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 在 **Subscription Name** 字段中指定您选择的名称。

b. 选择 **NetScaler Console** 作为**源**，然后单击**下一步**。

c. 选择 **Splunk**，然后单击**配置**。在**配置端点**页面中：

   i. **端点 URL** – 指定 Splunk 端点详细信息。端点必须采用 `<https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event>` 格式。

   > **注意：**
   >
   > 建议出于安全原因使用 HTTPS。

   - **SPLUNK_PUBLIC_IP** – 为 Splunk 配置的有效 IP 地址。
   - **SPLUNK_HEC_PORT** – 表示您在 HTTP 事件端点配置期间指定的端口号。默认端口号为 8088。
   - **Services/collector/event** – 表示 HEC 应用程序的路径。

   ii. **身份验证令牌** – 从 Splunk 复制并粘贴身份验证令牌。

   iii. 单击**提交**。

d. 单击**下一步**。

e. 单击**添加洞察**，然后在**选择功能**选项卡中，您可以选择要导出的功能，然后单击**添加选定项**。

   > **注意：**
   >
   > 如果您选择了 **NetScaler Console 审计日志**，则可以为将审计日志导出到 Splunk 的频率选择**每日**或**每小时**。

f. 单击**下一步**。

g. 在 **选择实例** 选项卡中，您可以选择 **选择所有实例** 或 **自定义选择**，然后单击 **下一步**。

   - **选择所有实例** - 将所有 NetScaler 实例的数据导出到 Splunk。
   - **自定义选择** - 使您能够从列表中选择 NetScaler 实例。如果您从列表中选择特定实例，则数据仅从选定的 NetScaler 实例导出到 Splunk。

h. 单击 **提交**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

在 NetScaler Console 中检测到违规后，所选洞察的数据会立即推送到 Splunk。

在 Splunk 中查看仪表板

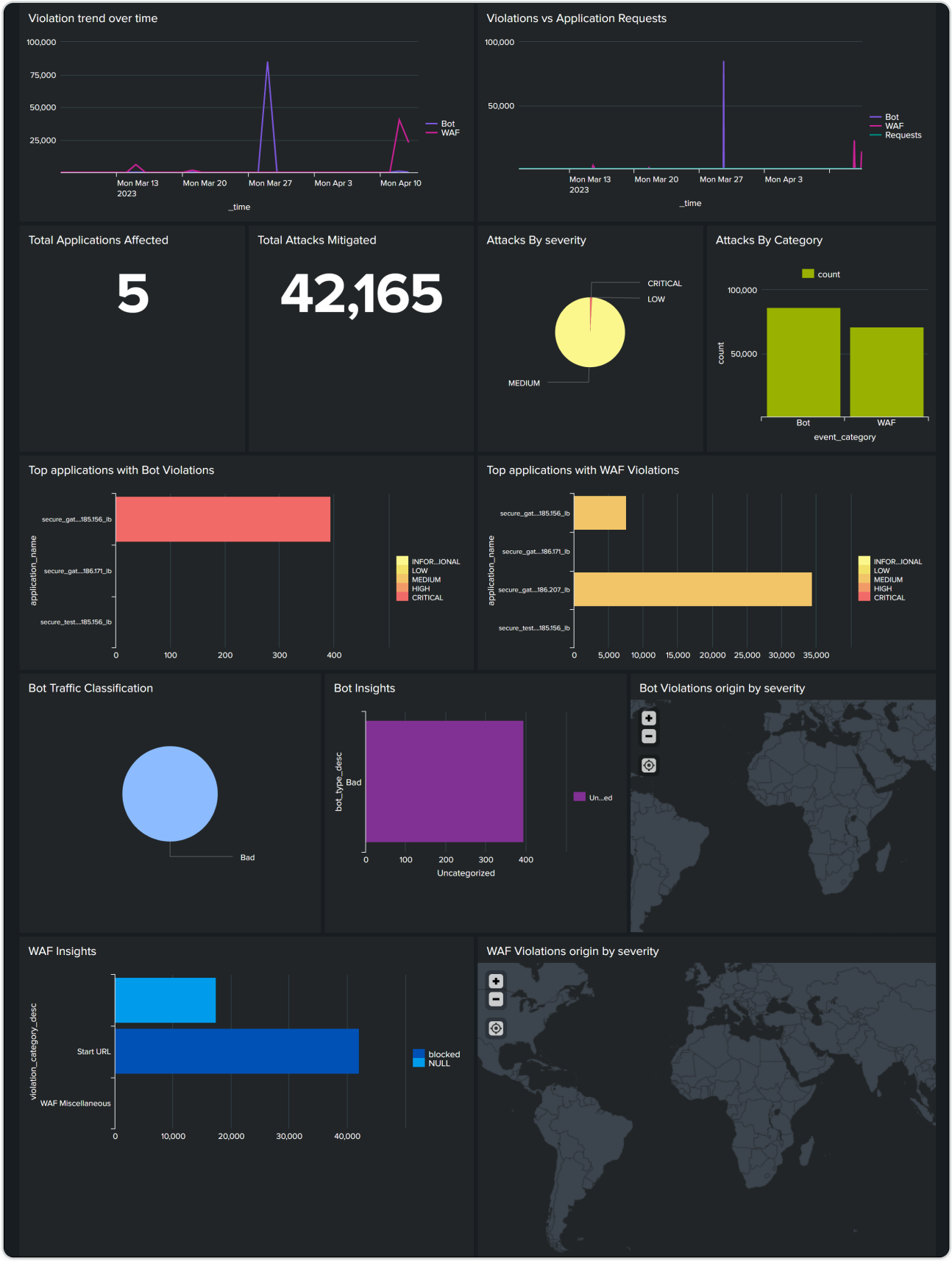
在 NetScaler Console 中完成配置后，数据将从 NetScaler Console 导出，并且事件将显示在 Splunk 中。

您已准备好在 Splunk 中查看更新后的仪表板，无需任何额外步骤。

转到 Splunk 并单击您已创建的仪表板以查看更新后的仪表板。

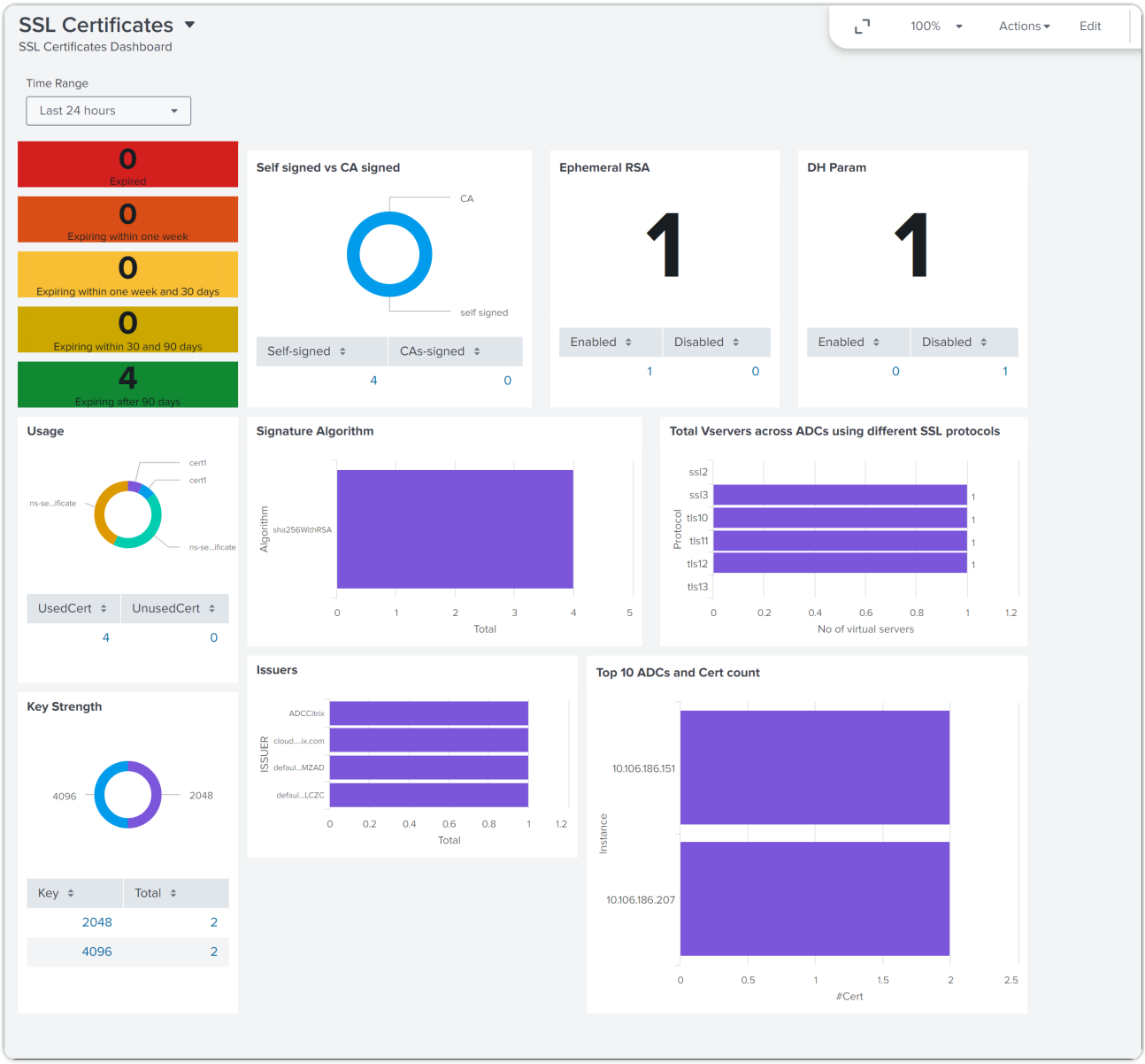
以下是更新后的 WAF 和 Bot 仪表板的示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



以下仪表板是更新后的 SSL 证书洞察仪表板的示例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

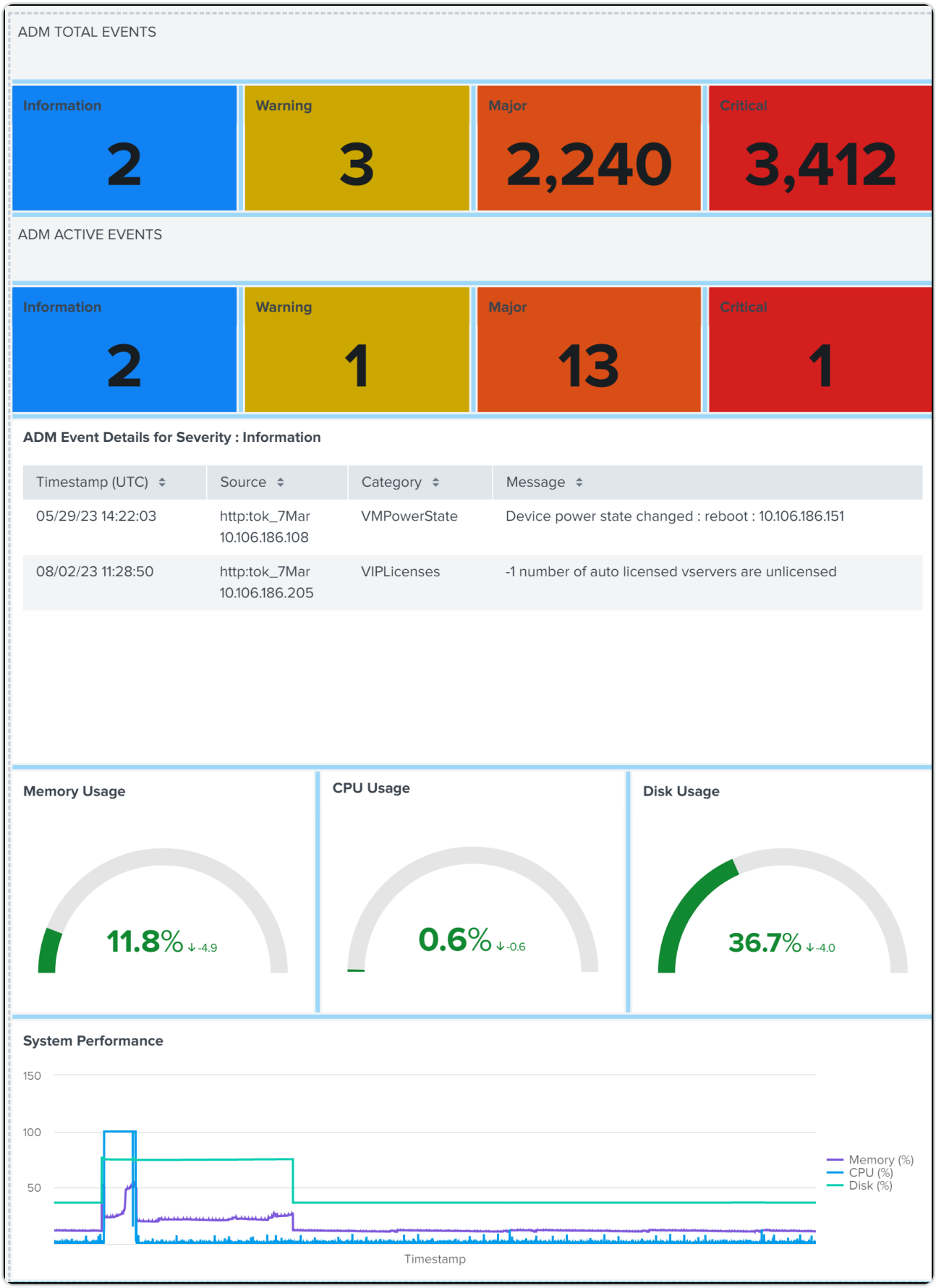


以下仪表板是更新后的事件和指标仪表板的示例。

注意：

内存、CPU 和磁盘的使用情况数据显示来自 NetScaler Console 的当前值。这些值的上升和下降趋势是根据每 5 分钟与前一个值的比较显示的。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



除了仪表板，您还可以在创建订阅后在 Splunk 中查看数据。

1. 在 Splunk 中，单击 **Search & Reporting**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 在搜索栏中：
   - 键入 `sourcetype="metrics"` 并从列表中选择持续时间以查看 NetScaler Console 指标数据。
   - 键入 `sourcetype="event"` 并从列表中选择持续时间以查看 NetScaler Console 事件数据。
   - 键入 `sourcetype="bot"` 或 `sourcetype="waf"` 并从列表中选择持续时间以查看 bot/WAF 数据。
   - 键入 `sourcetype="ssl"` 并从列表中选择持续时间以查看 SSL 证书洞察数据。
   - 键入 `sourcetype="gateway_insights"` 并从列表中选择持续时间以查看 Gateway 洞察数据。
   - 键入 `sourcetype="hdx_insights"` 并从列表中选择持续时间以查看 Gateway 洞察数据。
   - 键入 `sourcetype= "audit_logs"` 并从列表中选择持续时间以查看审计日志数据。

与 New Relic 集成

您现在可以将 NetScaler Console 与 New Relic 集成，以在 New Relic 控制面板中查看 WAF、Bot、SSL、Gateway Insights 和 NetScaler Console 审计日志的分析数据。通过此集成，您可以：

- 在 New Relic 控制面板中合并所有其他外部数据源。
- 在集中位置获取分析数据的可见性。

NetScaler Console 会收集 Bot 和 WAF 事件，并根据您的选择实时或定期将其发送到 New Relic。作为管理员，您还可以在 New Relic 控制面板中查看 Bot 和 WAF 事件。

先决条件

要成功集成，您必须：

- 获取以下格式的 New Relic 事件端点：

  `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`

  有关配置事件端点的更多信息，请参阅 New Relic 文档。

  有关获取帐户 ID 的更多信息，请参阅 New Relic 文档。
- 获取 New Relic 密钥。有关更多信息，请参阅 New Relic 文档。
- 在 NetScaler Console 中添加密钥详细信息

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 NetScaler Console 中添加密钥详细信息

生成令牌后，您必须在 NetScaler Console 中添加详细信息才能与 New Relic 集成。

1. 登录到 NetScaler Console。
2. 导航到 **设置 > 可观测性集成**。
3. 在 **集成** 页面中，单击 **添加**。
4. 在 **创建订阅** 页面中，指定以下详细信息：
   a. 在 **订阅名称** 字段中指定您选择的名称。
   b. 选择 **NetScaler® Console** 作为 **源**，然后单击 **下一步**。
   c. 选择 **New Relic**，然后单击 **配置**。在 **配置端点** 页面中：
      i. **端点 URL** – 指定 New Relic 端点详细信息。端点必须采用 `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events` 格式。

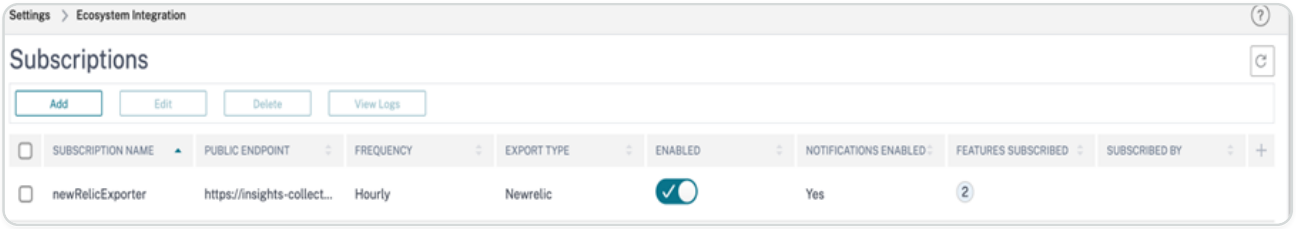
      > **注意**
      >
      > 建议出于安全原因使用 HTTPS。

   d. **身份验证令牌** – 从 New Relic 复制并粘贴身份验证令牌。
      i. 单击 **提交**。
   e. 单击 **下一步**。
   f. 单击 **添加洞察**，然后在 **选择功能** 选项卡中，您可以选择要导出的功能，然后单击 **添加选定项**。
   g. 单击 **下一步**。
   h. 在**选择实例**选项卡中，您可以选择**选择所有实例**或**自定义选择**，然后单击**下一步**。
      - **选择所有实例** - 将所有 NetScaler 实例的数据导出到 New Relic。
      - **自定义选择** - 使您能够从列表中选择 NetScaler 实例。如果您从列表中选择特定实例，则数据仅从选定的 NetScaler 实例导出到 New Relic。
   i. 单击**提交**。

   > **注意：**
   >
   > 在 NetScaler Console 中检测到违规后，所选洞察的数据会立即推送到 New Relic。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置已完成。您可以在**订阅**页面中查看详细信息。



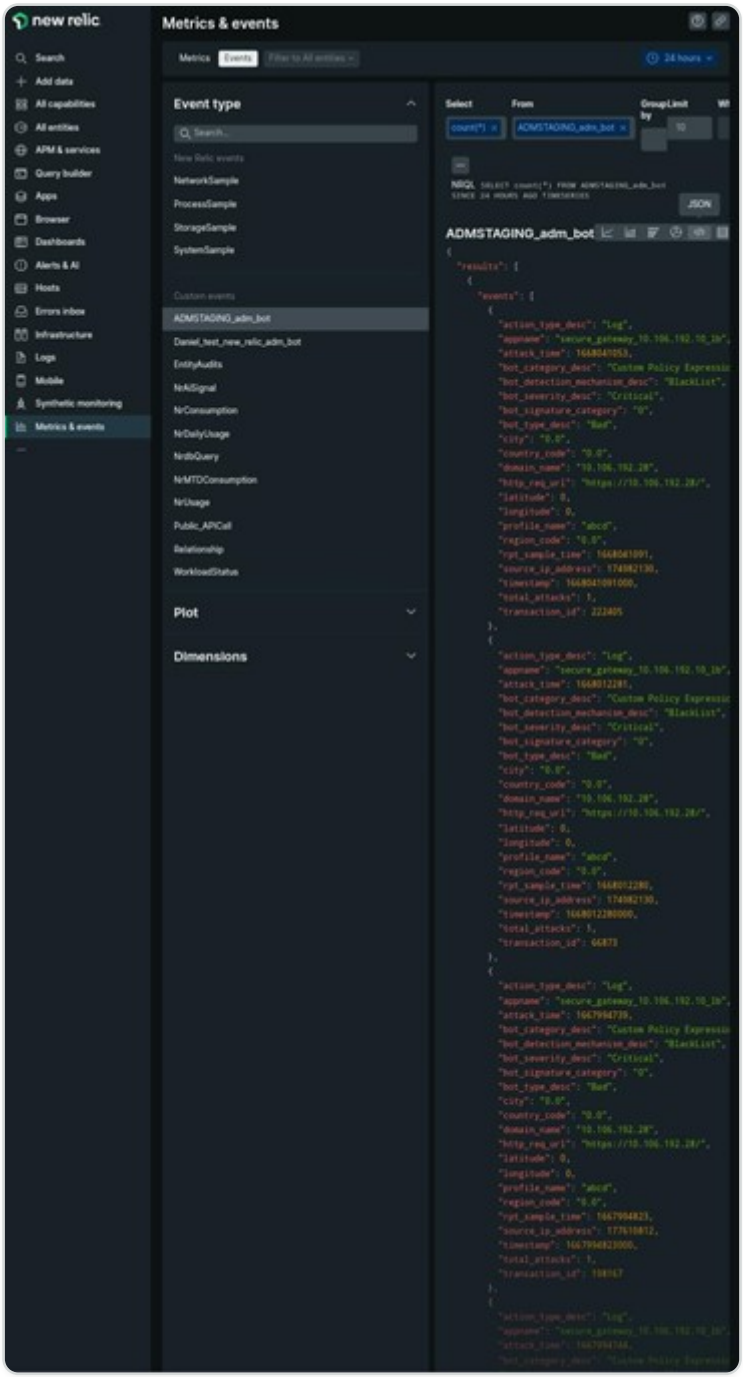
New Relic 控制板

当事件导出到 New Relic 后，您可以在**指标和事件**下以以下 JSON 格式查看事件详细信息：

`<subsription_name>_adm_<event name>` 其中事件名称可以是 Bot、WAF 等。

在以下示例中，ADMSTAGING 是 `<subscription_name>`，bot 是 `<event_name>`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



一旦将 JSON 数据摄取到 New Relic 控制板中，作为管理员，您可以使用 NRQL（New Relic 查询语言），并通过围绕摄取的数据构建查询，根据您的选择创建包含分面和小部件的自定义控制板。有关更多信息，请参阅 `https://docs.newrelic.com/docs/query-your-data/nrql-new-relic-query-language/get-started/introduction-nrql-new-relics-query-language/`

以下是使用 NRQL 创建的控制板示例：

示例仪表板(/en-us/netscaler-application-delivery-management-software/media/new-relic-example-dashboard.png)

要创建此仪表板，需要以下查询：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 小部件 1：事件表中的总唯一攻击

  `SELECT count(total_attacks) from <event_name> since 30 days ago`

- 小部件 2：事件表中的唯一事务 ID

  `SELECT uniqueCount(transaction_id) from <event_name> since 30 days ago`

- 小部件 3：总唯一机器人类型及其计数

  `SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc) from <event_name> since 30 days ago`

- 小部件 4：出现机器人违规的总唯一应用程序名称

  `SELECT uniques(appname) from <event_name> since 30 days ago`

与 Microsoft Sentinel 集成

您可以将 NetScaler Console 与 Microsoft Sentinel 集成，以将以下分析数据从 NetScaler Console 导出到 Microsoft Sentinel：

- WAF 违规
- Bot 违规
- SSL 证书洞察
- 网关洞察
- 指标和事件
- NetScaler® Console 审计日志

Microsoft Sentinel 提供集中式数据收集，可从应用程序、服务器等各种来源收集数据。作为管理员，您可以在 Microsoft Sentinel 中报告洞察或违规后查看数据并做出决策。

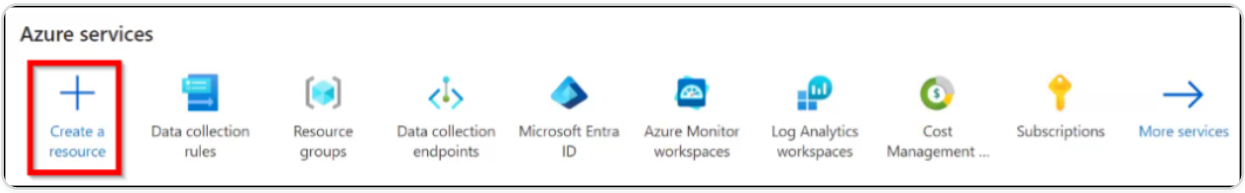
要成功集成，请确保您拥有有效的 Azure 订阅，然后按照每个部分下的步骤操作：

配置 Log Analytics 工作区

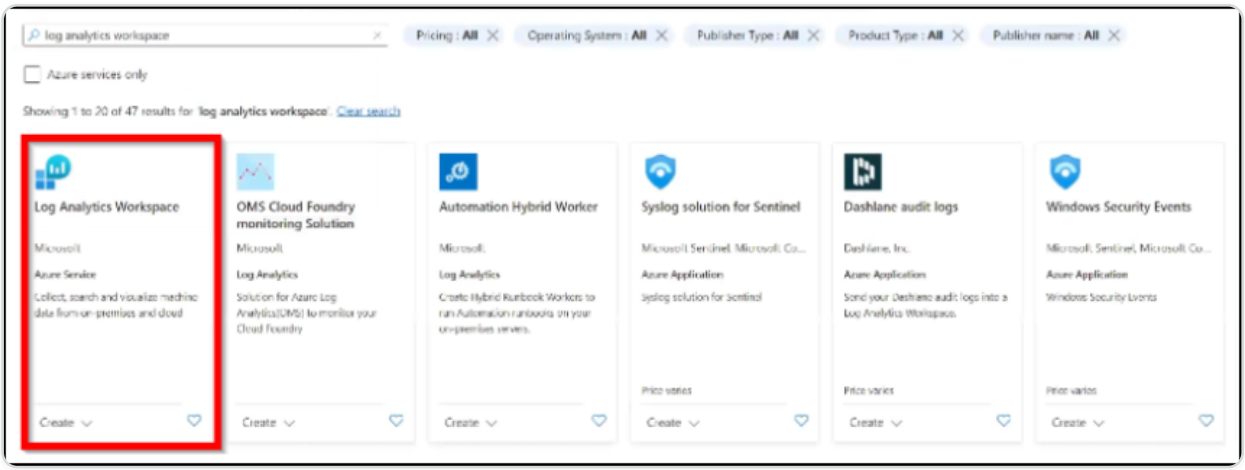
需要 Log Analytics 工作区来存储和分析收集的数据。

1. 登录 Azure。
2. 单击 **创建资源**。

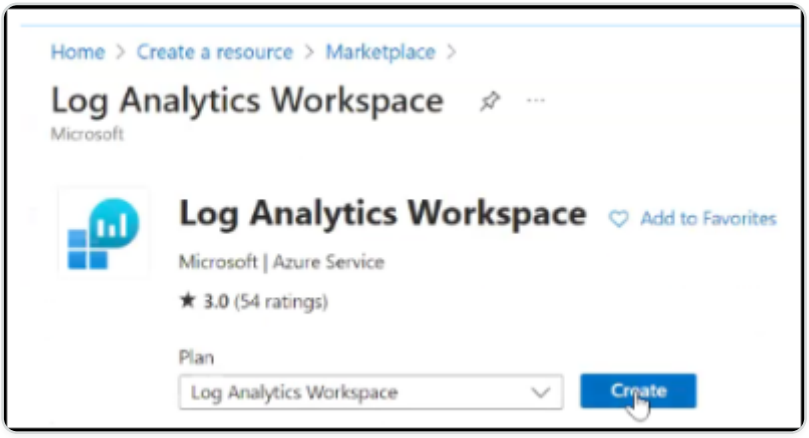
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 在搜索栏中，键入 log analytics workspace 并在 **Log Analytics Workspace** 下单击 **Create**。



4. 在 **Log Analytics Workspace** 主页中，单击 **Create**。



5. 在 **创建 Log Analytics 工作区** 中：

   a. 选择活动的订阅和资源组。

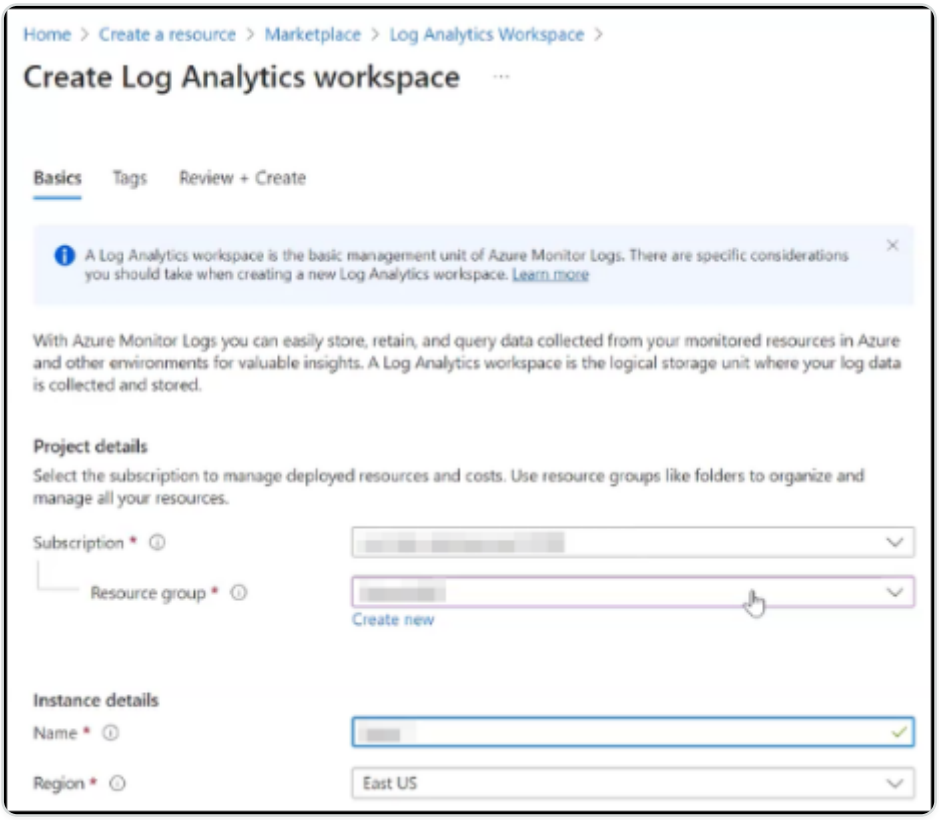
   > **注意：**
   >
   > 如果您有权限，也可以单击 **Create new** 以添加资源组。

   b. 指定一个您选择的名称。

   c. 从列表中选择您的区域。

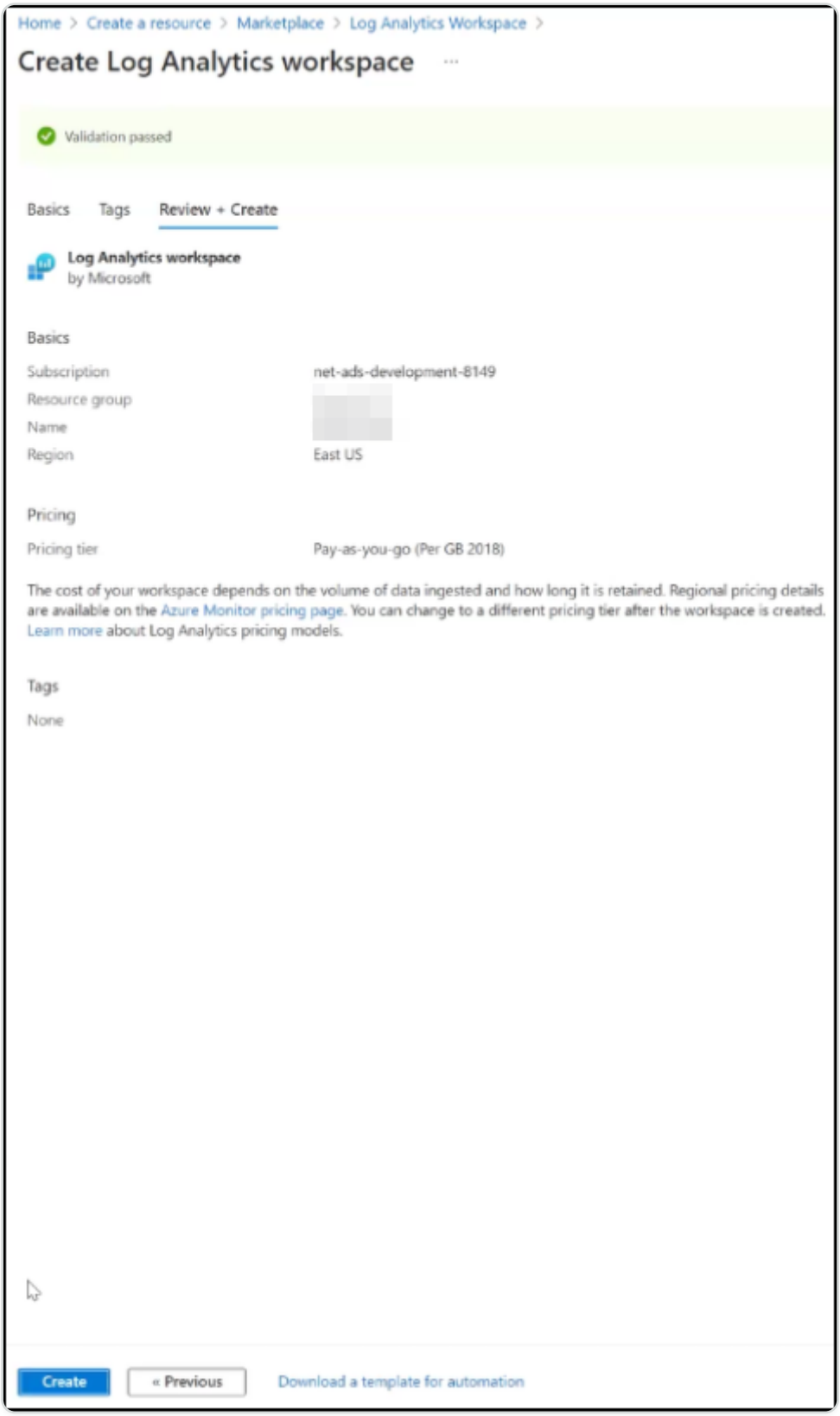
   d. 单击 **查看 + 创建**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



e. 出现验证通过消息。单击 **Create** 以部署工作区。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



f. 您可以看到部署正在进行的消息。在看到部署完成消息后，单击 **Go to resource**。

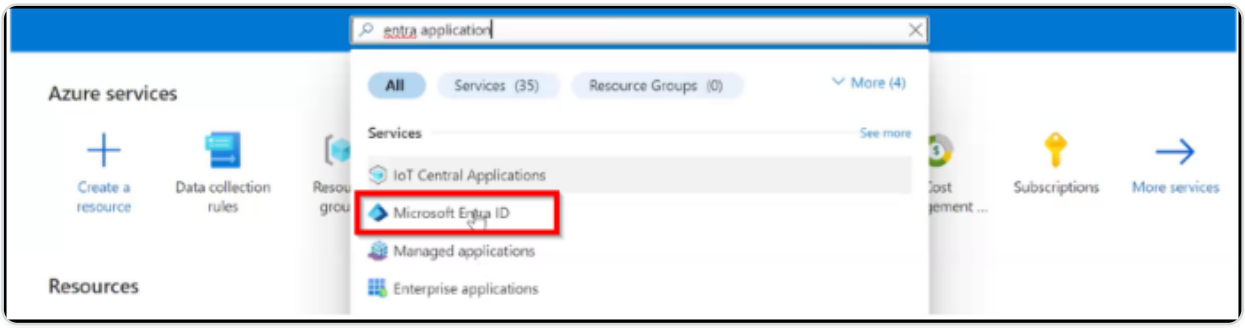
© 1997–2026 Citrix Systems, Inc. All rights reserved.

工作区已成功创建。

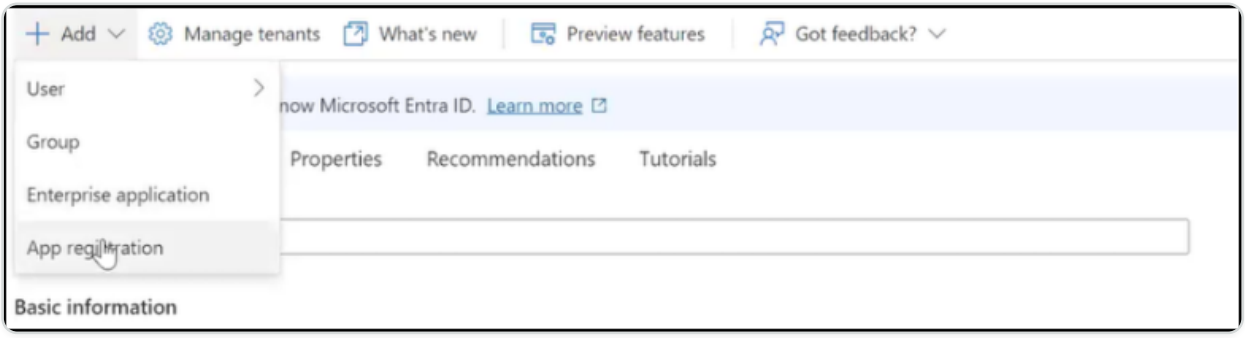
创建 Microsoft Entra 应用程序

您必须创建一个与 Azure 订阅关联的 Entra 应用程序，以便代表 Log Analytics 工作区进行通信。创建应用程序后，您还必须授予 **Microsoft Sentinel Contributor** 角色权限。该应用程序还提供诸如 **Client ID**、**Tenant ID** 和 **Client Secret** 等详细信息。建议您记下这些详细信息。在 NetScaler Console 中创建订阅以完成集成过程时，需要这些详细信息。

1. 在 Azure 门户中，在搜索栏中键入关键字。
2. 点击 **Microsoft Entra ID** 选项。

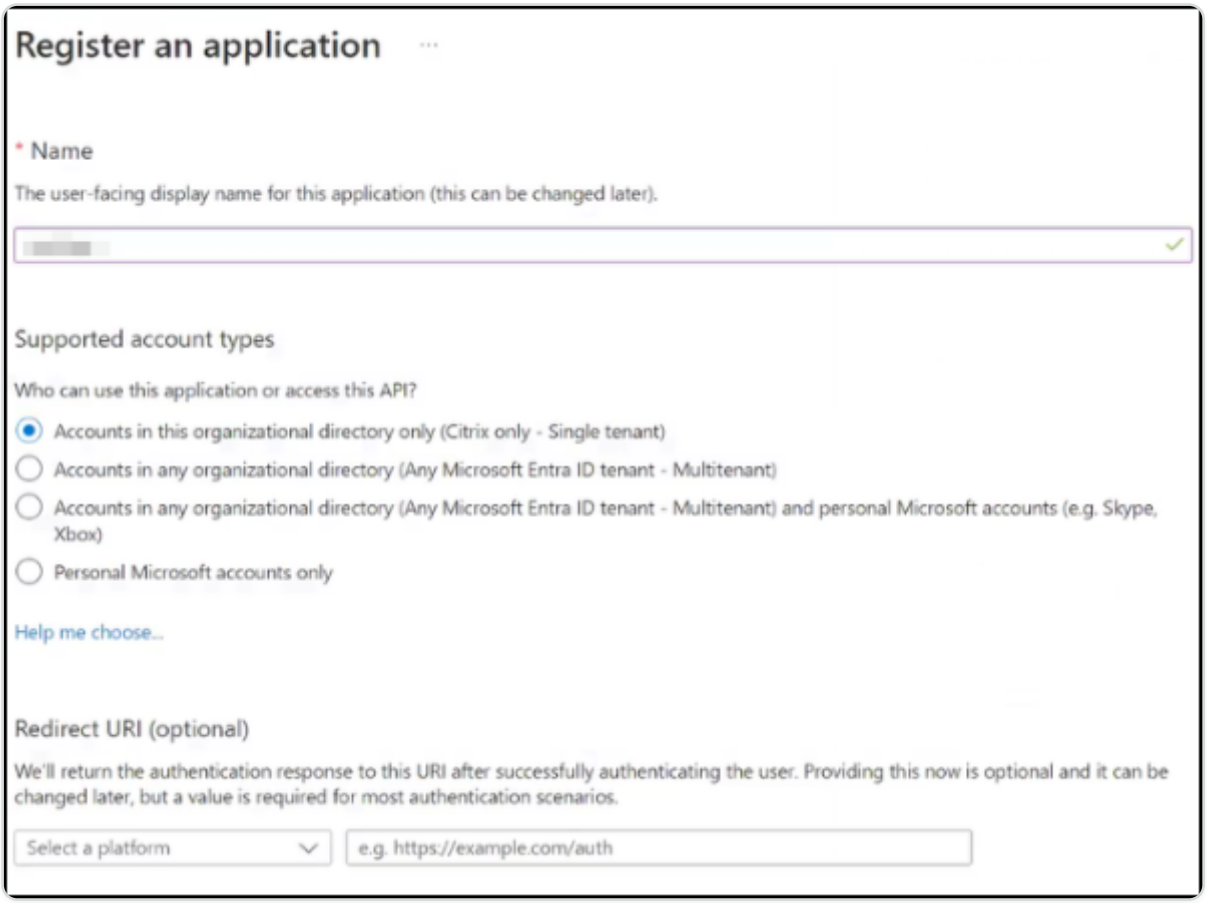


3. 单击 **Add** 并选择 **App registration**。



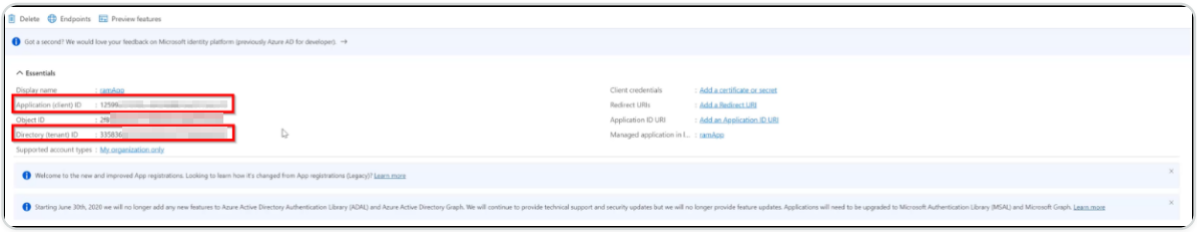
4. 为应用程序指定名称，在 **Supported account types** 下选择默认选项，然后单击 **Register**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

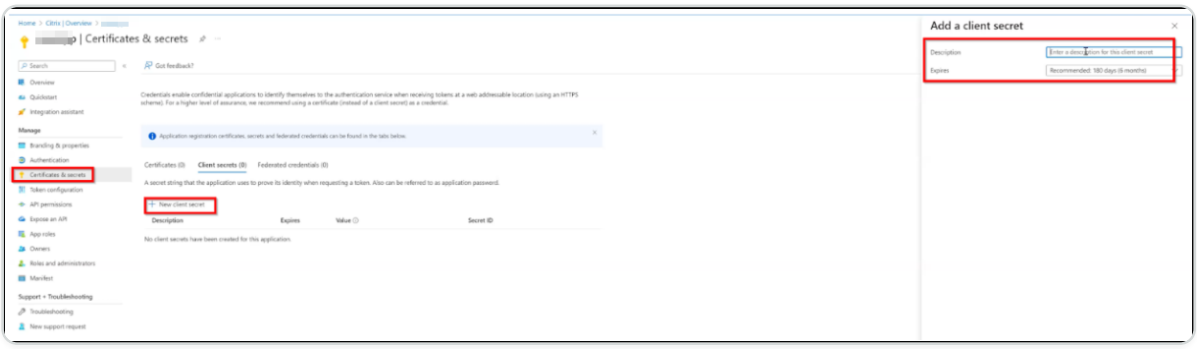


5. 注册应用程序后：

   a. 记下 **Client ID** 和 **Tenant ID**。

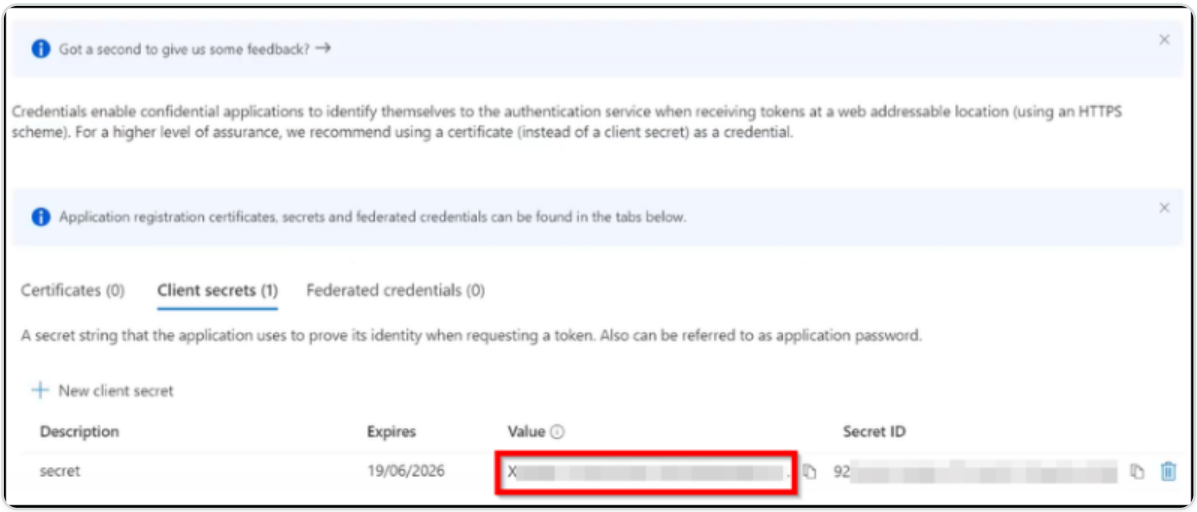


   b. 为您的应用程序创建 Secret ID。单击 **Certificates & secrets**，然后在 **Client secrets** 下单击 **New client secret**。提供描述、有效期，然后单击 **Add** 为您的应用程序创建 Secret ID。



   c. 您的应用程序的详细信息已显示。请务必在密钥创建后立即记下**值**下显示的 ID。如果您导航到任何其他 GUI 选项，此值将隐藏。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



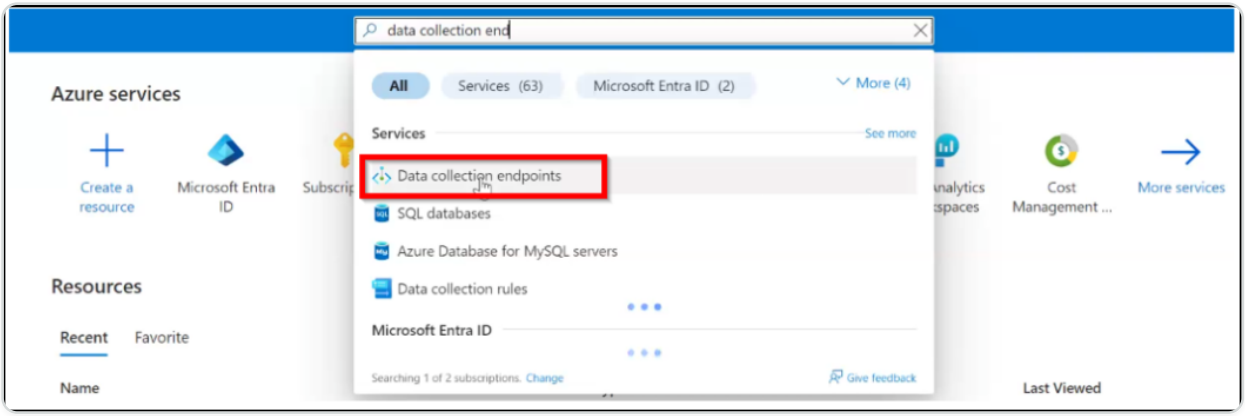
使用 Microsoft Entra ID 数据连接器将数据发送到 Microsoft Sentinel

Microsoft Entra ID 日志提供有关访问您的 Entra 租户的用户、应用程序和网络的全面信息。有关更多信息，请参阅使用 Microsoft Entra ID 数据连接器将数据发送到 Microsoft Sentinel。

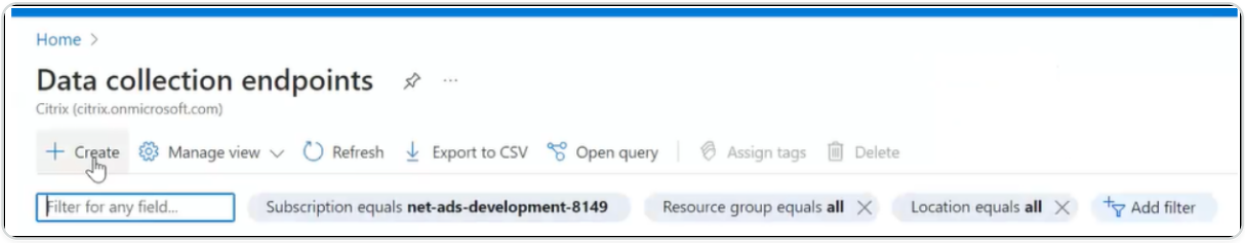
配置数据收集终结点

您必须创建一个数据收集终结点以获取终结点 URL。在 NetScaler Console 中创建订阅时需要此项。

1. 在 Azure 门户中，在**Azure 服务**下，选择**数据收集终结点**或在搜索栏中键入关键字。



2. 在**数据收集终结点**页面中，单击**创建**。



3. 在**创建数据收集终结点**中：

   a. 指定您选择的终结点名称

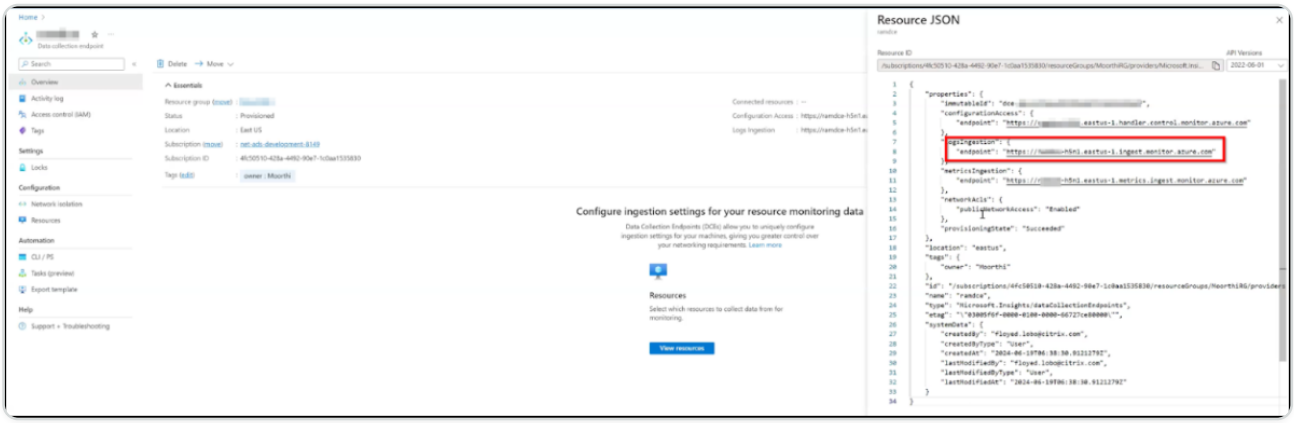
© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. 选择 **订阅、资源组** 和 **区域**。

c. 单击**审核 + 创建**。

d. 在看到验证通过消息后，点击 **创建**。

您必须记下端点 URL。在 **数据收集端点** 主页面中，选择已创建的端点，点击 **JSON 视图**，并记下端点 ID。



创建表以导出数据

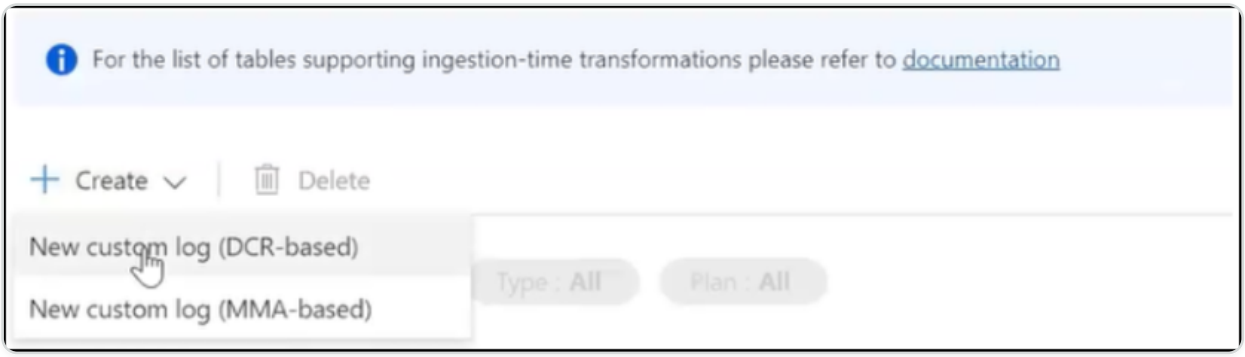
您必须为要从 NetScaler Console 导出到 Microsoft Sentinel 的每个洞察创建表并提供 JSON 信息。您可以参考以下有关每个洞察的表要求的详细信息：

洞察	所需的表总数
SSL 洞察	3
WAF	1
Bot	1
网关洞察	5
事件	1
指标	1
审计日志	1

每个数据收集规则 (DCR) 最多可以创建 10 个表。超过 10 个表，您必须创建另一个 DCR。

1. 在 Azure 门户中导航到您的工作区，然后单击“**设置**”下的“**表**”。
2. 单击“**创建**”并选择“**新建自定义日志（基于 DCR）**”

© 1997–2026 Citrix Systems, Inc. All rights reserved.



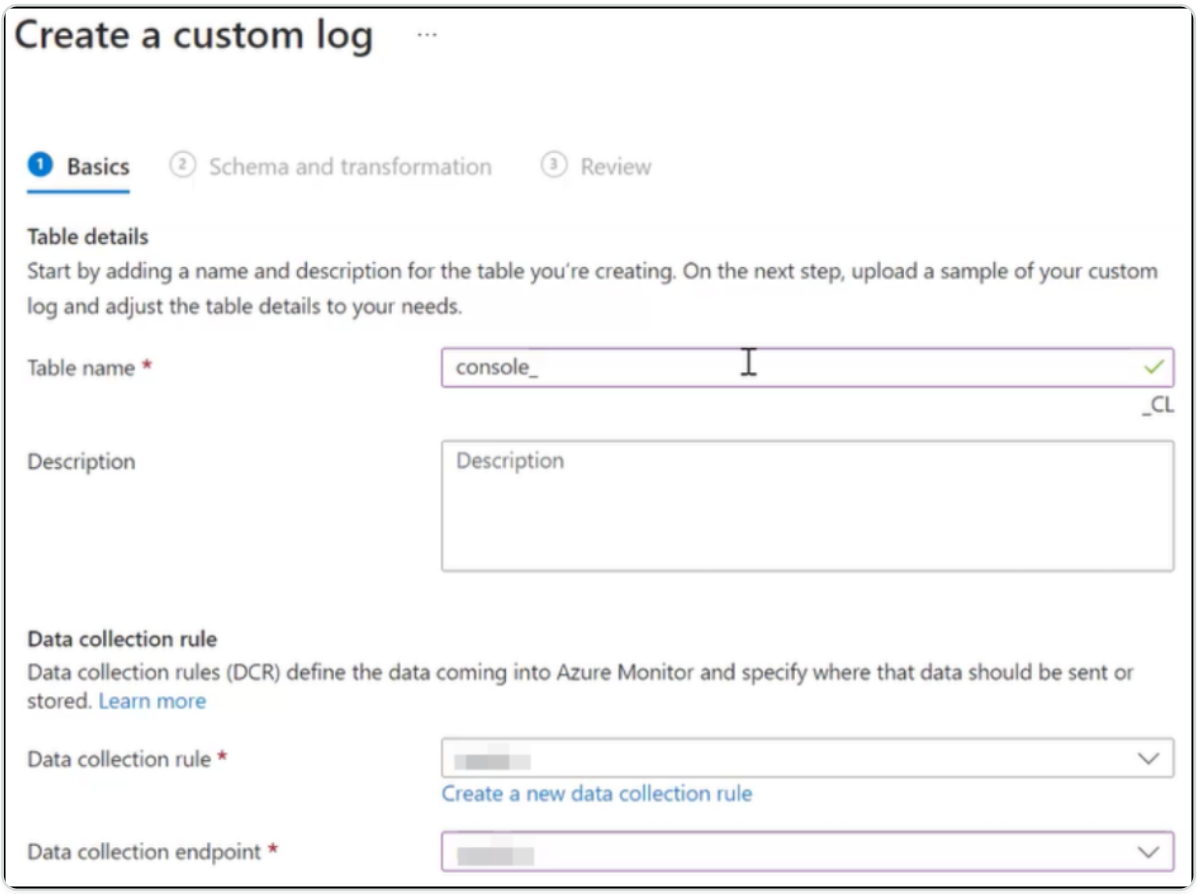
3. 在“**创建自定义日志**”中：

   a. 指定表名称。表名称必须采用 **console_insightname** 格式。例如：**console_ns_sslvserver**、**console_ns_ssl_certkey**。您可以参考步骤 4 获取适用于每个洞察的表名称。

   b. 提供描述以添加有关表名称的更多信息。这是可选的。

   c. 创建新的数据收集规则并添加。

   d. 从列表中选择数据收集终结点。



   e. 单击 **下一步**。

4. 在“**架构和转换**”选项卡中，您必须上传要导出的洞察的 JSON 示例日志。您可以为每个洞察使用以下示例 JSON 并创建一个 JSON 文件以上传：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

洞察	JSON	要使用的表名称
SSL (1)	{"id": "3eb05733-c326-493c-9aa0-f7db3a6b4277", "ns_ip_address": "10.106.186.141", "name": "zeta_192_168_110_250", "vsvr_ip_address": "", "vsvr_port": -1, "vsvr_type": "", "state": "", "partition_name": "", "display_name": "10.106.186.141", "poll_time": 1716539986, "managed": "f", "ssl2": "f", "ssl3": "t", "tls10": "t", "tls11": "t", "tls12": "t", "dh": "f", "ersa": "t", "sslprofile": "", "tls13": "f", "dhkeyexpsizelimit": "DISABLED", "pushenctriggertimeout": 1, "sessionticket": "", "includesubdomains": "f", "sessionticketkeyrefresh": "", "ssllogprofile": "", "serverauth": "", "ssltriggertimeout": 100, "ersacount": 0, "strictcachecks": "NO", "dhfile": "", "sessreuse": "ENABLED", "redirectportrewrite":	console_ns_sslvserver

© 1997–2026 Citrix Systems, Inc. All rights reserved.

洞察	JSON	要使用的表名称
	"DISABLED", "skipclientcertpolicycheck": "", "tls13sessionticketsperauthcontext": 1, "cipherredirect": "DISABLED", "dropreqwithnohostheader": "NO", "sessionticketlifetime": -1, "maxage": 0, "pushenctrigger": "Always", "strictsigdigestcheck": "f", "sslredirect": "DISABLED", "sessionkeylifetime": -1, "alpnprotocol": "", "clientauthuseboundcachain": "", "sesstimeout": 120, "clientcert": "", "snihttphostmatch": "CERT", "preload": "NO", "prevsessionkeylifetime": -1, "sessionticketkeydata": "", "encrypttriggerpktcount": 45, "cleartextport": "", "ssliocspcheck": "", "hsts": "f", "sslinterception": "", "commonname": "", "sslireneg": "", "ocspstapling": "DISABLED", "quantumsize": 8192, "insertionencoding":	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

洞察	JSON	要使用的表名称
	"Unicode", "sslimaxsessperserver": -1, "cipherurl": "", "pushflag": 0, "zerorttearlydata": "DISABLED", "allowextendedmastersecret": "", "dhekeyexchangewithpsk": "NO", "clientauth": "DISABLED", "denysslreneg": "NONSECURE", "sendclosenotify": "YES", "dhcount": 0, "snienable": "DISABLED", "table_name": "ns_sslvserver"}	
SSL (2)	{"id": "a6673ab2-0b59-47b9-b530-bc30fb2b937c", "ssl_certificate": "/nsconfig/ssl/ca-cert.pem", "ssl_key": "/nsconfig/ssl/ca-key.pem", "certkeypair_name": "athul-ca", "cert_format": "PEM", "days_to_expiry": 281, "ns_ip_address": "10.106.186.141", "status": "Valid", "device_name": "10.106.186.141", "file_location_path": "", "certificate_data": "", "key_data": "",	console_ns_ssl_certkey

© 1997–2026 Citrix Systems, Inc. All rights reserved.

洞察	JSON	要使用的表名称
	"poll_time": 1717434335, "no_domain_check": "f", "version": 3, "serial_number": "7B34B6A6A1A79E0FF168242D7BCFF78F04C9EE66", "signature_algorithm": "sha256WithRSAEncryption", "issuer": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "valid_from": "Mar 12 08:51:11 2024 GMT", "valid_to": "Mar 12 08:51:11 2025 GMT", "subject": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "public_key_algorithm": "rsaEncryption", "public_key_size": 4096, "no_of_bound_entities": 0, "partition_name": "", "display_name": "10.106.186.141", "hostname": "athulsadc", "key_name": "", "subjaltname": "", "managed_by": "", "certificate_dn": "", "linkcertkeyname": "", "table_name": "ns_ssl_certkey"}	
WAF	[{"ip_address": "10.106.185.156", "ctnsappname":	console_af_threat_exporter_data_l2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

洞察	JSON	要使用的表名称
	"vserver_1", "severity": 2, "violation_type": 19, "violation_type_desc": "Start URL", "block_flags": 1, "transformed_flags": 0, "not_blocked_flags": 0, "country_code": "-NA-", "region_code": "-NA-", "city": "-NA-", "latitude": 200.0, "longitude": 200.0, "signature_category": "", "attack_category": 2, "attack_category_desc": "Broken Authentication and Session Management", "total_attacks": 1, "rpt_sample_time": 1704783773, "source_ip_address": 174766492, "attack_time": 1704783538, "profile_name": "appfw_cs_lb_prof", "session_id": "", "http_req_url": "https://10.106.192.54/csrf_ffc/ffc.html?field10=asfasd", "violation_name": "-NA-", "violation_value": "-NA-", "violation_location": 4,	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

洞察	JSON	要使用的表名称
	"violation_threat_index": 5, "app_threat_index": 5, "http_method": 0, "violation_action": 3, "violation_action_desc": "Blocked", "severity_type": 2, "severity_type_desc": "Medium", "iprep_score": 0, "iprep_category": 0, "counter_value": 0, "appname": "vserver_1_10.106.185.156_lb", "violation_category": 12, "violation_category_desc": "Start URL", "source_ipv6_address": "", "true_client_ip": "\\N", "backend_vserver": "", "backend_appname": "", "transactionId": "0", "table_name": "af_threat_exporter_data_l2"}]	
机器人	{"ip_address": "10.106.186.122", "ctnsappname": "secure_gateway", "bot_type": "2", "bot_type_desc": "Bad", "action_type": "6", "action_type_desc": "Log", "country_code": "0.0", "region_code":	console_af_bot_attack_details_l2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

洞察	JSON	要使用的表名称
	"0.0", "city": "0.0", "bot_severity": "0", "bot_severity_desc": "Critical", "latitude": "0", "longitude": "0", "bot_detection_mechanism": "6", "bot_detection_mechanism_desc": "BlackList", "bot_category": "0", "bot_category_desc": "Uncategorized", "source_ip_address": "174758625", "bot_signature_category": "Custom Policy Expression", "appname": "secure_gateway_10.106.186.122_lb", "backend_vserver": "", "backend_appname": "", "total_attacks": "2", "rpt_sample_time": "1718783216", "table_name": "af_bot_attack_details_l2"}	
网关洞察 (1)	{"adc_ip_address": "10.106.186.141", "auth_server": "", "client_ip": 174766732, "epa_method_type": 0, "error_count": 14, "error_details": "Invalid credentials passed", "error_type": 1, "gateway_name": "vpn_vserver_142_6", "req_url": "",	console_af_vpn_error_details

© 1997–2026 Citrix Systems, Inc. All rights reserved.

洞察	JSON	要使用的表名称
	"resource": "", "rpt_sample_time": 1713505215, "sso_method_type": 0, "sta_ip": "", "table_name": "af_vpn_error_details", "username": "John"}	
网关洞察 (2)	{"adc_ip_address": "10.102.71.166", "display_name": "10.102.71.166", "gateway_name": "firsthop", "ip_address": "10.102.71.168", "rpt_sample_time": "1718812158", "state": "Up", "table_name": "ns_vpnvserver"}	console_ns_vpnvserver
网关洞察 (3)	{"adc_ip_address": "10.106.186.141", "gateway_name": "vpn_vserver_141_7", "rpt_sample_time": 1702011308, "sessions": 1, "table_name": "af_vpn_session_details", "users": 1}	console_af_vpn_session_details
网关洞察 (4)	{"active_sessions": 59, "active_users": 1, "adc_ip_address": "10.106.186.136", "gateway_name": "vpnathul2", "rpt_sample_time": 1698919848,	console_af_vpn_active_session_1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

洞察	JSON	要使用的表名称
	"table_name": "af_vpn_active_session_1"}	
网关洞察 (5)	{"adc_ip_address": "10.106.186.136", "entity_type": 3, "gateway_name": "vpnathul2", "hits": 3, "rpt_sample_time": 1698052438, "table_name": "af_vpn_error_reports"}	console_af_vpn_error_reports
事件	{"rpt_sample_time": -1, "category": "HealthMonitoring", "entity": "10.106.186.148:HealthMonitoring:System Disk Usage", "counter_threshold_value": "", "id": "0f2607cf-f97d-4f71-9162-11e580262e93", "timestamp": 1712927472, "message": "Disk Usage High: 63.24%", "severity": "Critical", "user_name": "", "device_entity_type": "", "device_type": "", "counter_actual_value": "", "cmd_auth_status": "", "source": "10.106.186.148", "history": "Update Time= Fri, 12 Apr 2024 06:32:49 UTC ,Previous	console_event

© 1997–2026 Citrix Systems, Inc. All rights reserved.

洞察	JSON	要使用的表名称
	`Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:27:46 UTC ,Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:22:44 UTC ,Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:17:41 UTC ,Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:12:38 UTC ,Previous Severity= Critical ,New Severity= Critical, Source= 10.106.186.148\nUpdate Time= Fri, 12 Apr 2024 06:07:36 U", "config_cmd": "", "failureobj": "System Disk Usage", "operation_type": "undefined", "device_entity_name": "", "cmd_exec_status": "", "device_family": "", "source_event_id": -1, "source_system_ip":`	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

洞察	JSON	要使用的表名称
	"10.106.186.148", "trap_id": 35, "table_name": "event"}	
指标	{"memory_free": 28830060544.0, "disk_used": 81248694272.0, "disk_free": 29632114688.0, "node_type": "", "memory_total": 34355544064.0, "cpu_usage": 0.49, "disk_total": 120522616832.0, "disk_usage": 73.28, "node_id": "", "id": "1be15a09-d078-469c-868a-bfbfcffe5ef1", "disk_total_capacity": 0.0, "page_size": 4096.0, "memory_usage": 16.08, "table_name": "mps_health"}	console_mps_health
审计日志	{"system_gmt_time":1721868291, "source":"X.X.X.X", "severity":"INFO", "module":"DEVICECONFIG", "event_type":"CMD_EXECUTED", "message":"Sample Mesage", "instance_ip":"X.X.X.X", "app_name":""}	console_syslog_messages

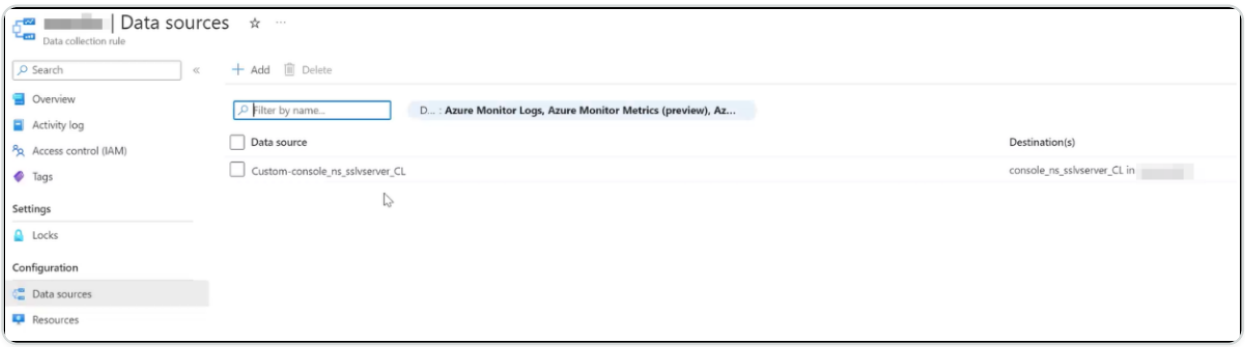
上传 JSON 后，您可以查看以下详细信息：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

单击 **Transformation editor**，输入适用于相应洞察的以下查询，然后单击 **Run** 以接受从 NetScaler Console 中的轮询时间开始的数据。

- **SSL** - `source | extend TimeGenerated = todatetime(poll_time) | project-rename sslvserver_id = id`
- **WAF** 和 **Bot** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`
- **网关洞察** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`

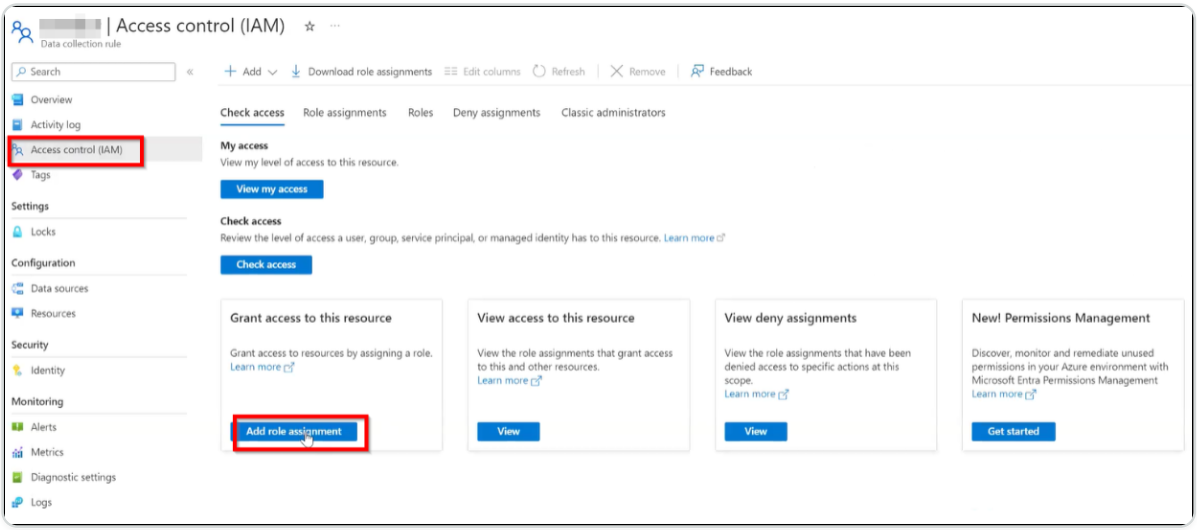
5. 单击“**下一步**”，然后单击“**创建**”以完成。
6. 导航到“**数据收集规则**”，单击您已创建的 DCR。
7. 在“**配置**”下，单击“**数据源**”以查看创建的表。



DCR（数据收集规则）需要访问“**监控指标发布者**”角色。

a. 导航到您可以从 Azure 门户的“**最近**”下访问的 DCR。
b. 在 DCR 页面中，单击“**访问控制 (IAM)**”，然后单击“**添加角色分配**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



c. 在搜索栏中，键入关键字“monitor”以选择“**监控指标发布者**”，然后单击“**下一步**”。

d. 在“**成员**”选项卡中，单击“**选择成员**”并选择您创建的 Entra 应用程序。

e. 单击“**审核 + 分配**”。

您必须记下数据收集规则 ID。导航到“数据收集规则”页面，选择您的 DCR，然后单击“JSON 视图”以记下 ID。

在 NetScaler Console 中创建订阅

您现在已准备就绪。最后一步是通过创建订阅并添加所需详细信息来配置 NetScaler Console。要在 NetScaler Console 中创建订阅，您需要以下已记下的详细信息：

- 端点 URL
- 数据收集规则 ID
- 租户 ID
- 客户端 ID

© 1997–2026 Citrix Systems, Inc. All rights reserved.

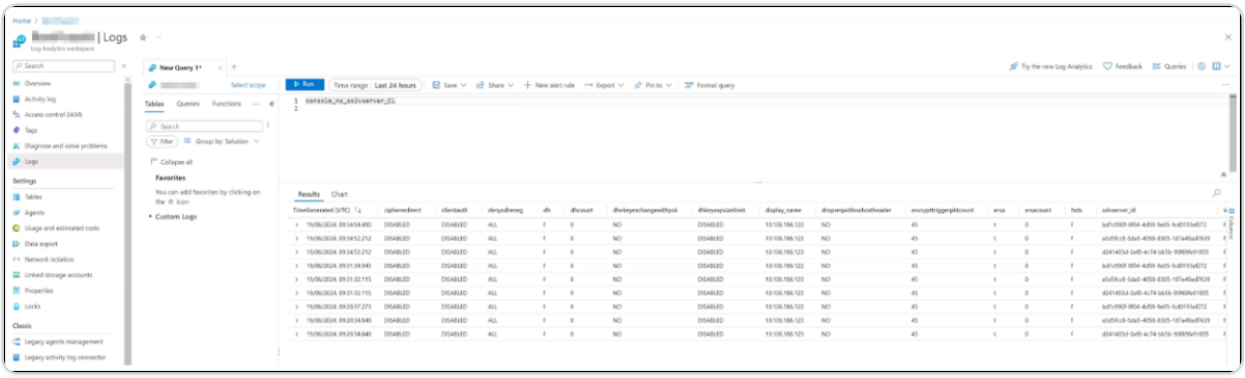
- 客户端密钥

1. 登录到 NetScaler Console。
2. 导航到“**设置 > 可观察性集成**”。
3. 在“**集成**”页面中，单击“**添加**”。
4. 在“**创建订阅**”页面中，指定以下详细信息：
   a. 在“订阅名称”字段中指定您选择的名称。
   b. 选择 **NetScaler Console** 作为**源**，然后单击“**下一步**”。
   c. 选择 **Microsoft Sentinel**，然后点击 **Configure**。在 **Configure Endpoint** 页面中，输入所有详细信息，然后点击 **Submit**。
   d. 点击 **Next**。
5. 点击 **Add Insights**，然后在 **Select Feature** 选项卡中，根据您在 Microsoft Azure 中添加的表，选择要导出的功能，然后点击 **Add Selected**，再点击 **Next**。
6. 在 **Select Instance** 选项卡中，您可以选择 **Select All Instances** 或 **Custom select**，然后点击 **Next**。
   - **Select All Instances** - 将所有 NetScaler 实例的数据导出到 Microsoft Sentinel。
   - **Custom select** - 允许您从列表中选择 NetScaler 实例。如果您从列表中选择特定实例，则数据将仅从选定的 NetScaler 实例导出到 Microsoft Sentinel。
7. 点击 **Submit**。

在 Microsoft Azure 中查看日志

配置完成后，建议您等待 30 分钟，然后在 Microsoft Azure 中查看详细信息。

1. 在您的 Azure 门户中，导航到您的 **Log Analytics Workspace**。
2. 点击 **Logs**，提供表名，然后点击 **Run** 查看结果。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

您还可以排查故障并使用日志来验证配置。例如，在 NetScaler Console GUI 中对已配置的洞察使用“立即轮询”选项，然后：

1. 使用 SSH 客户端登录到您的 NetScaler Console。
2. 键入 shell 进入 bash 模式。
3. 使用以下命令查看日志：

   `tail -f /var/mps/log/nbs/nbs_api.log`

以下示例可帮助您分析可能的错误以进行故障排除：

```
2024-06-25 12:10:13,413 [ERROR] [MainProcess] 1285: Owner: upload_chunk_to_end_point: failed, status code 401 message {"error":{"code":"InvalidToken","mess
age":"Make sure to pass a valid JWT token in the format Authorization:Bearer {JWT token}"}}
2024-06-25 12:10:13,465 [ERROR] [MainProcess] 1284: Owner: upload_chunk_to_end_point: failed, status code 401 message {"error":{"code":"InvalidToken","mess
age":"Make sure to pass a valid JWT token in the format Authorization:Bearer {JWT token}"}}
2024-06-25 12:10:14,475 [ERROR] [MainProcess] 1285: Owner: obtain_new_token_from_server: Failed status code 400 message {"error":"unauthorized_client","err
or_description":"AADSTS700016: Application with identifier '12599cf2-97bb-4342-8888-9c2011b22c1522' was not found in the directory 'Citrix'. This can happe
n if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You may have sent your authentica
tion request to the wrong tenant. Trace ID: 7f58f662-fe57-47fc-82c0-55c06454bc00 Correlation ID: 3edcab6c-d6e7-412d-baeb-0e3910eb2cba Timestamp: 2024-06-25
 06:34:37Z","error_codes":[700016],"timestamp":"2024-06-25 06:34:37Z","trace_id":"7f58f662-fe57-47fc-82c0-55c06454bc00","correlation_id":"3edcab6c-d6e7-412
d-baeb-0e3910eb2cba","error_uri":"https://login.microsoftonline.com/error?code=700016"}
2024-06-25 12:10:14,478 [INFO] [MainProcess] 1285: Total time taken 2.143172264099121 to upload the data for tenant- Owner data ssl
2024-06-25 12:10:14,479 [INFO] [MainProcess] 1285: http://127.0.0.1:6568/export/upload took time 2144.184350967407 ms
2024-06-25 12:10:14,479 [INFO] [MainProcess] 1285: 200 OK
```

1. 此日志表示您为 NetScaler Console 中 Microsoft Sentinel 订阅提供了无效的客户端 ID（**设置 > 可观测性集成**）。

   解决方法： 确保您已复制正确的客户端 ID，并通过提供正确的客户端 ID 来编辑订阅。有关更多信息，请参阅创建 Microsoft Entra 应用程序。

```
mpsdb=> \q
bash-3.2# tail -f /var/mps/log/nbs/nbs_api.log
2024-06-25 11:46:30,903 [INFO] [MainProcess] 1285: Uploading data - topic ssl - partition None for tenant Owner Subscription name ramsub - data length 3 Fi
ltered is True
2024-06-25 11:46:30,911 [INFO] [MainProcess] 1284: Uploading data - topic ssl - partition None for tenant Owner Subscription name ramsub - data length 2 Fi
ltered is True
2024-06-25 11:46:32,420 [ERROR] [MainProcess] 1285: Owner: upload_chunk_to_end_point: failed, status code 400 message {"error":{"code":"InvalidStream","mes
sage":"The stream Custom-console_ns_ssl_certkey_CL was not configured in the data collection rule with immutable Id dcr-6c91e6ee40064a0f8cda40ace25df33e."}
```

2. 此日志表示您尚未在 Microsoft Azure 中配置所需的 ssl_certkey 表。

   解决方法： 在 Microsoft Azure 中为 ssl_certkey 配置一个表。有关更多信息，请参阅创建表以导出数据。

配置 NetScaler® 实例以使用默认架构将洞察数据导出到 Prometheus

NetScaler 支持直接将指标导出到 Prometheus。您可以使用 NetScaler 实例提供的丰富指标集来监控 NetScaler 运行状况和应用程序运行状况。例如，您可以收集 CPU 和内存使用情况的指标，以了解 NetScaler 的运行状况。同样，您可以使用每秒接收的 HTTP 请求数或活动客户端数等指标来监控应用程序运行状况。

要将指标导出到 Prometheus，您必须配置一个类型为时间序列的分析配置文件。有关更多信息，请参阅 使用 Prometheus 监控 NetScaler、应用程序和应用程序安全性。

借助 NetScaler Console 中的可观测性集成功能，您可以使用默认架构配置将洞察数据导出到 Prometheus。

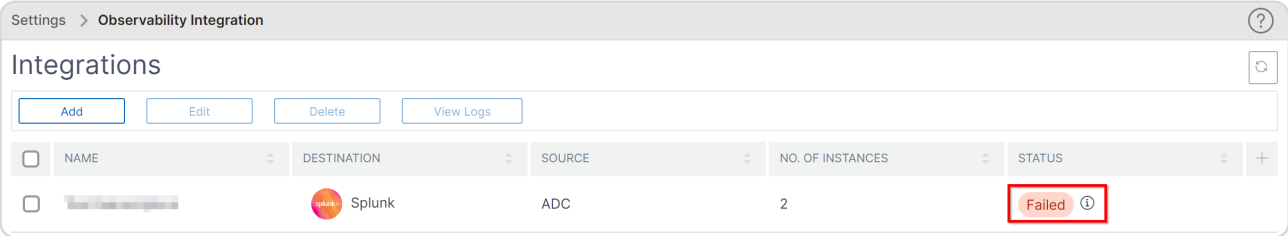
1. 导航到 **设置 > 可观测性集成**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

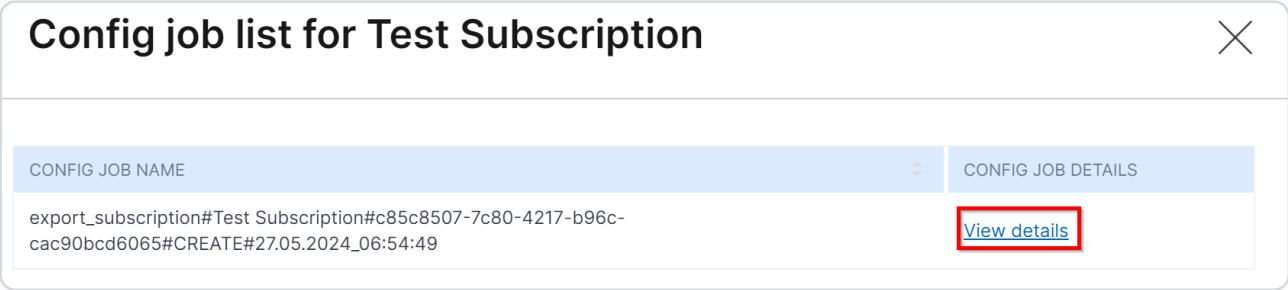
2. 在 **集成** 页面上，单击 **添加**。
3. 在 **创建订阅** 页面上，指定以下详细信息：
   a. 在 **订阅名称** 字段中指定一个您选择的名称。
   b. 选择 **NetScaler** 作为 **源**，然后单击 **下一步**。
   c. 选择 **Prometheus** 作为目标。
   d. 选择 **默认** 以导出默认洞察数据。
   e. 单击 **添加实例**，并选择要将洞察数据导出到 Prometheus 的实例。
   f. 单击 **提交**。

查看失败配置的日志

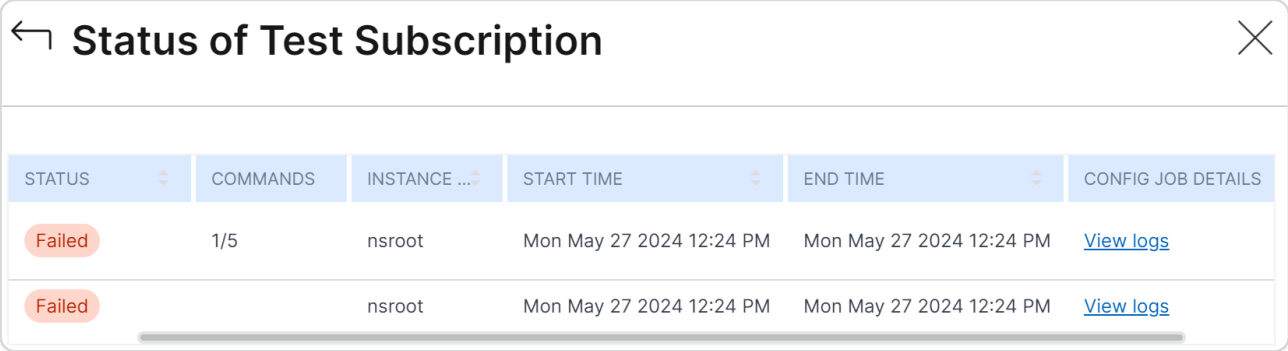
创建订阅后，您可以在 **设置 > 可观测性集成** 中查看已创建订阅的状态。如果状态显示为 **失败**，请单击以查看详细信息。



单击“**配置作业详细信息**”下的“**查看详细信息**”。



单击“**查看日志**”以查看问题的详细信息。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置将 NetScaler® 指标和审计日志导出到 Splunk

NetScaler 支持以 JSON 格式将指标直接导出到 Splunk。NetScaler 提供丰富的指标来监控您的应用程序健康状况和应用程序安全健康状况。通过将 NetScaler 提供的指标导出到 Splunk，您可以可视化这些指标并获得有意义的见解。

审计日志记录使您能够记录 NetScaler 中各个模块收集的 NetScaler 状态和状态信息。通过审查日志，您可以排查问题或错误并进行修复。

有关详细信息，请参阅：

- 将审计日志直接从 NetScaler 导出到 Splunk
- 将指标直接从 NetScaler 导出到 Splunk

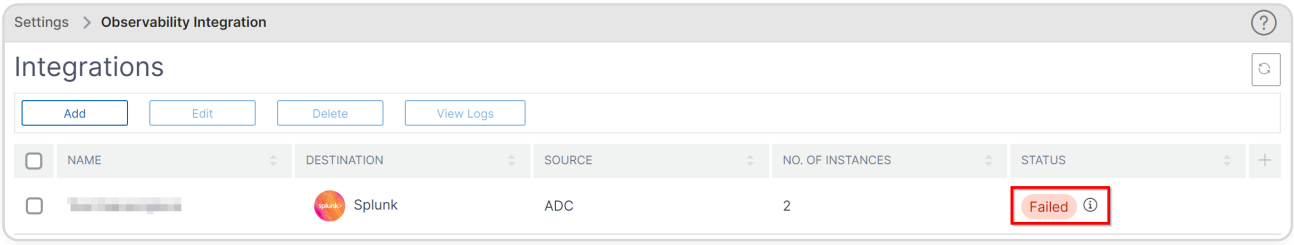
要通过 NetScaler Console 配置指标和审计日志导出到 Splunk：

1. 导航到 **设置 > 可观测性集成**。
2. 在“**集成**”页面上，单击“**添加**”。
3. 在“**创建订阅**”页面上，指定以下详细信息：
   a. 在“**订阅名称**”字段中指定一个您选择的名称。
   b. 选择 **NetScaler** 作为**源**，然后单击“**下一步**”。
   c. 选择 **Splunk** 作为**目标**，然后单击“**配置**”。在“配置端点”中：
      - **端点 URL** - 指定 Splunk 端点详细信息。端点必须采用 `https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event`` 格式。
      - **身份验证令牌** - 从 Splunk 复制并粘贴身份验证令牌。
      - 单击 **提交**。
   d. 单击 **下一步**。
   e. 单击 **添加洞察** 并选择 **NetScaler 指标** 和 **NetScaler 审计日志**，然后单击 **添加所选**。
   f. 单击 **下一步**。
   g. 单击 **添加实例** 并选择实例。
   h. 单击 **提交**。

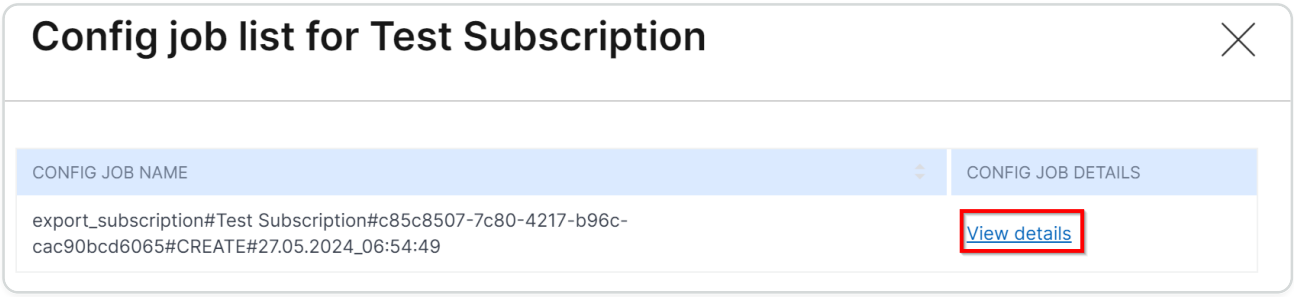
查看失败配置的日志

创建订阅后，您可以在 **设置 > 可观测性集成** 查看已创建订阅的状态。如果状态显示为 **失败**，请单击以查看详细信息。

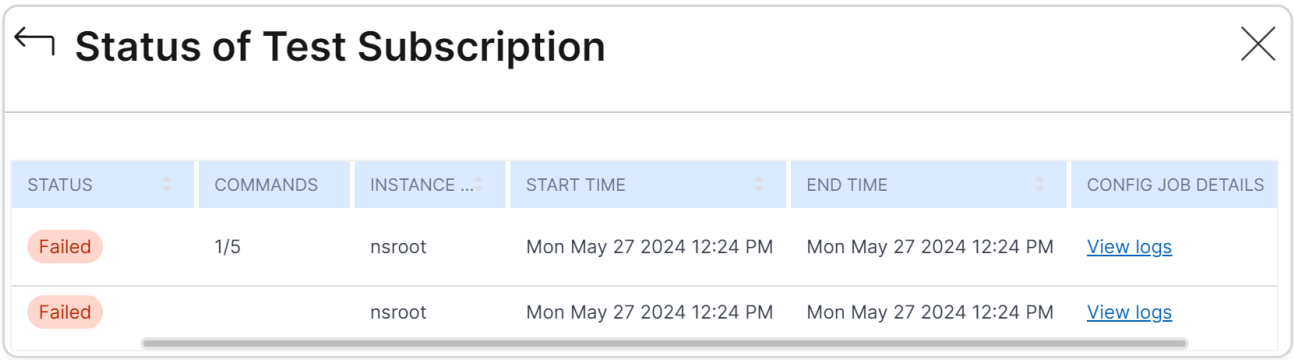
© 1997–2026 Citrix Systems, Inc. All rights reserved.



在 **配置作业详细信息** 下单击 **查看详细信息**。



单击 **查看日志** 以查看问题的详细信息。



访问控制列表

访问控制列表 (ACL) 是一组条件，您可以将其应用于网络设备以过滤 IP 流量并保护您的设备免受任何未经授权的访问。

您可以在 NetScaler Console GUI 中配置 ACL，以限制和控制对 NetScaler Console 的访问。NetScaler Console 上的 ACL 从 14.1-29.x 版本开始支持。

使用指南

- 当您将 NetScaler Console 升级到 14.1-29.x 版本时，ACL 功能默认是禁用的。
- 作为管理员，您只能通过 NetScaler Console 上的 ACL 控制入站数据包。
- NetScaler Console 上的任何配置都不需要更改现有的 ACL 配置。

如何配置 ACL

配置 ACL 涉及：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 启用 ACL 功能
- 创建 ACL 规则
- 启用 ACL 规则

启用 ACL 功能

1. 登录 NetScaler Console GUI 并导航到 **Settings > Access Control List (ACL)**
2. 使用切换按钮，打开 ACL 功能。

创建 ACL 规则

1. 在 ACL 页面上，单击 **创建规则**。
2. 在 **创建规则** 窗口中，添加下表中列出的详细信息：

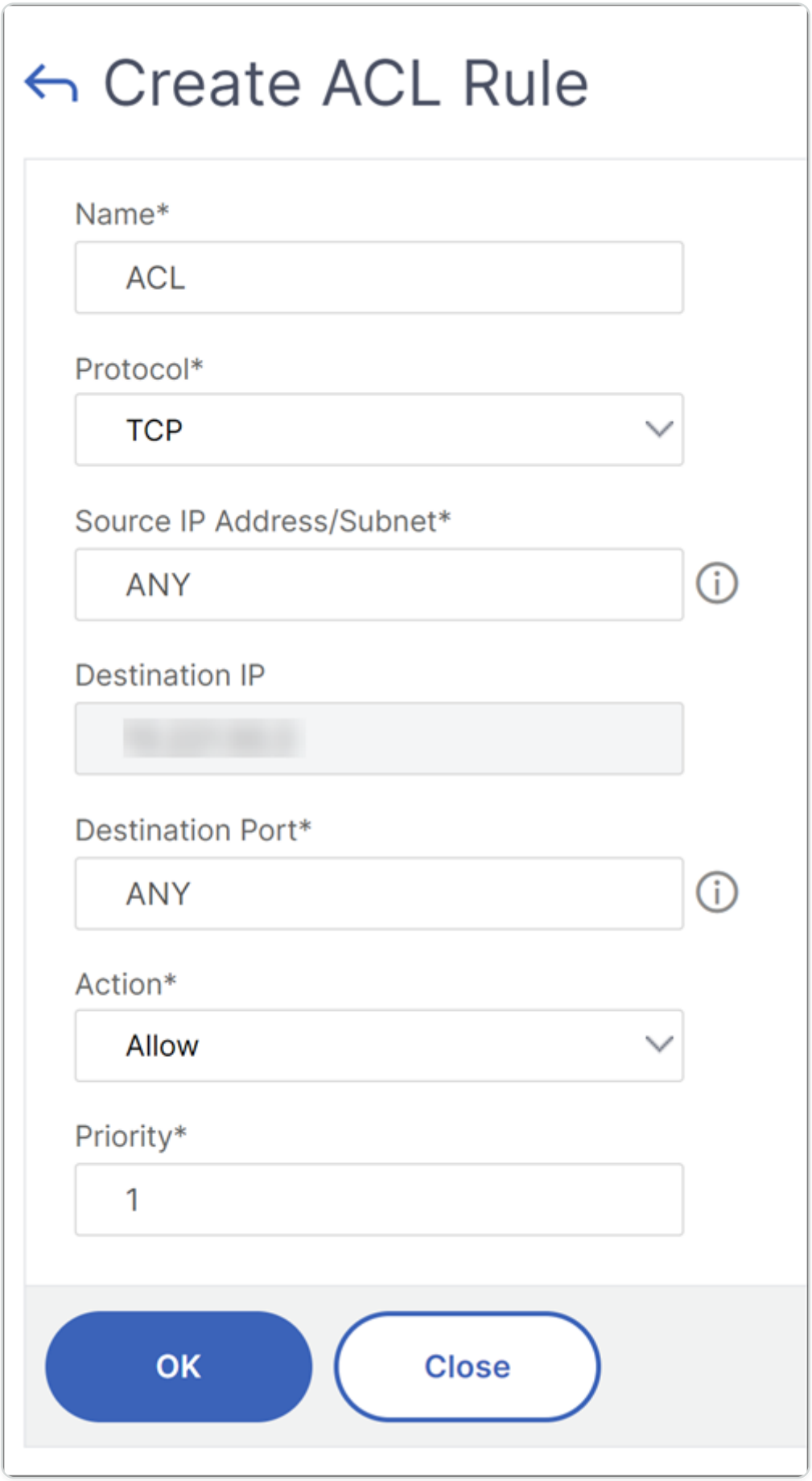
选项	描述
名称	指定一个您选择的名称。
协议	从菜单中选择一个协议。默认情况下，选择 TCP。您可以选择 ANY 以允许所有协议。
源 IP 地址/子网	指定规则适用的源 IP 地址或源子网。如果规则必须应用于所有传入流量，请选择 ANY。
目标 IP	NetScaler Console IP 地址会自动填充为目标 IP。此字段无法编辑。
目标端口	指定规则适用的目标端口。如果规则适用于所有目标端口，请选择“任意”。
操作	选择规则的操作，即“允许”或“拒绝”。
优先级	分配优先级以指定规则的评估顺序。优先级数字决定了 ACL 规则与传入数据包匹配的顺序。优先级数字越低，优先级越高。例如，优

© 1997–2026 Citrix Systems, Inc. All rights reserved.

选项	描述
	先级数字 1 的优先级高于优先级数字 2。如果没有规则与传入数据包匹配，则该数据包将被阻止。

3. 单击“**确定**”创建规则。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



规则创建后，处于禁用状态。要使规则生效，必须启用该规则。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

要启用规则，必须启用 ACL 功能。如果该功能被禁用，并且您尝试启用 ACL 规则，则会出现“ACL 未运行”的消息。

启用 ACL 规则

1. 将鼠标悬停在要启用的规则上，然后单击带有三个点的圆圈。
2. 从菜单中选择“**启用**”。
3. 或者，选择该规则的单选按钮，然后单击“启用”选项卡。
4. 在提示符处，单击“**是**”以确认。

ACL 规则的其他操作

您可以对 ACL 规则执行以下操作：

- 禁用 ACL 规则
- 编辑 ACL 规则
- 删除 ACL 规则
- 重新编号 ACL 规则的优先级

禁用 ACL 规则

1. 将鼠标悬停在要禁用的规则上，然后选择带有三个点的圆圈。
2. 从列表中单击 **禁用**。
3. 或者，选择该规则的单选按钮，然后单击 **禁用** 按钮。
4. 单击 **是** 确认。

注意：

禁用规则后，该规则不再适用于传入流量。但是，规则配置仍保留在 ACL 设置下。

编辑 ACL 规则

1. 将鼠标悬停在要编辑的规则上，然后选择带有三个点的圆圈。
2. 单击列表中的**编辑规则**。
3. 或者，选择该规则的单选按钮，然后单击**编辑规则**按钮。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 进行编辑，然后单击**确定**。

> **注意：**
>
> 您可以在启用和禁用状态下编辑规则。如果您编辑已启用的规则，则更改会立即应用。对于处于禁用状态的规则，更改会在您启用规则时应用。

删除 ACL 规则

1. 确保规则处于禁用状态。您无法删除处于启用状态的规则。
2. 将鼠标悬停在要删除的规则上，然后选择带有三个点的圆圈。
3. 单击列表中的**删除规则**。
4. 或者，选择该规则的单选按钮，然后单击**删除规则**按钮。
5. 单击**是**以确认。

重新编号 ACL 规则的优先级

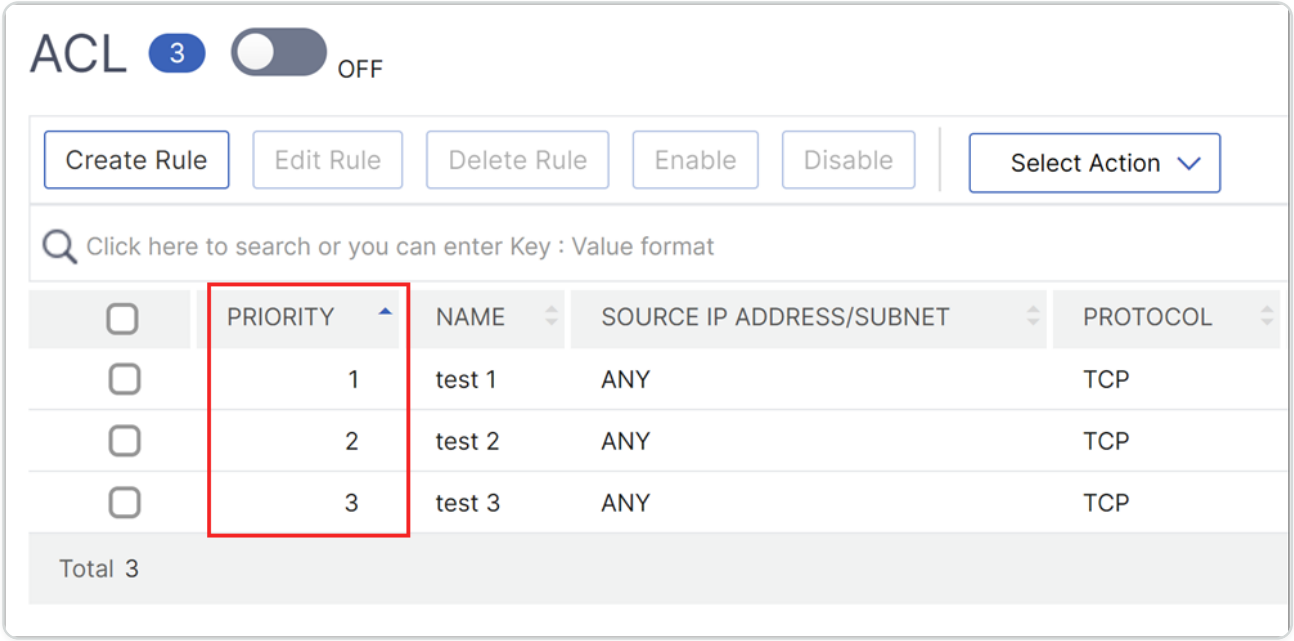
1. 将鼠标悬停在要重新编号优先级的规则上，然后选择带有三个点的圆圈。单击列表中的**重新编号优先级**。
2. 或者，选择该规则的单选按钮，然后从**选择操作**列表中选择**重新编号优先级**。

NetScaler® 自动为所有现有规则分配新的优先级编号（10 的倍数）。

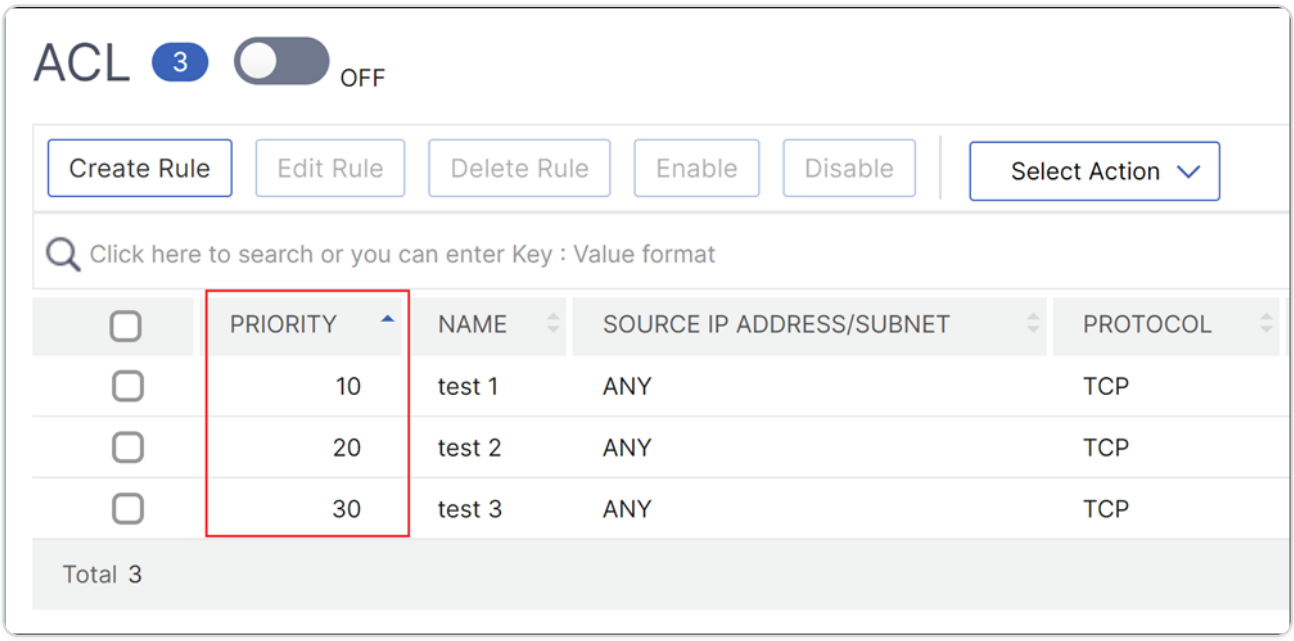
根据您的要求编辑规则以分配优先级编号。有关如何编辑规则的更多信息，请参阅“编辑 ACL 规则”部分。

现有优先级编号示例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



NetScaler Console 重新编号的优先级示例：



故障排除

如果 ACL 规则设置不当，所有用户帐户都可能被拒绝访问。如果您因 ACL 设置不当而意外失去对 NetScaler Console 的所有网络访问权限，请按照以下步骤获取访问权限：

1. 使用 SSH 客户端登录到 NetScaler Console。
2. 运行命令 `pfctl -d`。
3. 登录到 NetScaler Console GUI 并相应地重新配置 ACL。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 NetScaler Console 审计日志管理和监控您的基础架构

您可以使用 NetScaler Console 服务跟踪 NetScaler Console 上的所有事件以及在 NetScaler Console 管理的 NetScaler 实例上生成的 syslog 事件。这些消息可以帮助您管理和监控您的基础架构。但是，日志消息只有在您查看它们时才是一个很好的信息来源，而 NetScaler Console 简化了查看日志消息的方式。

您可以使用过滤器搜索 NetScaler Console syslog 和审计日志消息。这些过滤器有助于缩小结果范围，并实时准确地找到您要查找的内容。内置的搜索帮助会指导您过滤日志。查看日志消息的另一种方法是将其导出为 PDF、CSV、PNG 和 JPEG 格式。您可以安排在不同时间间隔将这些报告导出到指定的电子邮件地址。

您可以从 NetScaler Console GUI 查看以下类型的日志消息：

- NetScaler 实例相关的审计日志
- NetScaler Console 相关的审计日志
- 应用程序审计日志

NetScaler 实例相关的审计日志

在您可以通过 NetScaler Console 查看 NetScaler 实例相关的 syslog 消息之前，请将 NetScaler Console 服务配置为您的 NetScaler 实例的 syslog 服务器。配置完成后，所有 syslog 消息都将从实例重定向到 NetScaler Console。

将 NetScaler Console 服务配置为 syslog 服务器

请按照以下步骤将 NetScaler Console 配置为 syslog 服务器：

1. 在 NetScaler Console 图形用户界面中，导航到 **Infrastructure > Instances**。
2. 选择要从中收集 syslog 消息并在 NetScaler Console 中显示的 NetScaler 实例。
3. 在 **Select Action** 列表中，选择 **Configure Syslog**。
4. 单击 **Enable**。
5. 在“**Facility**”下拉列表中，选择本地或用户级别的设备。
6. 选择 syslog 消息所需的日志级别。
7. 单击“**确定**”。

在 NetScaler Console 上配置 syslog(/en-us/netscaler-application-delivery-management-software/media/configure-syslog-adm.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

这些步骤配置 NetScaler 实例中的所有 syslog 命令，NetScaler Console 开始接收 syslog 消息。您可以通过导航到“**基础架构 > 事件 > Syslog 消息**”来查看消息。单击“**需要帮助？**”以打开内置搜索帮助。有关详细信息，请参阅查看和导出 syslog 消息。

NetScaler Console 上的 Syslog 消息(/en-us/netscaler-application-delivery-management-software/media/adm-syslog-messages.png)

要导出日志消息，请单击右上角的箭头图标。

接下来，单击“**立即导出**”或“**计划导出**”。有关详细信息，请参阅查看和导出 syslog 消息。

NetScaler Console 相关的审核日志

根据预配置的规则，NetScaler Console 为相应的事件生成审核日志消息，帮助您监控基础架构的运行状况。

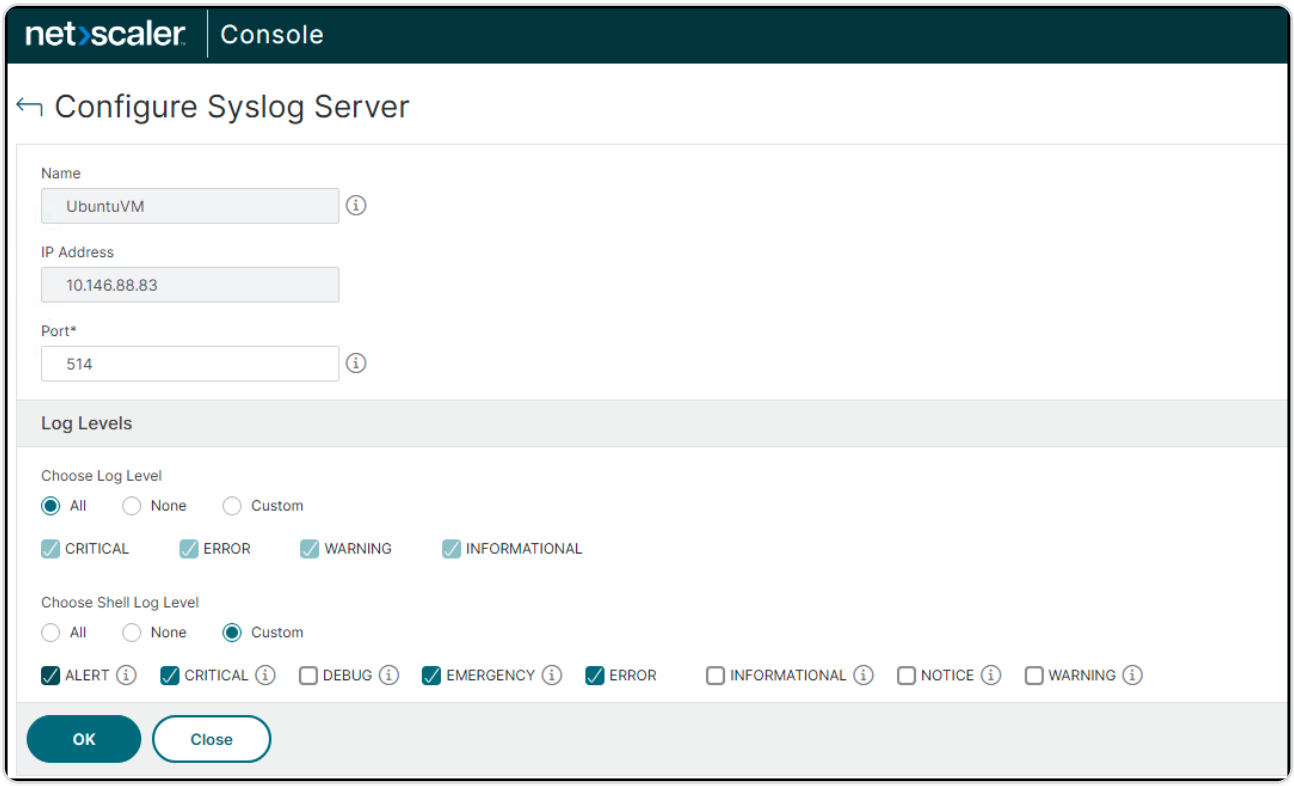
配置 syslog 服务器以监控审核日志和 shell 日志

您可以配置外部 syslog 服务器来监控 NetScaler Console 部署的审核日志和 shell 日志事件。对于 14.1-34.x 及更高版本，您可以配置 syslog 服务器以接收 shell 日志事件。这是对现有审核日志配置的补充。与审核日志类似，shell 日志可以配置为不同的日志级别。

请按照以下步骤在 NetScaler Console 上配置 syslog 服务器：

1. 导航到“**UI 设置 > 审核日志 > Syslog 服务器**”。
2. 选择审核日志、shell 日志或两者的日志级别。
   - **全部**：选择所有列出的用于审计或 shell 相关事件的日志级别。
   - **无**：清除所有选择，不选择任何日志级别。
   - **自定义**：允许您从以复选框形式提供的可用列表中选择特定的日志级别。
3. 单击 **确定** 以继续使用所选配置。这使 NetScaler Console 能够将审计和/或 shell 相关事件发送到配置的 syslog 服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



要查看 NetScaler Console 中存在的所有审计日志消息，请导航到 **Settings > Audit Log Messages**。

要导出日志消息，请单击右上角的箭头图标。

应用程序相关审计日志

您可以查看适用于所有 NetScaler Console 应用程序或特定应用程序的审计日志消息。

- 要查看 NetScaler Console 中所有应用程序的所有审计日志消息，请导航到 **Infrastructure > Network Functions > Auditing**。
- 要查看 NetScaler Console 中任何特定应用程序的审计日志消息，请导航到 **Applications > Dashboard**，单击虚拟服务器并选择 **Audit Log**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler 许可证

NetScaler Console 使您能够管理、分配和监控您的 NetScaler 实例的许可证。以下主题可帮助您管理 NetScaler 许可证：

- 许可证激活服务
- 最佳实践
- 许可证管理
- 签出许可证的最小和最大容量
- NetScaler Flexed 许可证
- 配置许可
- 许可证仪表板
- 许可证报告
- 过渡到 Flexed 许可
- Flexed 或 Pooled 许可证到期和连接问题行为的场景
- 将 NetScaler Console 配置为 Flexed 或 Pooled 许可证服务器
- 旧版许可证

许可证激活服务

重要提示：

传统上用于激活各种本地组件的基于文件的许可系统（也称为手动管理的授权）将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活所有 Citrix 产品的新一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler Flexed 许可证（Citrix 平台许可证/通用混合多云）、旧版 NetScaler 池许可证和 NetScaler 固定期限带宽许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是兼容 LAS 的版本。

兼容 LAS 的最低 NetScaler 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Console Service：自 2025 年 9 月初起支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： Console 本地部署的 LAS 支持从版本 14.1-51.x 开始。但是，自 April 15 2026 起，Console 本地部署版本 14.1-51.x 及更高版本以及 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署版本 14.1-51.x 或 13.1-60.x 或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署版本 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如 NetScaler 虚拟 CPU 许可（池化 vCPU）、NetScaler VPX 签入和签出 (CICO)，以及永久许可证将不受 LAS 支持。升级到上述软件版本后，使用没有有效维护的永久许可证的 NetScaler 实例将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。如果未能遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外，Citrix 还可能根据法律或衡平法采取任何其他补救措施。在法律或法规禁止的情况下，这些要求不适用。
在开始向 LAS 过渡之前，我们建议阅读 适用于 NetScaler 的 LAS。这可确保您了解一般先决条件、支持或不支持的许可证类型、适用于您的特定许可证和部署类型的准确工作流程以及其他重要信息。

许可证激活服务 (LAS) 是一种新的基于云的许可解决方案，它提供了传统基于文件的许可的替代方案。LAS 引入了用于激活 Citrix 和 NetScaler 产品的新模块，确保了无缝且现代的许可证管理方法。

备注：

- LAS 是一种许可机制，而不是许可类型。
- 基于文件的许可指的是使用手动授权的较旧许可方法。本文档中，“基于文件的许可”和“手动管理的授权”可互换使用，因为它们描述的是相同的概念。

以下是 LAS 的主要优势：

- 通过授权 blob 自动交付授权。
- 外部代理作为许可通信的代理是可选的。
- LAS 消除了 NetScaler MPX™ 和 SDX 实例上对 Z-Cap 软件许可证文件的需求。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意事项：

- 新的“同步许可证”选项允许您手动按需触发同步，确保授权立即更新。
- 如果 LAS 授权尚未与 NetScaler Console 服务同步，则授权同步的默认频率为每小时一次，此后每 24 小时一次。对于按需同步，请点击 `Sync Now`。

NetScaler 与 LAS 的版本兼容性

要使用 LAS，您的 NetScaler 实例必须运行以下最低版本之一：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console 服务：自 2025 年 9 月初起支持。
- NetScaler Console 本地部署：14.1-51.x

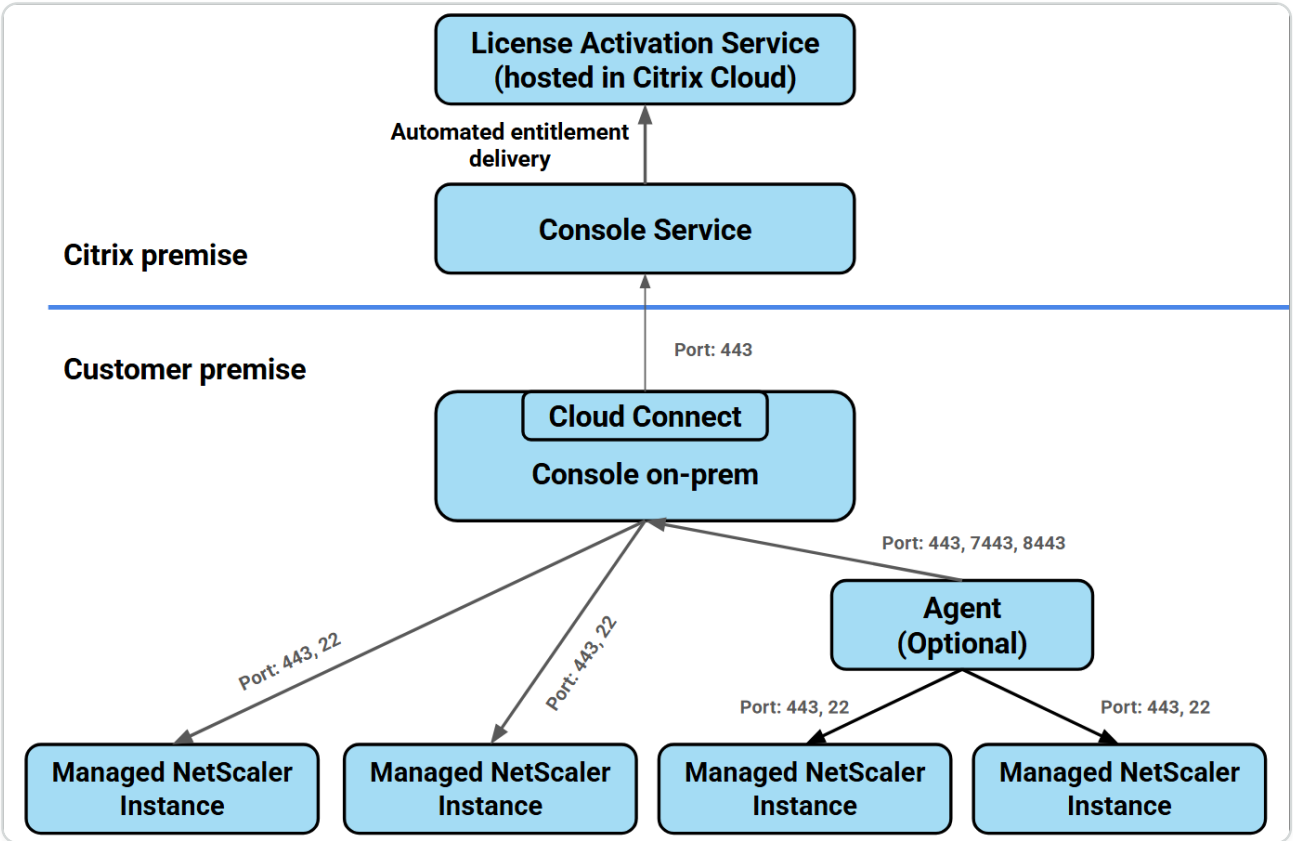
注意：

要使用 LAS，请确保已完成以下先决条件：

- 您必须拥有有效的 Citrix Cloud 帐户。有关现有云帐户或加入新云帐户的更多信息，请参阅 帐户管理。
- 用于 LAS 激活工作流的 Citrix Cloud 帐户关联的组织 ID (Org ID) 必须拥有有效的已购买权利。要查看当前权利，请访问 权利。
- NetScaler Console 和 NetScaler 实例必须运行与 LAS 兼容的版本。
- NetScaler 实例已作为托管实例添加到 NetScaler Console 中。
- LAS 支持弹性许可 (UHMC/CPL)、池带宽许可和固定期限带宽许可。LAS 不支持所有其他形式的传统 NetScaler 许可证，例如池化 vCPU、CICO。
- 对于 SDX 设备，请将 NetScaler SVM 升级到 LAS 支持的版本，并转换为基于 LAS 的许可。特定的 VPX 版本不影响 LAS 兼容性。

下图显示了带有 Console 本地 Cloud Connect 的 LAS。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

如果您是 NetScaler Console 的新用户，请从 入门 开始。

过渡到 LAS

通过 Cloud Connect 激活 LAS

通过 Cloud Connect 激活 LAS 选项适用于云连接的 Console 本地部署。此部署通过自动下载权利并直接从 Console 服务处理及时续订来简化许可证管理。

注意：

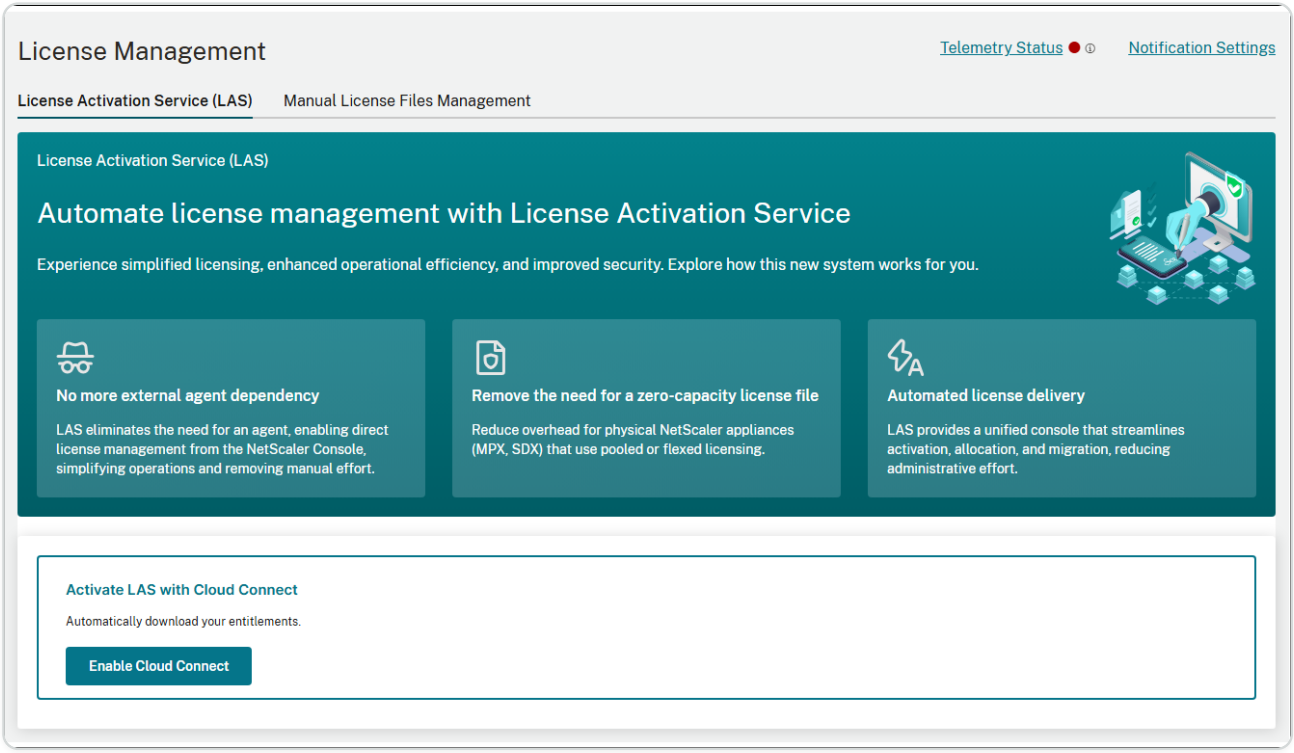
- 确保已启用“**启用云连接**”选项，以使用“**通过云连接激活 LAS**”部署方法。要启用此选项，请参阅启用云连接。
- 启用云连接后，LAS 会自动启用。

您可以通过检查 Console GUI 的右上角来验证云连接是否已启用。连接到 NetScaler Console Service 后，您将被定向到“**许可证管理**”下的“**LAS**”选项卡。在此处，您可以查看上次和下次续订日期，但无需手动操作。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

激活 LAS 涉及在本地 NetScaler Console 上获取许可证授权文件或 blob。当您导航到“**NetScaler 许可 > 许可证管理 > LAS**”时，将显示许可证激活服务 (LAS) 的简介。

在您的本地 Console 上启用 LAS 后，您的所有 NetScaler 弹性许可和池许可授权都将显示在“**NetScaler 许可 > 许可证管理 > 许可证激活服务 (LAS)**”部分。

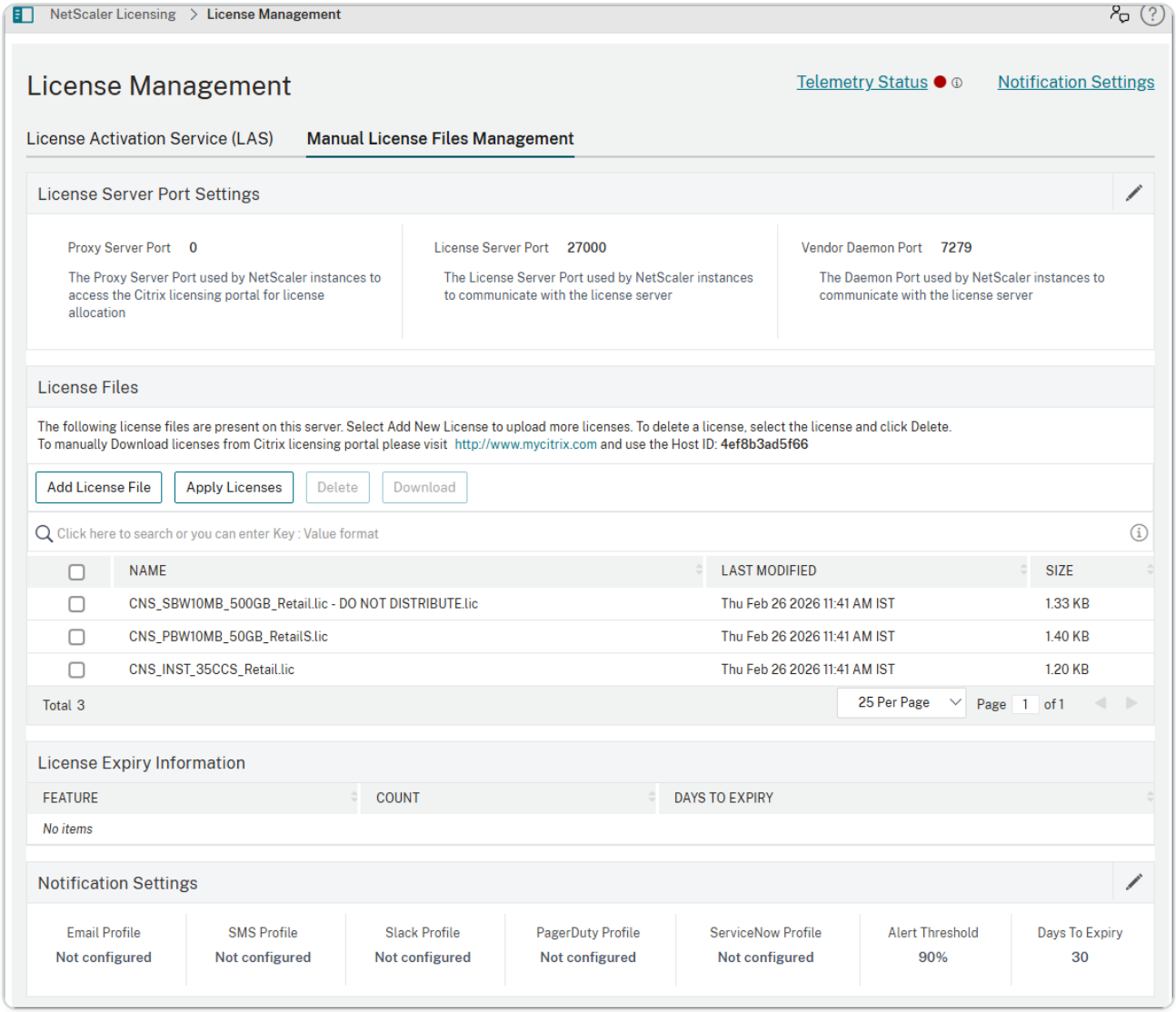


借助其云连接功能，本地 Console 连接到 Console Service，后者从 LAS 检索许可证授权文件或 blob。

此授权文件或 blob 有效期为 30 天。为确保持续许可，云连接的 Console 每天都会使用 LAS 自动刷新此授权 blob。

对于基于文件的许可，您应用的授权和配置在“**NetScaler 许可证 > 许可证管理 > 手动许可证文件管理**”选项卡下可见。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



许可证管理页面上的遥测状态指示器是维护遥测合规性的关键警报。

- **红色图标**：表示需要立即关注。系统未收集部分或所有托管 NetScaler 实例的遥测数据。此状态表示可能存在遥测不合规和许可影响。
- **绿色图标**：确认遥测处于活动状态，表明控制台正在成功地从所有托管 NetScaler 实例发送遥测数据。

如果状态需要立即关注，请单击指示器访问遥测页面。确保修复 NetScaler 遥测页面上突出显示的所有问题。有关更多详细信息，请参阅遥测数据收集和上传问题故障排除诊断。

许可或将 NetScaler 实例迁移到 LAS

当您导航到 **NetScaler Licenses > License management > License Activation Service (LAS)** 时，GUI 会根据您的 NetScaler 实例的兼容性动态更新。 如果您的 NetScaler 实例没有兼容 LAS 的版本，屏幕上会显示一条消息，指示您升级或添加 NetScaler。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

如果您的某些 NetScaler 实例已升级到兼容版本，您可以将 LAS 用于这些特定实例。

如果您的一个或多个 NetScaler 实例与 LAS 兼容，它们将分为两类：

使用 LAS 许可 NetScaler 实例： 这些是尚未启用 LAS 但兼容的实例。

将已许可的 NetScaler 实例迁移到 LAS： 这些是已通过其他方法许可并符合迁移到 LAS 条件的实例。

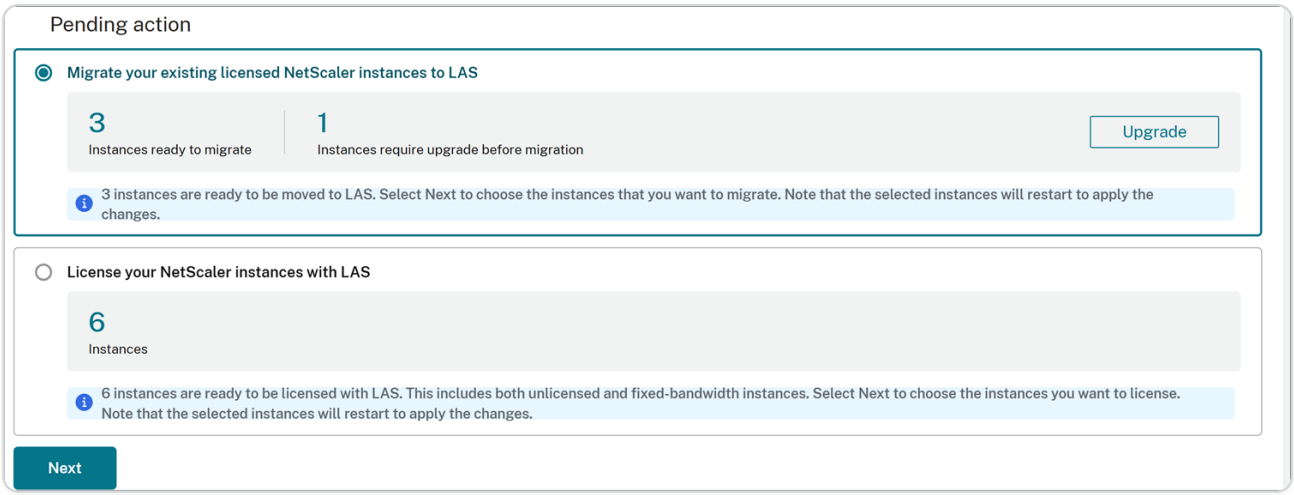
NetScaler GUI 会根据您是首次使用 LAS 的用户（LAS 上没有实例）还是现有用户（LAS 上已有实例，现在正在添加更多实例）进行动态调整。

注意：

一旦完成许可或迁移到 LAS，请删除 SVM 上的本地文件许可证。文件许可证位于 SVM 文件夹 `/mpsconfig/license` 中，必须使用 shell 提示符从该文件夹中删除。此注意事项适用于首次用户和现有用户的“**使用 LAS 许可**”和“**迁移到 LAS**”工作流。

首次用户

首次用户将显示以下图像：



使用 LAS 许可 NETSCALER 实例

“**使用 LAS 许可 NetScaler 实例**”部分列出了当前未许可或未使用弹性带宽或池化带宽文件许可证的 NetScaler 实例。

要使用 LAS 许可实例，请执行以下步骤：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 选择 **使用许可证激活服务 (LAS) 许可**，然后单击 **下一步**。
2. 选择一个实例，然后单击 **继续**。
3. 输入详细信息，然后单击 **提交**。 对要使用 LAS 许可的每个 NetScaler 实例重复这些步骤。

注意：

- 除 SDX 实例外，所选实例将重新启动以使许可证生效。

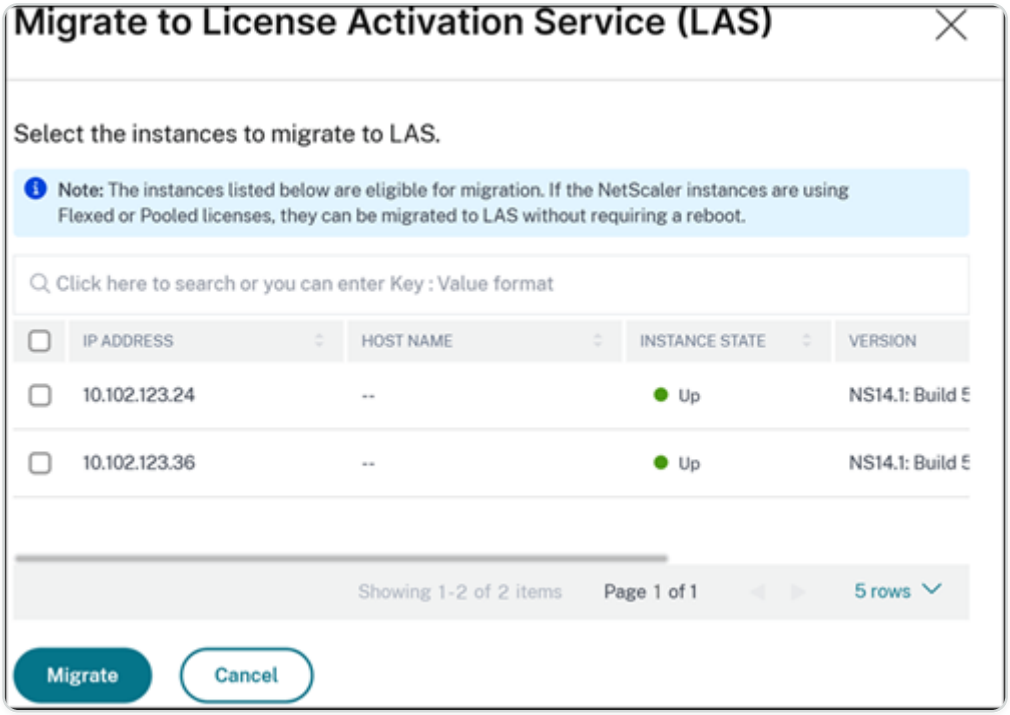
将现有许可的 NETSCALER 实例迁移到 LAS

将现有许可实例迁移到 LAS 部分列出了所有具有弹性或池化文件许可证的 NetScaler 实例。它们分类如下：

- **准备迁移的实例：** 列出处于 LAS 兼容版本或内部版本并准备迁移到 LAS 的实例。要迁移，请执行以下步骤：

  a. 选择 **将现有许可的 NetScaler 实例迁移到 LAS**，然后单击 **下一步**。

  b. 在 **迁移到许可证激活服务 (LAS)** 中，选择一个或多个 NetScaler 实例，然后单击 **迁移**。



。

- **迁移前需要升级的实例：** 列出在迁移前需要升级到兼容版本或内部版本的实例。要升级，请执行以下步骤：

  先决条件：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

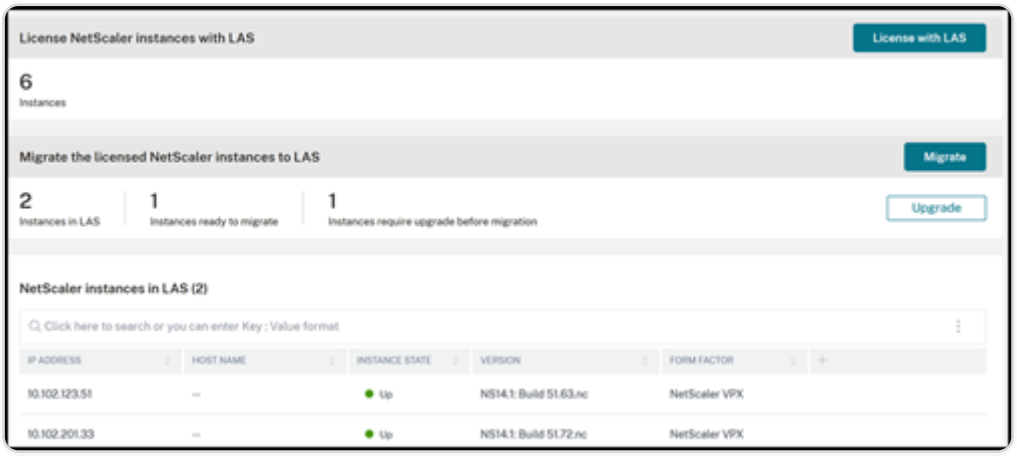
要使用基于 LAS 的许可，您的 NetScaler 实例版本必须与您的池化或弹性文件许可证版本匹配。在开始迁移之前，请确保将实例的版本更改为与新许可证匹配。

a. 选择 **将现有许可的 NetScaler 实例迁移到 LAS**，然后单击 **升级**。

b. 在 **升级 NetScaler** 页面中，选择实例并将实例升级到与 LAS 兼容的版本或内部版本。

现有 LAS 用户

如果您是现有 LAS 用户，您会看到以下 GUI。



。

注意： 要查看使用 LAS 许可的 CPX 实例，请参阅 Flexed Dashboard GUI。CPX 实例未在此处列在“使用 LAS 的 NetScaler 实例”下。

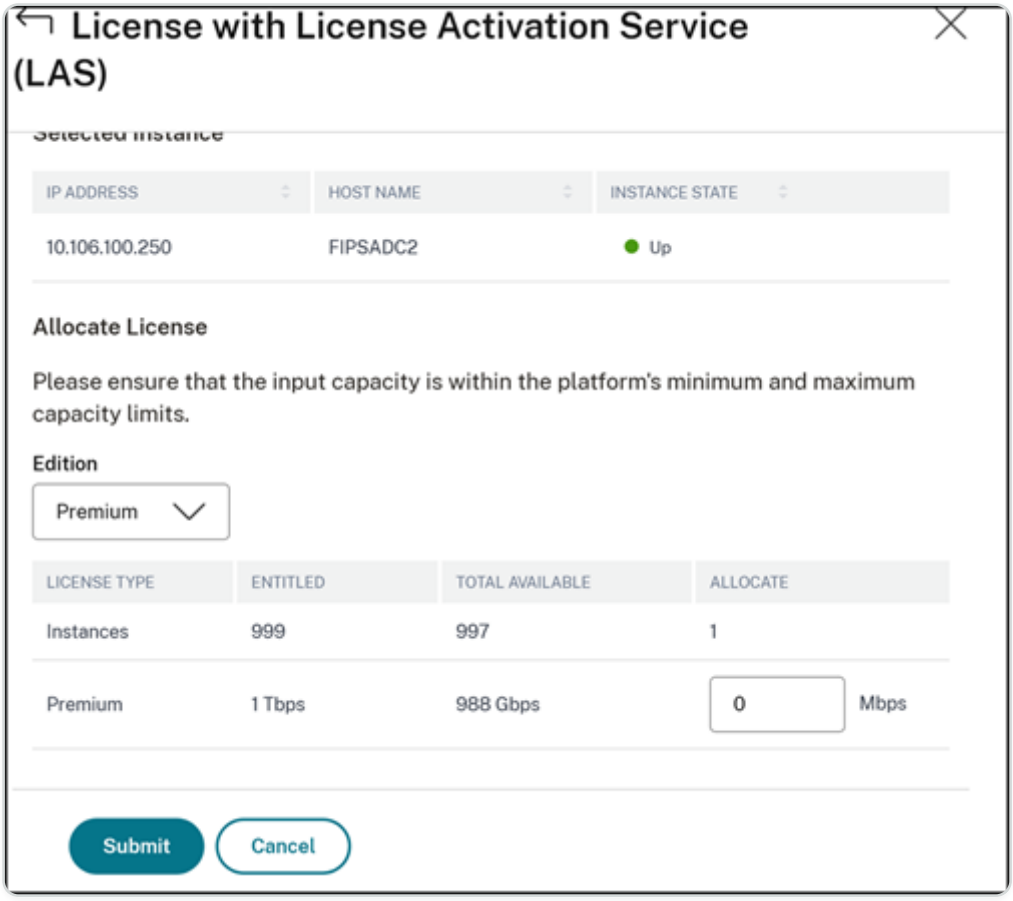
使用 LAS 许可 NETSCALER 实例

使用 LAS 许可 NetScaler 实例 部分列出了当前未获得许可或使用 Flexed 带宽或池化带宽文件许可证以外的任何许可证的 NetScaler 实例。

要使用 LAS 许可实例，请执行以下步骤：

1. 在 **使用许可证激活服务 (LAS) 许可** 下，单击 **使用 LAS 许可**。
2. 选择一个实例，然后单击 **继续**。
3. 输入详细信息，然后单击 **提交**。 对要使用 LAS 许可的每个 NetScaler 实例重复这些步骤。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



。

注意：

- 所选实例将重新启动以使许可证生效，SDX 实例除外。

将许可的 NETSCALER 实例迁移到 LAS

将许可的 NetScaler 实例迁移到 LAS 部分列出了所有具有弹性或池化文件许可证的 NetScaler 实例。它们分类如下：

- **LAS 中的实例：** 列出已使用基于 LAS 的许可的实例。
- **准备迁移的实例：** 列出兼容的、准备好迁移的实例。要迁移，请执行以下步骤：
  a. 选择**将许可的 NetScaler 实例迁移到 LAS**，然后单击**迁移**。
  b. 选择一个或多个 NetScaler 实例，然后单击**迁移**。
- **迁移前需要升级的实例：** 列出需要升级到兼容版本的实例。要升级，请执行以下步骤：

  先决条件：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要使用基于 LAS 的许可，您的 NetScaler 实例版本必须与您的池化或弹性许可证版本匹配。在开始迁移之前，请确保将实例的版本更改为与新许可证匹配。

a. 选择**迁移前需要升级的实例**，然后单击**升级**。
b. 选择一个或多个 NetScaler 实例，然后单击**升级**。
c. 输入详细信息，然后单击**提交**。

许可证激活 Blob 行为

NetScaler 实例作为**使用 LAS 许可或迁移到 LAS** 的一部分从本地控制台获取的许可证激活 Blob 有效期为 30 天。如果 NetScaler 失去连接然后重新获得与本地控制台的连接，许可证激活 Blob 将立即恢复。

当 NetScaler 无法在长达 24 小时内重新连接到本地控制台时，它将进入宽限期。 默认情况下，许可证激活 Blob 每 8 小时刷新一次。如果连续三次 8 小时刷新尝试在 24 小时内失败，NetScaler 将进入宽限期。

许可证宽限期警报

以下是许可证宽限期警报的通知点：

- 在 Flexed 控制面板上，会显示一个警告图标，指示实例处于宽限期以及许可证激活 blob 到期前的剩余天数。
- 每当管理员登录到 NetScaler 实例 GUI 时，都会出现一个弹出消息，指示实例处于宽限期以及许可证激活 blob 到期前的剩余天数。
- 电子邮件通知将发送到配置的电子邮件地址。有关详细信息，请参阅 配置电子邮件设置。

  注意： 请务必选择**许可证**作为系统事件类别，以接收与许可证相关的电子邮件通知。

当本地 Console 与 Console 服务之间的连接中断时，NetScaler 行为更新

在云连接部署中，LAS 直接向本地 NetScaler Console 颁发 LAS 激活 blob。本地 NetScaler Console 的激活 blob 每日刷新，有效期为 30 天，或直到许可证授权到期，以先到者为准。

一旦本地 NetScaler Console 收到此有效激活 blob，它就被授权向其获得许可的 NetScaler 实例颁发下游激活 blob。NetScaler Console 仅在其自身的 blob 有效时颁发这些下游 blob。

颁发给 NetScaler 实例的激活 blob 也有效期为 30 天，或直到 NetScaler Console 激活 blob 的剩余到期日期，以先到者为准。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

场景 A：NetScaler 与本地 NetScaler Console 之间的连接中断

如果 NetScaler 与本地 NetScaler Console 失去连接，本地 NetScaler Console 无法刷新实例的激活 blob。本地 NetScaler Console 每 8 小时重试刷新一次。

在 3 次失败尝试（总计 24 小时）后，NetScaler 实例进入**宽限**状态。受影响的 NetScaler 实例在本地 NetScaler Console GUI 中被标记为**宽限**状态。

> **注意：**
>
> 此行为适用于所有支持 LAS 的本地 NetScaler Console 版本。

场景 B：本地 NetScaler Console 与 NetScaler Console 服务之间的连接中断

如果本地 NetScaler Console 与 NetScaler Console 服务之间的链接中断，本地 NetScaler Console 无法刷新其自身的激活 blob。

在这种情况下，本地 NetScaler Console 无法颁发标准的 30 天滚动激活 blob，它会向 NetScaler 实例颁发有效期递减的 blob（29、28、27... 直到 0 天）。如果连接未在 30 天内恢复，NetScaler 实例将面临完全中断的风险。

在以前的版本中，这种情况会突然发生，NetScaler 实例从未进入 **Grace** 状态来警告管理员。

从版本 14.1-72.x 开始，此行为已更新，以防止意外中断。如果 NetScaler Console 服务连接中断且本地 NetScaler Console blob 无法刷新，则由本地 NetScaler Console 授权的 NetScaler 实例现在会自动进入 **Grace** 状态。

如果本地 NetScaler Console 与 NetScaler Console 服务之间的连接在 30 天内修复，NetScaler 实例将成功退出宽限期。

此更改可确保管理员通过 NetScaler Console GUI 中的 **Grace** 状态立即收到警报，以便他们在发生中断之前识别、排查并修复连接问题。

LAS 许可工作流期间发送到 LAS 的信息

本节详细介绍了在每个初始请求和每个 LAS 激活 blob 刷新请求期间，作为向 LAS 请求激活 blob 的一部分发送的所有信息。 下表总结了许可工作流期间发送到 LAS 的参数：

参数	描述	在 LAS 工作流中的用途
许可证服务器全局唯一标识符	UUID 格式的本地 Console 唯一 ID	LAS 绑定参数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述	在 LAS 工作流中的用途
许可证服务器ID	本地部署控制台的 SHA256 唯一 ID	LAS 绑定参数
公钥	用于 NetScaler 令牌分发的本地部署控制台的公钥	确保 LAS 已授权此控制台
客户端ID	用于载入本地部署控制台的 Citrix Cloud ID	LAS 绑定参数
许可证服务器版本	本地部署控制台的构建版本	LAS 激活要求
控制台 IP 和主机名	以 IP_hostname 格式表示的本地部署控制台的主机名	LAS 激活要求
activated_clients	具有 LAS 许可证、功能和请求时间的 NetScaler 列表。注意：NSIP 不共享；仅提供 LPEID（唯一 ID）。	此控制台生成的具有 LAS 激活 blob 的 NetScaler 列表。
上次激活ID	上一个 LAS 激活 ID，在续订时提供	用于 LAS 侧跟踪

注意：

从 NetScaler Console 本地部署版本 14.1-60.57 开始，适用于云连接部署的基于 LAS 的许可工作流不再使用 IP 地址和主机名。相反，LAS 使用系统标识符 (`lsguid`) 来唯一标识 NetScaler Console 本地部署的云连接部署。

监控已转换为 LAS 的 NetScaler Console 本地部署云连接环境的最佳实践

本文档重点介绍您可以遵循的、用于监控使用 LAS 的 NetScaler 环境的最佳实践。本文档适用于将 LAS 与 Console 本地部署结合使用的部署。

先决条件

- 阅读 适用于 NetScaler 的 LAS 页面，包括适用于 Console 服务的 LAS 常见问题解答。
- 阅读 许可证激活服务 并完成 LAS 迁移。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 确保设置相关通知，并定期监控 NetScaler GUI 和 CLI。

注意：

我们计划持续改进通知，并相应地更新本文档。

对于 NetScaler Console 本地部署，LAS 会向云连接的 NetScaler Console 本地部署提供 LAS 激活 Blob。该 Blob 的有效期为 30 天，或者直到许可证授权到期（以先到者为准），并且每天都会刷新。如果 NetScaler Console 本地部署与 NetScaler Console 服务之间的连接中断，NetScaler Console 本地部署将无法刷新其 LAS 激活 Blob。

监控 Console 本地部署 LAS 激活 Blob 过期 部分详细介绍了当 Console 本地部署 LAS 激活 Blob 在 30 天内到期时触发的通知。如果发生这种情况，您的云连接需要立即关注。要解决此问题，请运行云连接诊断工具以修复任何已识别的问题，或联系 Citrix 支持寻求帮助。

NetScaler Console 本地部署获取其 LAS 激活 Blob 后，它有权向所有需要通过 NetScaler Console 本地部署获得许可的 NetScaler 实例颁发激活 Blob。NetScaler Console 本地部署只能在其自己的 LAS 激活 Blob 仍然有效的情况下执行此操作。它向 NetScaler 实例颁发有效期为 30 天的 LAS 激活 Blob（或直到其自己的 Blob 到期，以先到者为准）。

如果 NetScaler 与 NetScaler Console 本地部署之间的连接丢失：

- Console 无法刷新 NetScaler 实例的 LAS 激活 Blob。
- Console 每八小时重试一次连接。
- 在三次尝试失败（总计 24 小时）后，NetScaler 进入“宽限期”状态，这将在 Console UI 中反映出来。

“(#monitor-netscaler-instances-las-activation-blob-expiry-netscaler-licensed-through-console-on-premises-cloud-connected)监控 LAS 激活 Blob 到期”部分详细介绍了临近其到期日期（少于 30 天）的 LAS 激活 Blob 的通知。如果发生这种情况，您的云连接需要立即关注。要解决此问题，请运行云连接诊断工具以修复任何已识别的问题，或联系 Citrix 支持寻求帮助。

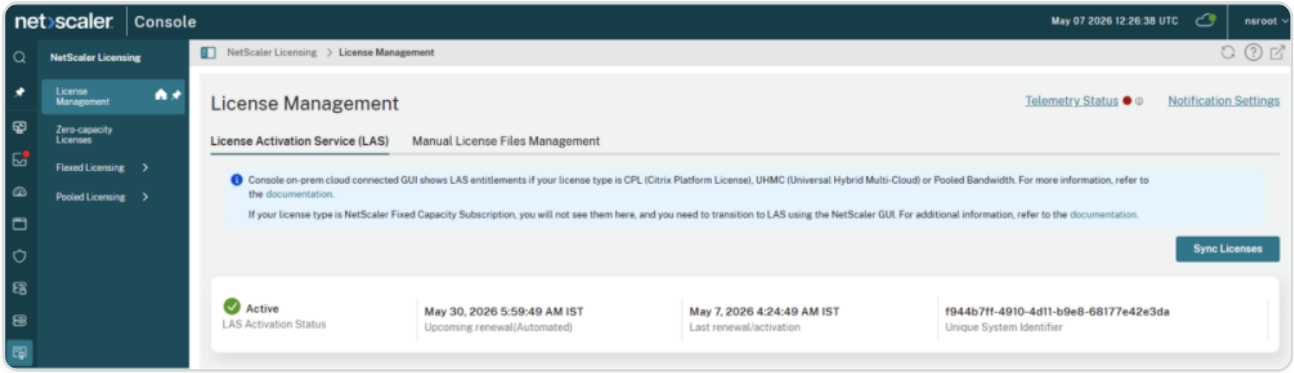
监控本地 Console LAS 激活 Blob 到期

使用 GUI 监控上次续订日期

要监控上次续订或激活日期，请导航到 Console on-premises GUI > NetScaler Licensing > License Management > LAS。

续订/刷新每天进行。如果上次续订/激活日期已超过几天，则表示存在连接或激活问题。

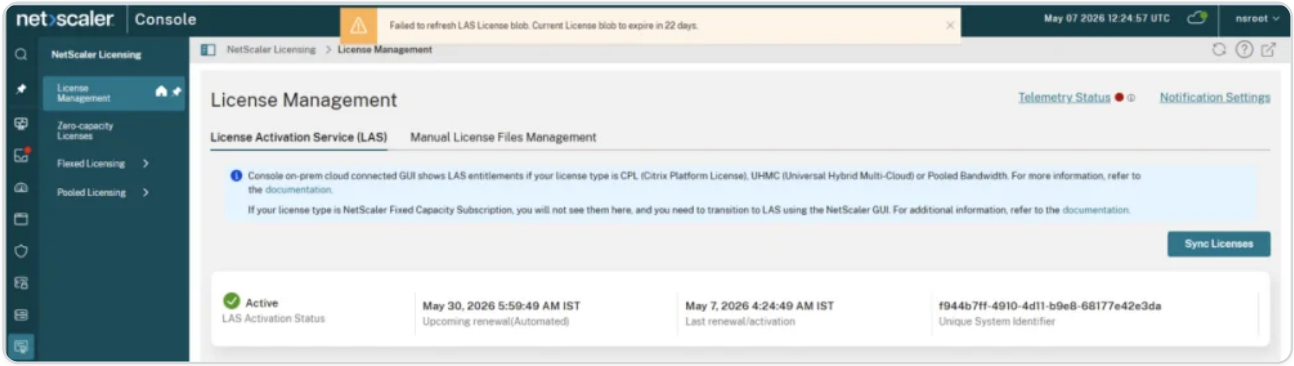
© 1997–2026 Citrix Systems, Inc. All rights reserved.



通知

NetScaler Console 本地部署 GUI 上的横幅：

当 NetScaler Console 本地部署无法刷新 LAS 激活 Blob 时，NetScaler Console GUI 中会出现警告横幅，如下图所示。



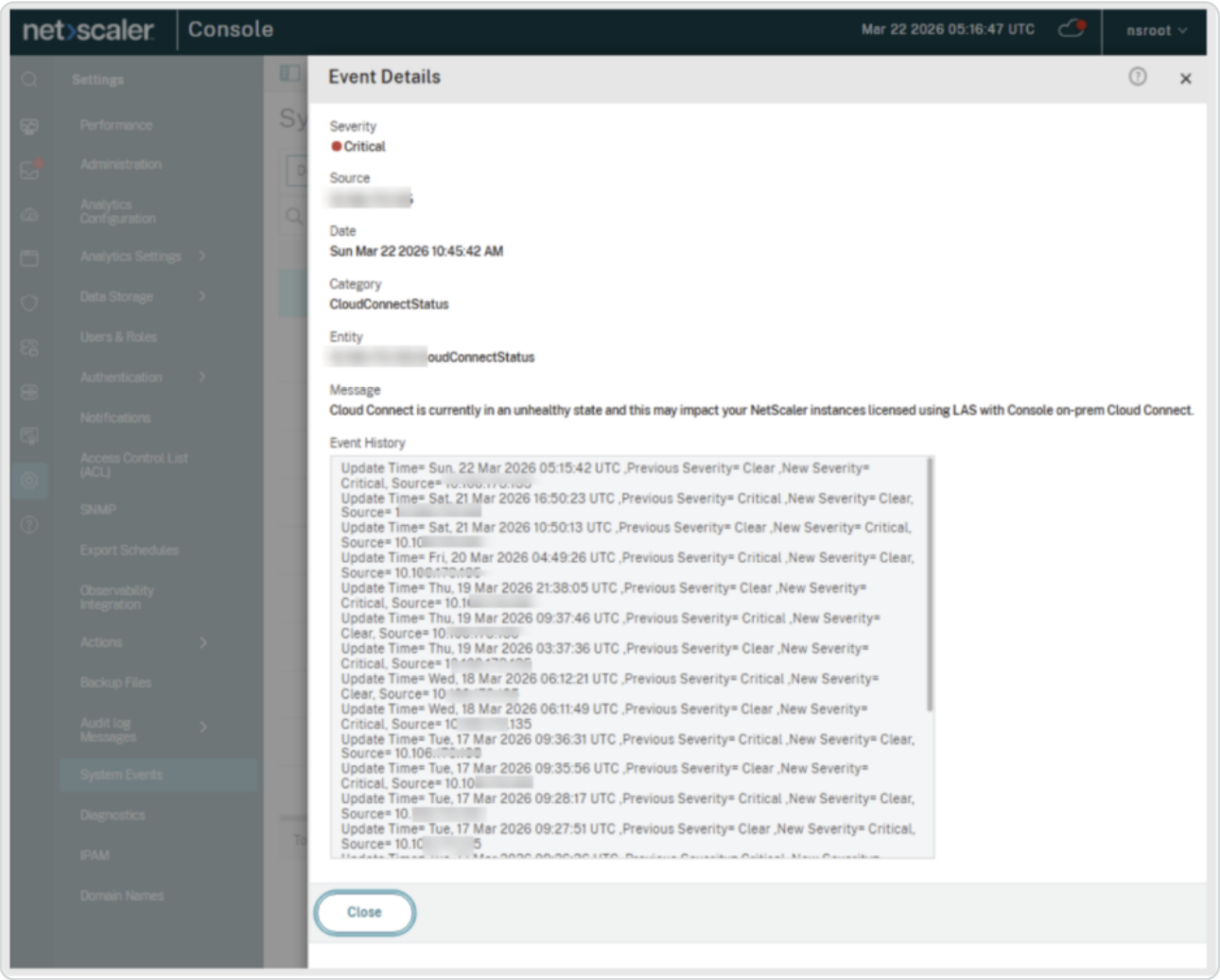
用于云连接问题的基于系统事件的通知：

NetScaler Console 会针对云连接状态的变化生成事件。当 NetScaler Console 本地部署与 Console 服务之间的连接状态发生变化时，会触发这些事件，包括以下转换：

- 从“已连接”到“已断开连接”或“错误”
- 从“已断开连接”或“错误”返回到“已连接”

要查看这些事件，请导航到 **Console on-premises GUI > Settings > System Events**。

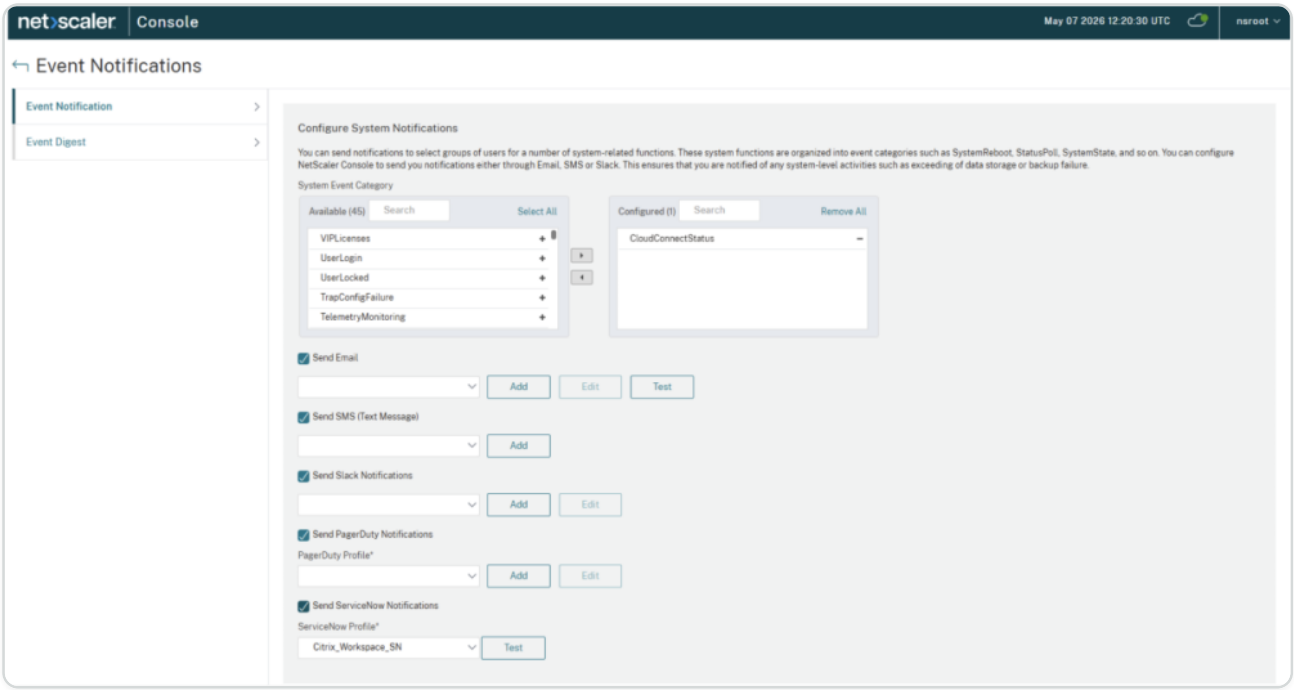
© 1997–2026 Citrix Systems, Inc. All rights reserved.



您还可以为云连接相关问题设置基于电子邮件的通知。

1. 导航到 **Console on-premises GUI > 设置 > 事件通知**。
2. 选择类别 **CloudConnectStatus**。
3. 选择并配置一种或多种通知形式，例如电子邮件、短信、PagerDuty。
4. 点击 **保存**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Console on-premises LAS 激活 blob 过期基于系统事件的通知：

NetScaler Console on-premises 会生成事件，以通知管理员 NetScaler Console on-premises 的 LAS 激活 blob 过期。您还可以为这些事件设置基于电子邮件的警报。

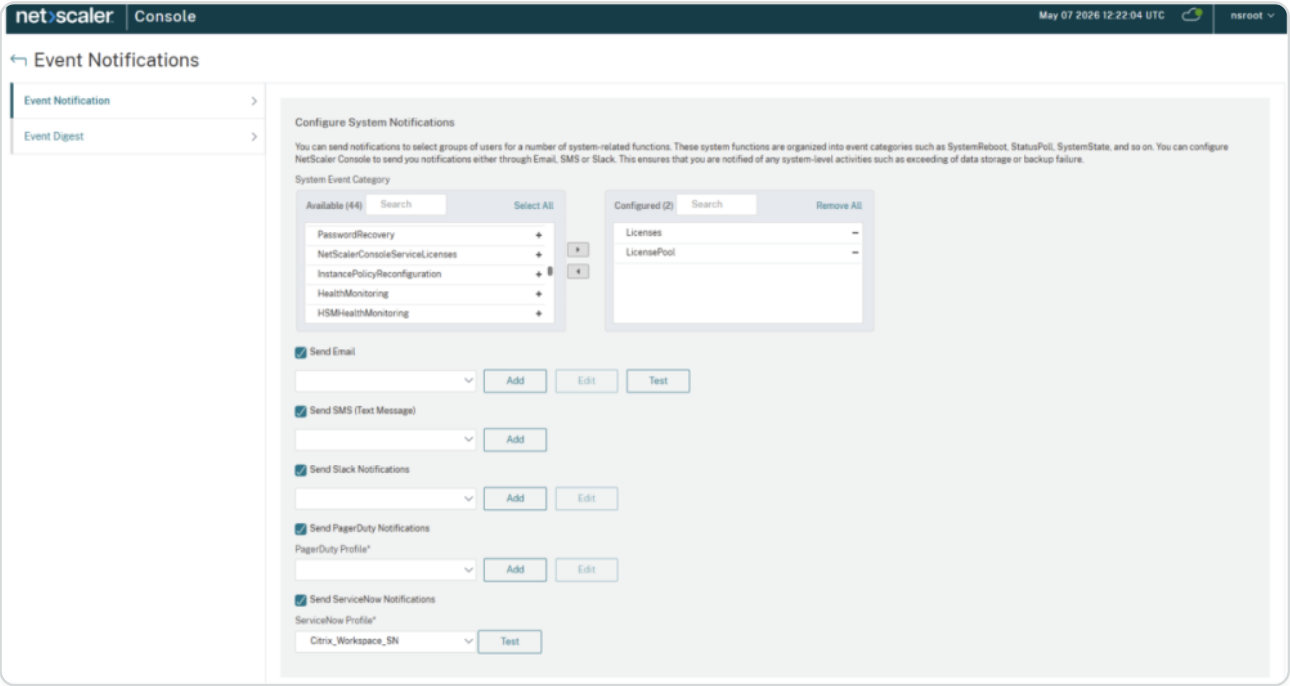
要配置 LAS 激活 blob 过期的通知：

1. 导航到 **Console on-premises GUI > 设置 > 事件通知**。
2. 选择 **许可证和许可证池** 类别。
3. 选择并配置一种或多种通知形式，例如电子邮件、短信、PagerDuty。
4. 点击 **保存**。

注意：

根据您的其他用例和配置的通知，配置的事件列表可能包含不止这两个。屏幕截图仅为简化起见显示这两个。

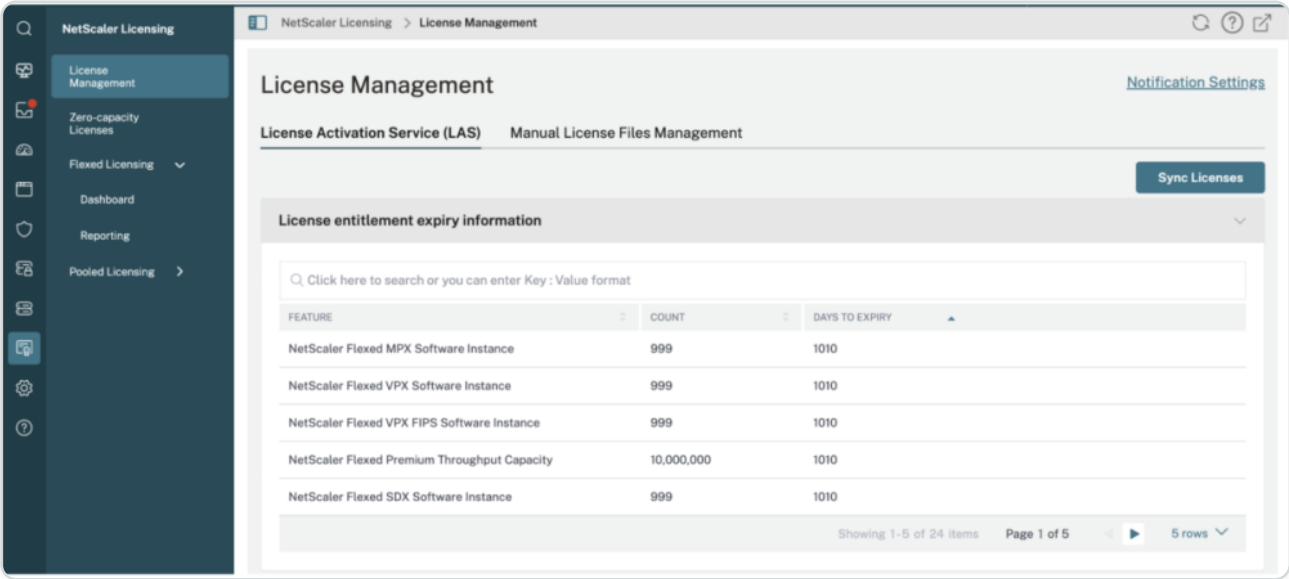
© 1997–2026 Citrix Systems, Inc. All rights reserved.



监控 NetScaler 实例 LAS 激活 blob 过期（通过本地部署云连接的 Console 授权的 NetScaler）

使用 GUI 查看 NetScaler 实例：

要查看处于宽限状态的 NetScaler 实例，请导航到 **本地部署 Console GUI > NetScaler 许可 > 弹性许可 > 仪表板**



使用 CLI 查看 NetScaler 实例状态

要查看处于宽限状态的 NetScaler 实例以及剩余的宽限期持续时间，请运行 `sh licenseserver` 命令。

示例：

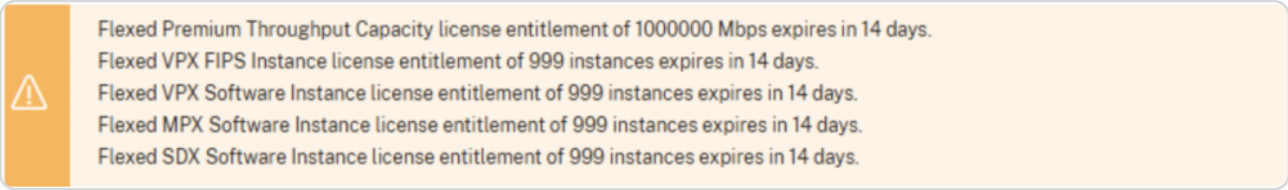
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> sh licenseserver

     License Server: 10.102.123.31 Status: Disconnected

        Grace: Yes         Grace Time Left: 652

Done
```

通知

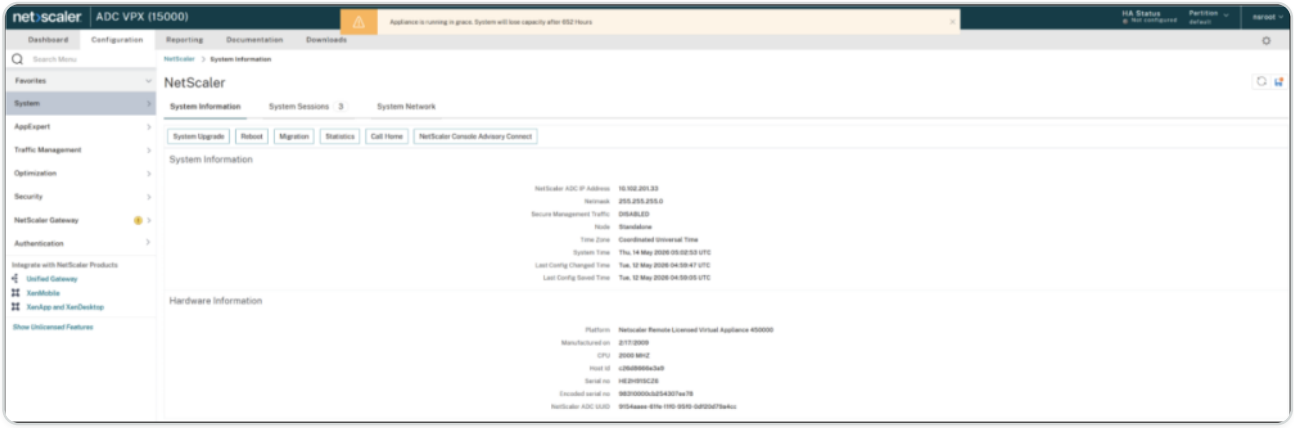
本地部署 NetScaler Console 上的横幅：

本地部署 NetScaler Console GUI 会显示一个横幅，列出其 LAS 激活 blob 将在 x 天内过期的 NetScaler 实例，其中 x 小于 30 天。



NetScaler GUI 上的横幅：

如果 NetScaler 实例处于宽限状态，本地部署 NetScaler Console GUI 会显示一个横幅。



基于系统事件的通知：

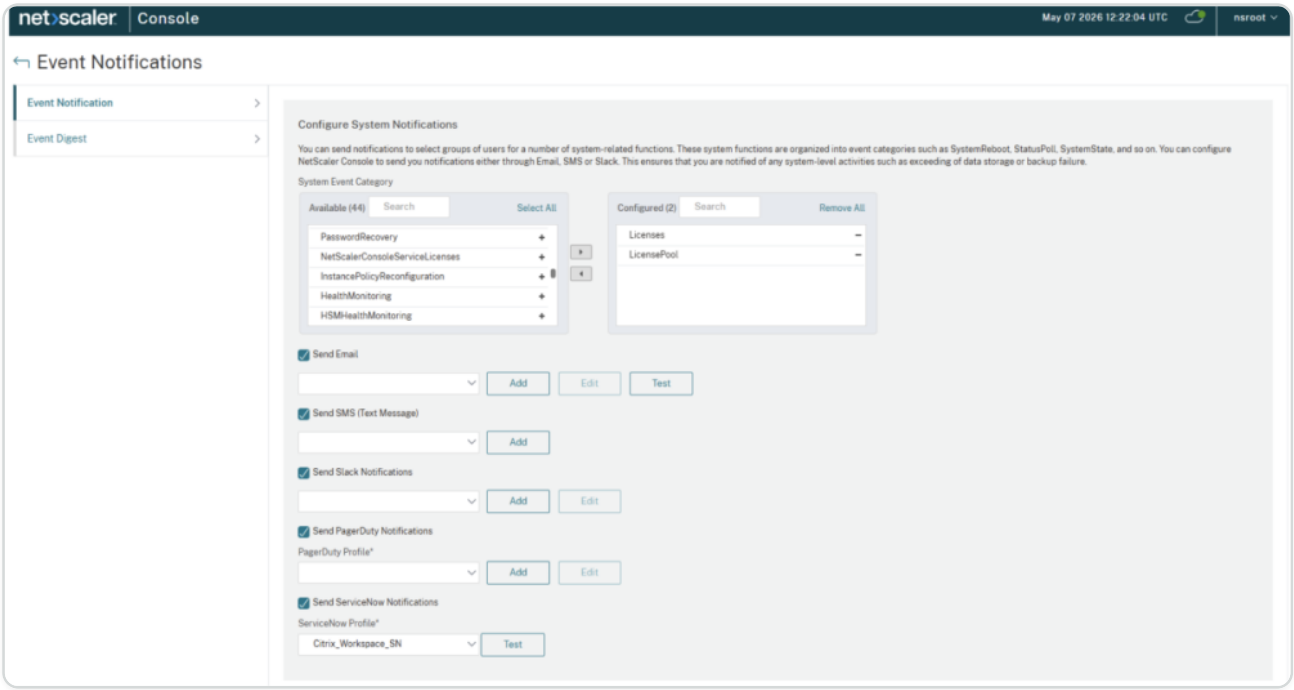
当 NetScaler 实例的 LAS 激活 blob 过期时，NetScaler Console on-premises 会生成事件。您还可以为这些事件设置基于电子邮件的警报。

要配置 LAS 激活 blob 过期通知：

1. 导航到 **Console on-premises GUI > 设置 > 事件通知**。
2. 选择**许可证和许可证池**类别。
3. 选择并配置一种或多种通知形式，例如电子邮件、短信、PagerDuty。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 单击“保存”。



NetScaler 为宽限状态生成的 SNMP trap：

如果 NetScaler 实例处于宽限状态，NetScaler 会生成以下 SNMP trap：

- pooledLicenseGraceStarted：当实例进入宽限期时触发。
- pooledLicenseGraceNormal：如果 NetScaler 已处于宽限期 30 天且宽限期已结束，则触发此事件，这意味着部署受到影响或变为未授权状态。
- pooledLicenseGracePeriodOver：当宽限期结束时触发。

示例：

```
May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGraceStarted
(nsPartitionName = default)

May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGraceNormal
(nsPartitionName = default)

May 15 05:17:21 <local0.info> 10.102.201.33  05/15/2026:11:17:21 GMT  0-
PPE-2 : default SNMP TRAP_SENT 0 0 :  pooledLicenseGracePeriodOver
(nsPartitionName = default)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

监控许可证权利到期

许可证授权到期日期是指客户许可证授权或合同的到期日期。

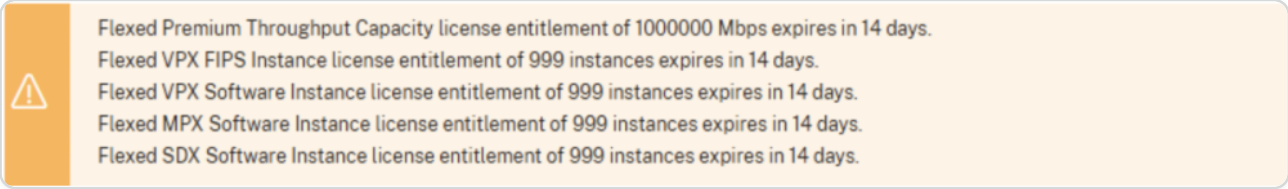
要使用 GUI 查看许可证授权到期信息，请导航到 **Console Service GUI > NetScaler Licensing > License Management > LAS**。

距离到期天数显示相应许可证的授权到期日期。

通知

NetScaler Console 服务 GUI 横幅：

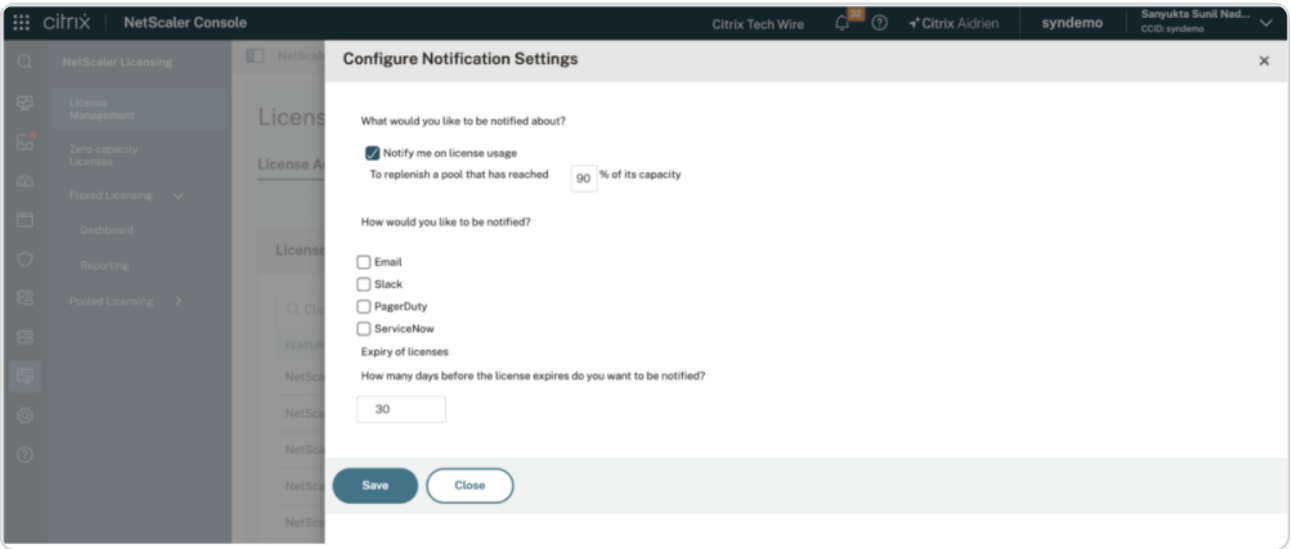
NetScaler Console 服务 GUI 显示一个横幅，指示许可证授权将在 x 天内到期。



基于电子邮件的通知

要配置基于电子邮件的通知：

1. 导航到 **控制台服务 GUI > NetScaler 许可 > 许可证管理 > 通知设置**。
2. 在 **您希望在许可证到期前多少天收到通知？** 中输入所需值。
3. 单击 **保存**。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

许可证管理

重要提示：

基于文件的许可系统（也称为手动管理的授权）传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活 Citrix 全套产品的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler Flexed 许可证 (CPL/UHMC)、旧版 NetScaler Pooled 许可证和 NetScaler Fixed term Bandwidth 许可证。为了获得持续支持，您的 NetScaler 和 NetScaler Console 部署必须是与 LAS 兼容的版本。

与 LAS 兼容的最低 NetScaler® 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：自 2025 年 9 月初起支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： Console 本地部署对 LAS 的支持始于 14.1-51.x 版本及更高版本。但是，自 April 15 2026 起，Console 本地部署 14.1-51.x 及更高版本和 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署 14.1-51.x 版本或 13.1-60.x 版本或更高版本，您可以继续使用基于文件的许可，直到 April 15 2026。但是，您必须在 April 15 2026 之前升级到 Console 本地部署 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如 Pooled vCPU、CICO、永久许可证，将不支持 LAS。升级到上述软件版本后，使用没有有效维护的永久许可证的 NetScaler 实例将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。如果不遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法规定的其他补救措施。在法律或法规禁止的情况下，这些要求不适用。
在继续操作之前，请阅读以下注意事项。

注意：

当您购买通用混合多云 (UHMC) 或 Citrix 平台许可证 (CPL) 时，交付的 NetScaler 许可证称为 Flexed 许可证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Flexed 许可证在 NetScaler Console on-prem 14.1 和 13.1 版本中受支持。为了获得更好的产品体验，展示 Flexed GUI 并提供捆绑权益，我们建议将您的 NetScaler Console on-prem 升级到 14.1–12.34 或更高版本。

在 NetScaler Console on-prem 14.1–12.34 及更高版本中：

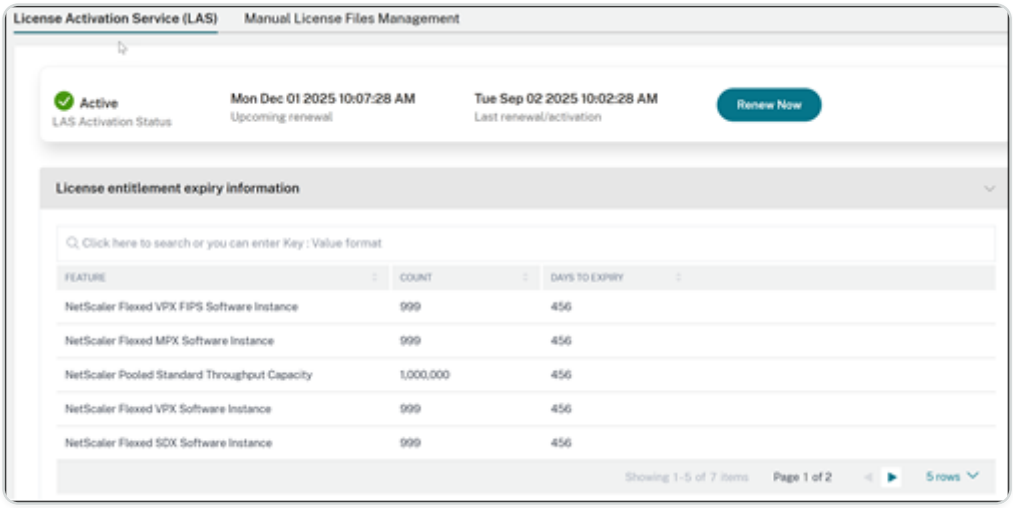
- 您可以通过 Flexed 控制板 UI（NetScaler® **许可 > Flexed 许可**）管理 Flexed 许可证。
- 如果您应用 Flexed 许可证，则可获得用于分析的无限 NetScaler Console VIP 的捆绑权益。

对于 NetScaler Console on-prem 13.1 版本和早于 14.1-12.34 的 14.1 版本：

- 当您应用 Flexed 许可证时，NetScaler Console 会将其视为与池化许可证相同，并在池化控制板 UI（**基础结构 > 池化许可**）中显示详细信息。
- 应用 Flexed 许可证后，这些版本中不提供用于分析的无限 NetScaler Console VIP 的捆绑权益。-

基于 LAS 的许可证

启用 LAS 后，您的权益将显示在 **控制台 UI > 许可证管理 > 许可证激活服务 (LAS)** 部分。



许可证服务器端口

LAS 使用端口 443 进行所有许可通信。

注意：

要使用 LAS，请将您的 NetScaler® 实例添加为托管实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

许可证到期信息

查看许可证到期

1. 导航到 **NetScaler 许可 > 许可证管理**。
2. **许可证权利到期信息**部分提供了有关即将到期的许可证的详细信息。
   - **功能**：即将到期的许可证类型。
   - **计数**：受影响的实例数或带宽（Mbps）。
   - **距离到期天数**：许可证到期（合同结束日期）前的天数。

启用 LAS 并建立云连接后，Pooled 或 Flexed 许可证的初始权利将在一个小时内获取。任何后续新增或续订的 Pooled 或 Flexed 许可证将在 24 小时内获取。

许可证到期行为

通过 NetScaler Console 管理的许可证到期后，关联的 NetScaler 实例将停止处理流量，并且其配置可能会丢失。

许可证结束日期（许可证合同结束日期）的通知电子邮件和弹出横幅

在 NetScaler Console GUI 中，将显示与许可证结束日期相关的弹出消息。默认情况下，从许可证结束日期前 30 天（默认）开始，您会在 GUI 中收到弹出消息（每次登录后）。 您可以在 **Notification settings > Expiry of license setting.** 中配置天数。

如果已在**通知设置**中配置了电子邮件通知，作为管理员，您还会收到一封关于许可证结束日期的通知电子邮件。通知电子邮件会在许可证结束日期前 30 天、20 天和 10 天发送。

通知设置

要为 LAS 管理的即将到期的 Flexed 或 Pooled 许可证设置通知，请按照以下步骤操作：

1. 导航到 NetScaler **许可证 > 许可证管理 > 通知设置**。
2. 在“通知设置”部分中，选择“**在许可证使用情况上通知我**”。将警报阈值设置为弹性或池化许可证容量的百分比，以便在达到该百分比时发送通知。
3. 通过选择相应的复选框，选择当许可证达到阈值或即将过期时要发送的通知类型。通知类型如下：
   - **电子邮件**：用于发送通知的电子邮件配置文件或分发列表。有关详细信息，请参阅创建电子邮件分发列表。
   - **Slack**：用于发送通知的 Slack 配置文件详细信息。
   - **PagerDuty**：用于发送通知的 PagerDuty 配置文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **ServiceNow**：Citrix ServiceNow 配置文件是默认指定的，也是唯一可用的选项。有关创建这些配置文件的详细信息，请参阅配置通知。

4. 选择通知类型，然后单击“**添加**”以添加详细信息。您还可以在保存设置之前测试每个通知系统。
5. 指定“到期天数”，即您希望在许可证到期前收到通知的天数。
6. 单击“**保存**”。

创建电子邮件分发列表

执行以下步骤创建电子邮件分发列表：

1. 选择“**电子邮件**”，然后单击“**添加**”。
2. 在“**创建电子邮件分发列表**”中，指定以下详细信息：
   - **名称** - 指定分发列表名称。
   - **电子邮件服务器** - 选择发送电子邮件通知的电子邮件服务器。要添加电子邮件服务器，请单击“添加”。指定服务器名称/IP 地址和端口。选择“身份验证”以强制要求通过身份验证才能访问电子邮件服务器。如果电子邮件服务器支持 SSL 身份验证，请选择“安全”。单击“创建”。
   - **发件人** - 指定 NetScaler Console 发送邮件的电子邮件地址。
   - **收件人** - 指定 NetScaler Console 发送邮件的电子邮件地址。
   - **抄送** - 指定 NetScaler Console 抄送邮件的电子邮件地址。
   - **密送** - 指定 NetScaler Console 密送（不显示电子邮件地址）邮件的电子邮件地址。
   - 单击**创建**。

创建 Slack 配置文件

执行以下步骤创建 Slack 配置文件：

1. 在 Slack 中，单击**添加**。
2. 在**创建 Slack 配置文件**中，指定以下详细信息：
   - **通知** - 启用后，直接向指定的 Slack 频道发送警报和事件通知。
   - **带附件的通知** - 启用后，有关触发警报和事件的详细信息将作为电子邮件附件或 Webhook 中的 JSON 有效负载发送。
   - **配置文件名称** - 指定配置文件名称。此名称将显示在 Slack 配置文件列表中。
   - **频道名称** - 指定 NetScaler Console 发送通知的 Slack 频道名称。
   - **Webhook URL** - 指定频道的 Webhook URL。传入 Webhook 是一种将外部源消息发布到 Slack 的简单方法。此 URL 在内部链接到频道名称。发送到此 URL 的所有事件通知都将发

© 1997–2026 Citrix Systems, Inc. All rights reserved.

布到指定的 Slack 频道。Webhook 示例如下：`<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`

创建 PagerDuty 配置文件

PagerDuty 允许您通过电子邮件、推送通知和注册电话号码配置通知。在 NetScaler Console 中添加 PagerDuty 配置文件之前，请确保您已在 PagerDuty 中完成所需的配置。要开始使用 PagerDuty，请参阅 PagerDuty 文档。

执行以下步骤创建 PagerDuty 配置文件：

1. 在 PagerDuty 中，单击 **Add**。
2. 在 **Create PagerDuty Profile** 中，指定以下详细信息：
   - **配置文件名称** - 指定配置文件名称。此名称由不同的模块（例如事件规则和 SSL 通知）用于发送 PagerDuty 警报。
   - **集成密钥** - 指定集成密钥。您可以从 PagerDuty 门户获取此密钥。在 PagerDuty 中创建用于集成的服务时，请使用 **Generic Events API Integration** 选项。
   - 单击 **Create**。

有关更多信息，请参阅 PagerDuty 文档中的 Services and Integrations。

查看 ServiceNow 配置文件

要为 NetScaler 事件启用 ServiceNow 通知，您必须使用 ITSM 连接器将 NetScaler Console 与 ServiceNow 集成。

有关更多信息，请参阅 Integrate NetScaler Console with the ServiceNow instance。

执行以下步骤查看和验证 ServiceNow 配置文件：

1. 在 **ServiceNow** 中，默认选择 **Citrix_Workspace_SN** 配置文件。
2. 单击 **Test** 自动生成 ServiceNow 票证并验证配置。

注意：

有关不同类型的 NetScaler 许可证的信息，请参阅 许可概述。

LAS 的 RBAC 支持

您可以使用基于角色的访问控制 (RBAC) 来管理 LAS 应用程序访问，并具有以下控制级别：

- **功能级别**：限制特定管理员对许可功能的可见性。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **实例级别**：限制授权管理员仅将许可证应用于选定的 NetScaler 实例。

有关配置详细信息，请参阅 基于角色的访问控制。

手动管理的权利（基于文件的许可证）

以下部分适用于手动管理的权利（基于文件的许可）。

许可证文件

NetScaler Flexed 许可证包含您必须从 MyCitrix 门户下载的以下文件。有关从当前类型的 NetScaler 许可过渡到 Flexed 许可的更多信息，请参阅 过渡到 Flexed 许可。

本节列出了 NetScaler 上存在的许可证文件。

文件名包含	描述	下载信息	许可证上传/应用位置
NetScaler 弹性 VPX 软件实例	授权您使用 VPX/CPX/BLX 软件实例	使用您的 NetScaler Console 主机 ID 下载此文件	在 NetScaler Console 上
NetScaler 弹性 MPX 软件实例	授权您使用 MPX 软件实例	使用您的 NetScaler Console 主机 ID 下载此文件	在 NetScaler Console 上
NetScaler 弹性 SDX 软件实例	授权您使用 SDX 软件实例	使用您的 NetScaler Console 主机 ID 下载此文件	在 NetScaler Console 上
NetScaler 弹性白金版带宽	授权您使用弹性白金版吞吐量容量	使用您的 NetScaler Console 主机 ID 下载此文件	在 NetScaler Console 上
NetScaler Flexed VPX FIPS 软件实例	授权您使用 VPX FIPS 软件实例	使用您的 NetScaler Console 主机 ID 下载此文件	在 NetScaler Console 上
零容量 MPX-Z 平台许可证	授权您的 NetScaler MPX 硬件/NetScaler MPX FIPS 硬件参与 Flexed 许可	下载此文件	在 NetScaler MPX 上
零容量 SDX-Z 平台许可证	授权您的 NetScaler SDX 硬件/NetScaler	下载此文件	在 NetScaler SDX 上

© 1997–2026 Citrix Systems, Inc. All rights reserved.

文件名包含	描述	下载信息	许可证上传/应用位置
	SDX FIPS 硬件参与 Flexed 许可		

重要注意事项

1. 如果您是正在过渡到 Flexed 许可的池许可客户，并且您的 MPX 和 SDX 硬件已经拥有 Z-Cap 永久许可证，则无需应用随 Flexed 获得的 Z-Cap 许可证。但是，如果当前应用于 NetScaler MPX/NetScaler SDX 的 Z-Cap 许可证在特定时期内有效，则必须应用随 Flexed 许可证获得的 Z-Cap 许可证。Flexed 软件许可证包括 NetScaler Flexed MPX/SDX/VPX/VPX FIPS 软件实例和 NetScaler Flexed Platinum 带宽许可证。
2. 您必须在 NetScaler Console 上应用 Flexed 许可证，适用于您部署中使用的 NetScaler 外形规格。例如：

   如果您使用的是 NetScaler SDX 外形规格，请应用以下许可证：

   |许可证文件|应用于| |-|-| |NetScaler Flexed SDX 软件实例|NetScaler 控制台| |NetScaler Flexed VPX 软件实例|NetScaler 控制台| |NetScaler 弹性白金带宽|NetScaler 控制台| |ADC 零容量 SDX-Z 平台|NetScaler SDX|

   如果您使用的是 NetScaler MPX 外形规格，请应用以下许可证：

   |许可证文件|应用于| |-|-| |NetScaler Flexed MPX 软件实例|NetScaler 控制台| |NetScaler 弹性白金带宽|NetScaler 控制台| |ADC 零容量 MPX-Z 平台|NetScaler MPX|

   如果您正在使用 NetScaler VPX、NetScaler BLX 或 NetScaler CPX 外形规格，请应用以下许可证：

   |许可证文件|应用于| |-|-| |NetScaler Flexed VPX 软件实例|NetScaler 控制台| |NetScaler 弹性白金带宽|NetScaler 控制台|

   如果您正在使用 NetScaler VPX FIPS 外形规格，请应用以下许可证

   |许可证文件|应用于| |-|-| |NetScaler Flexed VPX FIPS 软件实例|NetScaler 控制台| |NetScaler 弹性白金带宽|NetScaler 控制台|

应用许可证文件

您可以添加、删除和下载许可证。您必须先应用许可证才能使用它们。

1. 导航到 **NetScaler Licensing > 许可证管理**。
2. 在“**许可证文件**”部分中，单击“**添加许可证文件**”并选择以下选项之一：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **从本地计算机上传许可证文件**：如果许可证文件已存在于您的本地计算机上，您可以将其上传到 NetScaler Console。
- **使用许可证访问代码**：指定您从 Citrix 购买的许可证的许可证访问代码。单击“**获取许可证**”，然后单击“**完成**”。

3. 单击“**完成**”。 许可证文件已添加到 NetScaler Console。 “**许可证到期信息**”部分列出了 NetScaler Console 中存在的许可证、数量以及剩余到期天数。

   以下屏幕截图显示了 Flexed NetScaler VPX、NetScaler MPX、NetScaler SDX 和 NetScaler VPX FIPS 软件实例许可证的数量、Flexed 高级带宽容量以及到期天数（合同结束日期）。

License Expiry Information

FEATURE	COUNT	DAYS TO EXPIRY
Flexed FIPS Instance	5	360
Flexed MPX Software Instance	2	1090
Flexed SDX Software Instance	5	360
Flexed VPX Software Instance	25	360
Flexed VPX Software Instance	110	1090
Flexed Premium Bandwidth	100,000	1090

Total 6 25 Per Page Page 1 of 1

   以下屏幕截图显示了可用的池化标准、高级和高级带宽以及到期天数（合同结束日期）。

License Expiry Information

FEATURE	COUNT	DAYS TO EXPIRY
Pooled Premium Bandwidth	50,000	360
Pooled Advanced Bandwidth	10,000	360
Pooled Standard Bandwidth	50,000	360

Total 3 25 Per Page Page 1 of 1

4. 选择许可证文件，然后单击**应用许可证**。

删除许可证文件

要删除许可证文件，请选择一个或多个文件，然后单击**删除**。删除许可证时，您必须先添加许可证，然后才能应用它。

下载许可证文件

要下载许可证文件，请选择一个文件，然后单击**下载**。您可以将许可证文件离线保存作为备份。

许可证服务器端口设置

NetScaler 实例使用端口与许可证服务器通信。单击**编辑**图标，并为以下参数指定值：

- **许可证服务器端口**：NetScaler 实例用于访问 Citrix 许可门户以分配许可证的代理服务器端口。默认值：27000。
- **供应商守护程序端口**：NetScaler 实例用于与许可证服务器通信的许可证服务器端口。默认值：7279。
- **代理服务器端口**：NetScaler Console 可用作正向 HTTP 代理，供 NetScaler 实例访问 MyCitrix Portal 以自动检索许可证。要启用此功能，请指定代理侦听的 TCP 端口。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

许可证到期信息

您现在可以配置弹性或池化容量许可证的许可证到期阈值。设置阈值后，当许可证即将到期时，NetScaler Console 会通过电子邮件或短信发送通知。当许可证在 NetScaler Console 上过期时，还会发送 SNMP trap 和通知。

当发送许可证到期通知时，会生成一个事件，并且可以在 NetScaler Console 上从**基础架构 > 事件**查看此事件。

查看许可证到期

1. 导航到 **NetScaler 许可 > 许可证管理**。
2. 在 **许可证设置** 页面中，在 **许可证到期信息** 部分下，您可以找到即将到期的许可证的详细信息：
   - **功能**：即将到期的许可证类型。
   - **计数**：受影响的虚拟服务器或实例的数量。
   - **到期天数**：许可证到期（合同结束日期）前的天数。

注意：

当您向池中添加新许可证时，NetScaler 实例会在其现有许可证到期时使用新许可证。

通知设置

指定基于许可证分配和到期天数发送通知的设置。

1. 在 **通知设置** 部分中，单击 **编辑** 图标并选择 **在许可证使用情况上通知我**。将警报阈值设置为弹性或池化许可证容量的百分比，以便在达到该百分比时发送通知。
2. 选择当许可证达到阈值或即将到期时要发送的通知类型，方法是选中相应的复选框。通知类型如下。选择一个通知类型，然后单击 **添加** 以添加详细信息。您还可以在保存设置之前测试每个通知是否已送达。
   - **电子邮件**：用于发送通知的电子邮件配置文件或分发列表。有关详细信息，请参阅创建电子邮件分发列表。
   - **短信**：用于发送通知的短信配置文件或分发列表。
   - **Slack**：用于发送通知的 Slack 配置文件详细信息。
   - **PagerDuty**：用于发送通知的 PagerDuty 配置文件。
   - **ServiceNow**：Citrix ServiceNow 配置文件是默认指定的，也是目前唯一可用的选项。 有关创建这些配置文件的更多信息，请参阅配置通知

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 指定到期天数，即您希望在许可证到期前收到通知的天数。
4. 单击**保存**。

创建电子邮件分发列表

执行以下步骤以创建电子邮件分发列表：

1. 选择**电子邮件**，然后单击**添加**。
2. 在**创建电子邮件分发列表**中，指定以下详细信息：
   - **名称** - 指定分发列表名称。
   - **电子邮件服务器** - 选择发送电子邮件通知的电子邮件服务器。要添加电子邮件服务器，请单击“添加”。指定服务器名称/IP 地址和端口。选择“身份验证”以强制要求身份验证才能访问电子邮件服务器。如果电子邮件服务器支持 SSL 身份验证，请选择“安全”。单击“创建”。
   - **发件人** - 指定 NetScaler Console 发送消息的电子邮件地址。
   - **收件人** - 指定 NetScaler Console 发送消息的电子邮件地址。
   - **抄送** - 指定 NetScaler Console 抄送消息的电子邮件地址。
   - **密送** - 指定 NetScaler Console 密送（不显示电子邮件地址）消息的电子邮件地址。
3. 单击**创建**。

创建短信分发列表

执行以下步骤配置短信通知设置：

1. 在 **SMS** 中，单击 **Add**。
2. 在 **Create SMS Distribution List** 中，指定以下详细信息：
   - **Name** - 指定分发列表名称。
   - **SMS Server** - 选择发送短信通知的短信服务器。要添加短信服务器，请单击 **Add**。指定服务器详细信息，然后单击 **Create**。
   - **To** - 指定 NetScaler Console 发送消息的电话号码。
3. 单击 **Create**。

创建 Slack 配置文件

执行以下步骤创建 Slack 配置文件：

1. 在 **Slack** 中，单击 **Add**。
2. 在 **Create Slack Profile** 中，指定以下详细信息：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Profile Name** - 指定配置文件名称。此名称将显示在 Slack 配置文件列表中。
- **Channel Name** - 指定 NetScaler Console 发送通知的 Slack 频道名称。
- **Webhook URL** - 指定频道的 Webhook URL。传入 Webhook 是一种将外部源消息发布到 Slack 的简单方法。URL 在内部链接到频道名称。发送到此 URL 的所有事件通知都将发布到指定的 Slack 频道。Webhook 示例如下：`<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`。

创建 PagerDuty 配置文件

PagerDuty 允许您通过电子邮件、短信、推送通知和注册电话号码配置通知。在 NetScaler Console 中添加 PagerDuty 配置文件之前，请确保您已在 PagerDuty 中完成所需的配置。要开始使用 PagerDuty，请参阅 PagerDuty 文档。

执行以下步骤创建 PagerDuty 配置文件：

1. 在 **PagerDuty** 中，单击 **Add**。
2. 在 **Create PagerDuty Profile** 中，指定以下详细信息：
   - **配置文件名称** - 指定配置文件名称。此名称由不同的模块（例如事件规则和 SSL 通知）用于发送 PagerDuty 警报。
   - **集成密钥** - 指定集成密钥。您可以从 PagerDuty 门户获取此密钥。
3. 单击 **Create**。

有关详细信息，请参阅 PagerDuty 文档中的 服务和集成。

查看 ServiceNow 配置文件

要为 NetScaler 事件和 NetScaler Console 事件启用 ServiceNow 通知，您必须使用 ITSM 连接器将 NetScaler Console 与 ServiceNow 集成。有关详细信息，请参阅 将 NetScaler Console 与 ServiceNow 实例集成。

执行以下步骤查看和验证 ServiceNow 配置文件：

1. 在 **ServiceNow** 中，默认选择 **Citrix_Workspace_SN** 配置文件。
2. 单击 **Test** 自动生成 ServiceNow 票证并验证配置。

注意：

有关不同类型的 NetScaler 许可证的信息，请参阅 许可概述。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

弹性许可和池许可的最小和最大容量

重要：

基于文件的许可系统（也称为手动管理的权利），传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活 Citrix 产品套件中产品的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler 弹性许可 (CPL/UHMC)、旧版 NetScaler 池许可和 NetScaler 固定期限带宽许可。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是 LAS 兼容版本。

兼容 LAS 的最低 NetScaler® 版本是：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console 服务：从 2025 年 9 月初开始支持。
- NetScaler Console 本地部署版：14.1-51.x

  注意： LAS 对 Console 本地部署版的支持从版本 14.1-51.x 开始。但是，自 April 15 2026 起，Console 本地部署版 14.1-51.x 及更高版本和 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署版 14.1-51.x 或 13.1-60.x 或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署版 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署版 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可（例如池化 vCPU、CICO、永久许可）将不支持 LAS。升级到上述软件版本后，使用没有有效维护的永久许可的 NetScaler 实例将变为未许可状态。
在法律或法规禁止的情况下，基于 LAS 的许可可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。对于不遵守这些要求的行为，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法规定的任何其他补救措施。这些要求在法律或法规禁止的情况下不适用。
NetScaler 弹性许可使用配置为许可证服务器的 NetScaler Console 来管理弹性许可：带宽池许可和实例池许可。

从带宽池和实例池中签出许可时，零容量硬件上的 NetScaler 外形规格和硬件型号决定了：

- NetScaler 实例在正常运行之前必须签出的最小带宽和实例数。
- NetScaler 可以检出的最大带宽和实例数量。
- 每次带宽检出的最小带宽单位。最小带宽单位是 NetScaler 必须从池中检出的最小带宽单位。任何检出都必须是最小带宽单位的整数倍。例如，如果 NetScaler 的最小带宽单位是 1 Gbps，则

© 1997–2026 Citrix Systems, Inc. All rights reserved.

可以检出 1000 Mbps，但不能检出 200 Mbps 或 150.5 Gbps。最小带宽单位与最小带宽要求不同。NetScaler 实例只有在获得至少最小带宽的许可后才能运行。一旦满足最小带宽，实例就可以以最小带宽单位的倍数检出更多带宽。

表 1 至表 5 总结了所有受支持的 NetScaler 实例的最大带宽/实例数、最小带宽/实例数以及最小带宽单位。表 6 总结了所有受支持的 NetScaler 实例不同外形规格的许可证要求。下表指的是系统要求。

注意：

NetScaler CPX/BLX/VPX 的最小带宽检出单位为 10 Mbps。NetScaler MPX/SDX 的最小带宽检出单位为 1 Gbps。

表 1. MPX 支持的弹性容量

产品线	最小带宽 (GBPS)	最大带宽 (GBPS)	最小带宽单位
MPX 5900Z	1	10	1 吉比特/秒
MPX 8900Z	5	30	1 千兆位每秒
MPX 8900Z FIPS	5	20	1 千兆位每秒
MPX 9100Z	10	95	1 千兆位每秒
MPX 9200	10	95	1 千兆位每秒
MPX 9100Z FIPS	10	95	1 吉比特/秒
MPX 14000Z	20	100	1 吉比特/秒
MPX 14000Z-40G	20	100	1 吉比特/秒
MPX 14000Z-40S	40	100	1 千兆位/秒
MPX 14000Z FIPS	30	80	1 千兆位/秒
MPX 15000Z	20	120	1 千兆位/秒
MPX 15000Z-50G	20	120	1 千兆位/秒
MPX 15000Z FIPS	30	120	1 千兆位/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

产品线	最小带宽 (GBPS)	最大带宽 (GBPS)	最小带宽单位
MPX 16000Z	30	250	1 千兆位/秒
MPX 22000Z	40	120	1 千兆位/秒
MPX 24000Z	100	150	1 千兆位/秒
MPX 25000Z	100	160	1 千兆位/秒
MPX 25000Z-40G	100	200	1 千兆位/秒
MPX 26000Z	100	200	1 千兆位/秒
MPX 26000Z-50S	100	200	1 千兆位/秒
MPX 26000Z-100G	100	200	1 吉比特/秒

表 2A. 适用于低于版本 13.0-47.x 的 NetScaler SDX 支持的弹性容量

产品系列	最小带宽 (GBPS)	最大带宽 (GBPS)	最小实例数	最大实例数	最小带宽单位
SDX 8900Z	10	30	2	7	1 吉比特/秒
SDX 14000Z	20	100	5	25	1 吉比特/秒
SDX 14000Z-40G	40	100	20	25	1 吉比特/秒
SDX 15000Z	20	120	5	55	1 千兆位/秒
SDX 15000Z-50G	20	120	5	55	1 千兆位/秒
SDX 22000Z	40	120	80	80	1 千兆比特/秒
SDX 24000Z	100	150	80	80	1 千兆比特/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

产品系列	最小带宽 (GBPS)	最大带宽 (GBPS)	最小实例数	最大实例数	最小带宽单位
SDX 25000Z	100	200	20	115	1 千兆比特/秒
SDX 25000Z-40G	100	200	20	115	1 吉比特每秒
SDX 26000Z	100	200	20	115	1 吉比特每秒
SDX 26000Z-50S	100	200	20	115	1 千兆位/秒
SDX 26000Z-100G	100	200	20	115	1 千兆位/秒

表 2B. 适用于 NetScaler SDX 13 版（内部版本 13.0-47.x 及更高版本）、13.1 版（内部版本早于 51.x）和 14.1 版（内部版本早于 12.x）的支持弹性容量

产品线	最小带宽 (GBPS)	最大带宽 (GBPS)	最小实例数	最大实例数	最小带宽单位
SDX 8900Z	5	30	1	7	1 吉比特每秒
SDX 9100Z	10	95	2	7	1 吉比特每秒
SDX 14000Z	10	100	2	25	1 千兆位每秒
SDX 14000Z-40G	20	100	10	25	1 千兆位每秒
SDX 15000Z	10	120	2	55	1 千兆位每秒
SDX 15000Z-50G	10	120	2	55	1 千兆位/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

产品线	最小带宽 (GBPS)	最大带宽 (GBPS)	最小实例数	最大实例数	最小带宽单位
SDX 16000Z	15	250	10	55	1 千兆位/秒
SDX 22000Z	20	120	40	80	1 吉比特/秒
SDX 24000Z	50	150	40	80	1 吉比特/秒
SDX 25000Z	50	200	10	115	1 吉比特/秒
SDX 25000Z-40G	50	200	10	115	1 千兆位/秒
SDX 26000Z	50	200	10	115	1 千兆位/秒
SDX 26000Z-50S	50	200	10	115	1 千兆位/秒
SDX 26000Z-100G	50	200	10	115	1 千兆位/秒

表 2C. 适用于 NetScaler SDX 13.1 版（内部版本 51.x 及更高版本）和 14.1 版（内部版本 12.x 及更高版本）的支持弹性容量

产品系列	最小带宽 (GBPS)	最大带宽 (GBPS)	最小实例数	最大实例数	最小带宽单位
SDX 8900Z	5	30	1	7	1 千兆位/秒
SDX 9200Z	10	95	1	7	1 千兆位/秒
SDX 9100Z	10	95	1	7	1 千兆位/秒
SDX 14000Z	10	100	1	25	1 千兆位/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

产品系列	最小带宽 (GBPS)	最大带宽 (GBPS)	最小实例数	最大实例数	最小带宽单位
SDX 14000Z-40G	20	100	1	25	1 吉比特每秒
SDX 15000Z	10	120	1	55	1 吉比特每秒
SDX 15000Z-50G	10	120	1	55	1 吉比特每秒
SDX 16000Z	30	250	1	55	1 千兆比特/秒
SDX 17000Z	30	350	1	55	1 千兆比特/秒
SDX 22000Z	20	120	1	80	1 千兆比特/秒
SDX 24000Z	50	150	1	80	1 千兆比特/秒
SDX 25000Z	50	200	1	115	1 千兆比特/秒
SDX 25000Z-40G	50	200	1	115	1 千兆位每秒
SDX 26000Z	50	200	1	115	1 千兆位每秒
SDX 26000Z-50S	50	200	1	115	1 吉比特每秒
SDX 26000Z-100G	50	200	1	115	1 吉比特每秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

- 最小购买数量可以与最小系统要求不同。
- 在运行版本 14.1-12.x 及更高版本的 NetScaler SDX 上，使用弹性许可证时，取消了签出最少数量实例许可证的限制。也就是说，您最少可以签出一个实例许可证。

表 3. NetScaler CPX 实例支持的最小/最大带宽和最小/最大实例数

产品系列	最大带宽 (GBPS)	最小带宽 (MBPS)	最小实例数	最大实例数	最小带宽单位
CPX	10	10	1	1	10 兆比特/秒

表 4. Hypervisor 和云服务上 NetScaler VPX 实例支持的最小/最大带宽和最小/最大实例数

HYPERVISOR/云服务	最大带宽 (GBPS)	最小带宽 (MBPS)	最小实例数	最大实例数	最小带宽单位
Citrix 管理程序	四十 Gbps	10 兆比特/秒	1	1	10 兆比特/秒
威睿 ESXI	100 千兆位/秒	10 兆位/秒	1	1	10 兆位/秒
Linux KVM (Linux 内核虚拟机)	100 吉比特每秒	10 兆位/秒	1	1	10 兆比特/秒
微软 Hyper-V	3 吉比特/秒	10 兆比特/秒	1	1	10 兆比特/秒
AWS	30 吉比特/秒	10 兆比特/秒	1	1	10 兆比特/秒
艾哲尔	10 吉比特每秒	10 兆比特每秒	1	1	10 兆比特每秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HYPERVISOR/云服务	最大带宽 (GBPS)	最小带宽 (MBPS)	最小实例数	最大实例数	最小带宽单位
谷歌云	10 吉比特每秒	10 兆比特每秒	1	1	10 兆比特每秒

注意

最低购买数量与最低系统要求不同。

表 5. NetScaler BLX 实例支持的最小/最大带宽和最小/最大实例数

产品线	最大带宽 (GBPS)	最小带宽 (MBPS)	最小实例数	最大实例数	最小带宽单位
BLX	100	10	1	1	10 兆位/秒

表 6. 不同外形规格的零容量许可证要求

产品线	零容量硬件
MPX	需要许可证
SDX	需要许可证
VPX	-
CPX	-
BLX	-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

弹性容量许可证

重要提示：

基于文件的许可系统（也称为手动管理的授权）传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活所有 Citrix 产品套件的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler 弹性许可证 (CPL/UHMC)、旧版 NetScaler 池许可证和 NetScaler 固定期限带宽许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是 LAS 兼容版本。

兼容 LAS 的最低 NetScaler® 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：从 2025 年 9 月初开始支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： Console 本地部署的 LAS 支持从版本 14.1-51.x 开始。但是，自 April 15 2026 起，Console 本地部署版本 14.1-51.x 及更高版本以及 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署版本 14.1-51.x 或 13.1-60.x 或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署版本 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如池化 vCPU、CICO、永久许可证，将不支持 LAS。升级到上述软件版本后，使用没有有效维护的永久许可证的 NetScaler 实例将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。对于不遵守这些要求的行为，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外，Citrix 还可能拥有法律或衡平法规定的任何其他补救措施。在法律或法规禁止的情况下，这些要求不适用。
NetScaler 弹性许可是一种旨在简化许可证管理流程的新许可框架。您的弹性许可证包括软件实例许可证（VPX/CPX/BLX、SDX、MPX 和 VPX FIPS）和带宽容量许可证。

许可证激活服务 (LAS) - 通过 Cloud Connect 部署激活 LAS，以使您的弹性授权在 NetScaler Console 本地部署中可见。之后，将它们分配给 NetScaler Console 本地部署中的任何 NetScaler 外形规格。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

手动管理的授权（基于文件的许可） - 直接在 NetScaler Console 本地部署上应用弹性许可证。此外，您必须将 MPX Z-Cap 和 SDX Z-Cap 许可证应用于相应的 NetScaler MPX 和 NetScaler SDX 硬件。然后，您可以将这些授权分配给所有 NetScaler 外形规格，无论是在云部署还是本地部署中。

弹性许可证还为无限数量的虚拟服务器提供分析功能。

如果您拥有池化许可证并已购买弹性许可证，您可以在弹性许可证仪表板中查看您的许可证详细信息。组合带宽和实例将显示在弹性许可证仪表板中。

带宽许可证通常只包括高级版，除非您之前拥有池化标准版或高级版许可证，在这种情况下，标准版、高级版和高级版将显示在弹性许可证仪表板中。

弹性许可证和池化许可证的带宽和实例(/en-us/netscaler-application-delivery-management-software/media/flexed-pooled-bw-instance-license.png)

有关更多详细信息，请参阅弹性许可证仪表板。

您可以使用弹性许可来最大化带宽利用率，方法是确保为实例分配必要的带宽，且不超过其需求。在运行时增加或减少分配给实例的带宽，而不会影响流量。

零容量硬件

当通过 NetScaler® 弹性许可进行管理时，MPX 和 SDX 实例被称为“零容量硬件”，因为这些实例在从带宽池中检出资源之前无法运行。因此，这些平台也称为 MPX-Z 和 SDX-Z 设备。

零容量硬件需要 Z-cap 许可证才能从公共池中检出带宽。

注意：

- 零容量许可证的安装方式与其他 NetScaler 本地许可证相同。有关如何获取和安装零容量许可证的更多信息，请参阅NetScaler 许可指南。

管理和安装 Z-cap 许可证

您必须使用硬件序列号或许可证访问代码手动安装 Z-cap 许可证。安装 Z-cap 许可证后，它将锁定到硬件，并且无法按需在 NetScaler 硬件实例之间共享。但是，您可以手动将 Z-cap 许可证移动到另一个 NetScaler 硬件实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

运行 NetScaler 软件版本 11.1 build 54.14 或更高版本的 NetScaler MPX 实例以及运行 11.1 build 58.13 或更高版本的 NetScaler SDX 实例支持 NetScaler 弹性许可。有关更多信息，请参阅弹性许可和池化许可的最小和最大容量中的表 1 和表 2。

注意：

使用基于 LAS 的许可时，您无需应用 Z-Cap 许可证。

独立 NetScaler VPX 实例

在以下虚拟机管理程序上运行 NetScaler 软件版本 11.1 Build 54.14 及更高版本的 NetScaler VPX 实例支持弹性许可：

- 威睿 ESX 6.0
- 思杰 Hypervisor™
- Linux KVM 虚拟机

在以下虚拟机管理程序和云平台上运行 NetScaler 软件版本 12.0 Build 51.24 及更高版本的 NetScaler VPX 实例支持弹性许可：

- 微软 Hyper-V
- AWS
- 微软 Azure
- 谷歌云

在以下虚拟机管理程序和云平台上运行 NetScaler 软件版本 13.0 和 13.1（所有版本）的 NetScaler VPX 实例支持弹性许可：

- 威睿 ESX 6.0
- 思杰 Hypervisor
- Linux KVM 虚拟机
- 微软 Hyper-V
- AWS
- 微软 Azure
- 谷歌云

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

为了在 NetScaler Console 与 Microsoft Azure 或 AWS 之间启用通信，必须配置 IPSEC 隧道。有关详细信息，请参阅将部署在云中的 NetScaler VPX 实例添加到 NetScaler Console。与零容量硬件不同，NetScaler VPX 不需要零容量许可证。为了处理流量，它必须从池中检出带宽和实例许可证。

独立 NetScaler CPX 实例

部署在 Docker 主机上的 NetScaler CPX 实例支持弹性许可。与零容量硬件不同，NetScaler CPX 不需要 Z-cap 许可证。单个 NetScaler CPX 实例消耗高达 1 Gbps 的吞吐量时，仅从许可证池中检出 1 个实例，不检出带宽。例如，假设您有 20 个 NetScaler CPX 实例，带宽池为 20 Gbps。如果其中一个 NetScaler CPX 实例消耗 500 Mbps 吞吐量，则剩余 19 个 NetScaler CPX 实例的带宽池仍为 20 Gbps。

如果同一个 NetScaler CPX 实例开始消耗 1500 Mbps 吞吐量，则剩余 19 个 NetScaler CPX 实例的带宽池为 19.5 Gbps。

对于弹性许可，您只能以 10 Mbps 的倍数添加更多带宽。

独立 NetScaler BLX 实例

NetScaler BLX 实例支持弹性许可。NetScaler BLX 实例不需要 Z-cap 许可证。为了处理流量，NetScaler BLX 实例必须从池中检出带宽和实例许可证。

带宽池

带宽池是物理和虚拟 NetScaler 实例可以共享的总带宽。带宽池包含高级软件版本的池。如果您从池化许可切换到弹性许可，您可能会发现标准版、高级版和高级版软件版本的混合。给定的 NetScaler MPX/VPX/CPX/BLX 实例不能同时从不同的池中检出带宽。它可以从中检出带宽的带宽池取决于其获得许可的软件版本。

实例池

有三种软件实例池：

- VPX/CPX/BLX 软件实例
- MPX 软件实例（MPX FIPS 适用相同池）
- SDX 软件实例（SDX FIPS 适用相同池）
- VPX FIPS 软件实例

© 1997–2026 Citrix Systems, Inc. All rights reserved.

从池中检出后，许可证将解锁软件实例的资源，包括 CPU/PE、SSL 核心、每秒数据包和带宽。

配置许可证

重要提示：

基于文件的许可系统（也称为手动管理的授权），传统上用于激活各种本地部署组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于 Citrix 产品套件产品激活的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler 弹性许可证 (CPL/UHMC)、传统 NetScaler 池化许可证和 NetScaler 固定期限带宽许可证。为了保持受支持，您的 NetScaler 和 NetScaler Console 部署必须是兼容 LAS 的版本。

兼容 LAS 的最低 NetScaler 版本要求如下：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：从 2025 年 9 月初开始支持。
- NetScaler Console 本地部署版：14.1-51.x

  注意： Console 本地部署版对 LAS 的支持从 14.1-51.x 版本开始。但是，从 April 15 2026 起，Console 本地部署版 14.1-51.x 及更高版本和 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署版 14.1-51.x 版本或 13.1-60.x 版本或更高版本，您可以继续使用基于文件的许可直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署版 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署版 13.1 不支持 LAS。

所有其他形式的传统 NetScaler 许可证，例如池化 vCPU、CICO、永久许可证，将不支持 LAS。使用没有有效维护的永久许可证的 NetScaler 实例在升级到上述软件版本后将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有疑问或疑虑，请联系客户服务。Citrix 可能会在不承担任何责任的情况下限制或暂停您的 Citrix 维护，如果您的行为不符合这些要求，此外，Citrix 还可能根据法律或衡平法采取任何其他补救措施。在法律或法规禁止的情况下，这些要求不适用。
在继续之前，请阅读以下注意事项。

注意：

如果您拥有池化许可证，并且现在已购买并应用了弹性许可证，则组合授权将显示在弹性许可证仪表板中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler 弹性许可允许您在不同的 NetScaler 外形规格之间共享带宽或实例许可证。将此弹性容量用于数据中心或公共云中的实例。当实例不再需要资源时，它会将分配的容量检查回公共池。在需要资源的其他 NetScaler 实例上重用已释放的容量。

您可以使用弹性许可来最大化带宽利用率，方法是确保为实例分配必要的带宽，而不是超出其需求。在运行时增加或减少分配给实例的带宽，而不会影响流量。

您可以在 NetScaler Console 中执行以下任务：

- **对于 LAS：**
  a. 使用 Cloud Connect 激活许可证激活服务 (LAS)。
  b. 一旦许可证权利出现在 Console 本地许可证服务器上，即可为 NetScaler 实例签出许可证。
  c. 确保许可证基于每个实例的最小和最大容量。
- **对于基于文件的许可：**
  a. 将您的弹性许可证（包括带宽和软件实例池）上传到 NetScaler Console 本地许可证服务器。
  b. 将 SDX 或 MPX 零容量许可证直接上传到其各自的硬件。
  c. 按需将许可证池中的许可证分配给您的 NetScaler 实例。签出许可证时，请确保它们基于实例的最小和最大容量。

  您可以从 citrix.com 网站下载所有弹性许可证，包括带宽、实例和零容量 (Z-cap) 许可证。有关更多信息，请参阅 NetScaler® 许可指南。

基于 LAS 的许可

使用 LAS 时，外部代理是可选的。确保端口 443 可用于实例从 NetScaler Console 签出许可证。有关更多信息，请参阅 系统要求。

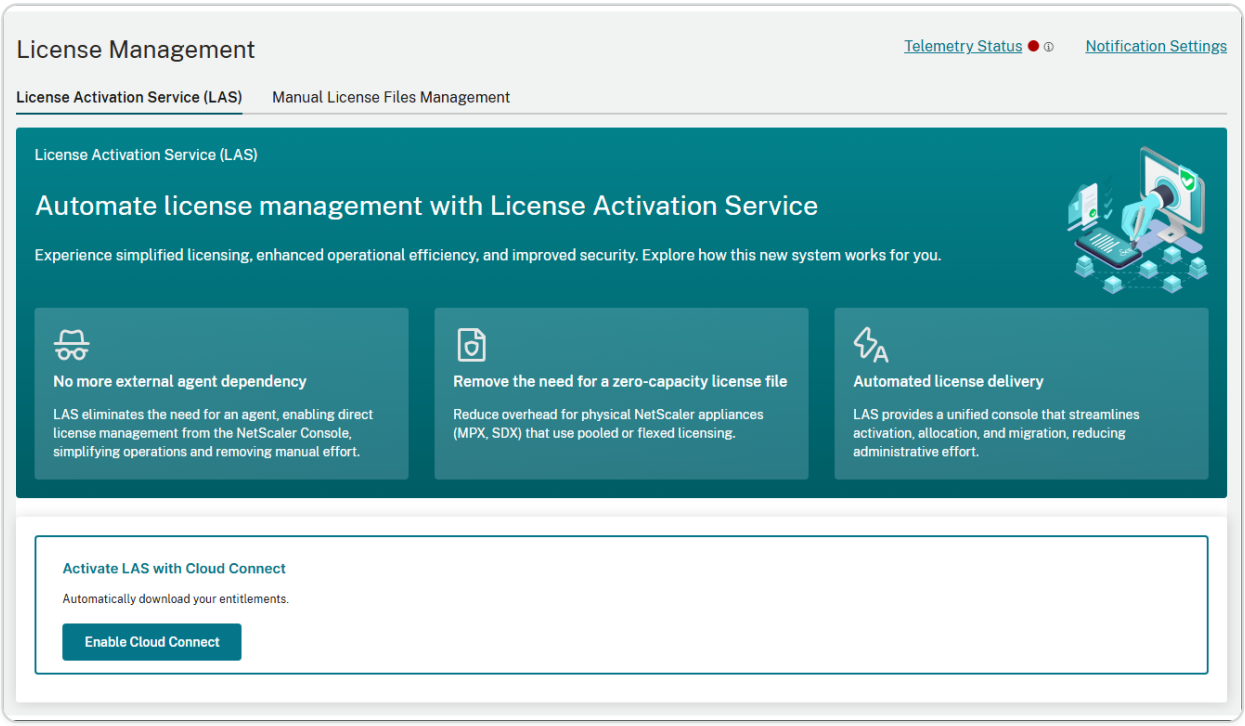
步骤 1：激活 LAS 并获取权利

1. 使用 **Cloud Connect** 激活 LAS。

   有关详细信息，请参阅激活许可证激活服务。

   激活后，您的弹性许可和池化许可权益将显示在**许可证管理 > LAS**中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



。

步骤 2：将 NetScaler 实例添加到 NetScaler Console On-prem

确保将 NetScaler 实例添加到 NetScaler Console On-prem，以便它们可以接收许可证。有关添加实例的详细信息，请参阅将 NetScaler 实例添加到 NetScaler Console On-prem。

步骤 3：许可或迁移 NetScaler 实例

1. 导航到**许可管理 > LAS**。
2. 单击**使用 LAS 许可或迁移到 LAS**。

   有关详细信息，请参阅许可证激活服务。

步骤 4：编辑弹性吞吐量容量

许可实例后，修改其分配的吞吐量容量。

1. 导航到**NetScaler 许可 > 弹性许可 > 仪表板**。
2. 选择**LAS 管理的权益**选项卡。
3. 在**已许可的 NetScaler** 部分中，选择一个实例，然后单击**编辑吞吐量容量**。
4. 在 **分配** 列中输入新容量，然后单击 **提交**。

未授权 MPX 设备专用许可

如果未授权的 MPX 直接或通过代理连接到本地 NetScaler Console，则不支持 HTTPS 连接。因此，步骤 2 不可行。请改为导航到 NetScaler 以完成以下步骤。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

先决条件： 如果您的 NetScaler MPX 直接（即不通过代理）连接到本地 NetScaler Console，请确保在本地 NetScaler Console 上启用基本身份验证。在初始设置（即在本地 NetScaler Console 中管理和许可您的 NetScaler MPX 之后）后，您可以出于安全目的禁用此基本身份验证设置。

1. 登录 NetScaler GUI。
2. 导航到 **系统 > 许可证 > ADC 许可证 > 管理许可证 > 添加新许可证**。
3. 在 **许可证** 页面中，选择 **使用远程许可** 单选按钮，然后从 **远程许可模式** 中选择 **LAS** 模式。
4. 在 **服务器名称/IP 地址** 字段中，输入 NetScaler Console 外部代理的 IP 地址。
5. 输入您的凭据以向 NetScaler Console 注册实例，然后单击 **继续**。

   注意：如果您有用于验证的数字证书，请选中“验证证书”复选框。
6. 在 **设备配置文件名称** 字段中，提供 NetScaler Console 用于访问实例的实例配置文件。此配置文件包含您要添加的实例的用户名和密码。默认配置文件为 ns_nsroot_profile。但是，如果您更改了默认管理员凭据，请确保定义自定义实例配置文件名称。
7. 在 **分配许可证** 下，选择许可证版本并指定所需的带宽。首次在 NetScaler 中分配许可证后，您可以稍后直接从 NetScaler Console GUI 修改或释放分配。
8. 单击 **获取许可证**。

注意：

更改许可证版本后，对实例执行热重启以使更改生效。

许可证激活 Blob 行为

NetScaler 实例从本地 Console 获取的作为 **License with LAS 或 Migrate to LAS** 一部分的许可证激活 Blob 有效期为 30 天。如果 NetScaler 失去与本地 Console 的连接，然后又重新获得连接，则许可证激活 Blob 会立即恢复。

当 NetScaler 无法在长达 24 小时内重新连接到本地 Console 时，它将进入宽限期。 默认情况下，许可证激活 Blob 每 8 小时刷新一次。如果在 24 小时内连续三次 8 小时刷新尝试失败，NetScaler 将进入宽限期。

许可证宽限期警报

以下是许可证宽限期警报的接触点：

- 在 Flexed 仪表板上，将显示一个警告图标，指示实例处于宽限期以及许可证激活 Blob 到期前的剩余天数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 每当管理员登录到 NetScaler 实例 GUI 时，都会出现一个弹出消息，指示实例处于宽限期以及许可证激活 Blob 到期前的剩余天数。
- 电子邮件通知将发送到配置的电子邮件地址。有关详细信息，请参阅配置电子邮件设置。

注意： 确保为“系统事件类别”选择“**许可证**”以接收与许可证相关的电子邮件通知。

手动管理的权利（基于文件的许可）

开始之前

在配置 Flexed 许可之前，请确保满足以下先决条件：

- 从 NetScaler 到 NetScaler Console 必须能够访问 `27000` 和 `7279` 端口，以便签出许可证。请参阅系统要求。

步骤 1 - 在 NetScaler Console 中应用许可证

1. 导航到 **NetScaler® 许可 > 许可证管理**。
2. 在**许可证文件**部分中，选择**添加许可证文件**并选择以下选项之一：
   - **从本地计算机上传许可证文件**。如果许可证文件已存在于您的本地计算机上，您可以将其上传到 NetScaler Console。
   - **使用许可证访问代码**。指定您从 Citrix 购买的许可证的许可证访问代码。然后，选择**获取许可证**。然后选择**完成**。

   注意：

   您可以随时从**许可证设置**向 NetScaler Console 添加更多许可证。

3. 单击**完成**。

   许可证文件已添加到 NetScaler Console。**许可证到期信息**部分列出了 NetScaler Console 中存在的许可证以及距离到期的剩余天数。
4. 在**许可证文件**中，选择要应用的许可证文件，然后单击**应用许可证**。

   此操作使 NetScaler 实例能够将所选许可证用作 Flexed 许可证。

步骤 2 - 将 NetScaler Console 注册为许可证服务器并分配许可证

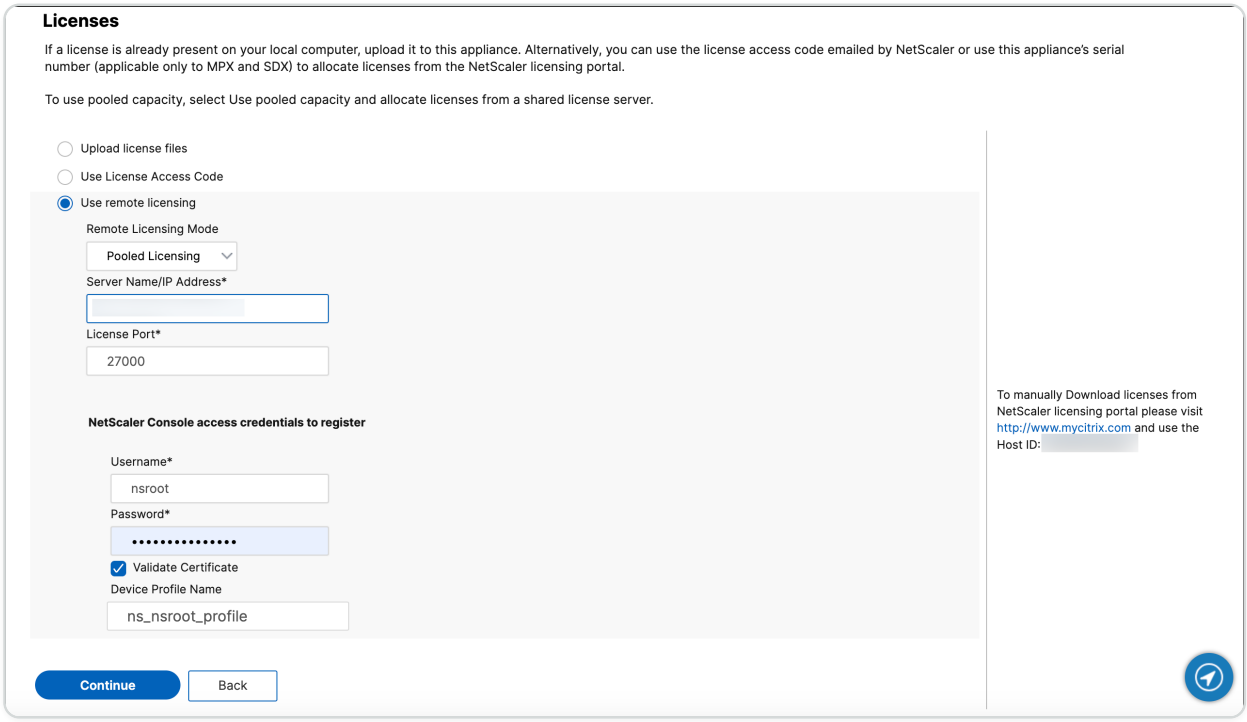
您可以将 NetScaler Console 注册为 NetScaler 实例的许可证服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 GUI 注册 NetScaler Console 服务器

在 NetScaler Console GUI 中，注册与 NetScaler 实例关联的 NetScaler Console 服务器。

1. 登录到 NetScaler GUI。
2. 导航到**系统 > 许可证 > 管理许可证**。
3. 点击 **添加新许可证**。
4. 选择 **使用远程许可**，并在 **远程许可模式** 下，从列表中选择 **池化许可**。
5. 在 **服务器名称/IP 地址** 字段中，指定 NetScaler Console 服务器 IP 地址。
6. 默认许可证端口是 27000。
7. 输入您的 NetScaler Console 服务器凭据以向 NetScaler Console 注册实例，然后点击 **继续**。在 NetScaler Console 中，其中一台服务器是许可证服务器。



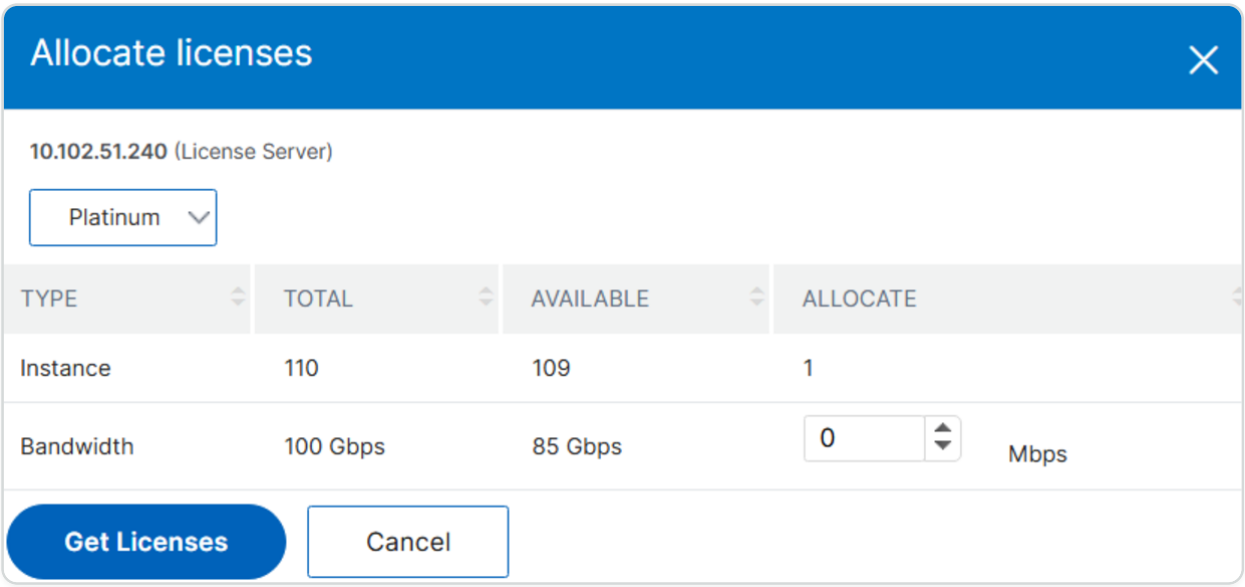
注意：

仅当您拥有用于验证的数字证书颁发机构 (CA) 证书时，才选择 **验证证书** 复选框。

8. 在 **设备配置文件名称** 下，指定 NetScaler Console 可用于访问实例的实例配置文件。此实例配置文件包含您要添加到 NetScaler Console 的实例的用户名和密码。默认配置文件是 **ns_nsroot_profile**。如果您已更改实例的默认管理员凭据，则可以定义自定义实例配置文件名称。
9. 在 **分配许可证** 中，选择许可证版本并指定所需的带宽。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

首次在 NetScaler 中分配许可证。您以后可以从 NetScaler Console GUI 更改或释放许可证分配。



点击 **获取许可证**。

重要提示

如果更改许可证版本，请热重启实例。配置更改在您重启实例后才会生效。

使用 CLI 添加 NetScaler Console 服务器

如果 NetScaler 实例没有 GUI，请使用以下 CLI 命令添加与实例关联的 NetScaler Console 服务器：

1. 登录到 NetScaler 控制台。
2. 添加已在 NetScaler Console 中注册的关联 NetScaler Console 服务器的 IP 地址。默认许可证端口为 27000。

```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-license-port-number>
```

3. 查看许可证服务器中可用的许可证带宽：

```
> sh ns licenseserverpool
```

4. 从所需的许可证版本中分配许可证带宽：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> set ns capacity -unit gbps -bandwidth <specify-license-bandwidth>
edition <specify-license-edition>
```

重要

如果更改许可证版本，请热重启实例。

`reboot -w`

配置更改在您重新启动实例后才会生效。

步骤 3 - 编辑 NetScaler 实例的弹性吞吐量容量

1. 导航到 **NetScaler 许可 > 弹性许可 > 仪表板**。
2. 在 **Licensed NetScalers** 部分，选择一个实例并单击 **Edit Throughput Capacity**。
3. 在 **Edit Throughput Capacity** 页面中，在 **Allocate** 列中输入一个数字。
4. 单击 **Submit**。

NetScaler MPX-Z

MPX-Z 是支持弹性容量的 NetScaler MPX 设备。MPX-Z 仅支持高级版许可证的带宽池。

MPX-Z 在连接到许可证服务器之前需要许可证。您可以通过以下方法之一安装 MPX-Z 许可证：

- 从本地计算机上传许可证文件。
- 使用实例的硬件序列号。
- 从实例 GUI 的“**系统**” > “**许可证**”部分获取许可证访问代码。

如果您移除 MPX-Z 许可证，MPX 将变为未授权状态。许可证将释放到许可证服务器。

您可以动态修改 MPX-Z 实例的带宽，而无需重新启动。仅当您要更改许可证版本时才需要重新启动。

注意：

重新启动实例时，它会自动签出其配置容量所需的弹性许可证。

NetScaler SDX-Z

SDX-Z 是支持弹性容量的 NetScaler SDX 设备。SDX-Z 支持高级版许可证的带宽和实例池。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SDX-Z 在连接到许可证服务器之前需要许可证。您可以通过以下方法之一安装 SDX-Z 许可证：

- 从本地计算机上传许可证文件。
- 使用实例的硬件序列号。
- 实例 GUI 的 **系统** > **许可证** 部分中的许可证访问代码。

如果删除 SDX-Z 许可证，SDX 将变为未授权状态。许可证将释放到许可证服务器。

您可以动态修改 SDX-Z 实例的带宽，而无需重新启动。

注意：

重新启动实例时，它会自动签出其配置容量所需的弹性许可证。

NetScaler 高可用性对的许可证要求（LAS 和基于文件的许可通用）

开始之前，请确保 NetScaler Console 服务器已配置为许可证服务器。有关详细信息，请参阅将 NetScaler Console 配置为许可证服务器

当您将带宽分配给 NetScaler HA 对时，NetScaler Console 会将分配的带宽签出到主实例。您必须对辅助实例重复此过程。

要将池许可证分配给 NetScaler HA 对，请参阅将弹性许可证分配给 NetScaler 实例

弹性容量页面分别显示实例及其分配的容量。

NetScaler 弹性许可状态（LAS 和基于文件的许可通用）

弹性许可状态指示 NetScaler 实例上的许可证要求。配置了弹性许可的 NetScaler 实例显示以下状态之一：

- **已分配**：实例正在以适当的许可证容量运行。
- **宽限期**：实例正在宽限期内运行。宽限期为 30 天，之后实例将变为未授权状态。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

弹性许可证仪表板

重要提示：

基于文件的许可系统（也称为手动管理的授权）传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活所有 Citrix 产品的新一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler 弹性许可证 (CPL/UHMC)、旧版 NetScaler 池许可证和 NetScaler 固定期限带宽许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是与 LAS 兼容的版本。

与 LAS 兼容的最低 NetScaler® 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：自 2025 年 9 月初起支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： Console 本地部署的 LAS 支持从版本 14.1-51.x 及更高版本开始。但是，自 April 15 2026 起，Console 本地部署版本 14.1-51.x 及更高版本以及 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署版本 14.1-51.x 或版本 13.1-60.x 或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署版本 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如池化 vCPU、CICO、永久许可证，将不支持 LAS。升级到上述软件版本后，使用没有有效维护的永久许可证的 NetScaler 实例将变为未授权状态。
基于 LAS 的许可证在法律或法规禁止的地区可能不向客户提供。
如果您有任何疑问或疑虑，请联系客户服务。如果未能遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外，Citrix 还可能根据法律或衡平法采取任何其他补救措施。在法律或法规禁止的地区，这些要求不适用。
在继续操作之前，请阅读以下注意事项。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意事项：

- 如果您之前拥有池许可证，并且现在购买并应用了弹性许可证，则合并后的授权现在显示在弹性许可证仪表板中。
- 如果您只有池化许可证，请查看池化许可证控制板。
- 如果您只有弹性许可证，或者同时拥有弹性许可证和池化许可证，请查看弹性许可证控制板。
- **基于许可方法的注意事项：**
  - 要查看基于 LAS 的许可许可证，请导航到 **NetScaler® 许可证 > 弹性许可 > 控制板 > LAS 管理的权利** 选项卡
  - 要查看手动管理的权利（基于文件的许可）许可证，请导航到 **NetScaler® 许可证 > 弹性许可 > 控制板 > 手动管理的权利** 选项卡
  - 如果您同时使用这两种许可机制，请参考这两个选项卡。 弹性许可证控制板为您提供了您购买的吞吐量容量和实例的全面视图。

此页面显示了不同版本和不同外形规格（如 MPX、VPX 和 SDX）的实例详细信息和吞吐量容量。NetScaler MPX 和 NetScaler MPX FIPS 具有相同的许可证文件。同样，NetScaler SDX 和 NetScaler SDX FIPS 具有相同的许可证文件。但是，NetScaler VPX FIPS 的文件与 NetScaler VPX 不同，并单独显示。此外，NetScaler VPX（包括 SDX 上的 VPX）、NetScaler BLX 和 NetScaler CPX 需要 NetScaler VPX 许可证，并且是 VPX 权利和分配的一部分。弹性许可证仅支持高级版。但是，如果您购买了弹性许可证，并且之前拥有池化标准版或高级版带宽容量，则与带宽容量（标准版或高级版）相关的详细信息也会在弹性许可证控制板中列出。

VPX（包括 SDX 上的 VPX）、BLX 和 CPX 外形规格需要 NetScaler 弹性 VPX 软件实例许可证文件。也就是说，这些外形规格是弹性 VPX 软件实例许可证的权利和分配的一部分。

有关您已许可的 NetScaler 实例的详细信息可在“**已许可的 NetScaler**”部分中找到。您可以选择一个实例并编辑带宽或在该实例上释放许可证。

您可以根据以下参数筛选结果：

- 按吞吐量容量筛选
  - 高级版
  - 高级
  - 标准版

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 外形规格
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
- 许可证状态
  - 连接丢失
  - 宽限
  - 已分配

编辑 NetScaler 实例上已分配的吞吐量容量

1. 导航到 **NetScaler 许可 > 弹性许可 > 控制板**。
2. 在**已许可的 NetScaler** 部分中，选择一个实例，然后单击**编辑吞吐量容量**。
3. 在**编辑吞吐量容量**页面中，在**分配**列中输入一个数字。
4. 单击**提交**。

在 NetScaler 实例上释放许可证

要将许可证传输到另一个实例，您必须在当前实例上释放许可证，然后将许可证应用于新实例。选择**释放许可证**将执行以下操作：

- 将该实例上所有已签出的许可证释放到许可证服务器。
- 删除该实例上的许可证服务器配置。

如果您选择**是**，您的 NetScaler 实例将变为未授权状态，并且无法处理任何流量。

弹性许可证报告

重要提示：

基于文件的许可系统（也称为手动管理的权利），传统上用于激活各种本地组件，将于 April 15, 2026 终止服务 (EOL)。许可证激活服务 (LAS) 是用于激活所有 Citrix 产品套件的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler 弹性许可证 (CPL/UHMC)、旧版 NetScaler 池许可证和 NetScaler 固定期限带宽许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是 LAS 兼容版本。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LAS 兼容的最低 NetScaler® 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：自 2025 年 9 月初起支持。
- NetScaler Console 本地部署：14.1-51.x

注意： Console 本地部署的 LAS 支持从 14.1-51.x 版本开始。但是，自 April 15 2026 起，Console 本地部署 14.1-51.x 及更高版本和 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署 14.1-51.x 或 13.1-60.x 或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如池化 vCPU、CICO、永久许可证，将不支持 LAS。升级到上述软件版本后，使用没有有效维护的永久许可证的 NetScaler 实例将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。如果未能遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法上的其他补救措施。在法律或法规禁止的情况下，这些要求不适用。
在此仪表板中，您可以查看以下详细信息：

- 软件实例（VPX、MPX、SDX 和 VPX FIP）的权利和分配
- 带宽/吞吐量容量的权利、分配和实际使用情况
- 跨所有托管或选定的实例的峰值和平均分配
- 跨所有托管或选定的实例的峰值和平均使用量

功能（适用于 NETSCALER 实例）	描述
权利	软件实例类型（VPX、SDX、MPX）的总实例权利。
分配	软件实例类型（VPX、SDX、MPX）的总实例分配。

功能（适用于带宽/吞吐量容量）	描述
权利	跨所有托管 NetScaler 实例的总带宽/吞吐量容量权利。总权利是根据许可证管理（**NetScaler**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

功能（适用于带宽/吞吐量容量）	描述
	Licensing > License Management）中应用的许可证计算的。
分配	在弹性许可仪表板 (**NetScaler Licensing > Flexed Licensing > Dashboard**) 中，分配给**许可的 NetScaler** 的带宽/吞吐量容量。
使用量	NetScaler 实例消耗的总吞吐量。

注意：

弹性许可证仅支持高级版。但是，如果您已购买并应用了弹性许可证，并且之前拥有池化标准或高级带宽容量，则也会列出与带宽/吞吐量容量（标准或高级）相关的详细信息。例如，如果您已应用 1000 Gbps 弹性许可证（高级版），并且还拥有 100 Gbps 高级带宽的活动池化许可证，则报告仪表板会同时显示 1000 Gbps 高级版和 100 Gbps 高级带宽。

以下示例可帮助您了解仪表板如何显示峰值使用量和平均使用量：

假设有 3 个托管的 NetScaler 实例（NetScaler A、NetScaler B 和 NetScaler C）具有弹性许可证（高级带宽），并且所选持续时间为 1 天。对于计算，NetScaler Console 会考虑每个 NetScaler 实例每小时的数据点（以 Mbps 为单位）。对于 1 天，每个 NetScaler 实例有 24 个数据点。因此，对于 3 个 NetScaler 实例，共有 (24 * 3) 个数据点。

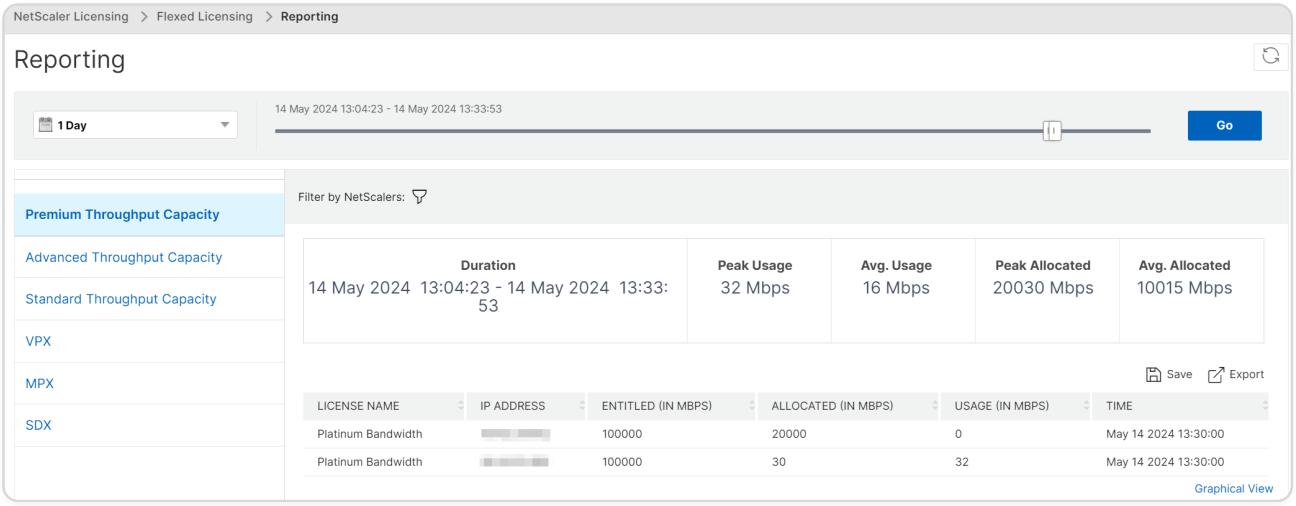
- **峰值使用量** = 所有 NetScaler 实例 24 小时内最高数据点 (Mbps) 的总和。例如，如果 NetScaler A 在 24 小时内的最高数据点为 30 Mbps，NetScaler B 为 45 Mbps，NetScaler C 为 120 Mbps，则峰值使用量显示为 195 Mbps (30 + 45 + 120)。
- **平均使用量** = 每个 NetScaler 实例所有 24 小时数据点的总和除以 24。因此，对于 3 个 NetScaler 实例，所有 3 个 NetScaler 实例的总平均值除以 3。例如，如果 NetScaler A 的平均值为 25 Mbps，NetScaler B 的平均值为 20 Mbps，NetScaler C 的平均值为 45 Mbps，则平均使用量显示为 30 Mbps (25 + 20 + 45 除以 3)。

同样，峰值和平均分配详细信息也使用相同的逻辑显示。

您可以从列表中选择持续时间，从一小时到一年不等，并以表格视图和图形视图查看详细信息。

以下示例显示了使用弹性许可证（高级带宽）的实例的表格视图：

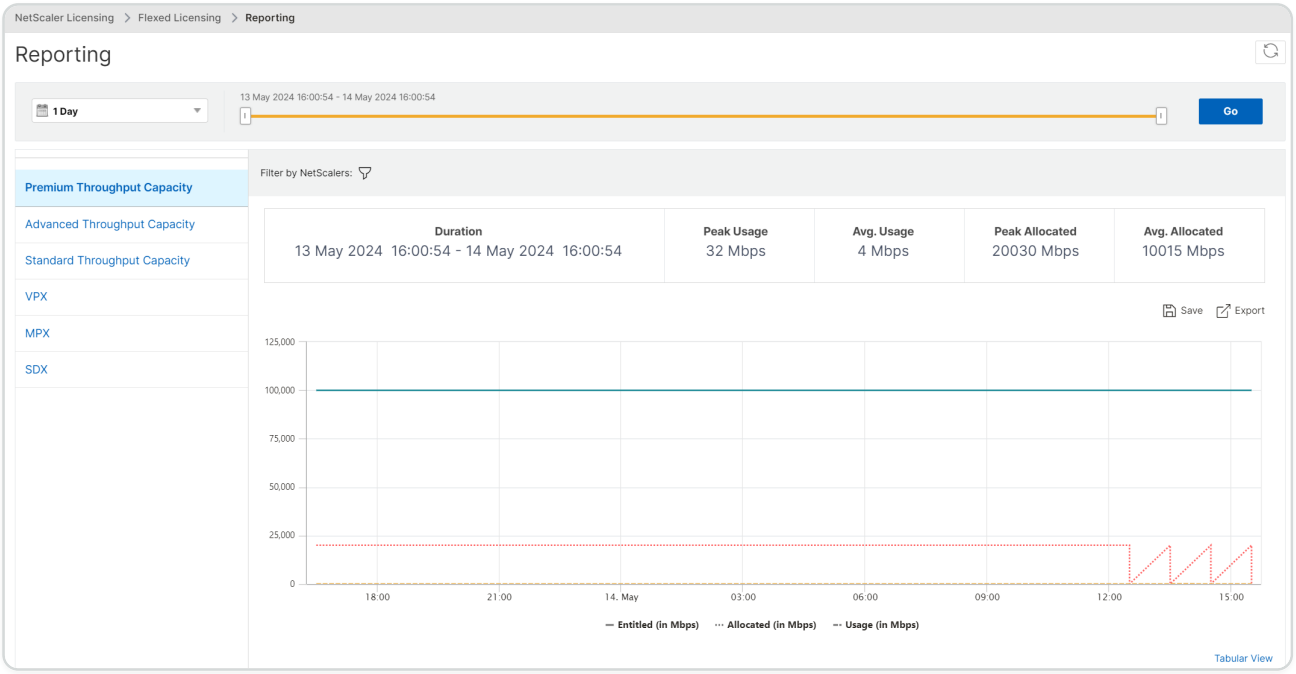
© 1997–2026 Citrix Systems, Inc. All rights reserved.



仪表板上显示以下详细信息：

- **峰值使用量** - 所选持续时间内的最高使用量（以 Mbps 为单位）。
- **平均使用量** - 所选持续时间内的平均使用量（以 Mbps 为单位）。
- **峰值分配** - 所选持续时间内的最高分配。
- **平均分配** - 所选持续时间的平均分配。
- **筛选** - 您可以选择一个或多个实例，以查看特定实例的使用情况和分配详细信息。
- **导出** - 您可以导出 PDF、JPEG 和 PNG 格式的详细信息。

以下示例显示了使用弹性许可证（高级带宽）的实例的图形视图：



© 1997–2026 Citrix Systems, Inc. All rights reserved.

过渡到 Flexed 许可

重要提示：

基于文件的许可系统（也称为手动管理的授权）传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活所有 Citrix 产品套件的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler Flexed 许可（CPL/UHMC）、旧版 NetScaler 池许可和 NetScaler 固定期限带宽许可。为了获得持续支持，您的 NetScaler 和 NetScaler Console 部署必须是与 LAS 兼容的版本。

兼容 LAS 的最低 NetScaler® 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console 服务：从 2025 年 9 月初开始支持。
- 本地部署的 NetScaler Console：14.1-51.x

  注意： LAS 对本地部署的 Console 的支持从 14.1-51.x 版本开始。但是，从 April 15 2026 起，本地部署的 Console 14.1-51.x 及更高版本以及 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到本地部署的 Console 14.1-51.x 版本或 13.1-60.x 版本或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到本地部署的 Console 14.1-51.x 或更高版本，并切换到 LAS，因为本地部署的 Console 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可，例如池化 vCPU、CICO、永久许可，将不支持 LAS。升级到上述软件版本后，使用没有有效维护的永久许可的 NetScaler 实例将变为未授权状态。
在法律或法规禁止的地区，基于 LAS 的许可可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。如果不遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法上的任何其他补救措施。这些要求在法律或法规禁止的地区不适用。
在继续之前，请阅读以下注意事项。

基于 LAS 的许可

注意：

确保您的 NetScaler (ADC 和 SDX) 实例运行在与 LAS 兼容的版本上。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关以下许可证的迁移信息，请参阅 (/zh-cn/netscaler-application-delivery-management-software/current-release/license-server/license-activation-service.html) 的“**迁移现有许可实例**”部分。

- 弹性许可（基于文件的许可证）到弹性许可（基于 LAS 的许可证）
- 池化许可（基于文件的许可证）到弹性许可（基于 LAS 的许可证）

有关以下许可证的过渡信息，请参阅 (/zh-cn/netscaler-application-delivery-management-software/current-release/license-server/license-activation-service.html) 的“**过渡到 LAS**”部分。

- 池化 vCPU 许可（基于文件的许可证）到弹性许可（基于 LAS 的许可证）
- 固定订阅或永久许可（基于文件的许可证）到弹性许可（基于 LAS 的许可证）
- 固定 vCPU 许可（基于文件的许可证）到弹性许可（基于 LAS 的许可证）
- CICO 许可（基于文件的许可证）到弹性许可（基于 LAS 的许可证）

手动管理的权利（基于文件的许可证）

注意：

您必须在当前许可证到期之前切换到弹性许可。在规划过渡时，请牢记以下步骤，如果这些步骤涉及许可证重新配置或 NetScaler® 重启，请规划维护窗口。

池化带宽许可证到弹性许可证

某些步骤适用于 MPX、SDX 和 VPX。这些步骤首先列出，然后是 MPX、SDX 或 VPX 特有的步骤。

VPX/MPX/SDX 的通用步骤

1. 在 NetScaler Console 上上传并应用 Flexed 软件许可证。请参阅 许可证文件。
2. 如果您有特定期限的 Z-Cap 软件许可证，请在 NetScaler 硬件（MPX/SDX）上应用该许可证。

对于 VPX/MPX

需要执行以下附加步骤：

1. 如果您有池化高级版 (Platinum) 带宽许可证，则该许可证将在旧许可证到期后自动切换到 Flexed。
2. 如果您有池化标准版或池化高级版带宽许可证，请手动签出高级版带宽并热重启 NetScaler。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

对于 SDX

注意：

请确保在当前许可证到期之前切换到 Flexed 许可证。

需要执行以下附加步骤：

1. 从 Flexed 许可证中签出所需的实例和带宽许可证到 SDX。无需重启 SDX。
2. 如果 SDX 上的所有 VPX 都具有高级版，则该许可证将在旧许可证到期后自动切换到 Flexed。
3. 将所有具有标准版或高级版的 VPX（在 SDX 上）的版次更改为高级版。这些 VPX 实例将自动重启。
4. 将 SDX 上的标准版和高级版带宽容量降至零。

池化 vCPU 到 Flexed 带宽容量

适用于 VPX

1. 在 NetScaler Console 上上传并应用 Flexed 软件许可证。请参阅许可证文件。
2. 使用 NetScaler GUI 删除现有许可证服务器。在所有步骤完成之前，NetScaler 将处于未授权状态。
3. 添加具有 Flexed/Pooled 选项的许可证服务器。
4. 将所需的实例和带宽许可证签出到 NetScaler。
5. 热重启 NetScaler。

适用于 CPX

1. 在 NetScaler Console 上上传并应用 Flexed 许可证。请参阅许可证文件。
2. 使用带宽要求更新 CPX YAML 或 HELM 清单文件。请参阅CPX 基于带宽的许可。
3. 使用 `kubectl apply -f cpx.yaml` 命令或 HELM 图表部署 CPX 实例。

从固定订阅或永久许可证到 Flexed 许可证

某些步骤适用于 MPX、SDX 和 VPX。这些步骤首先列出，然后是 MPX、SDX 或 VPX 特有的步骤。

VPX/MPX/SDX 的通用步骤

1. 载入 NetScaler Console。
2. 在 NetScaler Console 上上传并应用 Flexed 软件许可证。请参阅许可证文件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在 NetScaler 硬件 (MPX/SDX) 上应用 Z-Cap 软件许可证。

对于 VPX/MPX

需要执行以下附加步骤：

1. 将所需的实例和带宽许可证签出到 NetScaler。
2. 热重启 NetScaler。
3. NetScaler 重启后删除固定订阅许可证。

对于 SDX

需要执行以下附加步骤：

1. 从 SDX 上的 Flexed 许可证中签出所需的实例和带宽许可证。
2. 如果 SDX 上的所有 VPX 都具有高级版，则无需重启 SDX。
3. 如果任何 VPX 具有高级版或标准版，则该 VPX 必须切换到高级版。VPX 会自动重启。
4. 在 NetScaler SDX 上应用 Z-Cap 软件许可证。
5. 从 SDX 上的 Flexed 许可中签出所需的实例和带宽许可证。
6. NetScaler 重启后删除固定订阅许可证。

CICO 到 Flexed 带宽容量

适用于 VPX

1. 在 NetScaler Console 上上传并应用 Flexed 软件许可证。请参阅 许可证文件。
2. 使用 NetScaler GUI 删除现有许可证服务器。在所有步骤完成之前，NetScaler 将处于未授权状态。
3. 添加具有 Flexed/Pooled 选项的许可证服务器。
4. 将所需的实例和带宽许可证检出到 NetScaler。
5. 热重启 NetScaler。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

弹性或池化许可证到期和连接问题行为的场景

重要提示：

基于文件的许可系统（也称为手动管理的授权），传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于 Citrix 产品套件产品激活的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler 弹性许可证 (CPL/UHMC)、旧版 NetScaler 池化许可证和 NetScaler 固定期限带宽许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是 LAS 兼容版本。

最低要求的 LAS 兼容 NetScaler® 版本为：

- NetScaler 应用交付控制器：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：从 2025 年 9 月初开始支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： Console 本地部署的 LAS 支持从 14.1-51.x 版本开始。但是，自 April 15 2026 起，Console 本地部署 14.1-51.x 及更高版本和 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署 14.1-51.x 版本或 13.1-60.x 或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如池化 vCPU、CICO、永久许可证，将不支持 LAS。使用没有有效维护的永久许可证的 NetScaler 实例在升级到上述软件版本后将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。如果未能遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法上的任何其他补救措施。在法律或法规禁止的情况下，这些要求不适用。

基于 LAS 的许可证

在期限到期之前

- 许可证必须在其期限到期之前续订。
- 对于 NetScaler Console 本地部署（云连接），如果许可证合同在 24 小时内续订，则许可证授权将自动续订。
- 如果许可证在有效期届满前续订，只要设备正常运行，NetScaler 将在旧许可证到期后无缝切换到新许可证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 无需重新启动。
- NetScaler 不需要手动重新配置容量。

有效期届满后

如果许可证未在其有效期届满前续订，NetScaler 实例将停止正常运行。

- 它将丢失其配置。
- 所有流量处理将完全停止。

连接问题行为场景

NetScaler 实例作为 **License with LAS** 或 **Migrate to LAS** 过程的一部分从 Console 本地部署接收的许可证激活 blob 有效期为 30 天。

如果 NetScaler 与 Console 本地部署失去连接然后重新连接，它将立即收到许可证激活 blob，没有任何延迟。

如果 NetScaler 在长达 24 小时内无法重新连接到 Console 本地部署，它将进入宽限期。

默认情况下，许可证激活 blob 每 8 小时刷新一次。如果刷新尝试在 24 小时内连续失败三次，NetScaler 将进入宽限期。

宽限期：

- NetScaler 进入 30 天宽限期。
- 所有许可功能继续正常工作。但是，在第三十一天：
  - NetScaler VPX、NetScaler CPX、NetScaler BLX 和 NetScaler MPX 实例将强制重启并变为未授权状态。
  - NetScaler SDX 上所有 VPX 实例的吞吐量将降至 1 Mbps。

许可证宽限期警报

在 Flexed 仪表板上，将出现一个警告图标，指示实例处于宽限期，并显示许可证激活 blob 到期前的剩余天数。每次管理员登录到 NetScaler 实例 GUI 时，都会弹出一个消息，指示实例处于宽限期，并显示许可证激活 blob 到期前的剩余天数。

手动管理的许可证（基于文件的许可证）

本文介绍了 NetScaler MPX、NetScaler SDX 和 NetScaler VPX/NetScaler BLX/NetScaler CPX 中许可证到期和连接问题行为的不同场景。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Flexed 许可证类型

- 软件实例 (VPX/BLX/CPX, SDX, MPX, VPX FIPS)
- 带宽容量

场景：MPX 外形规格

您正在使用 Flexed/Pooled 许可，并且许可证即将到期。以下场景解释了在期限到期之前和之后在 NetScaler Console 上上传新许可证，或者当许可证文件不存在时的行为。

期限到期前

如果在期限到期前上传新许可证，并且旧许可证仍然有效，则可以使用两种不同的容量池（旧的和新的）。

- 如果 NetScaler 正在运行，它将在旧许可证到期后无缝切换到新的 Flexed/Pooled 许可证。
- 不需要重启。
- NetScaler 不需要手动重新配置容量。

期限到期后

NetScaler 实例在许可证到期后停止其正常运行，包括配置丢失和流量处理完全关闭。

场景：SDX 外形规格

您正在使用弹性/池化许可，并且许可证即将到期。以下场景解释了在期限到期前后将新许可证上传到 NetScaler Console 或许可证文件不存在时的行为。

期限到期前

如果新许可证在期限到期前上传，并且旧许可证仍然有效，则可以使用两种不同的容量池（旧的和新的）。

- 如果 NetScaler 正在运行，它会在旧许可证到期后无缝切换到新的弹性/池化许可证。
- 不需要重启。
- NetScaler 不需要手动重新配置容量。

期限到期后

NetScaler 实例在许可证到期后停止其正常运行，包括配置丢失和流量处理完全关闭。

场景：VPX/BLX/CPX 外形规格

您正在使用弹性/池化许可，并且许可证即将到期。以下场景解释了在期限到期前后将新许可证上传到 NetScaler Console 或许可证文件不存在时的行为。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

期限到期前

如果在期限到期前上传新许可证，且旧许可证仍然有效，则可以使用两种不同的容量池（旧和新）。

- 如果 NetScaler 正在运行，它会在旧许可证到期后无缝切换到新的 Flexed/Pooled 许可证。
- 无需重新启动。
- NetScaler 不需要手动重新配置容量。

期限到期后

许可证到期后，NetScaler 实例将停止其正常运行，包括配置丢失和流量处理完全关闭。

连接问题行为场景

如果 NetScaler 与 NetScaler Console 本地服务器之间的连接中断，则行为如下：

- NetScaler 将进入 30 天的宽限期。
- 在此宽限期内，许可功能将继续工作，直到第三十天。
- 在第三十一天，
  - NetScaler VPX/NetScaler CPX/NetScaler BLX 和 NetScaler MPX 将强制重启并变为未授权状态。
  - NetScaler SDX 上所有 VPX 的吞吐量将降至 1 Mbps。

将 NetScaler Console 服务器配置为弹性或池化许可证服务器

重要提示：

基于文件的许可系统（也称为手动管理的权利），传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活 Citrix 产品套件中产品的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler 弹性许可证 (CPL/UHMC)、旧版 NetScaler 池化许可证和 NetScaler 固定期限带宽许可证。为了获得持续支持，您的 NetScaler 和 NetScaler Console 部署必须是与 LAS 兼容的版本。

与 LAS 兼容的最低 NetScaler® 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console 服务：自 2025 年 9 月初起支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： Console 本地部署的 LAS 支持从 14.1-51.x 版本开始。但是，自 April 15 2026 起，Console 本地部署 14.1-51.x 及更高版本和 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署 14.1-51.x 或 13.1-60.x 或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如池化 vCPU、CICO、永久许可证，将不支持 LAS。使用没有有效维护的永久许可证的 NetScaler 实例在升级到上述软件版本后将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。如果未能遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法上的任何其他补救措施。在法律或法规禁止的情况下，这些要求不适用。
作为管理员，您只能将 NetScaler Console 服务器配置为弹性或池化许可证服务器。通过此配置，NetScaler Console 服务器仅从 NetScaler 实例接收许可数据。

有时，您可能需要遵守监管规定，限制 NetScaler 实例的数据离开监管区域。在这种情况下，您可以在您的监管区域部署 NetScaler Console 本地服务器的本地实例，以使用管理、监控和分析功能。当您采用相同的方法使用弹性或池化许可证功能时，您必须在不同的 NetScaler Console 许可证服务器之间拆分弹性或池化许可证。这种方法无法为您提供在全球部署的 NetScaler 实例之间分配弹性或池化许可证的灵活性。

因此，请仅将 NetScaler Console 服务器配置为弹性或池化许可证服务器。NetScaler Console 服务器仅从所有 NetScaler 实例接收许可数据。因此，您可以遵守监管规定，并在全球部署的 NetScaler 实例之间动态分配弹性或池化容量许可证。

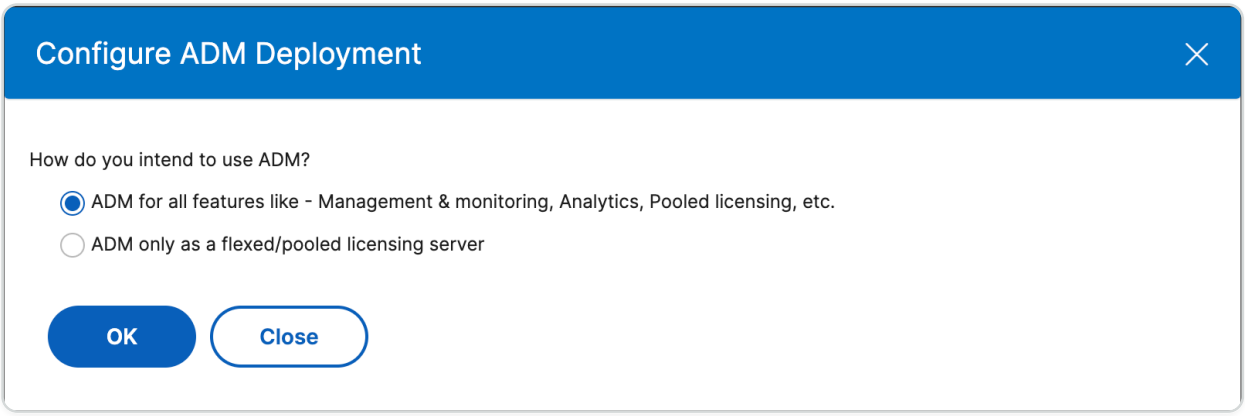
如何将 NetScaler Console 服务器配置为仅用作弹性或池化许可证服务器

在开始之前，请确保没有将 NetScaler 实例添加到 NetScaler Console 服务器。仅在完成步骤 4 后才添加 NetScaler 实例。

执行以下操作，将 NetScaler Console 服务器配置为仅用于弹性或池化许可证服务器：

1. 导航到 **设置 > 管理**。
2. 在 **系统配置** 部分中，选择 **系统部署**。
3. 在 **ADM 部署** 中，选择 **仅将 NetScaler Console 用作弹性/池化许可服务器**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 单击 **确定**。

   此操作仅保留弹性或池化许可功能，并禁用以下 NetScaler Console 功能：

   - NetScaler Console 备份
   - 事件管理
   - SSL 证书管理
   - 网络报告
   - 网络功能
   - 配置审计

   注意

   默认情况下，NetScaler Console 分析功能处于禁用状态。如果您已启用此功能，请务必将其禁用。

   在确认框中，单击“**是**”。

   NetScaler Console GUI 现在仅显示弹性或池化许可功能。其余功能不显示。

5. 在您仅为许可功能配置 NetScaler Console 后，请在“**基础架构 > 实例**”页面中添加 NetScaler 实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

- 您可以在一个或多个 NetScaler Console 服务器中添加 NetScaler 实例。当您更改此类 NetScaler 实例的密码时，请确保在发现该实例的所有 NetScaler Console 服务器上更新密码。
- 用户仍然可以在 NetScaler Console GUI 中执行一些禁用功能的操作。例如，事件轮询和 NetScaler 备份。作为超级管理员，如果您想限制此类操作，请使用适当的访问策略禁用其他管理员的用户访问。有关更多信息，请参阅在 NetScaler Console 上配置访问策略。

您还可以仅为弹性或池化许可证服务器部署 NetScaler Console 服务器，其规格要求如下：

组件	要求
RAM	8 GB
虚拟 CPU	4
存储	120 GB

旧版许可证

旧版许可证涵盖了适用于您的 NetScaler 实例的早期池容量、签入和签出以及虚拟 CPU 许可模型。以下主题可帮助您管理旧版许可证：

- NetScaler 池许可证
- 配置 NetScaler 池容量
- 将 NetScaler VPX 中的永久许可证升级到 NetScaler 池容量
- 将 NetScaler MPX 中的永久许可证升级到 NetScaler 池容量
- 将 NetScaler SDX 中的永久许可证升级到 NetScaler 池容量
- 群集模式下 NetScaler 实例上的 NetScaler 池容量
- NetScaler VPX 签入和签出许可
- NetScaler 虚拟 CPU 许可
- 出现问题时的预期行为

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler 池化容量

重要提示：

基于文件的许可系统（也称为手动管理的授权），传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活所有 Citrix 产品套件的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler Flexed 许可证 (CPL/UHMC)、旧版 NetScaler 池化许可证和 NetScaler 固定期限带宽许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是与 LAS 兼容的版本。

与 LAS 兼容的最低 NetScaler® 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：从 2025 年 9 月初开始支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： LAS 对 Console 本地部署的支持从版本 14.1-51.x 开始。但是，自 April 15 2026 起，Console 本地部署版本 14.1-51.x 及更高版本以及 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署版本 14.1-51.x 或 13.1-60.x 或更高版本，您可以继续使用基于文件的许可，直到 April 15 2026。但是，您必须在 April 15 2026 之前升级到 Console 本地部署版本 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证（例如池化 vCPU、CICO、永久许可证）将不支持 LAS。升级到上述软件版本后，使用没有有效维护的永久许可证的 NetScaler 实例将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。如果不遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外，Citrix 还可能根据法律或衡平法采取任何其他补救措施。在法律或法规禁止的情况下，这些要求不适用。
NetScaler 池化容量允许您在不同的 NetScaler 外形规格之间共享带宽或实例许可证。对于基于虚拟 CPU 订阅的实例，您可以在实例之间共享虚拟 CPU 许可证。将此池化容量用于数据中心或公共云中的实例。当实例不再需要资源时，它会将分配的容量检回公共池。将释放的容量重新用于需要资源的其他 NetScaler 实例。

您可以使用池化许可来最大化带宽利用率，方法是确保为实例分配必要的带宽，且不超过其需求。在运行时增加或减少分配给实例的带宽，而不会影响流量。借助池化容量许可证，您可以自动执行实例预配。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler 池化容量许可的工作原理

NetScaler 池化容量包含以下组件：

- NetScaler 实例，可分为：
  - 零容量硬件
  - 独立 NetScaler VPX 实例或 NetScaler CPX 实例或 NetScaler BLX 实例
- 带宽池
- 实例池
- 配置为许可证服务器的 NetScaler Console

零容量硬件

通过 NetScaler 池化容量进行管理时，MPX 和 SDX 实例被称为“零容量硬件”，因为这些实例必须从带宽池和实例池中检出资源后才能运行。因此，这些平台也称为 MPX-Z 和 SDX-Z 设备。

零容量硬件需要平台许可证，才能从公共池中检出带宽和实例许可证。

注意

- MPX 实例不需要实例许可证订阅。有关 MPX 和 SDX 实例支持的池化容量，请参阅本页中的表 1。有关不同 MPX 和 SDX 外形规格的许可证要求，请参阅表 5。
- 零容量许可证的安装方式与其他 NetScaler 本地许可证相同。有关如何获取和安装零容量许可证的更多信息，请参阅NetScaler 许可指南。

管理和安装平台许可证

您必须手动安装平台许可证，方法是使用硬件序列号或许可证访问代码。安装平台许可证后，它将锁定到硬件，并且无法按需在 NetScaler 硬件实例之间共享。但是，您可以手动将平台许可证移动到另一个 NetScaler 硬件实例。

运行 NetScaler 软件版本 11.1 build 54.14 或更高版本的 NetScaler MPX 实例以及运行 11.1 build 58.13 或更高版本的 NetScaler SDX 实例支持 NetScaler 池化容量。有关详细信息，请参阅 **表 1. 支持 MPX 和 SDX 实例的池化容量**。

独立 NetScaler VPX 实例

在以下虚拟机管理程序上运行 NetScaler 软件版本 11.1 Build 54.14 及更高版本的 NetScaler VPX 实例支持池化容量：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 威睿 ESX 6.0
- 思杰 Hypervisor™
- Linux KVM 虚拟机

在以下虚拟机管理程序和云平台上运行 NetScaler 软件版本 12.0 Build 51.24 及更高版本的 NetScaler VPX 实例支持池化容量：

- 微软 Hyper-V
- AWS
- 微软 Azure
- 谷歌云

在以下虚拟机管理程序和云平台上运行 NetScaler 软件版本 13.0 和 13.1（所有版本）的 NetScaler VPX 实例支持池化容量：

- 威睿 ESX 6.0
- 思杰 Hypervisor
- Linux KVM 虚拟机
- 微软 Hyper-V
- AWS
- 微软 Azure
- 谷歌云

注意

为了在 NetScaler Console 与 Microsoft Azure 或 AWS 之间启用通信，必须配置 IPSEC 隧道。有关详细信息，请参阅 将部署在云中的 NetScaler VPX 实例添加到 NetScaler Console。与零容量硬件不同，NetScaler VPX 不需要平台许可证。为了处理流量，它必须从池中检出带宽和实例许可证。

独立 NetScaler CPX 实例

部署在 Docker 主机上的 NetScaler CPX 实例支持池容量。与零容量硬件不同，NetScaler CPX 不需要平台许可证。单个 NetScaler CPX 实例消耗高达 1 Gbps 的吞吐量时，仅从许可证池中检出 1 个实例，不检出带宽。例如，假设您有 20 个 NetScaler CPX 实例，带宽池为 20 Gbps。如果其中

© 1997–2026 Citrix Systems, Inc. All rights reserved.

一个 NetScaler CPX 实例消耗 500 Mbps 吞吐量，则带宽池对于剩余的 19 个 NetScaler CPX 实例仍为 20 Gbps。

如果同一个 NetScaler CPX 实例开始消耗 1500 Mbps 吞吐量，则带宽池对于剩余的 19 个 NetScaler CPX 实例为 19.5 Gbps。

对于池许可，您只能以 10 Mbps 的倍数添加更多带宽。

独立 NetScaler BLX 实例

NetScaler BLX 实例支持池容量许可证。NetScaler BLX 实例不需要平台许可证。为了处理流量，NetScaler BLX 实例必须从池中检出带宽和实例许可证。

带宽池

带宽池是 NetScaler 实例（包括物理和虚拟实例）可以共享的总带宽。带宽池包含每个软件版本（Standard、Advanced 和 Premium）的独立池。给定的 NetScaler 实例不能同时从不同的池中检出带宽。它可以从中检出带宽的带宽池取决于其获得许可的软件版本。

实例池

实例池定义了可以通过 NetScaler 聚合容量管理的 NetScaler VPX 实例、NetScaler CPX 实例或 NetScaler BLX 实例的数量，或者 SDX-Z 实例中 NetScaler VPX 实例的数量。

从池中检出许可证后，该许可证将解锁 MPX-Z、SDX-Z、VPX、NetScaler CPX 和 NetScaler BLX 实例的资源，包括 CPU/PE、SSL 核心、每秒数据包数和带宽。

注意

SDX-Z 的管理服务不占用实例。

NetScaler Console 许可证服务器

NetScaler 聚合容量使用配置为许可证服务器的 NetScaler Console 来管理聚合容量许可证：带宽池许可证和实例池许可证。您可以使用 NetScaler Console 软件管理聚合容量许可证，而无需 NetScaler Console 许可证。

从带宽池和实例池中检出许可证时，零容量硬件上的 NetScaler 外形规格和硬件型号决定了

- NetScaler 实例在正常运行之前必须检出的最小带宽和实例数量。
- NetScaler 可以检出的最大带宽和实例数量。
- 每次带宽检出的最小带宽单位。最小带宽单位是 NetScaler 必须从池中检出的最小带宽单位。任何检出都必须是最小带宽单位的整数倍。例如，如果 NetScaler 的最小带宽单位为 1 Gbps，则

© 1997–2026 Citrix Systems, Inc. All rights reserved.

可以检出 1000 Mbps，但不能检出 200 Mbps 或 150.5 Gbps。最小带宽单位与最小带宽要求不同。NetScaler 实例只有在获得至少最小带宽的许可后才能运行。一旦满足最小带宽，实例就可以以最小带宽单位检出更多带宽。

表 1、2、3 和 4 总结了所有受支持的 NetScaler 实例的最大带宽/实例数、最小带宽/实例数和最小带宽单位。表 5 总结了所有受支持的 NetScaler 实例不同外形规格的许可证要求：

表 1. MPX 和 SDX 实例支持的聚合容量

产品线	最大带宽 (GBPS)	最小带宽 (GBPS)	最小实例数	最大实例数	最小带宽单位
MPX 5900Z	10	1	N/A	N/A	1 千兆位每秒
MPX 8900Z	30	5	NA	NA	1 千兆位每秒
MPX 9100Z	30	10	NA	NA	1 吉比特/秒
MPX 8900Z FIPS	33	5	NA	NA	1 吉比特/秒
MPX 14000Z 系列	100	20	不适用	不适用	1 吉比特每秒
MPX 14000Z 40G 系列	100	20	不适用	不适用	1 吉比特每秒
MPX 14000Z FIPS 系列	100	20	不适用	不适用	1 吉比特每秒
MPX 14000Z 40S 系列	100	20	N/A	N/A	1 千兆位/秒
MPX 15000Z 系列	120	20	N/A	N/A	1 千兆位/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

产品线	最大带宽 (GBPS)	最小带宽 (GBPS)	最小实例数	最大实例数	最小带宽单位
MPX 15000Z FIPS 系列	120	20	N/A	N/A	1 吉比特每秒
MPX 15000Z 50G 系列	120	20	N/A	N/A	1 吉比特每秒
MPX 16000Z 系列	200	30	N/A	N/A	1 吉比特每秒
MPX 22000Z 系列	120	40	N/A	N/A	1 吉比特每秒
MPX 24000Z 系列	150	100	N/A	N/A	1 吉比特每秒
MPX 25000Z 40G	200	100	N/A	N/A	1 吉比特/秒
MPX 25000ZA	200	100	N/A	N/A	1 吉比特/秒
MPX 26000Z 系列	200	100	N/A	N/A	1 吉比特/秒
MPX 26000Z 100G 系列	200	100	N/A	N/A	一 Gbps
MPX 26000Z 50S 系列	200	100	N/A	N/A	一 Gbps
SDX 8900Z	30	10	1	7	1 千兆位/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

产品线	最大带宽 (GBPS)	最小带宽 (GBPS)	最小实例数	最大实例数	最小带宽单位
SDX 9100Z	95	20	1	7	1 千兆位/秒
SDX 14000Z 系列	100	10	1	25	1 千兆位/秒
SDX 14000Z 40G 系列	100	1	2	25	1 千兆位/秒
SDX 14000Z 40S 系列	100	20	1	25	1 千兆位/秒
SDX 14000Z FIPS 系列	100	10	1	25	1 吉比特每秒
SDX 15000Z 50G	120	10	1	55	1 吉比特每秒
SDX 15000Z	120	10	1	55	1 吉比特每秒
SDX 16000Z 系列	200	15	1	55	1 千兆位/秒
SDX 22000Z 系列	120	20	1	80	1 千兆位/秒
SDX 25000Z 40G	200	50	1	115	1 吉比特每秒
SDX 25000ZA	200	50	1	115	1 吉比特每秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

产品线	最大带宽 (GBPS)	最小带宽 (GBPS)	最小实例数	最大实例数	最小带宽单位
SDX 26000Z 100G	200	50	1	115	1 吉比特每秒
SDX 26000Z	200	50	1	115	1 千兆位/秒
SDX 26000Z 50S	200	50	1	115	1 千兆位/秒
SDX 24000Z 系列	150	50	1	80	1 吉比特每秒

注意

> 最小带宽和实例适用于运行以下版本及更高版本的 SDX 实例：11.1 64.x、12.0 63.x、12.1 54.x 和 13.0 41.x。

最小购买数量与最低系统要求不同。

表 2. NetScaler CPX 实例支持的池容量

产品线	最大带宽 (GBPS)	最小带宽 (MBPS)	最小实例数	最大实例数	最小带宽单位
CPX	10	10	1	1	10 兆比特/秒

表 3. 虚拟机管理程序和云服务上 NetScaler VPX 实例支持的池化容量

虚拟机管理程序/云服务	最大带宽 (GBPS)	最小带宽 (MBPS)	最小实例数	最大实例数	最小带宽单位
思杰虚拟机监控程序	40 吉比特/秒	10 兆比特/秒	1	1	10 兆位/秒
威睿 ESXI	100 吉比特每秒	10 兆位/秒	1	1	10 兆位/秒

© 1997–2026 Citrix Systems, Inc. All rights reserved.

虚拟机管理程序/云服务	最大带宽 (GBPS)	最小带宽 (MBPS)	最小实例数	最大实例数	最小带宽单位
Linux KVM 平台	100 吉比特每秒	10 兆比特每秒	1	1	10 兆比特每秒
微软 Hyper-V	3 千兆位/秒	10 兆位/秒	1	1	10 兆位/秒
AWS	30 吉比特/秒	10 兆比特/秒	1	1	10 兆比特/秒
Azure 云	10 千兆位/秒	10 兆位/秒	1	1	10 兆比特每秒
谷歌云	10 吉比特每秒	10 兆比特每秒	1	1	10 兆比特每秒

注意

最低购买数量与最低系统要求不同。

表 4. NetScaler BLX 实例支持的池化容量

产品线	最大带宽 (GBPS)	最小带宽 (MBPS)	最小实例数	最大实例数	最小带宽单位
BLX	100	10	1	1	10 兆比特每秒

表 5. 不同外形规格的许可证要求

产品线	零容量硬件采购	带宽和版本订阅	实例订阅
MPX	所需许可证	需要许可证	-
SDX	需要许可证	需要许可证	需要许可证
VPX	-	需要许可证	需要许可证
CPX	-	-	需要许可证

© 1997–2026 Citrix Systems, Inc. All rights reserved.

产品线	零容量硬件采购	带宽和版本订阅	实例订阅
BLX	-	需要许可证	需要许可证

配置 NetScaler 池化容量

重要提示：

基于文件的许可系统（也称为手动管理的授权），传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于 Citrix 产品套件产品激活的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler 弹性许可证 (CPL/UHMC)、旧版 NetScaler 池化许可证和 NetScaler 固定期限带宽许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是 LAS 兼容版本。

LAS 兼容的最低 NetScaler® 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console 服务：自 2025 年 9 月初起支持。
- NetScaler Console 本地部署：14.1-51.x

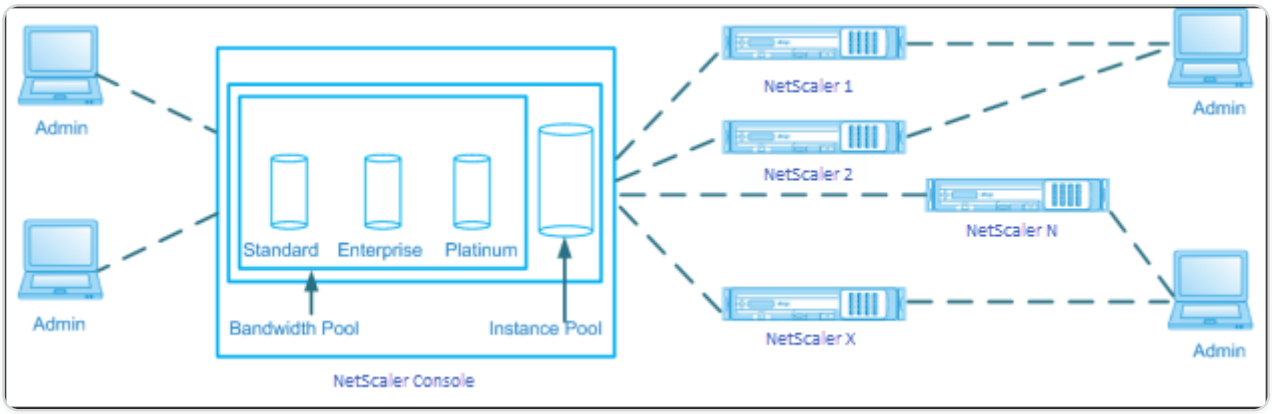
  注意： Console 本地部署的 LAS 支持从 14.1-51.x 版本开始。但是，自 April 15 2026 起，Console 本地部署 14.1-51.x 及更高版本和 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署 14.1-51.x 或 13.1-60.x 或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如池化 vCPU、CICO、永久许可证，将不支持 LAS。使用没有有效维护的永久许可证的 NetScaler 实例在升级到上述软件版本后将变为未授权状态。
在法律或法规禁止的情况下，客户可能无法获得基于 LAS 的许可证。
如果您有疑问或疑虑，请联系客户服务。Citrix 可能会在不承担责任的情况下限制或暂停您的 Citrix 维护，以应对不符合这些要求的情况，此外，Citrix 还可能根据法律或衡平法采取任何其他补救措施。这些要求在法律或法规禁止的情况下不适用。
要使用 NetScaler 池化容量，请将 NetScaler Console 配置为所需 NetScaler 实例的许可证服务器。NetScaler 实例从 NetScaler Console 签入和签出许可证。您可以在 NetScaler Console GUI 中执行以下任务：

- 将池化容量许可证文件（带宽和实例池）上传到许可证服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 按需从许可证池中为 NetScaler 实例分配许可证。
- 根据实例的最小和最大容量，从 NetScaler 实例 (MPX-Z /SDX-Z/VPX/CPX/BLX) 中检出许可证。
- 为 NetScaler FIPS 实例配置池容量，以检入或检出许可证。



支持的硬件和软件版本

有关池容量支持的硬件和软件版本，请参阅 NetScaler 池容量。

NetScaler 池容量状态

池容量状态指示 NetScaler 实例上的许可证要求。配置了池容量的 NetScaler 实例会显示以下状态之一：

- **最佳**：实例以适当的许可证容量运行。
- **容量不匹配**：实例以低于用户配置的容量运行。
- **宽限期**：实例正在使用宽限期许可证运行。
- **宽限期和不匹配**：实例正在使用宽限期许可证运行，但容量低于用户配置。
- **不可用**：实例未在 NetScaler Console 中注册进行管理，或者 NetScaler Console 到实例的 NITRO 通信不工作。
- **未分配**：许可证未在实例中分配。

步骤 1 - 在 NetScaler Console 中应用许可证

1. 在 NetScaler 控制台 中，导航到 **NetScaler 许可 > 池化许可**。
2. 在“**许可证文件**”部分中，选择“**添加许可证文件**”，然后选择以下选项之一：
   - “**从本地计算机上传许可证文件**”。如果许可证文件已存在于本地计算机上，则可以将其上传到 NetScaler Console。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- “**使用许可证访问代码**”。指定您从 Citrix 购买的许可证的许可证访问代码。然后，选择“**获取许可证**”。然后选择“**完成**”。

“

注意

随时可以通过“**许可证设置**”向 NetScaler Console 添加更多许可证。

3. 单击“**完成**”。

   许可证文件已添加到 NetScaler Console。“**许可证到期信息**”选项卡列出了 NetScaler Console 中存在的许可证以及距离到期的剩余天数。

4. 在“**许可证文件**”中，选择要应用的许可证文件，然后单击“**应用许可证**”。

   此操作使 NetScaler 实例能够将所选许可证用作池容量。

步骤 2 - 将 NetScaler Console 注册为许可证服务器

要将 NetScaler Console 注册为 NetScaler 实例的许可证服务器，请按照以下过程之一操作：

- 使用 GUI
- 使用 CLI

使用 GUI 将 NetScaler Console 注册为许可证服务器

在 NetScaler GUI 中，将 NetScaler Console 服务器注册为许可证服务器。

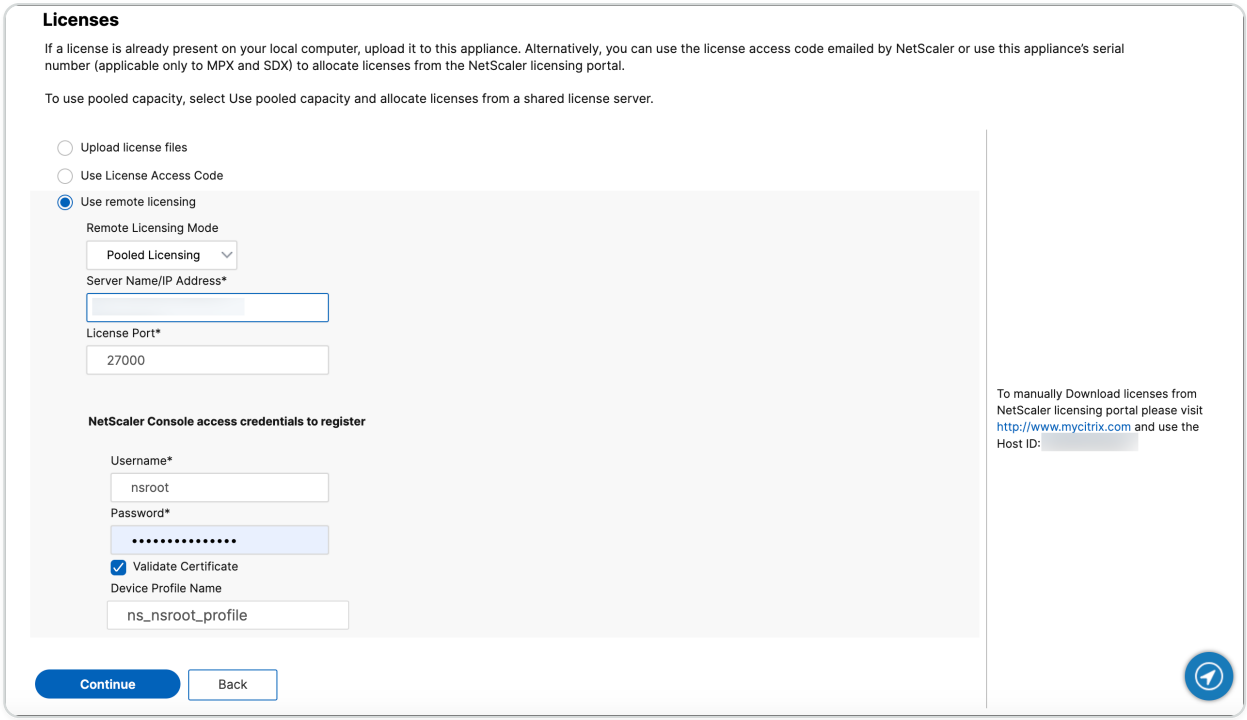
1. 登录到 NetScaler GUI。
2. 导航到 **系统** > **许可证** > **管理许可证**。
3. 单击 **添加新许可证**。
4. 选择 **Use remote licensing**，然后在 **Remote Licensing Mode** 下，从列表中选择 **Pooled Licensing**。
5. 在 **Server Name/IP address** 字段中，指定 NetScaler Console 服务器的 IP 地址。

   对于 HA 部署，请使用浮动 IP。有关配置的更多信息，请参阅 Configure High Availability Deployment。

   对于使用独立 NetScaler Console 或代理的部署，请参阅 Licensing overview

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. 默认许可证端口是 27000。
7. 输入您的 NetScaler Console 服务器凭据以向 NetScaler Console 注册实例，然后单击 **Continue**。在 NetScaler Console 中，其中一台服务器是许可证服务器。



注意：

- 仅当 NetScaler Console 具有由证书颁发机构 (CA) 颁发的有效数字证书时（在 **Settings > Administration > SSL Settings** 下），才选中 **Validate Certificate** 复选框。
- 如果 NetScaler 只能通过 NAT IP 访问，则设备注册可能会失败。您仍然可以签出许可证，但 NetScaler Console 会将这些 NetScaler 实例显示为非托管实例。

8. 在 **Device Profile Name** 下，指定 NetScaler Console 可用于访问实例的实例配置文件。此实例配置文件包含您要添加到 NetScaler Console 的实例的用户名和密码。默认配置文件是 **ns_nsroot_profile**。如果您已更改实例的默认管理员凭据，则可以定义自定义实例配置文件名称。
9. 在 **Allocate licenses** 中，选择许可证版本并指定所需的带宽。

   首次在 NetScaler 中分配许可证。之后，您可以从 NetScaler Console GUI 更改或释放许可证分配。

   a. 单击 **获取许可证**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要提示：

如果更改许可证版本，请热重启实例。配置更改在您重启实例后才会生效。

使用 CLI 将 NetScaler Console 添加为许可证服务器

如果 NetScaler 实例没有 GUI，请使用以下 CLI 命令将 NetScaler Console 服务器添加为许可证服务器：

1. 登录到 NetScaler 控制台。
2. 添加 NetScaler Console 服务器 IP 地址：

   ```
   > add ns licenseserver <adm-server-IP-address> -port <adm-server-port-number> -licensemode <license-mode>
   ```

   有关详细信息，请参阅许可概述。

3. 查看许可证服务器中可用的许可证带宽。

   ```
   > sh ns licenseserverpool
   ```

   此命令根据添加许可证服务器时指定的许可证模式列出许可证。

   示例 1：

   如果指定的许可证模式为 `CICO`，则输出仅包含 CICO 许可证。

   ```
   > add licenseserver [redacted] -licensemode CICO
   Done
   > sh licenseserverpool
         VPX8000P Total                    : 1
         VPX8000P Available                : 1
   ```

   示例 2：

   如果指定的许可证模式是 `Pooled`，则输出仅包含池化容量许可证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> add licenseserver [redacted] -licensemode Pooled
 Done
> sh licenseserverpool
        Instance Total                      : 40
        Instance Available                  : 38
        Standard Bandwidth Total            : 210.00 Gbps
        Standard Bandwidth Available        : 210.00 Gbps
        Enterprise Bandwidth Total          : 50.00 Gbps
        Enterprise Bandwidth Available      : 50.00 Gbps
        Platinum Bandwidth Total            : 210.00 Gbps
        Platinum Bandwidth Available        : 205.00 Gbps
```

示例-3：

如果指定的许可证模式是 `vCPU`，则输出仅包含虚拟 CPU 许可证。

```
> add licenseserver [redacted] -licensemode vCPU
 Done
> sh licenseserverpool
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

要一起查看所有许可证，请运行以下命令：

```
> sh ns licenseserverpool -getallLicenses
```

示例输出：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
> sh licenseserverpool -getallLicenses
        Instance Total                      : 40
        Instance Available                  : 33
        Standard Bandwidth Total            : 210.00 Gbps
        Standard Bandwidth Available        : 210.00 Gbps
        Enterprise Bandwidth Total          : 50.00 Gbps
        Enterprise Bandwidth Available      : 50.00 Gbps
        Platinum Bandwidth Total            : 210.00 Gbps
        Platinum Bandwidth Available        : 205.00 Gbps
        VPX8000P Total                      : 1
        VPX8000P Available                  : 1
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

4. 从所需的许可证版本中分配许可证带宽：

```
> set ns capacity -unit <specify-mbps-or-gbps> -bandwidth <specify-amount-license-bandwidth> -edition <specify-license-edition>
```

许可证版本可以是 **Standard**、**Enterprise** 或 **Platinum**。

重要

如果更改许可证版本，请热重启实例。

`reboot -w`

配置更改在您重启实例后才会生效。

步骤 3 - 将池化许可证分配给 NetScaler 实例

要从 NetScaler Console GUI 分配池化容量许可证：

1. 登录到 NetScaler Console。
2. 导航到 **基础架构 > 许可证 > 带宽许可证 > 池化容量**。

   FIPS 实例容量仅在您将 FIPS 实例许可证上传到 NetScaler Console 后才会显示。

3. 单击要管理的许可证池。

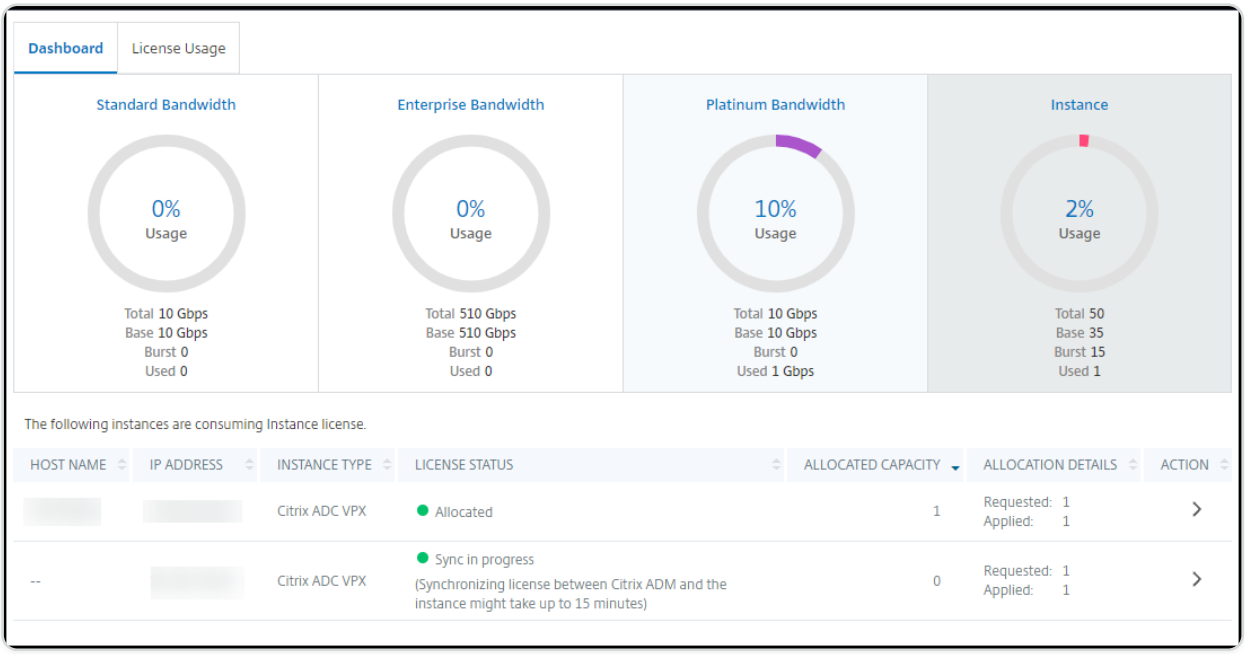
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

已分配容量 字段不会立即反映更改的带宽。带宽更改在 NetScaler 热重启后生效。

在 **分配详细信息** 中，当您更改实例的带宽分配时，**请求** 和 **已应用** 字段会更新。

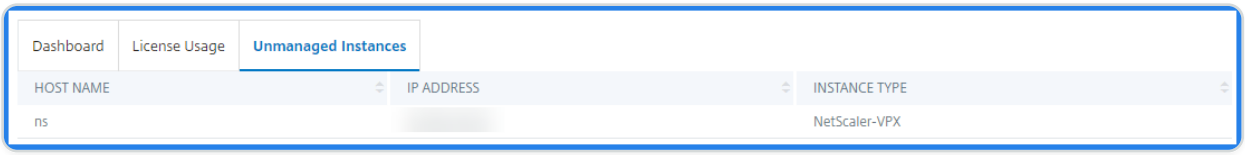
4. 通过单击 **>** 按钮，从可用实例列表中选择一个 NetScaler 实例。



许可证状态 列显示相应的许可证分配状态消息。

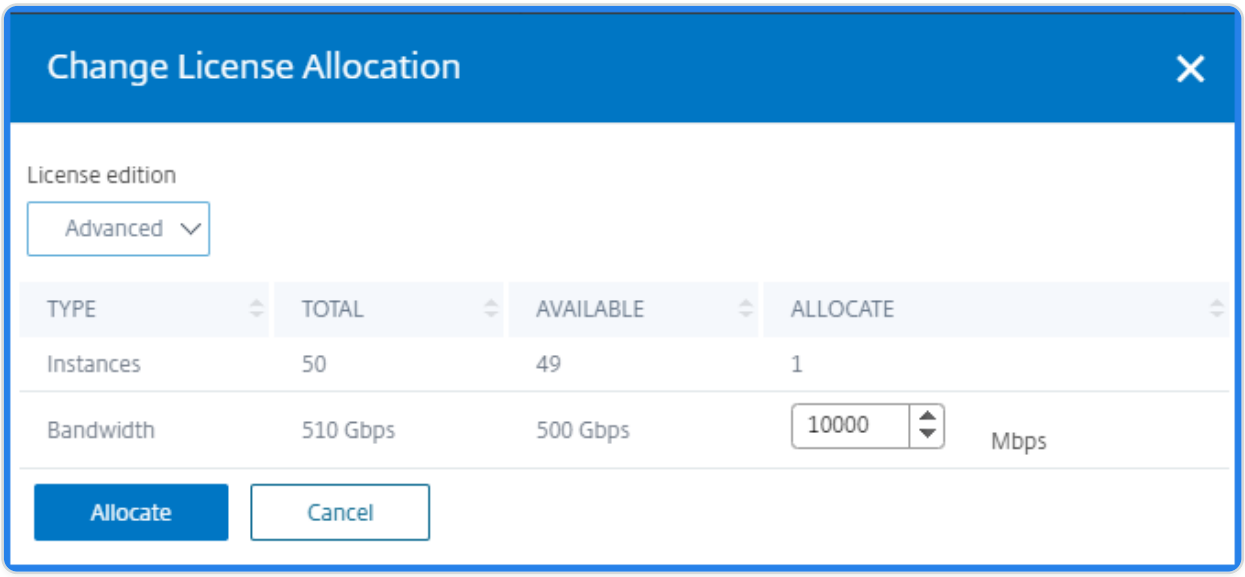
注意：

未管理实例 选项卡显示在 NetScaler Console 中发现但未管理的实例。



5. 单击 **更改分配** 或 **释放分配** 以修改许可证分配。
6. 许可证服务器中显示一个包含可用许可证的弹出窗口。
7. 您可以通过设置“**分配**”列表选项来选择分配给实例的带宽或实例。做出选择后，单击“**分配**”。
8. 您还可以从“**更改许可证分配窗口**”中的列表选项更改已分配的许可证版本。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意

如果更改许可证版本，请热重启实例。

有关如何更改带宽分配的更多信息，请参阅相关视频：

<iframe src="https://www.youtube.com/embed/AMaHr-ska8s" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

在 NetScaler 实例上配置池容量

您可以在以下 NetScaler 实例上配置池容量许可证：

- NetScaler 实例
- NetScaler VPX™ 实例
- NetScaler 高可用性对

NetScaler MPX™ 实例

MPX-Z 是启用池容量的 NetScaler MPX 设备。MPX-Z 支持高级版、增强版或标准版许可证的带宽池。

MPX-Z 在连接到许可证服务器之前需要平台许可证。您可以通过以下任一方式安装 MPX-Z 平台许可证：

- 从本地计算机上传许可证文件。
- 使用实例的硬件序列号。
- 实例 GUI 的“**系统**”>“**许可证**”部分中的许可证访问代码。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

如果您删除 MPX-Z 平台许可证，则池容量功能将被禁用。实例许可证将释放到许可证服务器。

您可以动态修改 MPX-Z 实例的带宽，而无需重新启动。仅当您要更改许可证版本时才需要重新启动。

注意：

重新启动实例时，它会自动签出其配置容量所需的池许可证。

NetScaler VPX 实例

启用了池容量的 NetScaler VPX 实例可以从带宽池（高级版/高级版/标准版）中签出许可证。您可以使用 NetScaler GUI 从许可证服务器签出许可证。

您可以动态修改 VPX 实例的带宽，而无需重新启动。仅当您要更改许可证版本时才需要重新启动。

注意：

重新启动实例时，配置的池容量许可证会自动从 NetScaler Console 服务器签出。

NetScaler 高可用性对

在开始之前，请确保 NetScaler Console 服务器已配置为许可证服务器。有关更多信息，请参阅将 NetScaler Console 配置为许可证服务器。

对于配置为高可用性模式的 NetScaler 实例，您必须在高可用性对的每个节点上配置池化容量。对于主节点和辅助节点，您需要分配相同容量的许可证。例如，如果您希望 HA 对中的每个实例具有 1 Gbps 容量，则需要从公共池中获取两倍的容量（2 Gbps）。然后，您可以为每个节点分配 1 Gbps 容量。

要为对中的每个节点分配池许可证，请遵循 将池化许可证分配给 NetScaler 实例 中给出的步骤。首先为第一个节点分配许可证，然后重复相同的步骤为第二个节点分配许可证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

将 NetScaler VPX 中的永久许可证升级到 NetScaler 池容量

重要提示：

基于文件的许可系统（也称为手动管理的权利），传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活 Citrix 产品套件中产品的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler 弹性许可证 (CPL/UHMC)、旧版 NetScaler 池许可证和 NetScaler 固定期限带宽许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是 LAS 兼容版本。

兼容 LAS 的最低 NetScaler 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：自 2025 年 9 月初起支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： Console 本地部署的 LAS 支持从 14.1-51.x 版本开始。但是，自 April 15 2026 起，Console 本地部署 14.1-51.x 及更高版本和 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署 14.1-51.x 版本或 13.1-60.x 版本或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须升级到 Console 本地部署 14.1-51.x 或更高版本，并在 15th April 2026 之前切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如池化 vCPU、CICO、永久许可证，将不支持 LAS。升级到上述软件版本后，使用没有有效维护的永久许可证的 NetScaler 实例将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。如果未能遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法规定的任何其他补救措施。在法律或法规禁止的情况下，这些要求不适用。
具有永久许可证的 NetScaler VPX 实例可以升级到 NetScaler 池容量许可证。升级到池容量许可证后，您可以按需将许可证从许可证池分配给 VPX 实例。您还可以为在高可用性模式下配置的 NetScaler 实例配置池容量许可证。要为高可用性模式下的 VPX 实例配置池容量许可证，请参阅 将 NetScaler VPX 高可用性对中的永久许可证升级到 NetScaler 池容量。

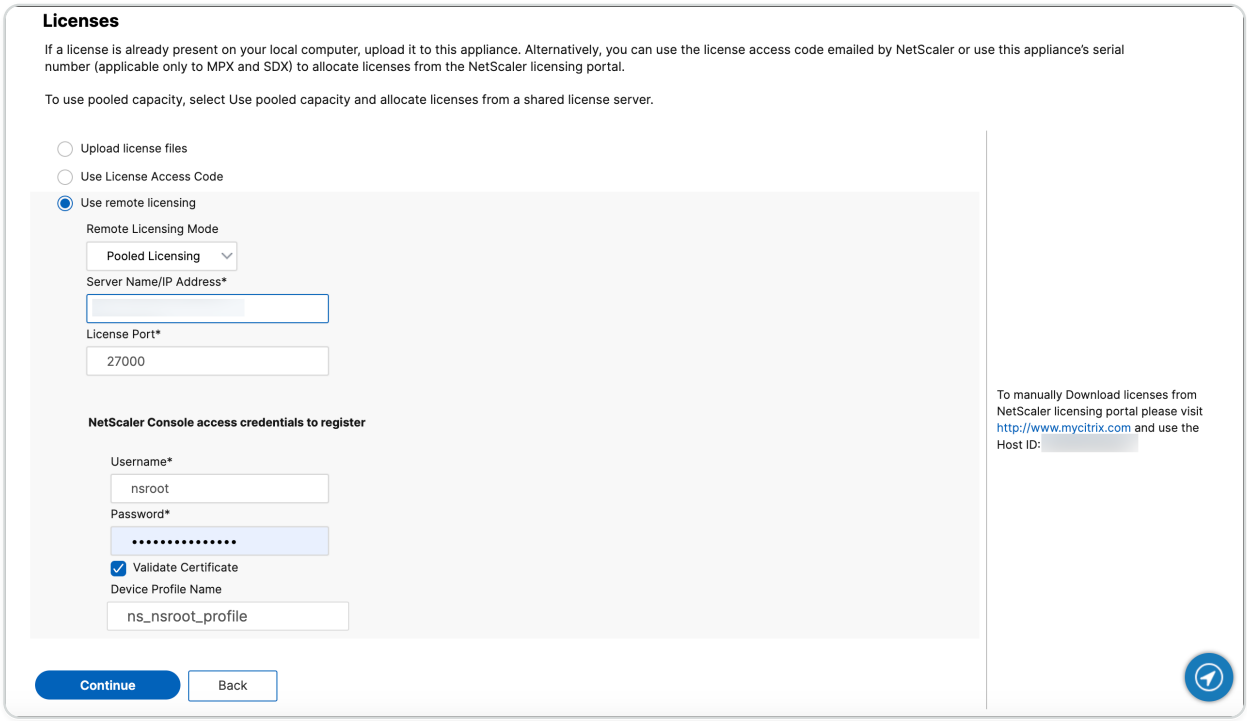
先决条件

要升级到 NetScaler 池容量：

1. 在 Web 浏览器中，键入 VPX 实例的 IP 地址，例如 `<http://192.168.100.1>`。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 在“**用户名**”和“**密码**”中，键入管理员凭据。
3. 在“**欢迎**”页面上，单击“**继续**”。
4. 在“**配置**”选项卡上，导航到“**系统 > 许可证**”，然后单击“**管理许可证**”。
5. 在“**许可证**”页面上，单击“**添加新许可证**”。
6. 在“**许可证**”页面上，选择“**使用远程许可**”并执行以下操作：

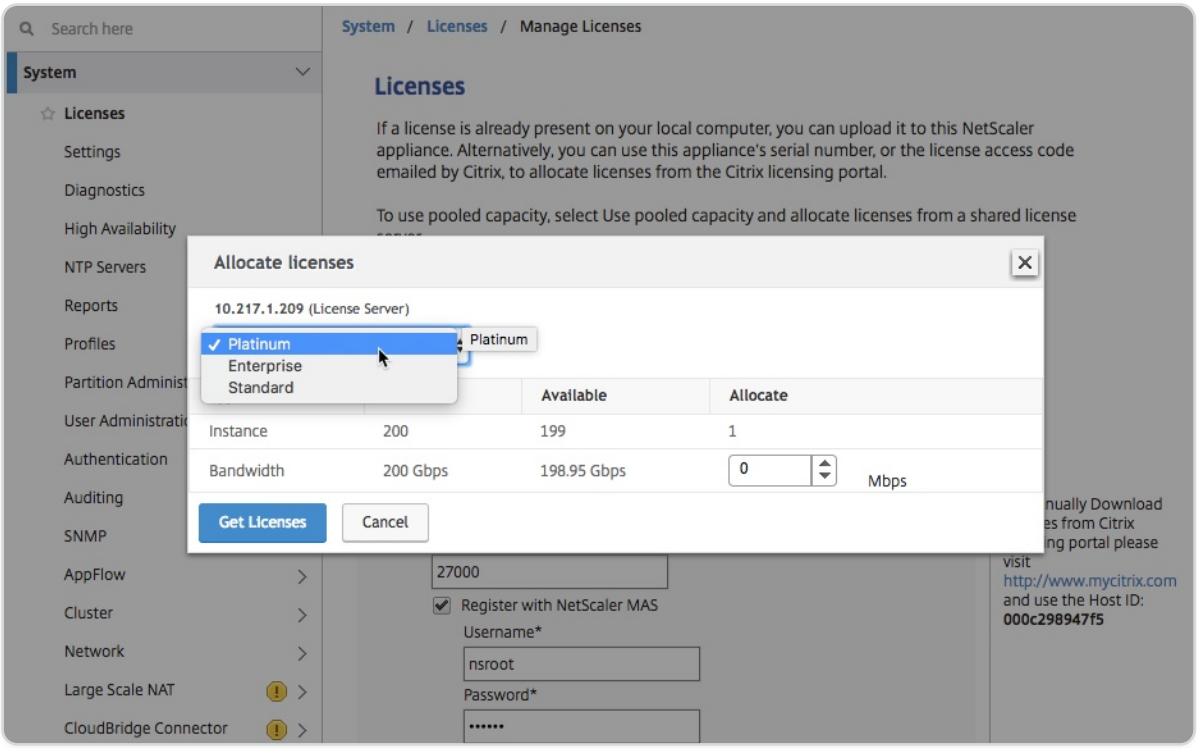


   a. 在“**远程许可模式**”下拉列表中，选择“**池化许可**”。
   b. 在“**服务器名称/IP 地址**”字段中，输入许可证服务器的详细信息。
   c. 单击“**继续**”。

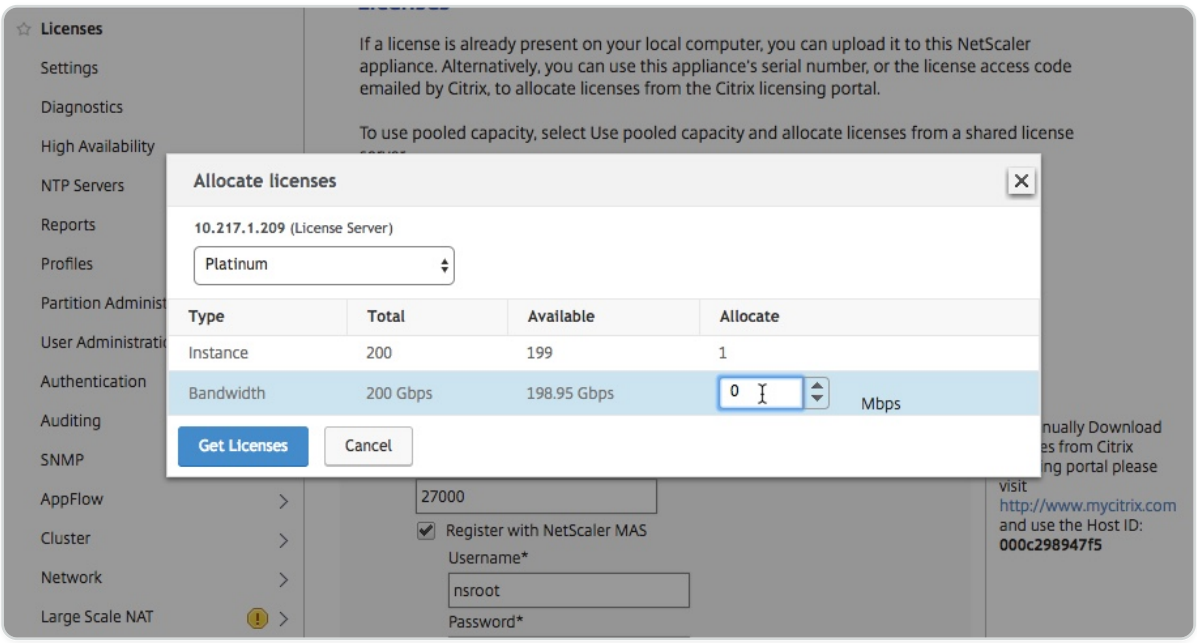
7. 在“**分配许可证**”中，执行以下操作：

   a. 从下拉列表中选择许可证版本。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

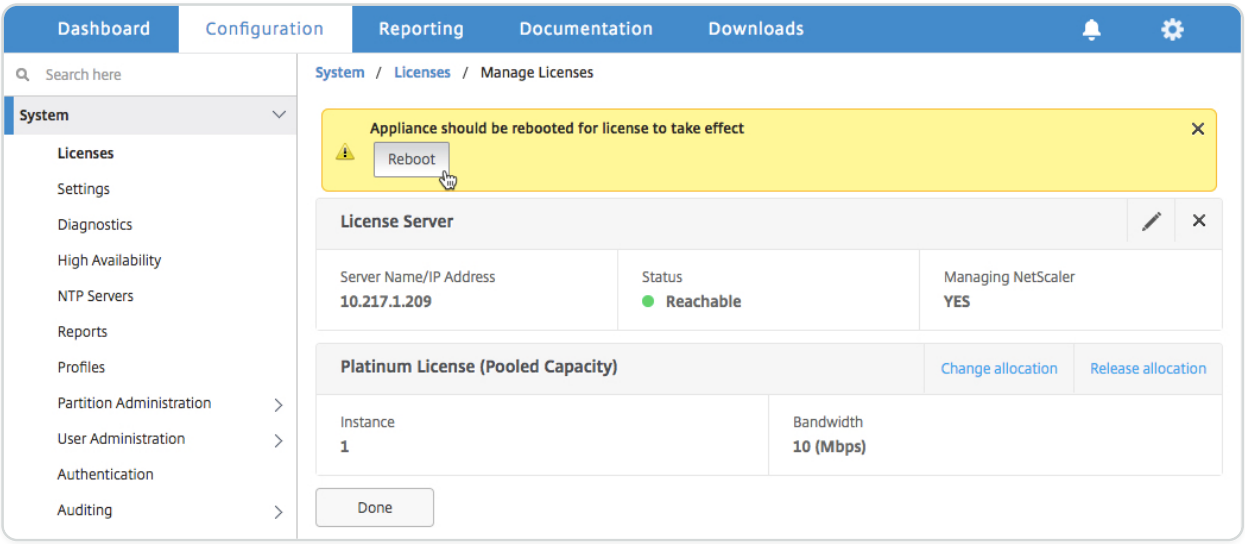


b. 从“**分配**”菜单中将带宽分配给 NetScaler 设备，然后单击“**获取许可证**”。



8. 出现提示时，单击“**重新启动**”以重新启动设备。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. 在“确认”对话框中，单击“**是**”。
10. VPX 实例重新启动后，登录到该实例。在“**欢迎**”页面上，单击“**继续**”。

    “**许可证**”页面显示 NetScaler VPX 设备上获得许可的所有功能。单击“**X**”。
11. 导航到“**系统 > 许可证**”，然后单击“**管理许可证**”。

    在“**管理许可证**”页面上，您可以查看许可证服务器、许可证版本和分配的带宽的详细信息。

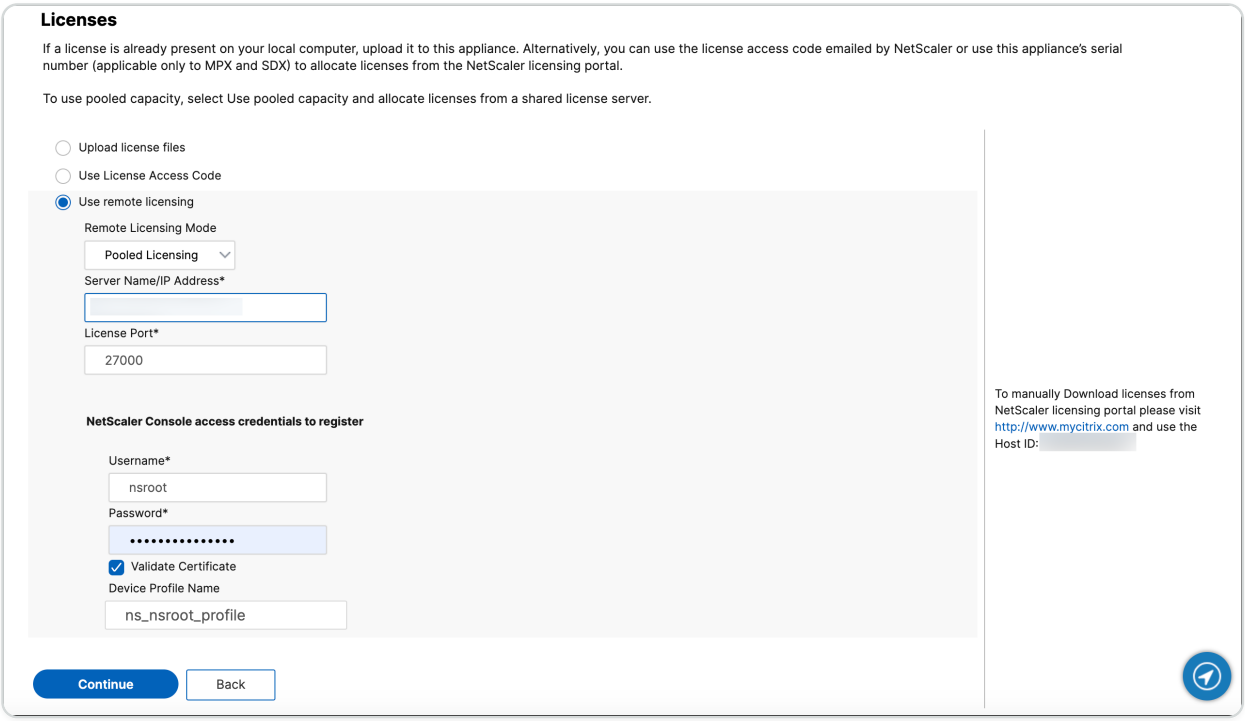
将 NetScaler VPX 高可用性对中的永久许可证升级到 NetScaler 池容量

对于配置为高可用性模式的 VPX 实例，您必须在 HA 对中的主实例和辅助实例上配置池容量。对于主实例和辅助实例，您需要分配相同容量的许可证。例如，如果您希望 HA 对中的每个实例具有 1 Gbps 容量，您需要从公共池中获取两倍的容量（2 Gbps）。然后，您可以为 HA 对中的主实例和辅助实例各分配 1 Gbps 容量。

要将现有 NetScaler VPX HA 设置升级到 NetScaler 池容量：

1. 登录到辅助 VPX（节点 2）实例。在 Web 浏览器中，键入 NetScaler 设备的 IP 地址，例如 `http://192.168.100.1`。
2. 在“**用户名**”和“**密码**”中，键入管理员凭据。
3. 在“**欢迎**”页面上，单击“**继续**”。
4. 在“配置”选项卡上，导航到“**系统 > 许可证**”，然后单击“**管理许可证**”。
5. 在“**许可证**”页面上，单击“**添加新许可证**”。
6. 选择 **使用远程许可** 并执行以下操作：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. 在 **远程许可模式** 下拉列表中，选择 **池化许可**。

b. 在 **服务器名称/IP 地址** 字段中，输入许可证服务器的详细信息。

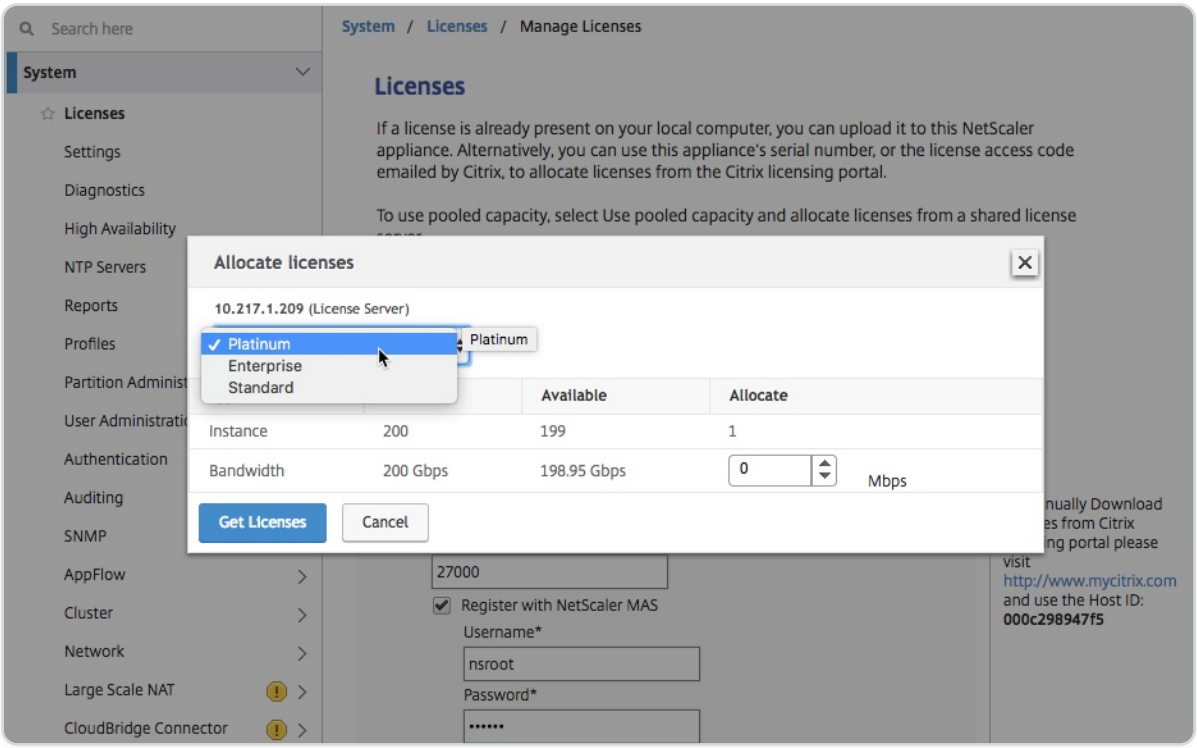
c. 确保 **注册到 NetScaler Console** 复选框已选中，并输入 NetScaler Console 凭据，如果您希望通过 NetScaler Console 管理实例的池许可证。

d. 单击 **继续**。

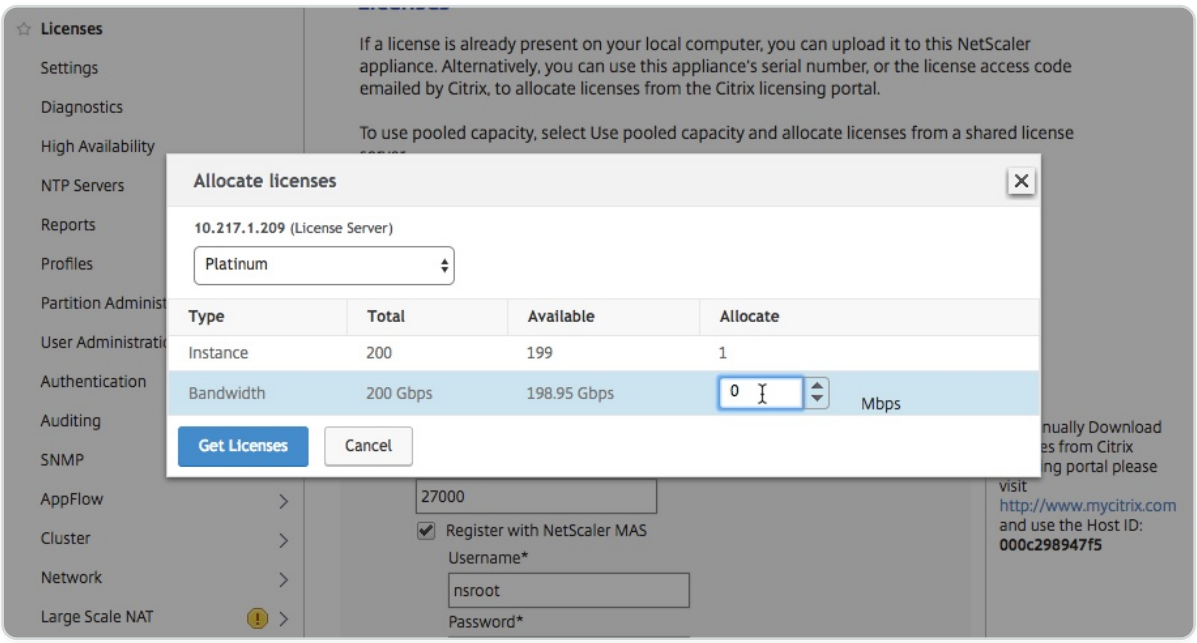
7. 在 **分配许可证** 中，执行以下操作：

   a. 从下拉列表中选择许可证版本。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

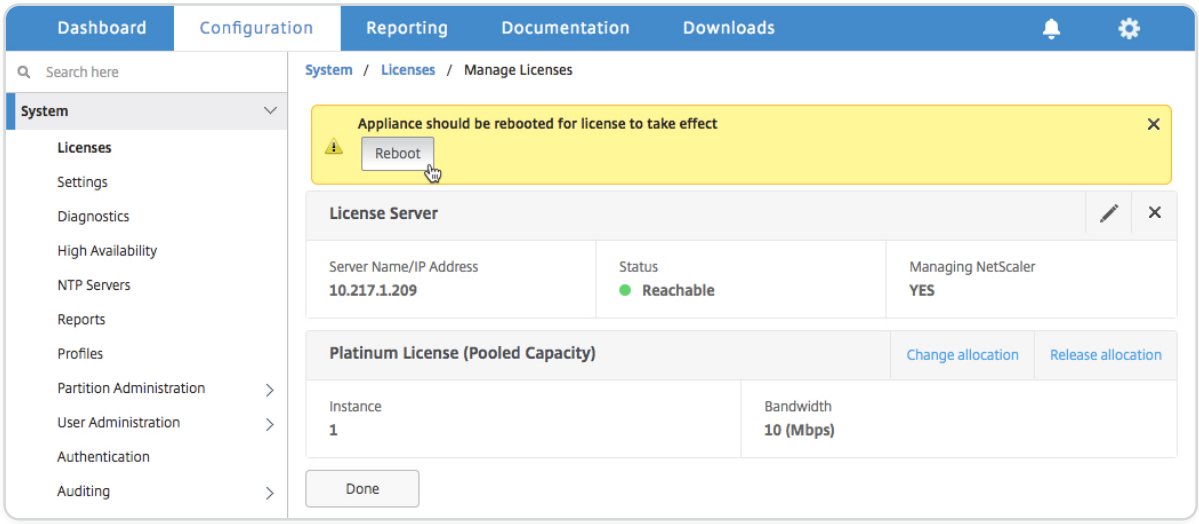


b. 从 **分配** 菜单中将带宽分配给 NetScaler 设备，然后单击 **获取许可证**。



c. 出现提示时，单击 **重新启动** 以热重启实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. 在 **确认** 对话框中，单击 **是**。

   VPX 实例重新启动。

   出现提示时，单击“**重新启动**”以重新启动设备。设备使用新许可证启动并运行后，通过键入 `force ha failover` 强制执行故障转移。此故障转移可确保 HA 对处于良好状态。

9. 故障转移后，登录到新的辅助 VPX 实例（节点 1），并重复相同的过程将新的辅助实例添加到池中。

   如果要将 HA 对中的主实例和辅助实例更改回原始 HA 对配置，请强制执行故障转移。在 HA 对中的任何实例上运行以下命令：

   ```
   > force ha failover
   ```

10. 要验证 VPX 实例是否已升级到池容量许可证，请登录主实例和辅助实例并完成以下步骤。

    a. 在“**欢迎**”页面上，单击“**继续**”。

    b. 在“配置”选项卡上，导航到“**系统 > 许可证**”，然后单击“**管理许可证**”。在“**管理许可证**”页面上，您可以查看许可证服务器、许可证版本和已分配带宽的详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

将 NetScaler MPX 中的永久许可证升级到 NetScaler Pooled Capacity

重要提示：

基于文件的许可系统（也称为手动管理的权利），传统上用于激活各种本地组件，将于 April 15, 2026 终止服务 (EOL)。许可证激活服务 (LAS) 是用于激活 Citrix 产品套件中产品的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler Flexed 许可证 (CPL/UHMC)、旧版 NetScaler Pooled 许可证和 NetScaler Fixed term Bandwidth 许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是 LAS 兼容版本。

兼容 LAS 的最低 NetScaler 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：自 2025 年 9 月初起支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： Console 本地部署的 LAS 支持从版本 14.1-51.x 及更高版本开始。但是，自 April 15 2026 起，Console 本地部署版本 14.1-51.x 及更高版本和 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署版本 14.1-51.x 或版本 13.1-60.x 或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署版本 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如 Pooled vCPU、CICO、永久许可证，将不支持 LAS。升级到上述软件版本后，使用没有有效维护的永久许可证的 NetScaler 实例将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。如果违反这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法规定的任何其他补救措施。在法律或法规禁止的情况下，这些要求不适用。
在继续操作之前，请阅读以下注意事项。

具有永久许可证的 NetScaler MPX 可以升级到 NetScaler Pooled Capacity 许可证。升级到 NetScaler Pooled Capacity 许可证后，您可以按需将许可证从许可证池分配给 NetScaler 设备。您还可以为配置为高可用性模式的 NetScaler 实例配置 NetScaler Pooled Capacity 许可证。要为高可

© 1997–2026 Citrix Systems, Inc. All rights reserved.

用性模式下的 NetScaler MPX 实例配置 NetScaler Pooled Capacity 许可证，请参阅 将 NetScaler MPX 高可用性对中的永久许可证升级到 NetScaler Pooled Capacity。

注意

将永久许可证转换为池容量许可证是许可证授权的单向过程。您无法将池容量许可证恢复为永久许可证。 **重要**

要将 NetScaler MPX 升级到 NetScaler 池容量许可证，您需要将 MPX-Z 许可证上传到设备。

升级到 NetScaler 池容量：

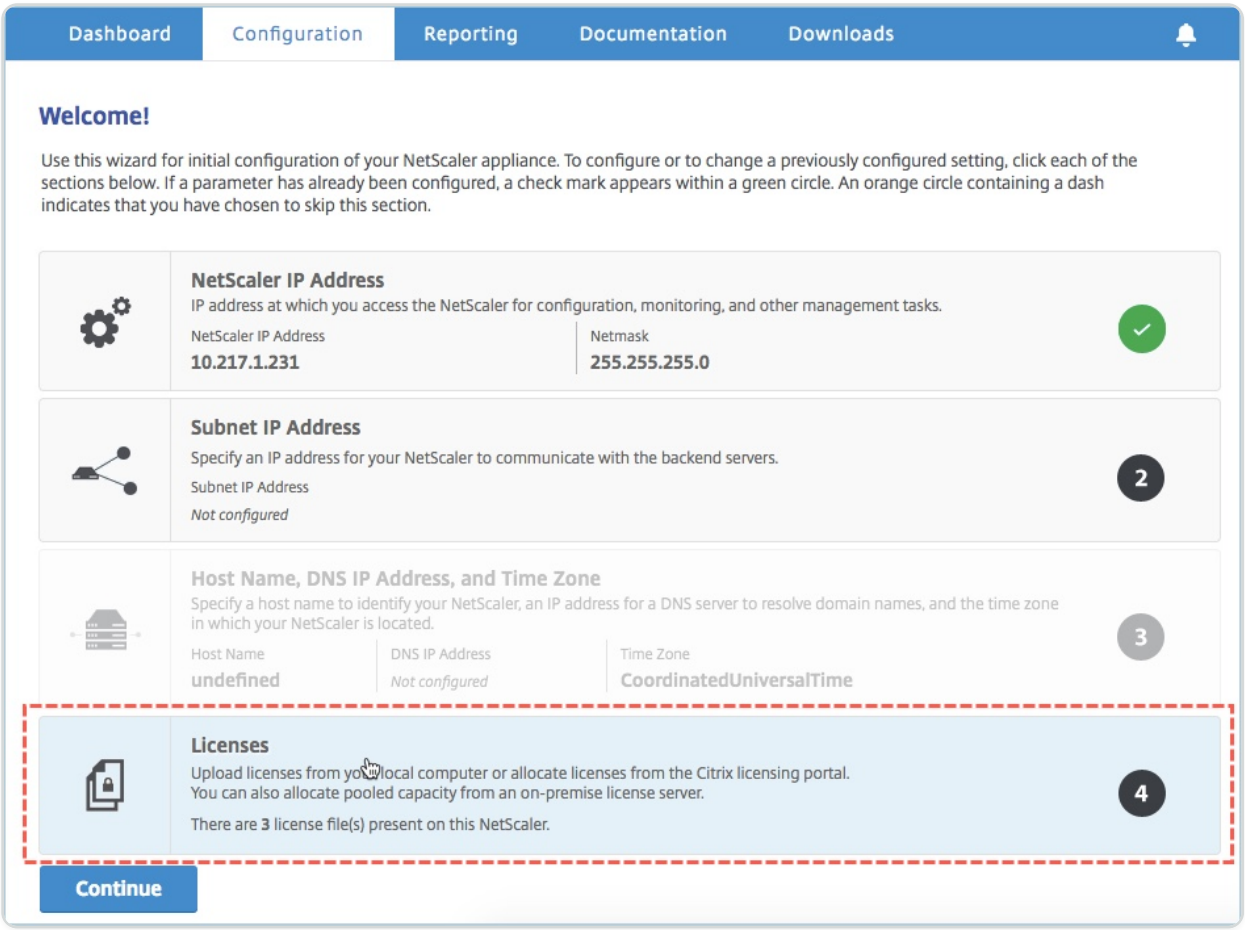
1. 在 Web 浏览器中，键入 NetScaler 的 IP 地址，例如 `<http://192.168.100.1>`。
2. 在“**用户名**”和“**密码**”中，键入管理员凭据。
3. 在“**欢迎**”页面上，单击“**继续**”。
4. 上传零容量许可证（MPX-Z 许可证）。在“配置”选项卡上，导航到“**系统**” \> “**许可证**”。
5. 在详细信息窗格中，单击“**管理许可证**”，单击“添加**新许可证**”。
6. 在“**许可证**”页面中，选择“**上传许可证文件**”并单击“**浏览**”以从本地计算机中选择零容量许可证。
7. 许可证上传后，单击“**重新启动**”以重新启动设备。

   警告

   应用 MPX-Z 许可证后，设备上的功能（包括 SSL 卸载）将变为未授权。设备将停止处理 HTTPS 请求。

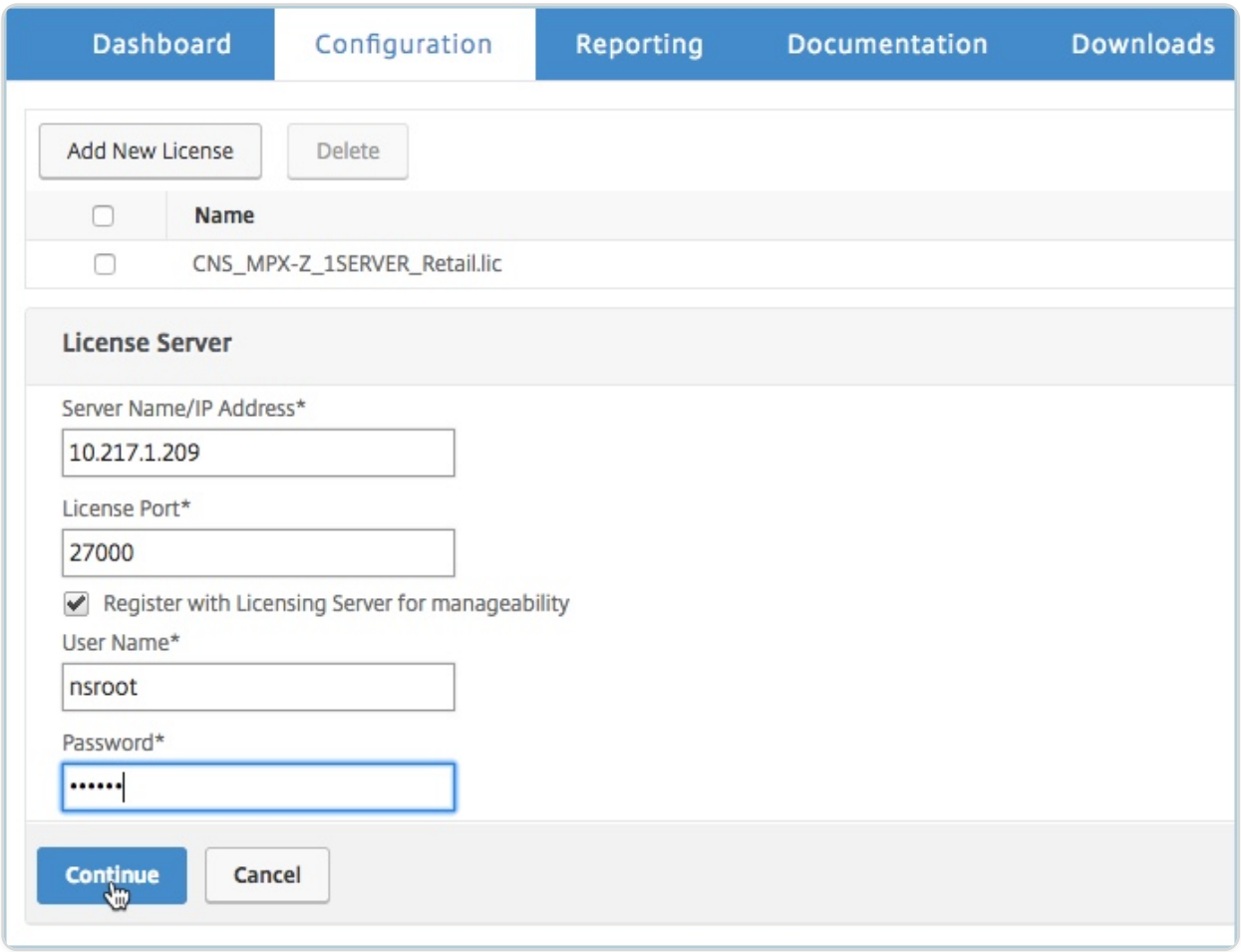
   如果在升级之前设备上启用了“**仅安全访问**”选项，您将无法通过 NetScaler Console GUI 使用 HTTPS 连接到设备。
8. 在“**确认**”页面上，单击“**是**”。
9. 设备重新启动后，登录到设备。
10. 在“欢迎”页面上，点击“**许可证**”部分。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



11. 在“**许可证服务器**”部分中，执行以下操作：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. 在“**服务器名称/IP 地址**”字段中，输入许可证服务器详细信息。

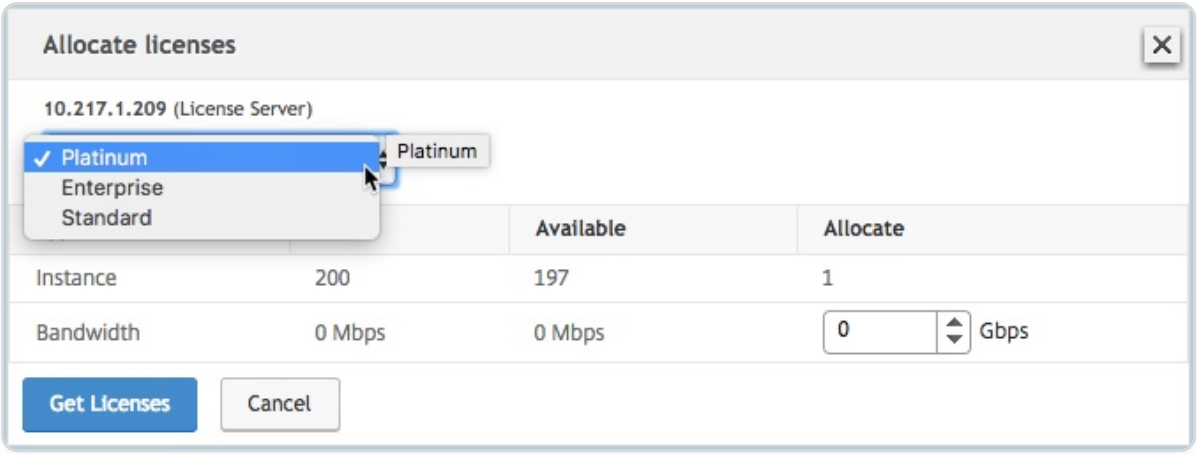
b. 在“**许可证端口**”字段中，输入许可证服务器端口。默认值：27000。

c. 如果您希望通过 NetScaler Console 管理实例的池许可证，请选中“**注册到许可服务器以进行可管理性**”复选框并输入 NetScaler Console 凭据。

d. 点击“**继续**”。

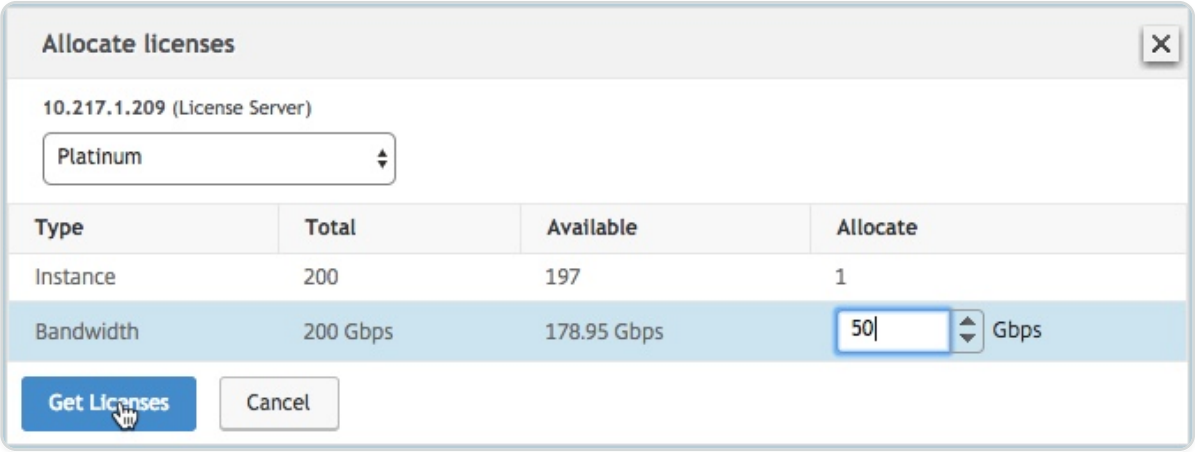
12. 在“**分配许可证**”中，执行以下操作：

a. 从下拉列表中选择许可证版本。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. 从“**分配**”菜单中为 NetScaler 分配带宽，然后点击“**获取许可证**”。



c. 出现提示时，点击“**重新启动**”以重新启动设备。

13. NetScaler MPX 重新启动后，登录到 NetScaler MPX。在“**欢迎**”页面上，点击“**继续**”。

    许可证页面列出了所有已许可的功能。

14. 导航到 **System > Licenses** 并单击 **Manage Licenses**。

    在**管理许可证**页面上，您可以查看许可证服务器、许可证版本以及分配的带宽的详细信息。

    许可证服务器的许可证详细信息(/en-us/netscaler-application-delivery-management-software/media/upgrade-mpx-10.jpg)

将 NetScaler MPX 高可用性对中的永久许可证升级到 NetScaler 池化容量

对于配置为高可用性模式的 MPX 设备，您必须在 HA 对中的主 NetScaler 实例和辅助 NetScaler 实例上配置池化容量。为 HA 对中的主 NetScaler 实例和辅助 NetScaler 实例分配相同容量的许可证。例如，如果您希望 HA 对中的每个实例具有 1 Gbps 容量，则需要从公共池中分配 2 Gbps 容量。通过 2 Gbps 容量，您可以为 HA 对中的主 NetScaler 实例和辅助 NetScaler 实例各分配 1 Gbps。

重要

要将 NetScaler MPX 升级为使用 NetScaler 池化容量许可证，您需要将 MPX-Z 上传到设备。

先决条件

请确保您已将 MPX-Z 许可证上传到 HA 对中的主实例和辅助实例。

要将 MPX-Z 许可证上传到 HA 对中的 NetScaler MPX 实例：

1. 在 Web 浏览器中，键入设备的 IP 地址，例如 `<http://192.168.100.1>`。
2. 在**用户名**和**密码**中，键入管理员凭据。

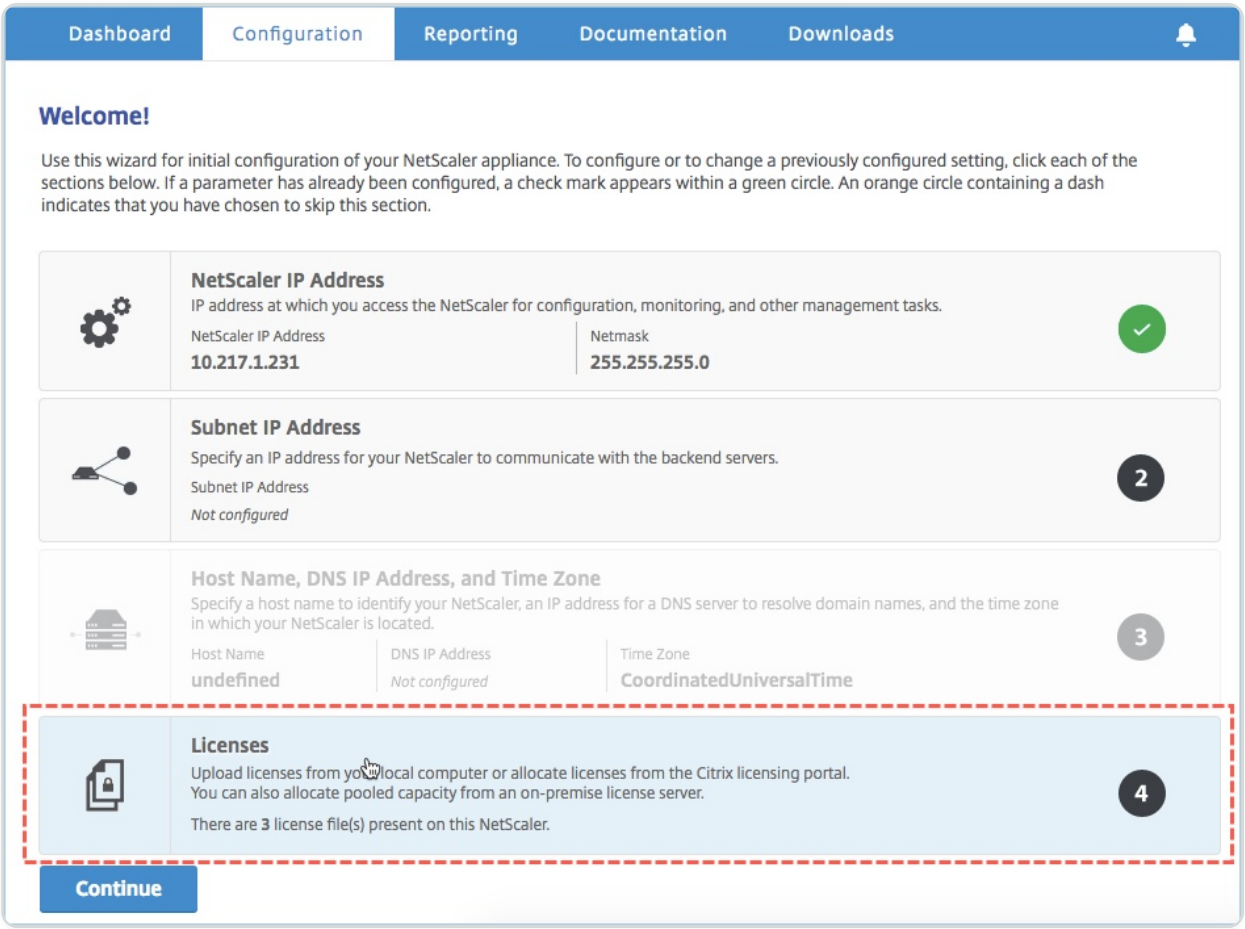
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在**欢迎**页面上，单击**继续**。
4. 上传零容量许可证（MPX-Z 许可证）。在**配置**选项卡上，导航到 **System \> Licenses**。
5. 在详细信息窗格中，单击**管理许可证**，然后单击**添加新许可证**。
6. 在**许可证**页面中，选择**上传许可证文件**，然后单击**浏览**以从本地计算机中选择零容量许可证。

   许可证上传后，系统会提示您重新启动设备。
7. 单击**重新启动**以重新启动设备。
8. 在**确认**页面上，单击**是**。

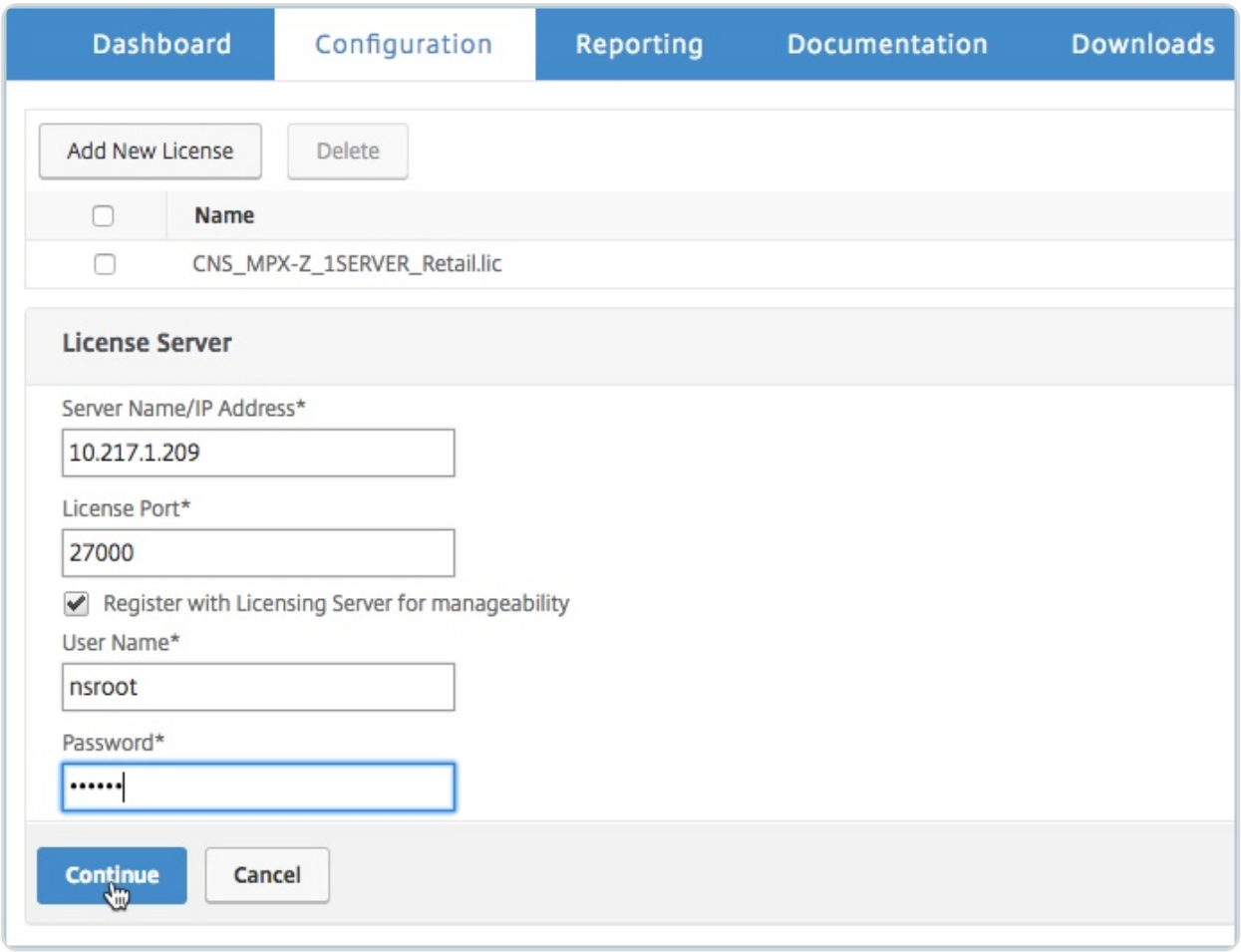
将现有 HA 设置升级到 NetScaler 池容量：

1. 登录到辅助 NetScaler MPX 实例。在 Web 浏览器中，键入 NetScaler 的 IP 地址，例如 `<http://192.168.100.1>`。
2. 在**用户名**和**密码**中，键入管理员凭据。
3. 在**欢迎**页面上，单击**许可证**部分。



4. 在**许可证服务器**部分中，执行以下操作：

© 1997–2026 Citrix Systems, Inc. All rights reserved.



a. 在**服务器名称/IP 地址**字段中，输入许可证服务器详细信息。

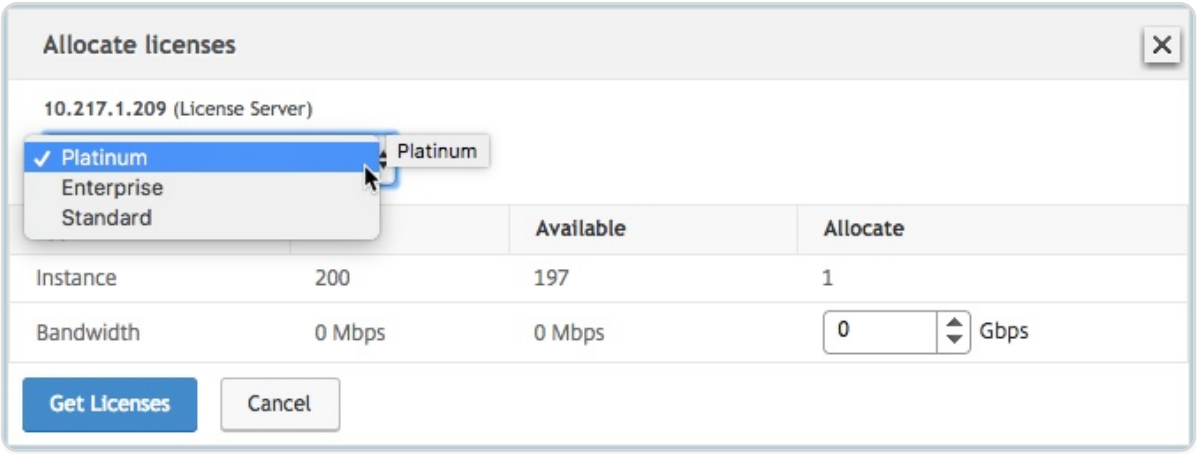
b. 在**许可证端口**字段中，输入许可证服务器端口。默认值：27000。

c. 如果您希望通过 NetScaler Console 管理实例的池许可证，请选中**注册到许可服务器以进行可管理性**复选框并输入 NetScaler Console 凭据。

d. 点击**继续**。

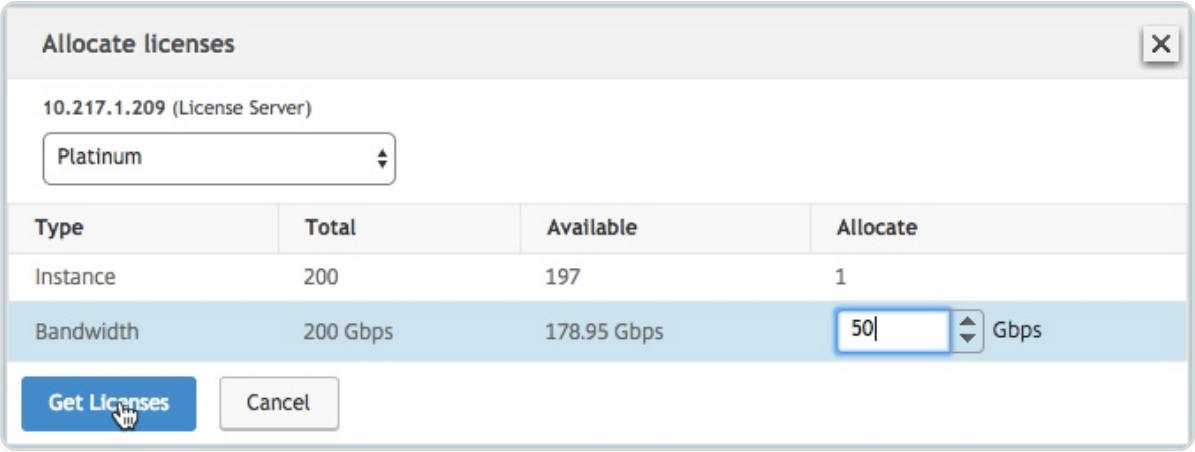
5. 在**分配许可证**中，执行以下操作：

a. 从下拉列表中选择许可证版本。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. 从**分配**菜单中将带宽分配给 NetScaler，然后点击**获取许可证**。



c. 出现提示时，点击**重新启动**以重新启动设备。设备使用新许可证启动并运行后，通过键入 `force ha failover` 强制执行故障转移。此故障转移可确保 HA 对处于良好状态。

6. 登录到现有的主 NetScaler MPX 并重新启动设备。执行以下操作：

   a. 在 Web 浏览器中，键入 NetScaler 的 IP 地址，例如 `<http://192.168.100.1>`。

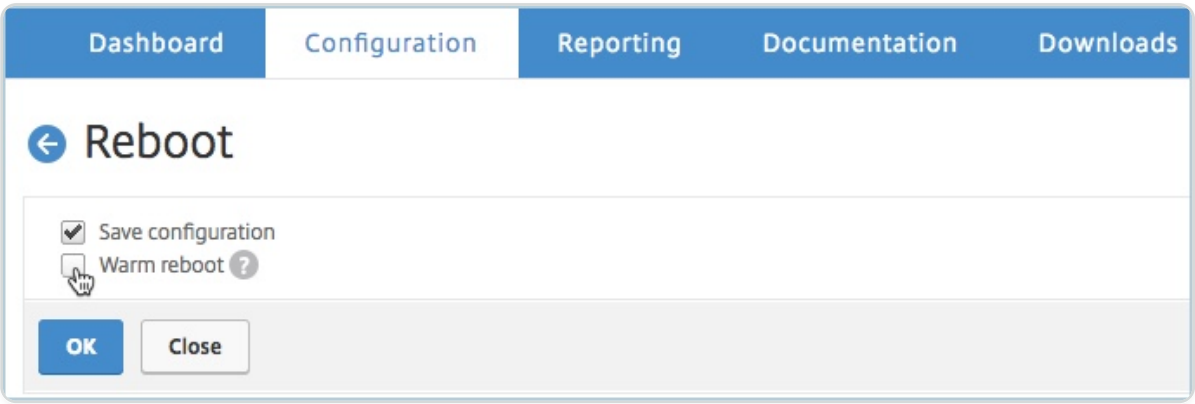
   b. 在**用户名**和**密码**中，键入管理员凭据。

   c. 在**欢迎**页面上，点击**继续**。

   d. 在**配置**选项卡上，点击**系统**。

   e. 在**系统**页面上，点击**重新启动**。

   f. 在**重新启动**页面上，选择**热重新启动**并点击**确定**。



主 NetScaler MPX 重启后，它将成为 HA 对中的辅助 NetScaler MPX。如果您想将 HA 对中的主实例和辅助实例更改回原始的 HA 对配置，请强制执行故障转移。在 HA 对中的任何实例上运行以下命令：

```
> force ha failover
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

将 NetScaler SDX 中的永久许可证升级到 NetScaler Pooled 容量

重要提示：

基于文件的许可系统（也称为手动管理的权利），传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活 Citrix 产品套件中产品的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler Flexed 许可证 (CPL/UHMC)、旧版 NetScaler Pooled 许可证和 NetScaler Fixed term Bandwidth 许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是 LAS 兼容版本。

兼容 LAS 的最低 NetScaler 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：自 2025 年 9 月初起支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： Console 本地部署的 LAS 支持从版本 14.1-51.x 开始。但是，自 April 15 2026 起，Console 本地部署版本 14.1-51.x 及更高版本以及 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署版本 14.1-51.x 或版本 13.1-60.x 或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署版本 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如 Pooled vCPU、CICO、永久许可证，将不支持 LAS。利用没有有效维护的永久许可证的 NetScaler 实例在升级到上述软件版本后将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。对于不遵守这些要求的情况，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法规定的任何其他补救措施。在法律或法规禁止的情况下，这些要求不适用。
具有永久许可证的 NetScaler SDX 可以升级到 NetScaler Pooled 容量许可证。升级到 NetScaler Pooled 容量许可证使您能够按需从许可证池中分配许可证给 NetScaler。您还可以为配置为高可用性模式的 NetScaler 实例配置 NetScaler Pooled 容量许可证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

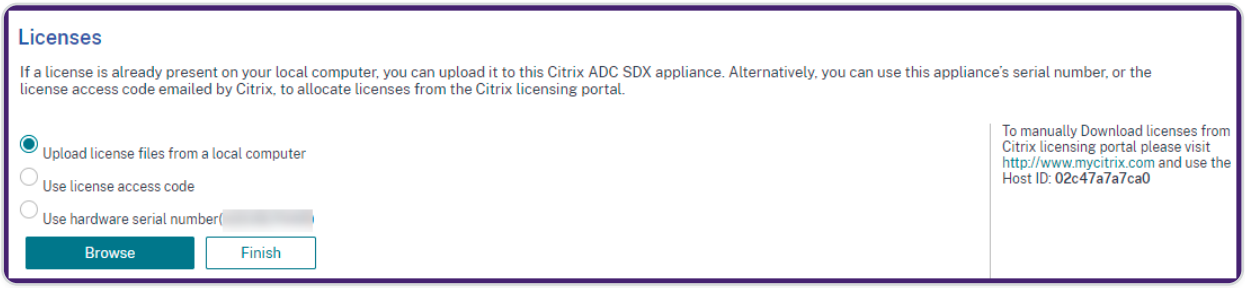
重要提示

从永久许可证转换为 Pooled 容量许可证是单向的许可证授权过程。您无法将 Pooled 容量许可证恢复为永久许可证。

- 要将 NetScaler SDX 升级到 NetScaler Pooled Capacity 许可证，您必须将 SDX-Z 许可证上传到设备。
- 确保您拥有在 NetScaler Console 中添加 NetScaler 实例的权限。
- 为确保对当前许可证没有影响，客户必须分配与永久许可证中可用的相同数量的实例和带宽。

要升级到 NetScaler Pooled capacity：

1. 在 Web 浏览器中，键入 NetScaler SDX 的 IP 地址，例如 `<http://192.168.100.1>`。
2. 在“**用户名**”和“**密码**”中，键入管理员凭据。
3. 在“**欢迎**”页面上，单击“**继续**”。
4. 上传零容量许可证。在“配置”选项卡上，导航到“**系统**”>“**许可证**”。
5. 在“**管理许可证**”页面上，单击“**添加许可证文件**”。
6. 在“**许可证**”页面中，选择“**从本地计算机上传许可证文件**”，然后单击“**浏览**”以从本地计算机中选择零容量许可证。然后，单击“**完成**”。



成功应用零容量许可证后，“**池化许可证**”部分将显示在“**许可证**”页面上。

注意

要删除旧许可证文件，您无需重新启动 NetScaler SDX，因此可避免停机。如需更多帮助，请联系 NetScaler 支持。

7. 在“**池化许可证**”部分中，执行以下操作：

   a. 在**许可服务器名称或 IP 地址**字段中，输入许可服务器详细信息。如果要将 NetScaler Console 服务器配置为许可服务器，请指定 NetScaler Console 服务器的 IP 地址。

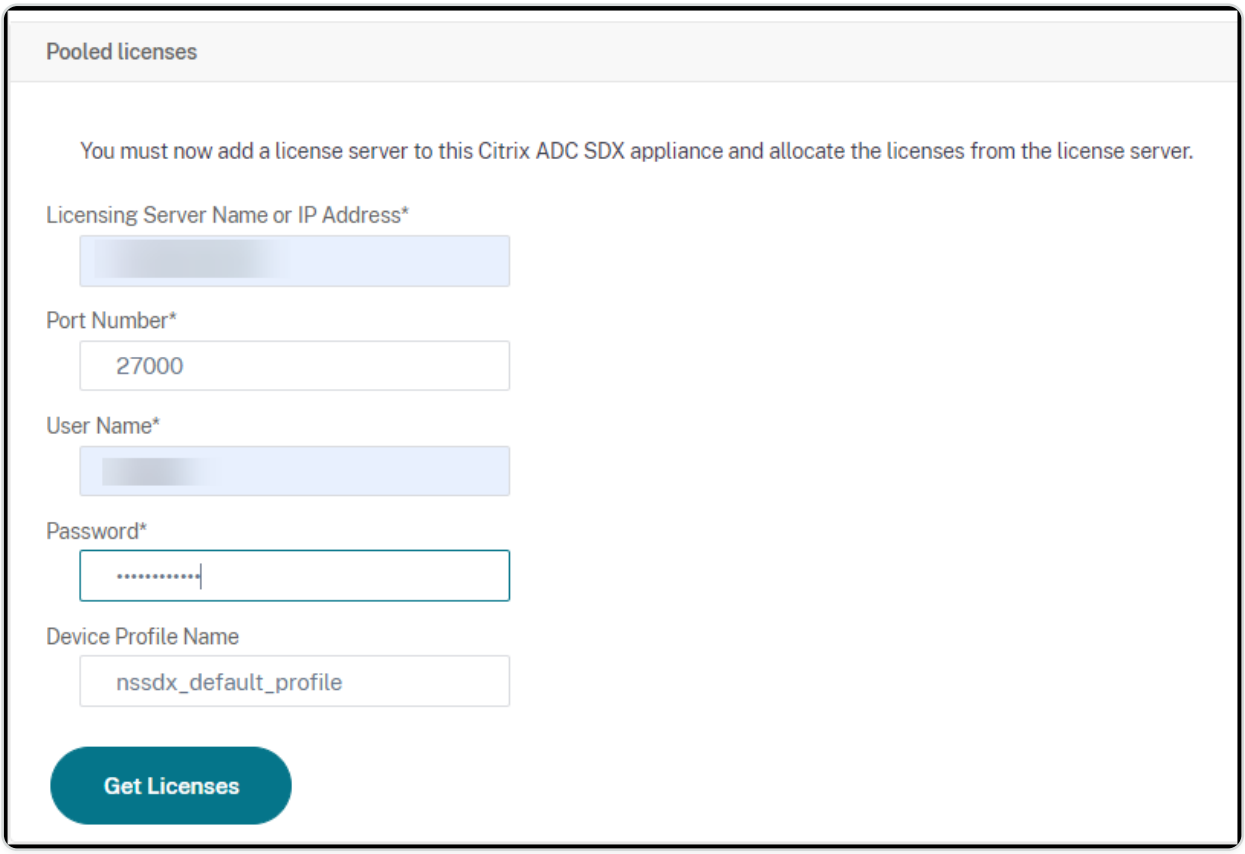
© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. 在**端口号**字段中，输入许可服务器端口。默认值：27000。

c. 指定许可服务器的**用户名**和**密码**。

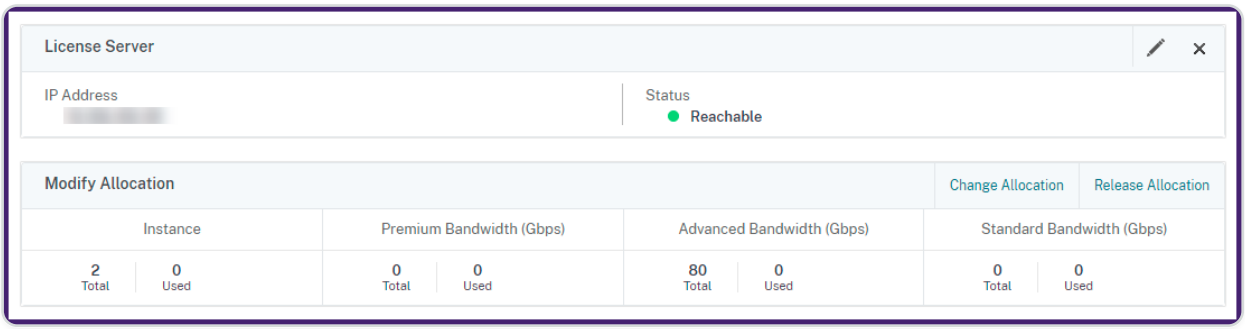
- 对于 NetScaler Console 服务器，输入管理员凭据。
- 对于 NetScaler Console 代理，输入代理凭据。

d. 单击**获取许可证**。



8. 在**分配许可证**窗口中，指定所需的实例和带宽，然后单击**分配**。

在**管理许可证**页面上，您可以查看许可服务器、许可证版本以及从池中分配的实例和带宽的详细信息。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

将永久许可证升级到池容量不需要重新启动 SDX 设备。

群集模式下 NetScaler 实例上的 NetScaler 池化容量

重要提示：

基于文件的许可系统（也称为手动管理的授权），传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活 Citrix 产品套件中所有产品的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler 弹性许可证 (CPL/UHMC)、旧版 NetScaler 池化许可证和 NetScaler 固定期限带宽许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是与 LAS 兼容的版本。

兼容 LAS 的最低要求的 NetScaler® 版本包括：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console 服务：自 2025 年 9 月初起支持。
- 本地 NetScaler Console：14.1-51.x

  注意： LAS 对本地 Console 的支持始于 14.1-51.x 版本。但是，自 April 15 2026 起，本地 Console 14.1-51.x 及更高版本以及 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到本地 Console 14.1-51.x 或 13.1-60.x 或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到本地 Console 14.1-51.x 或更高版本，并切换到 LAS，因为本地 Console 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如池化 vCPU、CICO、永久许可证，将不支持 LAS。升级到上述软件版本后，使用没有有效维护的永久许可证的 NetScaler 实例将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。如果不遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法上的其他补救措施。在法律或法规禁止的情况下，这些要求不适用。
您可以在配置为群集的 NetScaler 实例上配置 NetScaler 池化容量。以下是在群集模式下 NetScaler 实例上配置池化容量的先决条件：

- 实例单独以池化容量许可模式运行以形成群集。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 所有实例必须以相同的带宽运行。
- 所有实例都从同一个 NetScaler Console 签出了池化容量。
- 新实例无法添加到现有 NetScaler 群集，除非它们的容量和 NetScaler Console 配置与群集中现有实例的容量和配置相同。

从 NetScaler 群集签出的任何容量都会将相同的容量分配给所有群集节点，并且签出带宽 = 提供的带宽 * 节点数。

例如，如果您从 NetScaler 群集签出 50 Mbps 的带宽，并且群集包含 12 个实例，则每个实例会自动获得 50 Mbps。并且从池中签出 600 Mbps。

注意

如果群集中的一个或多个实例无响应，群集将继续使用剩余实例的容量处理流量。

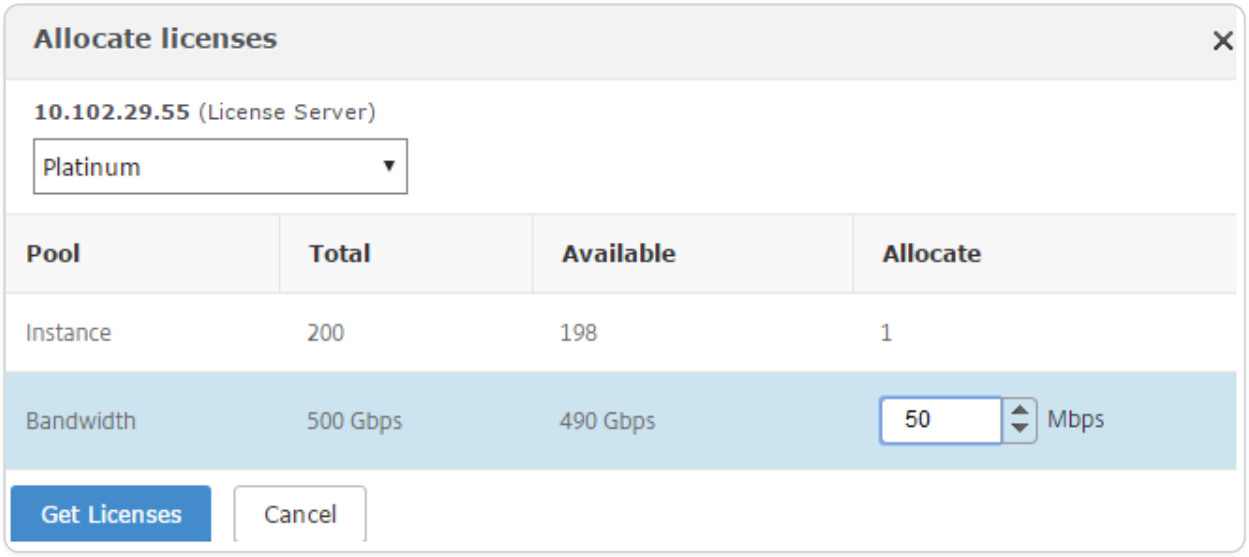
将 NetScaler 池化容量分配给 NetScaler 群集

单独为每个群集节点分配许可证。因为跨群集节点传播和同步许可证的命令已被禁用。

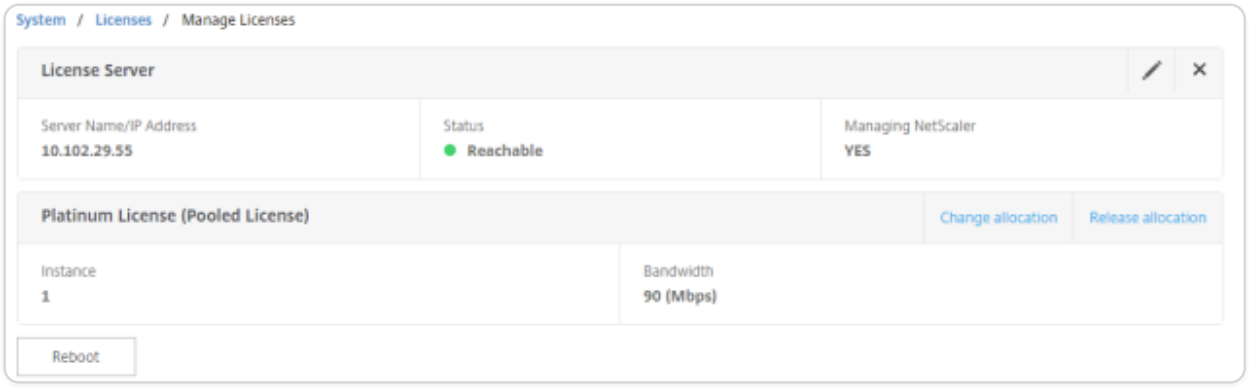
在每个群集节点上重复以下过程：

1. 在 Web 浏览器中，键入 NetScaler IP 地址 (NSIP)。例如，`http://192.168.100.1`。
2. 在“**用户名**”和“**密码**”字段中，输入管理员凭据。
3. 在“**配置**”选项卡上，导航到“**系统 > 许可证 > 管理许可证**”。单击“**添加新许可证**”，然后选择“**使用池化许可**”。
4. 在“**服务器名称/IP 地址**”字段中输入许可证服务器的名称或地址。
5. 如果您希望通过 NetScaler Console 管理实例的池许可证，请选中“**注册到 NetScaler Console 以进行可管理性**”复选框并输入 NetScaler Console 凭据。
6. 选择许可证版本和所需的带宽，然后单击“**获取许可证**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



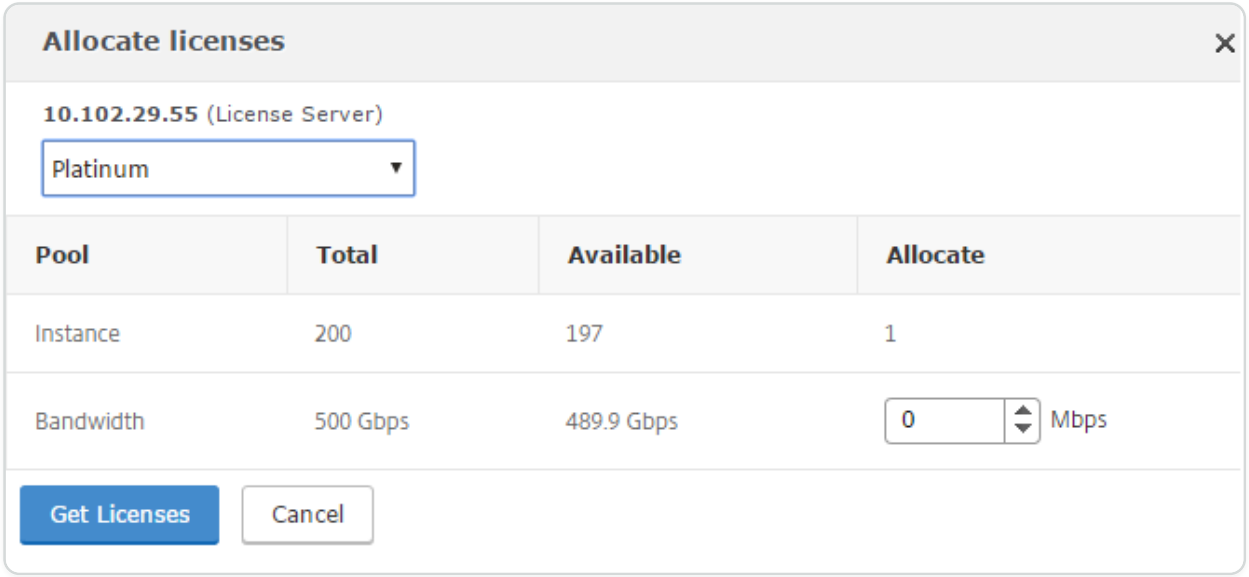
7. 您可以通过选择**更改分配**或**释放分配**来更改或释放许可证分配。



8. 如果您单击**更改分配**，将弹出一个窗口，显示许可证服务器上可用的许可证。

注意

带宽分配必须是相应外形规格的最小带宽单位的整数倍。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. 您可以从**分配**下拉列表中为 NetScaler 实例分配带宽或实例。然后单击**获取许可证**。
10. 您可以从弹出窗口中的下拉列表中选择许可证版本和所需的带宽。

> **注意**
>
> 如果更改带宽分配，则无需重新启动，但如果更改许可证版本，则需要热重新启动。

使用 CLI 将 NetScaler 池容量分配给 NetScaler 群集

单独为每个群集节点分配许可证。因为跨群集节点传播和同步许可证的命令已被禁用。

在每个群集节点上重复以下过程：

1. 在 SSH 客户端中，输入 NetScaler IP 地址 (NSIP)，然后使用管理员凭据登录。
2. 要添加许可服务器，请输入以下命令：

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <port number >]
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. 要显示许可服务器上的可用许可证，请输入以下命令：

```
sh licenseserverpool
```

```
> sh licenseserverpool
        Instance Total                    : 0
        Instance Available                : 0
        Standard Bandwidth Total          : 0 Mbps
        Standard Bandwidth Availabe       : 0 Mbps
        Enterprise Bandwidth Total        : 0 Mbps
        Enterprise Bandwidth Available    : 0 Mbps
        Platinum Bandwidth Total          : 0 Mbps
        Platinum Bandwidth Available      : 0 Mbps
        VPX25S Total                      : 1
        VPX25S Available                  : 1
        VPX200E Total                     : 1
        VPX200E Available                 : 1
        VPX1000S Total                    : 1
        VPX1000S Available                : 1
        VPX8000E Total                    : 2
        VPX8000E Available                : 1
 Done
```

4. 要将许可证分配给 NetScaler VPX 设备，请输入以下命令：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set capacity -platform V\[S/E/P\]\[Bandwidth\]
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

签入和签出 NetScaler VPX 和 NetScaler BLX 许可证

重要提示：

基于文件的许可系统（也称为手动管理的授权），传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于 Citrix 产品套件中产品激活的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler Flexed 许可证 (CPL/UHMC)、旧版 NetScaler Pooled 许可证和 NetScaler Fixed term Bandwidth 许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是 LAS 兼容版本。

兼容 LAS 的最低 NetScaler® 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：从 2025 年 9 月初开始支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： Console 本地部署的 LAS 支持从版本 14.1-51.x 及更高版本开始。但是，自 April 15 2026 起，Console 本地部署版本 14.1-51.x 及更高版本和 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署版本 14.1-51.x 或版本 13.1-60.x 或更高版本，则可以继续使用基于文件的许可，直到 April 15 2026。但是，您必须在 April 15 2026 之前升级到 Console 本地部署版本 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如池化 vCPU、CICO、永久许可证，将不支持 LAS。使用没有有效维护的永久许可证的 NetScaler 实例在升级到上述软件版本后将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。对于不符合这些要求的行为，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能根据法律或衡平法采取任何其他补救措施。
在法律或法规禁止的情况下，这些要求不适用。
您可以根据需要从 NetScaler Console 向 NetScaler 实例分配 NetScaler VPX 和 NetScaler BLX 许可证。NetScaler Console 软件存储和管理许可证，该软件具有一个许可框架，可提供可扩展的自动

© 1997–2026 Citrix Systems, Inc. All rights reserved.

化许可证预配。实例在预配时可以从 NetScaler Console 签出许可证。当实例被移除或销毁时，该实例会将其许可证签回 NetScaler Console 软件。

先决条件

确保满足以下先决条件：

- 您正在使用运行软件版本 12.0 的 NetScaler VPX 映像。

  例如：NSVPX-ESX-12.0-xx.xx_nc.zip

- 您已安装运行版本 12.0 的 NetScaler Console。

  例如：MAS-ESX-12.0-xx.xx.zip

注意

要通过 NetScaler Console 管理现有 NetScaler VPX 许可证，您需要将许可证重新托管到 NetScaler Console。

在 NetScaler Console 中安装许可证

注意

在安装许可证之前，如果您更改了软件版本或带宽，请重新启动 NetScaler Console 虚拟设备。

在 NetScaler Console 上安装许可证文件：

1. 在 Web 浏览器中，键入 NetScaler Console 的 IP 地址（例如，`<http://192.168.100.1>`）。
2. 在“用户名”和“密码”中，输入管理员凭据。
3. 导航到 **基础架构 > 池化许可**。
4. 在“**许可证文件**”部分中，选择以下选项之一：

   - **从本地计算机上传许可证文件** - 如果许可证文件已存在于您的本地计算机上，您可以将其上传到 NetScaler Console。

     要添加许可证文件，请单击“**浏览**”并选择要添加的许可证文件 (.lic)。然后单击“**完成**”。

   - **使用许可证访问代码** - Citrix 会通过电子邮件发送您购买的许可证的许可证访问代码。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要添加许可证文件，请在文本框中输入许可证访问代码，然后单击“**获取许可证**”。

> **注意**
>
> 在使用许可证访问代码安装许可证之前，请确保您已连接到互联网。

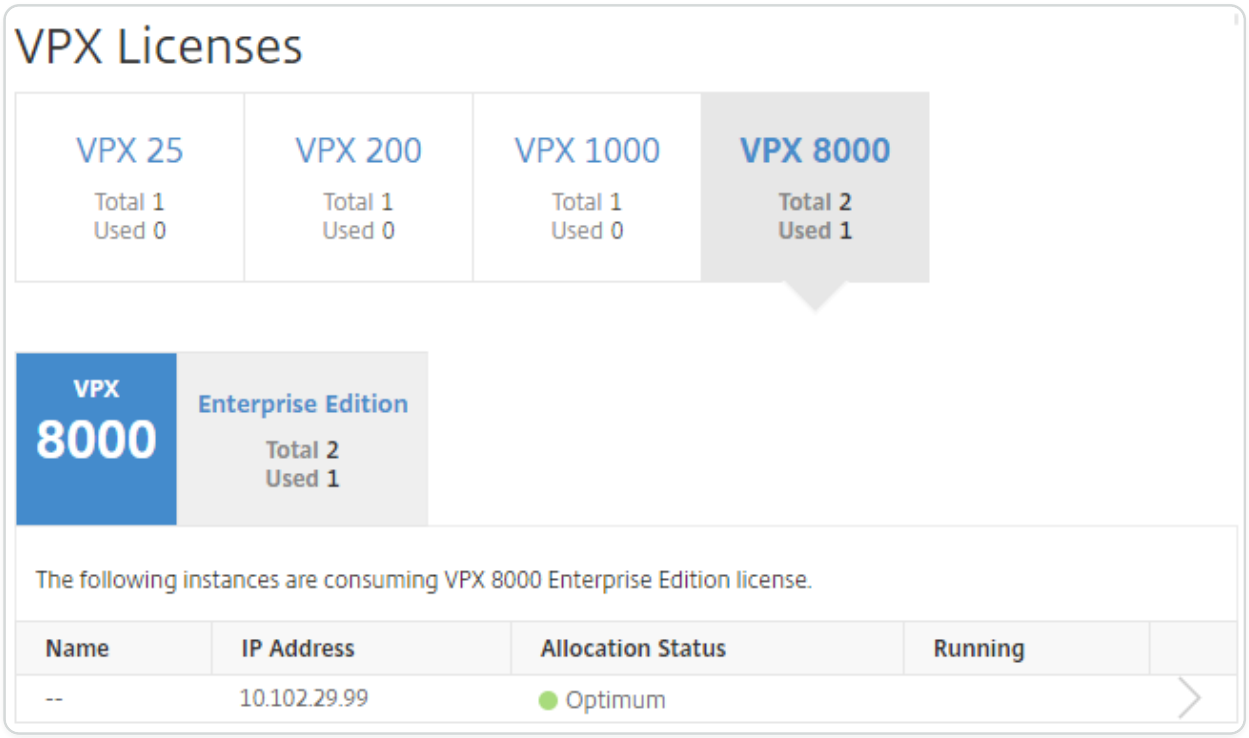
您可以随时从“**许可证设置**”页面向 NetScaler Console 添加更多许可证。

验证

您可以在 NetScaler Console GUI 中查看可用和已分配的许可证。

要显示许可证：

1. 在 Web 浏览器中，键入 NetScaler Console 的 IP 地址（例如，`<http://192.168.100.1>`）。
2. 在“**用户名**”和“**密码**”中，输入管理员凭据。
3. 在“配置”选项卡上，导航到“**基础结构 > 池化许可 > VPX 许可证**”。



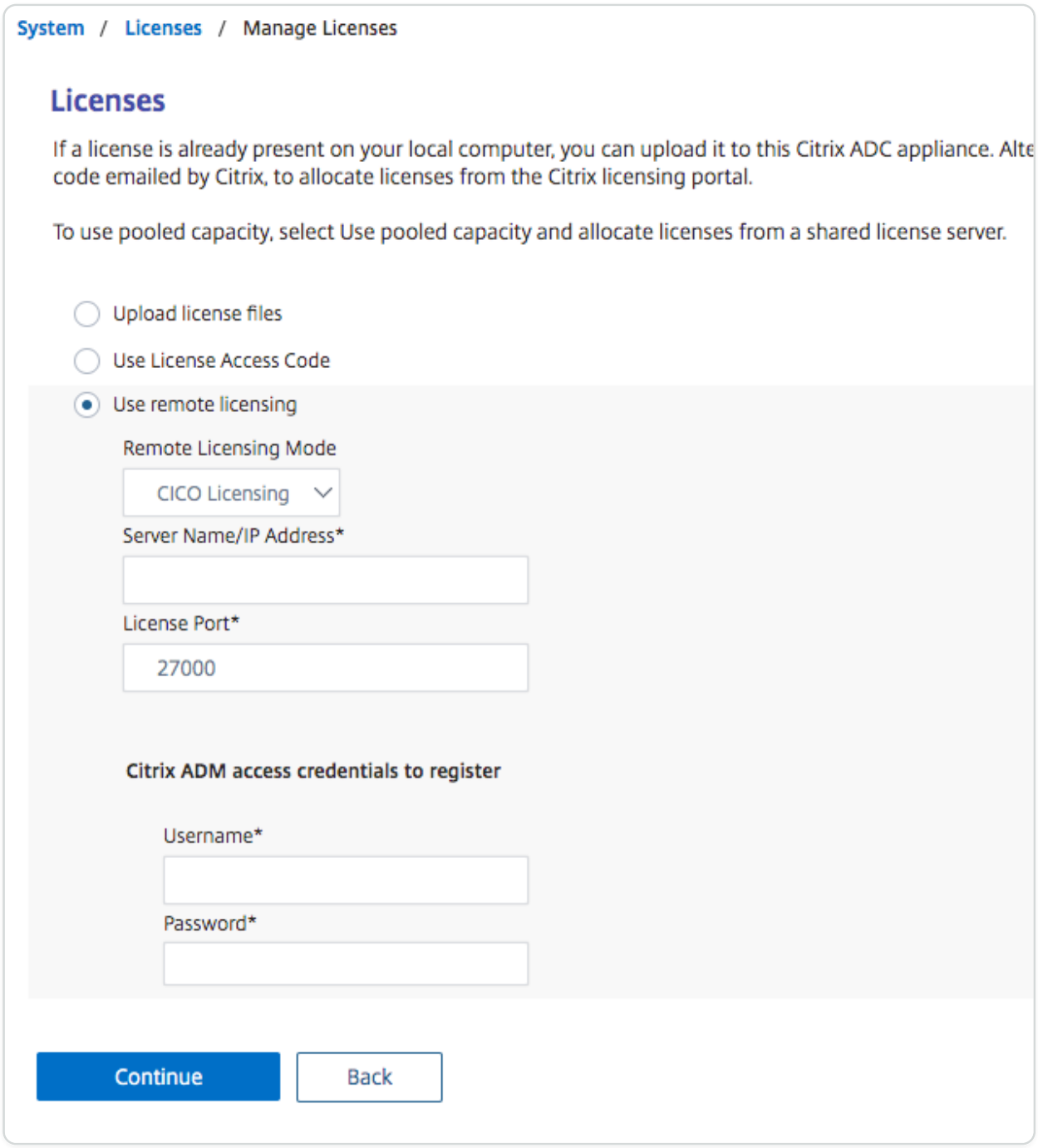
4. 您可以在可用许可证部分下的表中查看已分配的许可证。

使用 NetScaler GUI 将 NetScaler VPX 和 NetScaler BLX 许可证分配给 NetScaler 实例

1. 在 Web 浏览器中，键入 NetScaler 实例的 IP 地址（例如，`<http://192.168.100.1>`）。
2. 在“**用户名**”和“**密码**”字段中，输入管理员凭据。

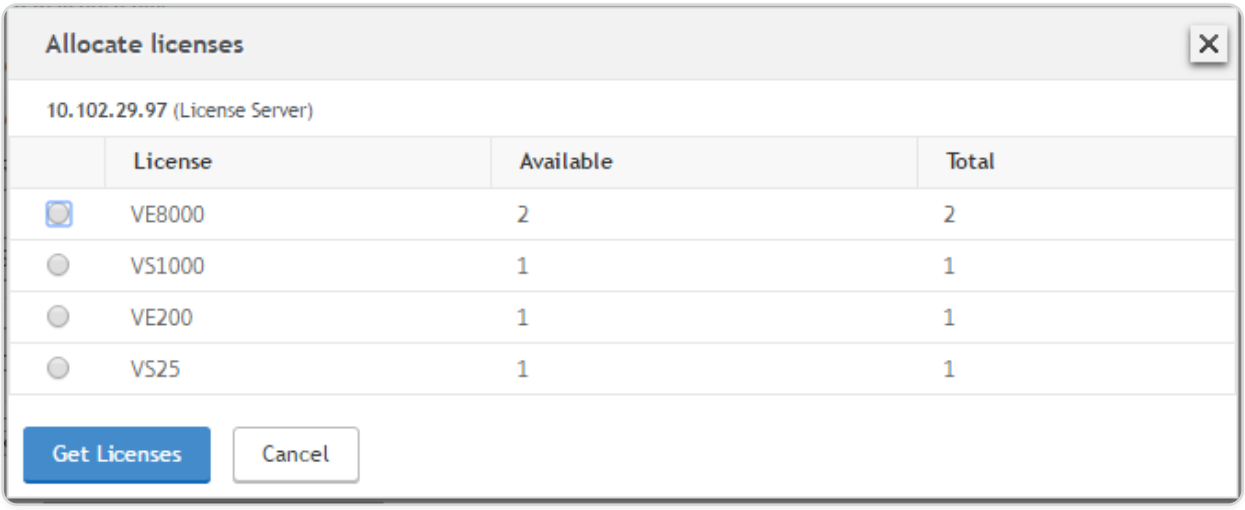
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在“配置”选项卡上，导航到“**设置 > 许可证 > 管理许可证**”，单击“**添加新许可证**”，然后选择“**使用远程许可 > CICO 许可**”。
4. 在“**服务器名称/IP 地址**”字段中输入许可证服务器的详细信息。
5. 在 **用户名** 和 **密码** 中，输入 NetScaler Console 凭据，然后单击 **继续**。

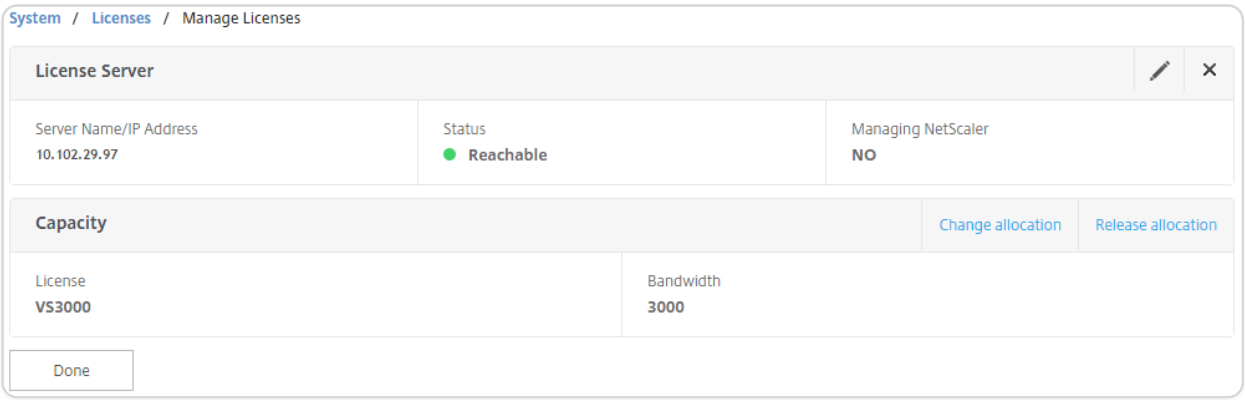


6. 选择具有所需带宽的许可证版本，然后单击 **获取许可证**。

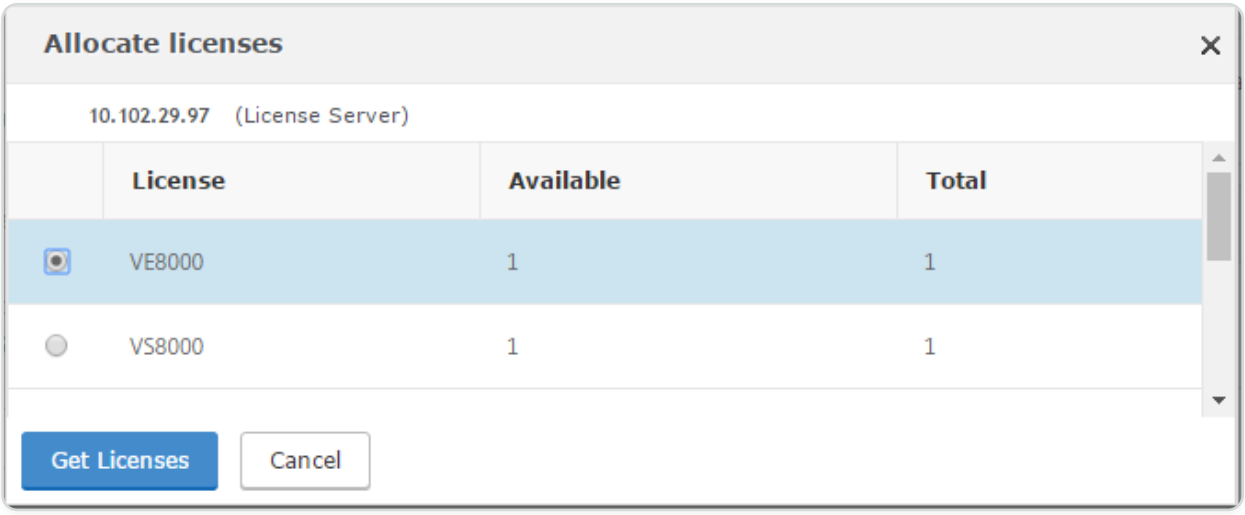
© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. 单击 **重新启动**，您的 NetScaler 实例将重新启动。
8. 您可以通过导航到 **系统 > 许可证 > 管理许可证**，然后选择 **更改分配** 或 **释放分配** 来更改或释放许可证分配。



9. 如果您单击 **更改分配**，将弹出一个窗口显示许可证服务器上可用的许可证。选择所需的许可证，然后单击 **获取许可证**。



使用 NetScaler CLI 将 NetScaler VPX 和 NetScaler BLX 许可证分配给 NetScaler 实例

1. 在 SSH 客户端中，输入 NetScaler 实例的 IP 地址，然后使用管理员凭据登录。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 要添加许可证服务器，请输入以下命令：

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <port
number >]
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. 要显示许可证服务器上可用的许可证，请输入以下命令：

```
sh licenseserverpool
```

```
> sh licenseserverpool
        Instance Total                    : 0
        Instance Available                : 0
        Standard Bandwidth Total          : 0 Mbps
        Standard Bandwidth Availabe       : 0 Mbps
        Enterprise Bandwidth Total        : 0 Mbps
        Enterprise Bandwidth Available    : 0 Mbps
        Platinum Bandwidth Total          : 0 Mbps
        Platinum Bandwidth Available      : 0 Mbps
        VPX25S Total                      : 1
        VPX25S Available                  : 1
        VPX200E Total                     : 1
        VPX200E Available                 : 1
        VPX1000S Total                    : 1
        VPX1000S Available                : 1
        VPX8000E Total                    : 2
        VPX8000E Available                : 1
 Done
```

4. 要将许可证分配给 NetScaler，请输入以下命令：

```
set capacity –platform V\[S/E/P\]\[Bandwidth\]
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

使用 API 将 NetScaler VPX 和 NetScaler BLX 许可证分配给 NetScaler 实例

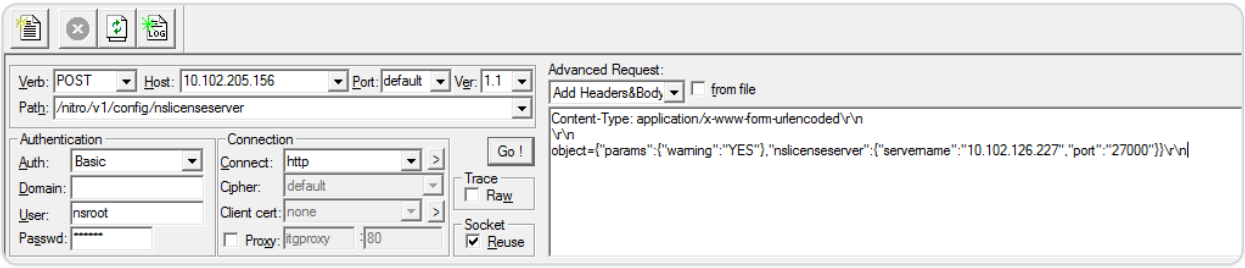
在 Web 浏览器或 API 客户端中，使用管理员凭据登录到 NetScaler 实例。

添加许可服务器：

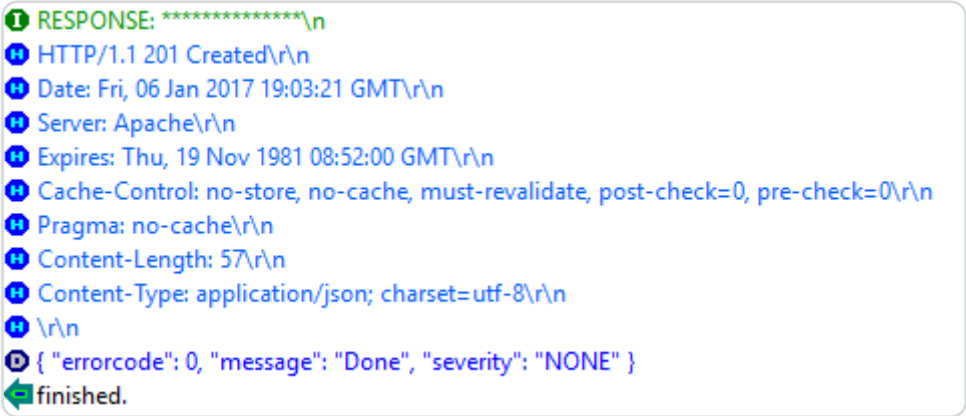
1. 将请求类型设置为 **Post**。
2. 将路径设置为 /nitro/v1/config/nslicensingserver。
3. 按如下方式设置有效负载：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
content-type: application/x-www-form-urlencoded\\r\\n

\\r\\n

object= {“params”;{warning”:”yes”},”nslicensing server”;
{servername”:”\<NetScaler Console IP\>”, “port”:”27000”}}\\r\\n
```

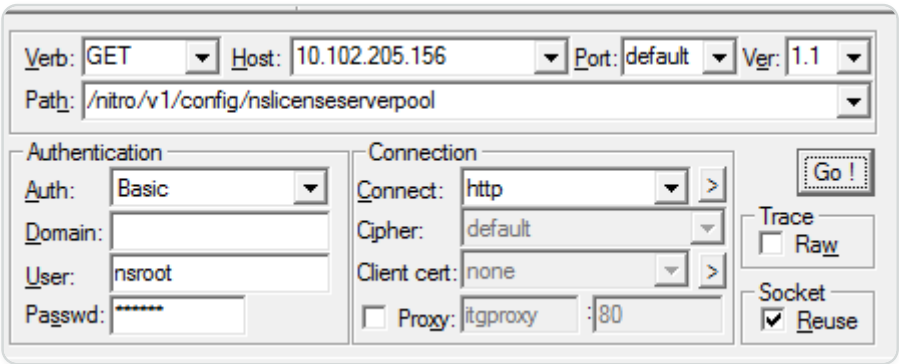


NetScaler Console 响应请求。以下示例响应显示成功。



查看许可服务器上的可用许可证：

1. 将请求类型设置为 **Get**。
2. 将路径设置为 /nitro/v1/config/nslicenseserverpool



NetScaler Console 响应请求。以下示例响应显示成功以及许可证服务器上可用许可证的列表。

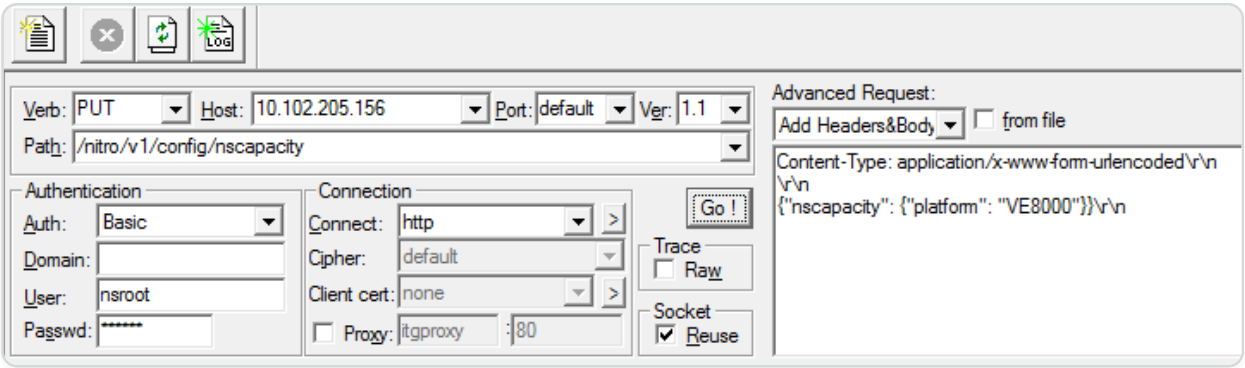
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
RESPONSE: **************\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:18:54 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 1874\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE", "nslicenseserverpool": { "instancetotal": 0, "instanceavailable": 0, "standardbandwidthtotal":
0, "standardbandwidthavailable": 0, "enterprisebandwidthtotal": 0, "enterprisebandwidthavailable": 0, "platinumbandwidthtotal": 0, "platinumbandwidthav
ailable": 0, "cpxinstancetotal": 0, "cpxinstanceavailable": 0, "vpx1stotal": 0, "vpx1savailable": 0, "vpx1ptotal": 0, "vpx1pavailable": 0, "vpx5stotal"
: 0, "vpx5savailable": 0, "vpx5ptotal": 0, "vpx5pavailable": 0, "vpx10stotal": 0, "vpx10savailable": 0, "vpx10etotal": 0, "vpx10eavailable": 0, "vpx10p
total": 0, "vpx10pavailable": 0, "vpx25stotal": 0, "vpx25savailable": 0, "vpx25etotal": 0, "vpx25eavailable": 0, "vpx25ptotal": 0, "vpx25pavailable": 0
, "vpx50stotal": 0, "vpx50savailable": 0, "vpx50etotal": 0, "vpx50eavailable": 0, "vpx50ptotal": 0, "vpx50pavailable": 0, "vpx100stotal": 0, "vpx100sav
ailable": 0, "vpx100etotal": 0, "vpx100eavailable": 0, "vpx100ptotal": 0, "vpx100pavailable": 0, "vpx200stotal": 0, "vpx200savailable": 0, "vpx200etota
l": 0, "vpx200eavailable": 0, "vpx200ptotal": 0, "vpx200pavailable": 0, "vpx500stotal": 0, "vpx500savailable": 0, "vpx500eto
tal": 0, "vpx500eavailable": 0, "vpx500ptotal": 0, "vpx500pavailable": 0, "vpx1000stotal": 0, "vpx1000savailable": 0, "vpx1000etotal": 0, "vpx1000eavail
able": 0, "vpx1000ptotal": 0, "vpx1000pavailable": 0, "vpx2000ptotal": 0, "vpx2000pavailable": 0, "vpx3000stotal": 0, "vpx3000savailable": 0, "vpx3000e
total": 0, "vpx3000eavailable": 0, "vpx3000ptotal": 0, "vpx3000pavailable": 0, "vpx4000ptotal": 0, "vpx4000pavailable": 0, "vpx5000stotal": 0, "vpx5000
savailable": 0, "vpx5000etotal": 0, "vpx5000eavailable": 0, "vpx5000ptotal": 0, "vpx5000pavailable": 0, "vpx8000stotal": 1, "vpx8000savailable": 1, "vp
x8000etotal": 2, "vpx8000eavailable": 1, "vpx8000ptotal": 1, "vpx8000pavailable": 1 } }
finished.
```

将许可证分配给 NetScaler：

1. 将请求类型设置为 **Post**。
2. 将路径设置为 /nitro/v1/config/nscapacity。
3. 按如下方式设置有效负载：

```
content-type: application/x-www-form-urlencoded\\r\\n

\\r\\n

{“nscapacity:{“platform”:”VE8000”}}\\r\\n
```



NetScaler Console 响应请求。以下示例响应显示成功。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
RESPONSE: **************\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:16:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

更新许可服务器 IP 地址

您可以更新 NetScaler VPX 和 NetScaler BLX 实例中的许可服务器 IP 地址，而不会影响实例上分配的许可证带宽和数据丢失。

使用 CLI 更新：要使用 CLI 更新许可服务器 IP 地址，请在实例上键入以下命令：

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

此命令连接到新服务器并释放与以前的许可服务器关联的资源。

使用 GUI 更新：要使用 GUI 更新许可服务器 IP 地址，请导航到 **System > Licenses > Manage Licenses**，然后单击 **Add New License**。有关更多信息，请参阅使用 NetScaler GUI 将 NetScaler VPX 和 NetScaler BLX 许可证分配给 NetScaler 实例。

配置 NetScaler VPX 和 NetScaler BLX 签入和签出许可证的到期检查

您现在可以为 NetScaler VPX 和 NetScaler BLX 许可证配置许可证到期阈值。通过设置阈值，NetScaler Console 会通过电子邮件或短信发送通知，告知许可证即将到期。当许可证在 NetScaler Console 上过期时，还会发送 SNMP trap 和通知。

发送许可证到期通知时会生成一个事件，该事件可在 NetScaler Console 上查看。

配置许可证到期检查：

1. 导航到 **基础设施 > 许可池**。
2. 在 **License Settings** 页面中，**License Expiry Information** 部分下，您可以找到即将到期的许可证的详细信息：
   - **Feature**：即将到期的许可证类型。
   - **Count**：受影响的虚拟服务器或实例的数量。
   - **Days to expiry**：许可证到期前的天数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在 **Notification Settings** 部分中，单击 **Edit** 图标并指定警报阈值。您可以设置一个池化许可证容量的百分比，用于通知管理员。
4. 通过选择相应的复选框来选择您要发送的通知类型。通知类型如下：
   a. **Email Profile**：指定邮件服务器和配置文件详细信息。当您的许可证即将到期时，将触发一封电子邮件。
   b. **SMS Profile**：指定短消息服务 (SMS) 服务器和配置文件详细信息。当您的许可证即将到期时，将触发一条短信。
5. 然后，指定您希望在许可证到期前多少天发送通知。
6. 单击 **Save**。

NetScaler 虚拟 CPU 许可

重要提示：

基于文件的许可系统（也称为手动管理的授权），传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活 Citrix 产品套件的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler Flexed 许可证 (CPL/UHMC)、旧版 NetScaler Pooled 许可证和 NetScaler Fixed term Bandwidth 许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是兼容 LAS 的版本。

最低要求的 NetScaler® 版本兼容 LAS 的包括：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：从 2025 年 9 月初开始支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： Console 本地部署的 LAS 支持从版本 14.1-51.x 及更高版本开始。但是，自 April 15 2026 起，Console 本地部署版本 14.1-51.x 及更高版本和 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署版本 14.1-51.x 或版本 13.1-60.x 或更高版本，您可以继续使用基于文件的许可直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署版本 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

所有其他形式的旧版 NetScaler 许可证，例如 Pooled vCPU、CICO、永久许可证，将不支持 LAS。使用没有有效维护的永久许可证的 NetScaler 实例在升级到上述软件版本后将变为未授权状态。
基于 LAS 的许可证在法律或法规禁止的情况下可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。如果未能遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外 Citrix 还可能拥有法律或衡平法上的其他补救措施。在法律或法规禁止的情况下，这些要求不适用。
在继续之前，请阅读以下注意事项。

注意：

vCPU 许可证不再可供购买。有关更多信息，请参阅 许可。

像您这样的数据中心管理员正在转向更新的技术，这些技术可以简化网络功能，同时提供更低的成本和更高的可扩展性。新的数据中心架构至少必须包含以下功能：

- 软件定义网络 (SDN)
- 网络功能虚拟化 (NFV)
- 网络虚拟化 (NV)
- 微服务

这种转变也要求软件需求具有动态性、灵活性和敏捷性，以满足不断变化的业务需求。许可证也应由中央管理工具进行管理，并能完全了解其使用情况。

NetScaler VPX 的虚拟 CPU 许可

以前，NetScaler VPX 许可证是根据实例的带宽消耗进行分配的。NetScaler VPX 只能根据其绑定的许可证版本使用特定的带宽和其他性能指标。要增加可用带宽，您必须升级到提供更多带宽的许可证版本。在某些情况下，带宽要求可能较低，但对其他 L7 性能（如 SSL TPS 和压缩吞吐量）的要求较高。在这种情况下，升级 NetScaler VPX 许可证可能不合适。但您可能仍然需要购买具有大带宽的许可证，以解锁 CPU 密集型处理所需的系统资源。NetScaler Console 现在支持根据虚拟 CPU 要求为 NetScaler 实例分配许可证。

在基于虚拟 CPU 使用的许可功能中，许可证指定了特定 NetScaler VPX 有权使用的 CPU 数量。因此，NetScaler VPX 只能从许可证服务器检出在其上运行的虚拟 CPU 数量的许可证。NetScaler VPX 根据系统中运行的 CPU 数量检出许可证。NetScaler VPX 在检出许可证时不会考虑空闲 CPU。

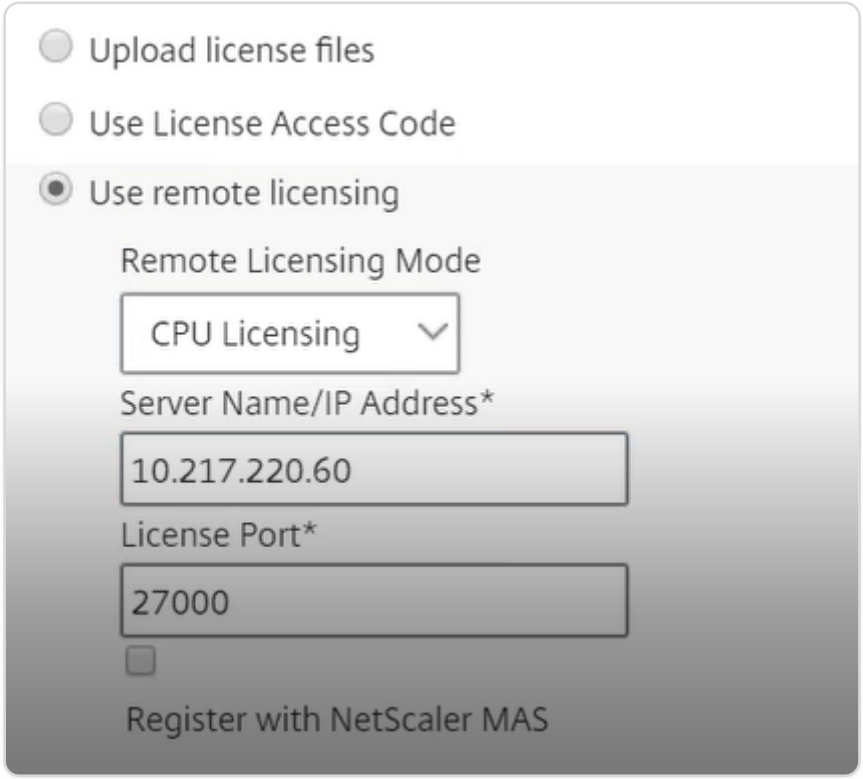
© 1997–2026 Citrix Systems, Inc. All rights reserved.

与池化许可证容量和 CICO 许可功能类似，NetScaler Console 许可证服务器管理着一套独立的虚拟 CPU 许可证。同样，虚拟 CPU 许可证管理的三个版本是标准版、高级版和白金版。这些版本解锁的功能与带宽许可证版本解锁的功能相同。

虚拟 CPU 数量或许可证版本可能会发生变化。在这种情况下，您必须在发起新许可证请求之前始终关闭实例。检出许可证后重新启动 NetScaler VPX。

使用 GUI 在 NetScaler VPX 中配置许可服务器：

1. 在 NetScaler VPX 中，导航到 **System > Licenses**，然后单击 **Manage Licenses**。
2. 在 **License** 页面上，单击 **Add New License**。
3. 在 **Licenses** 页面上，选择 **Use remote licensing** 选项。
4. 从“**远程许可模式**”列表中选择“**CPU 许可**”。
5. 键入许可证服务器的 IP 地址和端口号。
6. 单击“**继续**”。

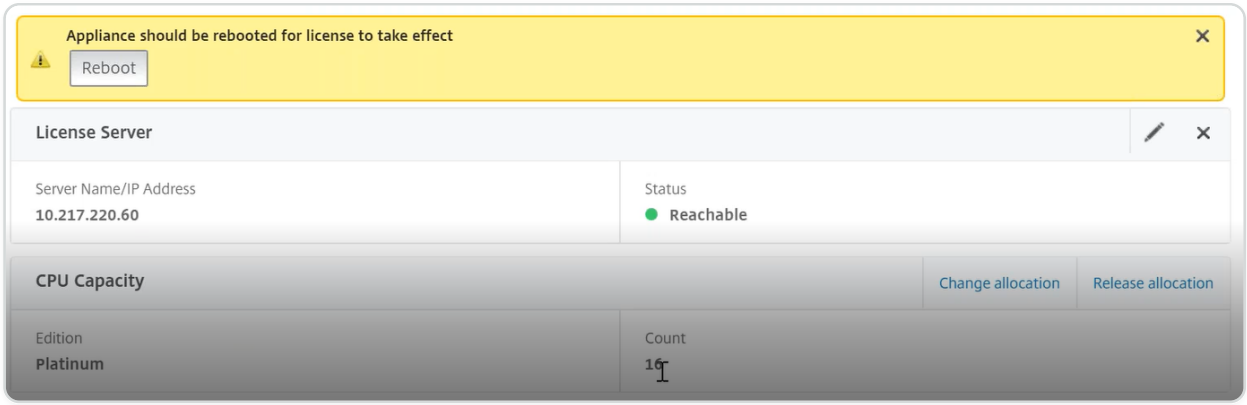


注意

您必须始终将 NetScaler VPX 实例注册到 NetScaler Console。如果尚未完成，请启用“**注册到 NetScaler Console**”并键入 NetScaler Console 登录凭据。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. 在“**分配许可证**”窗口中，选择许可证类型。该窗口显示总虚拟 CPU 和可用虚拟 CPU，以及可分配的 CPU。单击“**获取许可证**”。
8. 在下一页上单击“**重新启动**”以申请许可证。



注意

您还可以释放当前许可证并从其他版本中签出。例如，您已在实例上运行标准版许可证。您可以释放该许可证，然后从高级版中签出。

使用 CLI 在 NetScaler VPX 许可证中配置许可服务器

在 NetScaler VPX 控制台中，键入以下命令以执行以下两项任务：

1. 要将许可服务器添加到 NetScaler VPX：

```
add licenseserver <IP address of the license server>
```

2. 要申请许可证：

```
set capacity -vcpu - edition premium
```

当出现提示时，通过键入以下命令重新启动实例：

```
reboot -w
```

更新许可服务器 IP 地址

您可以在 NetScaler VPX 实例中更新许可服务器 IP 地址，而不会对实例上分配的许可带宽和数据丢失造成任何影响。要更新许可服务器 IP 地址，请在 NetScaler VPX 实例上键入以下命令：

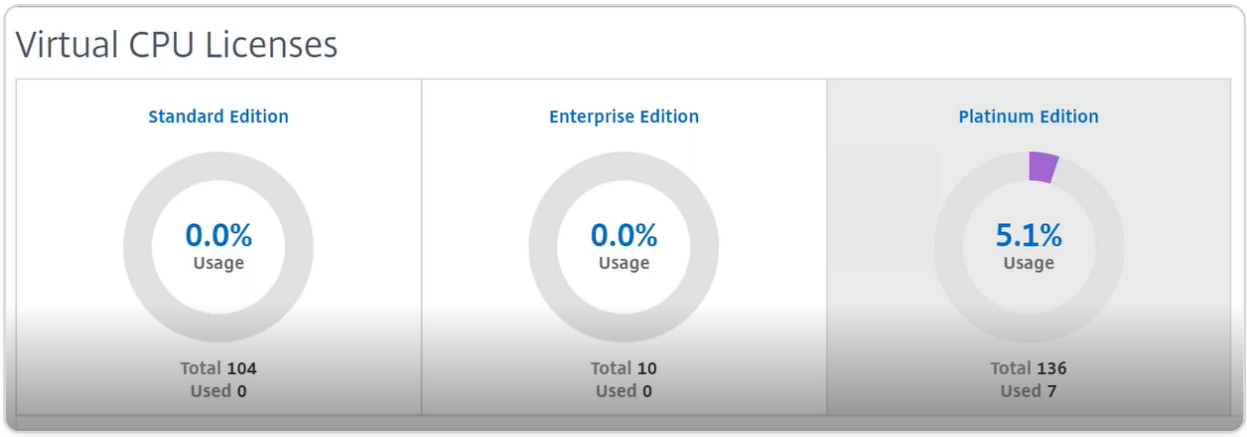
```
add licenseserver <licensing server IP address> -forceUpdateIP
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

此命令连接到新服务器并释放与以前的许可服务器关联的资源。

在 NetScaler Console 上管理虚拟 CPU 许可证

1. 在 NetScaler Console 中，导航到 **基础架构 > 池化许可 > 池化虚拟CPU**。
2. 此页面显示为每种许可证版本分配的许可证。
3. 单击每个圆环图中的数字以查看正在使用此许可证的 NetScaler 实例。



NetScaler CPX 的虚拟 CPU 许可

在预置 NetScaler CPX 实例时，您可以根据实例上的 CPU 使用情况，将 NetScaler CPX 实例配置为从许可证服务器签出许可证。

NetScaler CPX 依赖于在 NetScaler Console 上运行的许可证服务器来管理许可证。NetScaler CPX 在启动时从许可证服务器签出许可证。当 NetScaler CPX 关闭时，许可证将签回许可证服务器。

您可以使用 'docker pull' 命令从 Quay 容器注册表下载 NetScaler CPX 映像，并将其部署到您的环境中。

NetScaler CPX 许可有三种许可证类型可用：

1. NetScaler CPX 和 VPX 支持的虚拟 CPU 订阅许可证
2. 池化容量许可证
3. 仅适用于 NetScaler CPX 的 CP1000 许可证，支持从单个到多个 vCPU

在预配 NetScaler CPX 实例时配置 vCPU 订阅许可证：

指定 NetScaler CPX 实例使用的 vCPU 许可证数量。

- 此值通过 Docker、Kubernetes 或 Mesos/Marathon 作为环境变量输入。
- 目标变量是“CPX_CORES”。NetScaler CPX 支持 1 到 16 个核心。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要指定 2 个核心，您可以按如下方式执行 docker run 命令：

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e
EULA=yes -e CPX_CORES=2
```

在预配 NetScaler CPX 实例时，在 **docker run** 命令中将 NetScaler 许可服务器定义为环境变量，如下所示：

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e
EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT>
cpx:11.1
```

其中，

- *\<LS_IP_ADDRESS\>* 是 NetScaler 许可服务器的 IP 地址。
- *\<LS_PORT\>* 是 NetScaler 许可服务器的端口。默认情况下，端口为 27000。

注意

默认情况下，NetScaler CPX 实例从 vCPU 订阅池中检出许可证。如果实例以“n”个 CPU 运行，则 NetScaler CPX 实例会检出“n”个许可证。

在预配 NetScaler CPX 实例时配置 NetScaler 池化容量或 CP1000 许可证：

如果您想使用池化许可（基于带宽）或 NetScaler CPX 私有池（CP1000 或基于私有池）为 NetScaler CPX 实例签出许可证，则必须相应地提供环境变量。

例如，

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e
EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> -e
PLATFORM=CP1000 cpx:11.1
```

CP1000。此命令触发从 CP1000 池（NetScaler CPX 私有池）签出。然后，NetScaler CPX 实例会为 CPX_CORES 指定的“n”个核心检索“n”个实例。最常见的用例是指定 n = 1 以签出单个实例。多核 NetScaler CPX 用例签出“n”个 vCPU（其中“n”为 1 到 7）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e
EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> -e
BANDWIDTH=2000 cpx:11.1
```

池化容量。此命令从实例池中签出一个许可证，并从高级带宽池中消耗 1000 Mbps 带宽，但仍允许 NetScaler CPX 运行高达 2000 Mbps。在池化许可中，前 1000 Mbps 不收费。

注意

从带宽池签出时，请根据下表中的详细信息，为所需的目标带宽指定相应的 vCPU 数量：

核心数 (VCPU)	最大带宽
1	1000 兆比特每秒
2	2000 兆比特每秒
3	3500 兆比特每秒
4	5000 兆比特每秒
5	6500 兆比特每秒
6	8000 兆比特每秒
7	9300 兆比特每秒

出现问题时的预期行为

以下是许可服务器和 NetScaler 实例在遇到所述问题时的预期行为：

许可服务器停止响应

重要提示：

文件许可系统（也称为手动管理的授权）传统上用于激活各种本地组件，将于 April 15, 2026 终止生命周期 (EOL)。许可证激活服务 (LAS) 是用于激活 Citrix 产品套件中产品的下一代技术。在 April 15, 2026 之后，LAS 将是激活和许可 NetScaler 实例的唯一方式，支持 NetScaler Flexed 许可证 (CPL/UHMC)、旧版 NetScaler 池许可证和 NetScaler 固定期限带宽许可证。为了获得支持，您的 NetScaler 和 NetScaler Console 部署必须是与 LAS 兼容的版本。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

与 LAS 兼容的最低 NetScaler® 版本为：

- NetScaler ADC：14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1-51.x、13.1-60.x
- NetScaler Console Service：自 2025 年 9 月初起支持。
- NetScaler Console 本地部署：14.1-51.x

  注意： Console 本地部署对 LAS 的支持始于 14.1-51.x 版本。但是，自 April 15 2026 起，Console 本地部署 14.1-51.x 及更高版本和 13.1-60.x 及更高版本将弃用基于文件的许可。如果您升级到 Console 本地部署 14.1-51.x 版本或 13.1-60.x 版本或更高版本，您可以继续使用基于文件的许可，直到 15th April 2026。但是，您必须在 15th April 2026 之前升级到 Console 本地部署 14.1-51.x 或更高版本，并切换到 LAS，因为 Console 本地部署 13.1 不支持 LAS。

所有其他形式的旧版 NetScaler 许可证，例如池化 vCPU、CICO、永久许可证，将不支持 LAS。升级到上述软件版本后，使用没有有效维护的永久许可证的 NetScaler 实例将变为未授权状态。
在法律或法规禁止的情况下，基于 LAS 的许可证可能不适用于客户。
如果您有任何疑问或疑虑，请联系客户服务。如果不遵守这些要求，Citrix 可能会限制或暂停您的 Citrix 维护，且不承担任何责任，此外，Citrix 还可能依法或衡平法采取其他补救措施。在法律或法规禁止的情况下，这些要求不适用。
在继续之前，请阅读以下说明。

警告

许可证服务器无响应。NetScaler 将以当前容量继续运行 30 天。30 天后，如果与许可证服务器的连接未恢复，NetScaler 将失去其当前容量并停止处理流量。如果在 30 天内恢复连接，NetScaler 将以当前容量继续运行并继续处理流量。

NetScaler 池化实例停止响应

如果 NetScaler 池化实例停止响应且许可证服务器处于正常状态，许可证服务器会在 10 分钟后签入所有 NetScaler 实例的许可证。当实例重新启动时，它会发送请求以从许可证服务器签出所有许可证。

许可证服务器和 NetScaler 池化实例都停止响应

如果许可证服务器和 NetScaler 池化实例都重新启动并重新建立连接，许可证服务器会在 10 分钟后签入所有许可证，NetScaler 池化实例会在重新启动完成后自动签出许可证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler 池化实例正常关机

在正常关机期间，您可以选择签入许可证，或保留在正常关机前分配的许可证。如果您选择签入许可证，NetScaler 池化实例在重新启动后将处于未授权状态。如果您选择保留许可证，它们会在实例关机时签入到许可证服务器。实例重新启动后，它会重新建立与许可证服务器的连接，并按照保存的配置签出许可证。

如果系统重新启动，并且由于池中没有可用容量而导致签出失败，NetScaler 会检查 NetScaler Console 池许可证的库存并签出任何可用容量。如果 NetScaler 未按配置以全容量运行，则会触发 SNMP 警报以通知用户此情况。如果带宽池中没有可用容量，则池实例将变为未授权状态。

网络连接问题

错误消息 (系统日志)
许可证服务器无响应。

如果许可证服务器和 NetScaler 池化实例处于正常状态但网络连接丢失，实例将以当前容量继续运行 30 天。30 天后，如果与许可证服务器的连接未恢复，实例将失去其容量并停止处理流量，并且许可证服务器会签入所有许可证。在许可证服务器重新建立与 NetScaler 实例的连接后，实例会再次签出许可证。

宽限期

当 NetScaler 池化实例处于正常状态且许可证服务器停止响应时，实例将以当前容量继续运行 30 天。如果 30 天后与许可证服务器的连接未恢复，实例将失去其容量并停止处理流量。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

管理系统设置

下表描述了**设置** > **管理**下可用的选项列表：

网络配置

网络配置	选项	描述
IP 地址、第二个 NIC、主机名和代理服务器	IP 地址	显示用于部署 NetScaler Console 的 NetScaler Console 网络配置 IP 地址详细信息
	第二个 NIC	使您能够配置第二个 NIC 以隔离 NetScaler Console 管理访问。有关详细信息，请参阅配置双 NIC 以访问 NetScaler Console
	主机名	使您能够为 NetScaler Console 分配主机名。有关详细信息，请参阅为 NetScaler Console 服务器分配主机名
	代理服务器	使您能够将 NetScaler Console 配置为代理服务器。有关详细信息，请参阅将 NetScaler Console 用作 API 代理服务器
静态路由		允许您配置静态路由，以在 NetScaler Console 和 NetScaler VPX 实例之间建立连接
NTP 服务器		确保 NetScaler Console 时钟与网络上的其他服务器具有相同的日期和时间设置。有关详

© 1997–2026 Citrix Systems, Inc. All rights reserved.

网络配置	选项	描述
		细信息，请参阅 配置 NTP 服务器
NetScaler Console 端口信息		使您能够了解 NetScaler Console 和 NetScaler 实例之间通信需要打开哪些端口。有关详细信息，请参阅 支持的端口

系统配置

系统配置	选项	描述
系统、时区、允许的 URL 和每日消息	基本设置	允许您修改系统设置，例如启用 `nsrecover` 登录、启用会话超时等
	时区	允许您修改 NetScaler Console 中使用的时区。默认时区为 UTC
	允许的 URL 列表	使您能够配置 URL 以向 NetScaler Console 发送不间断的请求。如果无需添加 URL，则可以将其配置为“none”值
	每日消息	使您能够在 NetScaler Console 中创建欢迎消息。您可以使用此功能为自己或登录到 NetScaler Console 的用户设置提醒消息。单击 **Enable Message**（启用消息），在消息框中键入消息，然后单击 **Save**（保存）
查看 NetScaler Console 指纹		使您能够复制唯一的 NetScaler Console 指纹 ID 以开始使用服务图

© 1997–2026 Citrix Systems, Inc. All rights reserved.

系统配置	选项	描述
配置客户身份		使您能够通过仅允许经过身份验证的客户或用户访问其网络来保护网络资源。有关详细信息，请参阅数据治理
CUXIP 设置		如果选中此复选框，则会收集使用情况统计信息，其唯一目的是改进 GUI。收到的数据仅供 Citrix 工程师使用，不会与任何人共享

系统维护

系统维护	描述
升级 NetScaler Console	使您能够通过 GUI 升级 NetScaler Console。有关详细信息，请参阅升级
重新启动 NetScaler Console	使您能够重新启动 NetScaler Console
关闭 NetScaler Console	使您能够关闭 NetScaler Console
灾难恢复	使您能够查看灾难恢复节点信息。有关详细信息，请参阅配置灾难恢复

数据清理

数据清理	选项	描述
系统和实例数据清理	系统	使您能够限制存储在 NetScaler Console 服务器数据库中的报告数据量。有关详细信息，请参阅配置系统清理设置
	实例事件	使您能够限制存储在 NetScaler Console 中的事件消息报告数据

© 1997–2026 Citrix Systems, Inc. All rights reserved.

数据清理	选项	描述
	实例系统日志	允许您限制数据库中存储的系统日志数据量。有关详细信息，请参阅配置实例系统日志清除设置
	网络报告	允许您限制存储在 NetScaler Console 中的网络报告数据

备份

备份	选项	描述
配置系统和实例备份	系统	允许您在执行系统备份之前配置初始备份设置。有关详细信息，请参阅系统备份设置
	实例	允许您在 NetScaler Console 上配置设置，以备份选定的 NetScaler 实例或多个实例。有关详细信息，请参阅配置实例备份设置

事件通知

事件通知	选项	描述
配置事件通知和摘要	事件通知	您可以向选定的用户组发送与系统相关功能的通知。这些系统功能分为事件类别，例如 SystemReboot、StatusPoll、SystemState 等。您可以配置 NetScaler Console 通过电子邮件、短信或 Slack 向您发送通知。这可确保您收到任何系统级活动的通知，例如数据存储超出限制或备份失败。
	事件摘要	使您能够获取重要系统和功能事件的综合报告

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL 设置

SSL 设置	描述
安装 SSL 证书	使您能够安装 SSL 证书和 SSL 密钥文件
查看 SSL 证书	使您能够查看 SSL 证书详细信息
配置 SSL 设置	有关详细信息，请参阅 配置 SSL 设置
SSL 证书	使您能够上传、下载或删除 SSL 证书或 SSL 密钥文件
密码组	有关详细信息，请参阅 配置密码组

配置功能

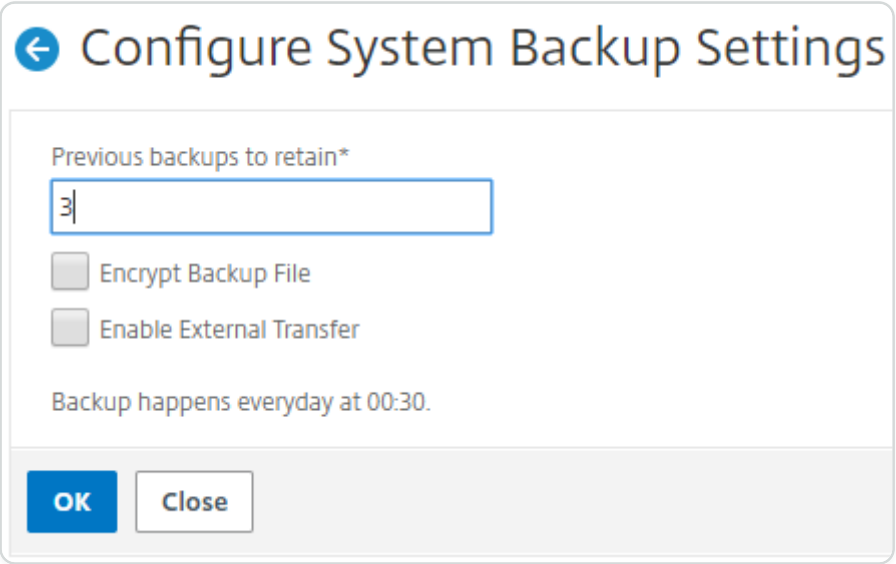
配置功能	描述
禁用或启用功能	您可以在 NetScaler Console 中启用或禁用功能。有关详细信息，请参阅 启用或禁用 NetScaler Console 功能

配置系统备份设置

在需要备份和恢复 NetScaler Console 之前，请设置初始的系统备份设置。

1. 导航到 **设置 > 管理**。在 **备份** 下，单击 **配置系统和实例备份**。
2. 在 **备份 > 系统** 页面上，指定以下内容：
   - 要保留的先前备份。您最多只能保留 10 个备份。
   - 选择 **加密备份文件** 以加密备份文件。
   - 选择 **启用外部传输** 以将备份文件的副本传输到另一个系统。当您要恢复配置时，必须首先将文件上传到 NetScaler Console 服务器，然后执行恢复操作。指定服务器、用户名和密码、端口、要使用的传输协议以及目录路径。要了解有关外部传输的更多信息，请参阅 将 NetScaler Console 备份文件传输到外部系统。
3. 单击 **确定**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



配置代理服务器设置

NetScaler Console® 允许您为出站连接配置代理服务器。您还可以为 SSL 检查代理拦截出站流量的 NetScaler Console 部署上传其 CA 证书。NetScaler Console 仅在上传其 CA 证书时才信任代理的证书。此功能可确保来自 NetScaler Console 的所有外部通信都通过安全受控的代理服务器。

此功能提供以下优势：

- 确保代理执行 SSL 拦截时通信安全。
- 防止遥测上传和 Cloud Connect 通信的连接问题。

要配置代理服务器，请导航到 **设置 > 管理**，然后单击 **代理服务器**。

代理服务器配置(/en-us/netscaler-application-delivery-management-software/media/proxy-server.png)

注意事项

- 确保 NetScaler Console 可以通过指定的 IP/端口访问代理服务器。
- 如果启用了 SSL 拦截，请在 NetScaler Console 中导入代理的 CA 证书，以避免连接失败。
- 在添加新详细信息之前，代理配置的更改可能会影响自动遥测上传或 Cloud Connect。

代理服务器配置

您可以使用 **代理服务器配置** 选项卡添加代理详细信息和凭据。

先决条件

- 将 `adm.cloud.com` 添加到允许列表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要添加代理服务器以路由所有出站流量，请执行以下步骤：

1. 导航到 **设置 > 管理**，然后单击 **代理服务器**。
2. 在 **代理服务器配置** 选项卡上，选择 **启用代理服务器**。
3. 指定代理服务器的 **IP 地址/主机名** 及其侦听 **端口**。

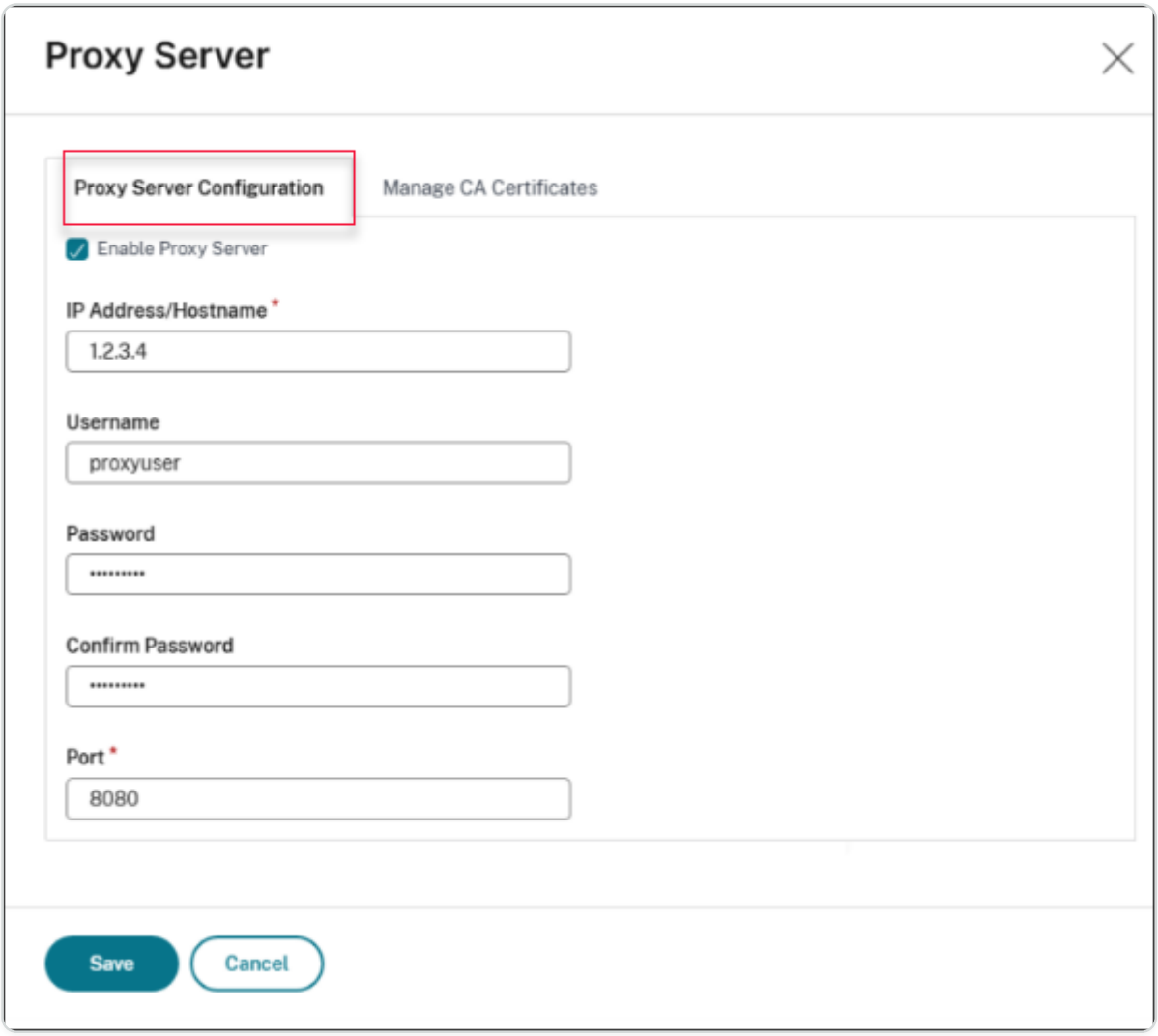
> **注意：**
>
> - 从 14.1 版本 build 56.x 开始，NetScaler Console 除了支持 IP 地址外，还支持使用 DNS 主机名 (FQDN) 进行代理配置。
> - 在以下环境中，使用主机名是有益的：
> - 使用基于 DNS 的冗余（例如 GSLB）来路由跨多个代理服务器的流量。
> - 没有负载均衡器，但依赖 DNS 来管理高可用性和故障转移。
> - 需要跨数据中心的可扩展且具有弹性的代理配置。
>
> 支持使用 DNS 主机名使 NetScaler Console 能够动态解析最合适的代理端点，从而提高可靠性并简化管理。

4. 如果代理需要凭据，请提供 **用户名** 和相应的 **密码**。

> **注意：**
>
> NetScaler Console 目前支持代理的基本身份验证。

5. 单击 **保存**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



管理 CA 证书

如果代理服务器执行 SSL 检查，请使用“**管理 CA 证书**”选项卡上传代理服务器的 CA 证书。您可以根据需要添加或删除证书。

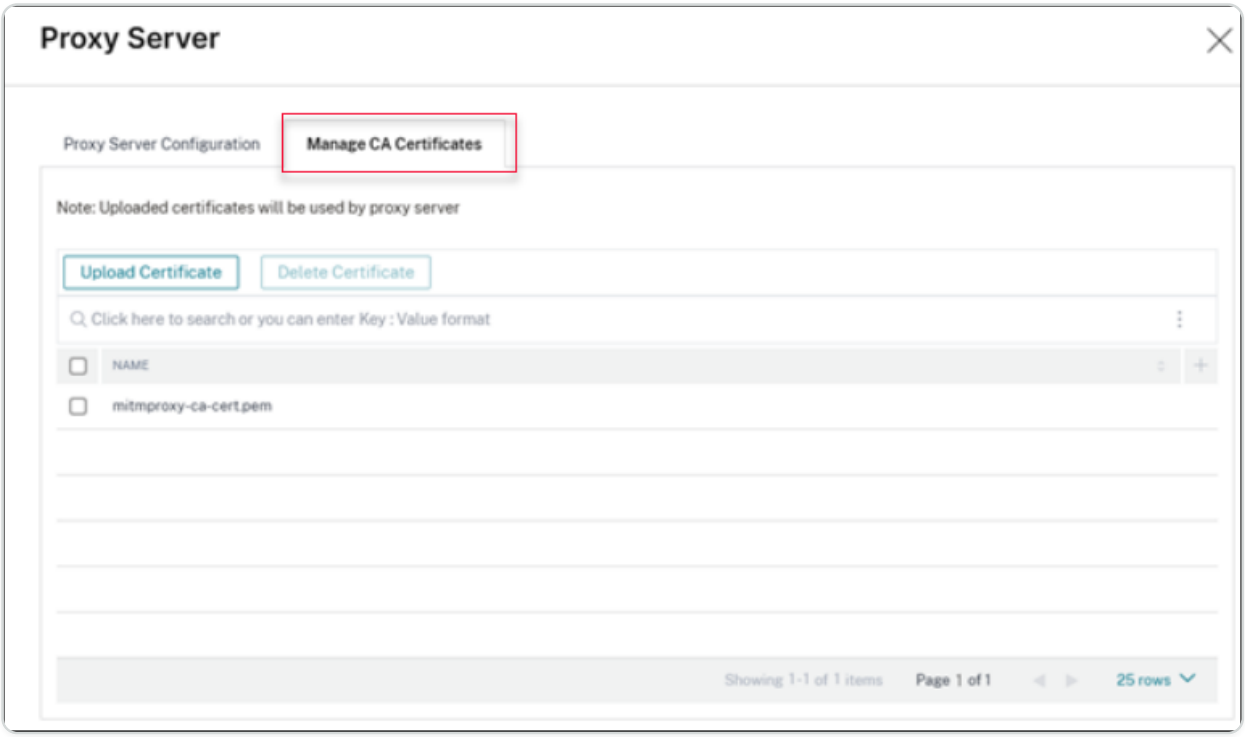
要上传代理服务器的 CA 证书，请执行以下步骤：

1. 导航到“**设置 > 管理**”，然后单击“**代理服务器**”。
2. 单击“**上传证书**”。

要删除代理服务器的 CA 证书，请执行以下步骤：

1. 导航到“**设置 > 管理**”，然后单击“**代理服务器**”。
2. 选择要删除的证书。
3. 单击“**删除证书**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



代理配置支持

NetScaler Console 支持以下代理部署模型，以适应不同的企业网络架构。您可以根据您的环境和安全要求，选择以下受支持的代理配置之一：

- 无代理
- 显式正向代理
- 显式 SSL 拦截代理
- 透明 SSL 拦截代理

重要

- 对于显式 SSL 拦截和透明 SSL 拦截代理部署，上传代理 CA 证书是强制性的。如果未上传代理 CA 证书，NetScaler Console 的出站流量将失败。
- 当使用透明 SSL 拦截代理时，请勿在本地 NetScaler Console 上配置代理。

无代理（直接互联网访问）

在此部署模型中，本地 NetScaler Console 不使用代理直接连接到 Citrix Cloud。

- 通信仅使用出站 HTTPS 流量。
- 本地 NetScaler Console 上无需代理配置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

显式正向代理（非拦截）

在显式正向代理设置中，来自本地 NetScaler Console 的出站流量通过代理服务器显式路由。

- NetScaler Console 流量通过配置的正向代理发送。
- 代理转发 HTTPS 流量而不解密 SSL/TLS。
- 必需：必须在本地 NetScaler Console 上配置代理详细信息。
- 可选：身份验证是可选的。用户可以在提供代理配置时提供用户名和密码进行身份验证。仅支持基本身份验证。

显式 SSL 拦截代理

在此部署模型中，代理通过终止并重新加密 SSL/TLS 连接来检查加密流量。

- 代理执行 SSL 解密和重新加密。
- 必需：NetScaler Console 上需要代理配置。
- 必需：代理 CA 证书必须上传到 NetScaler Console。有关详细信息，请参阅 管理 CA 证书。
- 可选：身份验证是可选的。用户可以在提供代理配置时提供用户名和密码进行身份验证。仅支持基本身份验证。

透明 SSL 拦截代理

在透明代理设置中，流量在网络级别被拦截，无需在客户端进行显式代理配置。

- SSL 检查透明地进行，无需在 NetScaler Console 上进行代理设置。
- 网络设备自动将流量重定向到代理。
- 必需：代理 CA 证书必须上传到 NetScaler Console 以进行 SSL 验证。有关详细信息，请参阅 管理 CA 证书。
- NetScaler Console 上不需要代理配置。

配置 NTP 服务器

您可以在 NetScaler Console 中配置网络时间协议 (NTP) 服务器，以使其时钟与 NTP 服务器同步。配置 NTP 服务器可确保 NetScaler Console 时钟与网络上的其他服务器具有相同的日期和时间设置。

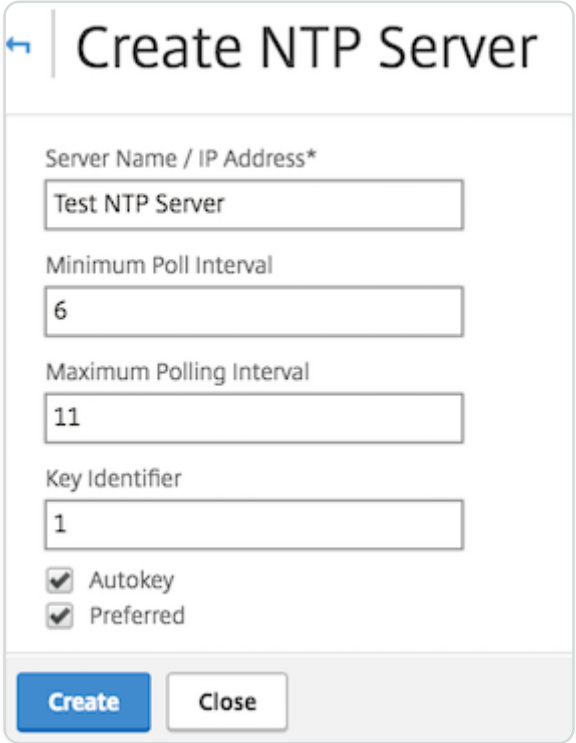
在 NetScaler Console 上配置 NTP 服务器：

1. 导航到 **“设置”>“NTP 服务器”**，然后单击**“添加”**。
2. 在**“创建 NTP 服务器”**页面上，输入以下详细信息：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **服务器名称/IP 地址** – 输入 NTP 服务器的域名或 IP 地址。添加 NTP 服务器后，无法更改名称或 IP 地址。
- **最小轮询间隔** – 指定传输的 NTP 消息之间间隔的最小值，以 2 的幂次方表示的秒数。例如，如果您希望最小轮询间隔为 64 秒（可表示为 2\^6），请输入 6。
- **最大轮询间隔** – 指定传输的 NTP 消息之间间隔的最大值，以 2 的幂次方表示的秒数。例如，如果您希望最大轮询间隔为 256 秒（可表示为 2\^8），请输入 8。
- **密钥标识符** - 输入可用于与 NTP 服务器进行对称密钥身份验证的密钥标识符。如果选择“自动密钥”，请勿添加密钥标识符。
- **自动密钥** - 如果要使用公钥身份验证与 NTP 服务器，请选择**“自动密钥”**。如果要添加密钥标识符，请勿选择。
- **首选** – 如果要将此 NTP 服务器指定为时钟同步的首选服务器，请选择此选项。仅当配置了多个服务器时，此选项才适用。

3. 单击**“创建”**。



在 NetScaler Console 上启用 NTP 同步：

1. 导航到 **“设置”>“NTP 服务器”**。
2. 单击 **NTP 同步** 并选择 **启用 NTP 同步** 复选框。
3. 单击 **确定**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

您可以在 /var/log 目录中的 `/var/log/ntpd.log` 文件中找到 NTP 日志消息。

升级 NetScaler Console

重要提示：

基于文件的许可将从 April 15, 2026 起终止支持。在此日期之前，所有 NetScaler (ADC, SVM) 实例都必须升级到兼容 LAS 的版本并转换为使用基于 LAS 的许可。 兼容 LAS 的最低 NetScaler 版本为：

- NetScaler ADC：14.1–51.80、13.1-60.29、13.1-37.247 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM：14.1–51.83、13.1-60.30

在 April 15, 2026 之后，在 NetScaler ADC 和 SVM 14.1-66.x 及更高版本中，NetScaler 升级之前将触发一项升级相关检查。此检查会验证您的 NetScaler (ADC, SVM) 是否仍在使用基于文件的许可，如果为真，则升级将被阻止并显示错误“NetScaler Upgrade Blocked: File-based licensing in use”。此预防措施可避免您的 NetScaler 实例在 April 15, 2026 之后继续升级并变为未授权状态。 请联系 Citrix 支持或您的 ATS 代表，了解如何解除升级阻止以及其中涉及的风险。

升级前检查

在从 NetScaler Console 触发升级之前，系统会自动执行升级前检查，以验证系统就绪情况和升级映像完整性。此检查可确保升级顺利进行，并降低在升级过程中遇到故障的可能性。

注意：

升级前检查功能从 NetScaler Console 14.1 版本 build 56.x 开始提供。通过本地 NetScaler Console 启动的每次升级之前，都会自动运行此检查。

如果检查检测到任何问题，NetScaler Console 会显示有关差异的详细信息，并提示您在继续升级之前解决这些问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

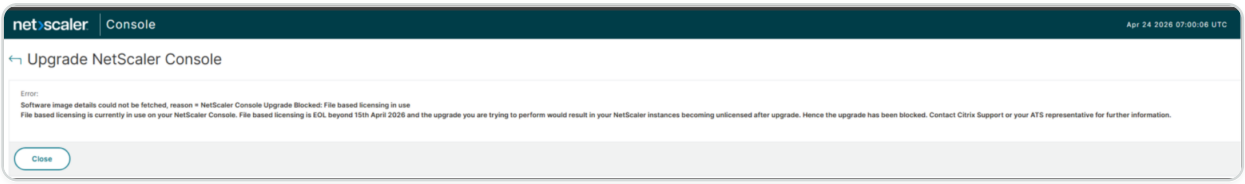
升级前检查包括以下验证：

- 内存可用性检查 – 验证 NetScaler Console 是否有足够的可用 RAM 来安全地执行升级。
- 磁盘空间检查 – 确保有足够的可用磁盘空间来提取和安装升级映像。
- 映像文件要求检查 – 确认升级所需的所有强制映像文件均可用。
- 映像文件完整性检查 – 验证升级映像的校验和，以确保文件完整且未损坏。
- LAS 迁移检查 - 验证 NetScaler Console 在 April 15, 2026 之后是否仍在使用基于文件的许可，用于池化或弹性许可类型。

  注意：

  LAS 迁移检查将于 April 15, 2026 生效，适用于池化和弹性许可类型。从该日期起，如果您尝试在仍使用基于文件的许可的情况下升级到 NetScaler Console 14.1-66.x 或更高版本，则不允许升级。执行此检查是为了避免您的本地 NetScaler Console 在 April 15, 2026 之后继续升级，以及 NetScaler 实例在升级后变为未授权状态。如果您遇到此限制，必须联系 Citrix 支持或您的 ATS 代表寻求指导。

  当 LAS 预升级检查失败时，将显示以下错误：



除了资源和文件验证之外，NetScaler Console 还会验证系统的运行状况和连接性，以确保安全升级。验证包括以下检查：

- 数据库完整性检查 – 检测丢失或损坏的数据库文件，以防止升级失败。
- 数据库流通道状态 – 确认流通道处于活动和运行状态。
- 辅助节点连接 – 确保与辅助节点进行正常通信以实现冗余。
- 无密码 SSH 验证 – 确认到辅助节点的无密码 SSH 登录正常工作。

预升级检查功能提供以下优势：

- 在升级前执行这些验证有助于防止因资源不足或映像文件损坏而导致的故障。
- 通过提前识别潜在问题，预升级检查可提高升级可靠性，并最大限度地减少因恢复或重新安装工作而导致的停机时间。

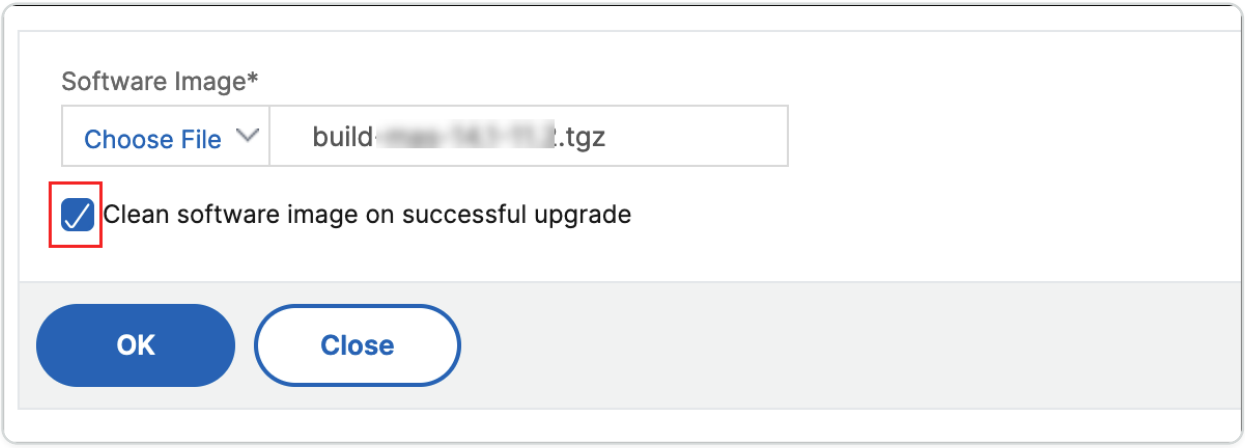
升级 NetScaler Console：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 导航到 **设置 > 管理**。在 **系统维护** 下，单击 **升级 NetScaler Console**。
2. 在升级 NetScaler Console 页面上，通过选择 **本地**（您的本地计算机）或 **设备** 上传新的映像文件。

   > **注意**
   >
   > 当您选择 **设备** 时，请确保升级映像在 NetScaler Console 中的 `/var/mps/mps_images` 可用。

   默认情况下，软件映像在成功升级后会被清理。
3. 单击 **确定**。



当 LAS 预升级检查失败时解除 NetScaler Console 升级阻止

仅当您必须立即继续进行 NetScaler Console 升级并且您理解并接受下面描述的许可影响时，才使用此选项。如果您的目标是在升级后保持获得许可，请联系 Citrix 支持或您的 ATS 代表。

先决条件： 您必须拥有 NetScaler Console 或 VM 的 shell 访问权限，以及在 `/var/tmp` 下创建文件的足够权限。

要解除升级阻止：

1. 登录到 NetScaler Console shell。
2. 创建旁路标志文件。

   ```
   touch /var/tmp/skip_las_checks
   ```
3. 重新运行升级。NetScaler Console 检测到 `skip_las_checks` 标志并跳过 LAS 验证，从而允许升级工作流继续。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要提示：

如果您绕过 LAS 升级前检查并继续操作，而基于文件的池化或弹性许可仍在被使用，则所有受管 NetScaler 实例在 NetScaler Console 升级后预计将变为未授权。

在 NetScaler Console 本地部署升级后，完成池化或弹性许可的 LAS 转换，并确认每个 NetScaler 实例都已正确获得许可。

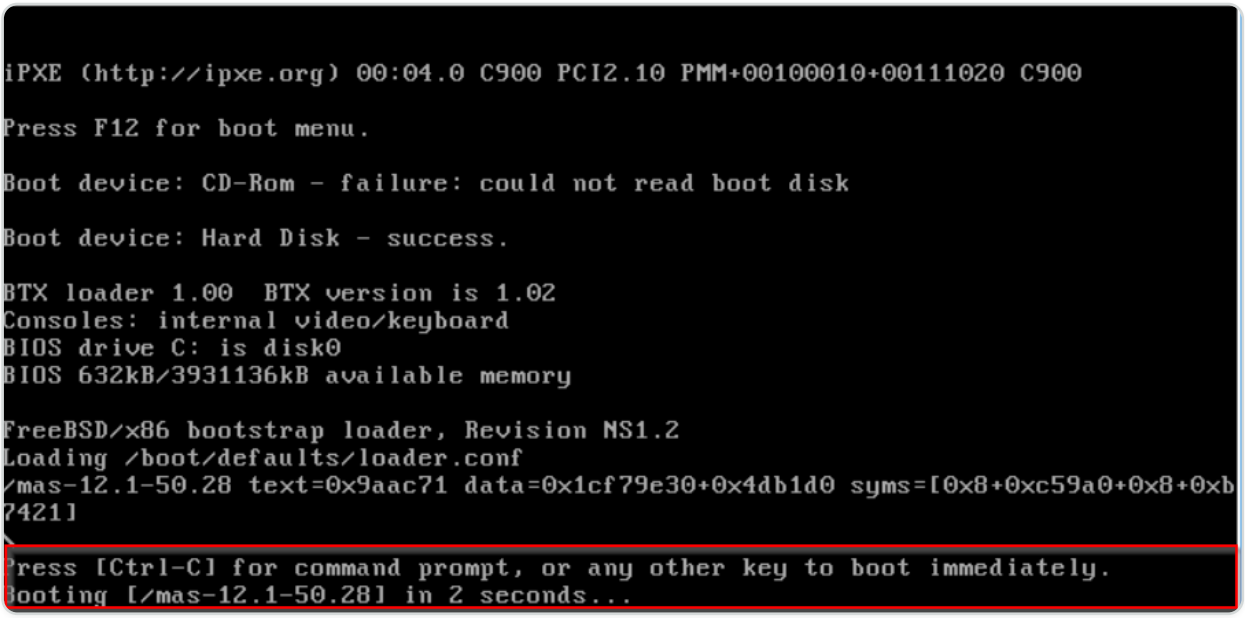
如果您需要替代方法或转换序列方面的帮助，请联系 Citrix 支持或您的 ATS 代表。

如何重置 NetScaler Console 的密码

在托管 NetScaler Console 的虚拟机管理程序上，重置其密码的步骤可能有所不同。如果您已更改默认密码并希望重置为默认密码，可以通过重新启动 NetScaler Console 节点来重置密码。

使用 XenCenter 的 Citrix Hypervisor™:

1. 使用 XenCenter 登录到 Citrix Hypervisor。
2. 选择 NetScaler Console 节点，右键单击，然后选择“**重新启动**”。
3. 在“**控制台**”选项卡上，按 **CTL + C** 中断启动序列。



4. 在 OK 提示符下运行 **boot -s** 命令。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
iPXE (http://ipxe.org) 00:04.0 C900 PCI2.10 PMM+00100010+00111020 C900

Press F12 for boot menu.

Boot device: CD-Rom - failure: could not read boot disk

Boot device: Hard Disk - success.

BTX loader 1.00  BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 632kB/3931136kB available memory

FreeBSD/x86 bootstrap loader, Revision NS1.2
Loading /boot/defaults/loader.conf
/mas-12.1-50.28 text=0x9aac71 data=0x1cf79e30+0x4db1d0 syms=[0x8+0xc59a0+0x8+0xb
7421]
\
Press [Ctrl-C] for command prompt, or any other key to boot immediately.
Booting [/mas-12.1-50.28] in 1 second...

Type '?' for a list of commands, 'help' for more detailed help.
OK _
```

NetScaler Console 重新启动并显示以下消息：

```
talk_to_backend: xn_num_q 1 max_q 16  err 0
xn0: backend features:xbd0: 122880MB <Virtual Block Device> at device/vbd/768 on
 xenbusb_front0
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
```

5. 按 **Enter** 键获取 /u@ 提示符。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
xn0: backend features:xbd0: 122880MB <Virtual Block Device> at device/vbd/768 on
 xenbusb_front0
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
u@
```

6. 使用以下命令挂载闪存分区：

   `mount /dev/ada0s1a /flash`

```
 xenbusb_front0
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
u@mount dev/ad0s1a /flash
u@
```

7. 使用以下命令创建文件：

   `touch /flash/mpsconfig/.recover`

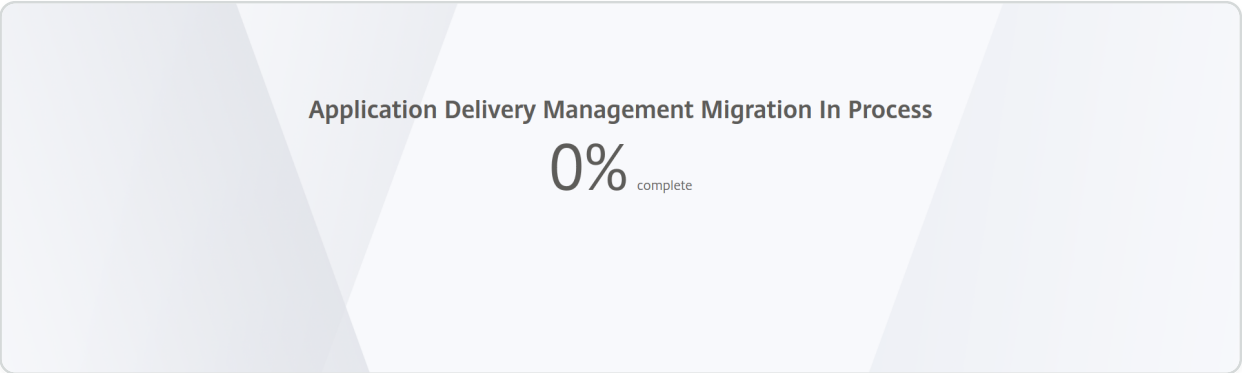
   密码现已重置为默认密码。

8. 运行 **Reboot** 命令以重新启动 NetScaler Console。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
\u@mount dev/ad0s1a /flash
\u@touch /flash/mpsconfig/.recover
\u@reboot
```

9. 访问 NetScaler Console GUI 并等待重新启动完成。



您现在可以使用 *nsroot/nsroot* 凭据从 GUI 登录，并使用 *nsrecover/nsroot* 从虚拟机管理程序登录。

注意

> 重新启动后，如果密码未重置为默认密码，请重复相同的过程（步骤 1 到步骤 7）。然后，运行以下命令并重新启动 NetScaler Console：

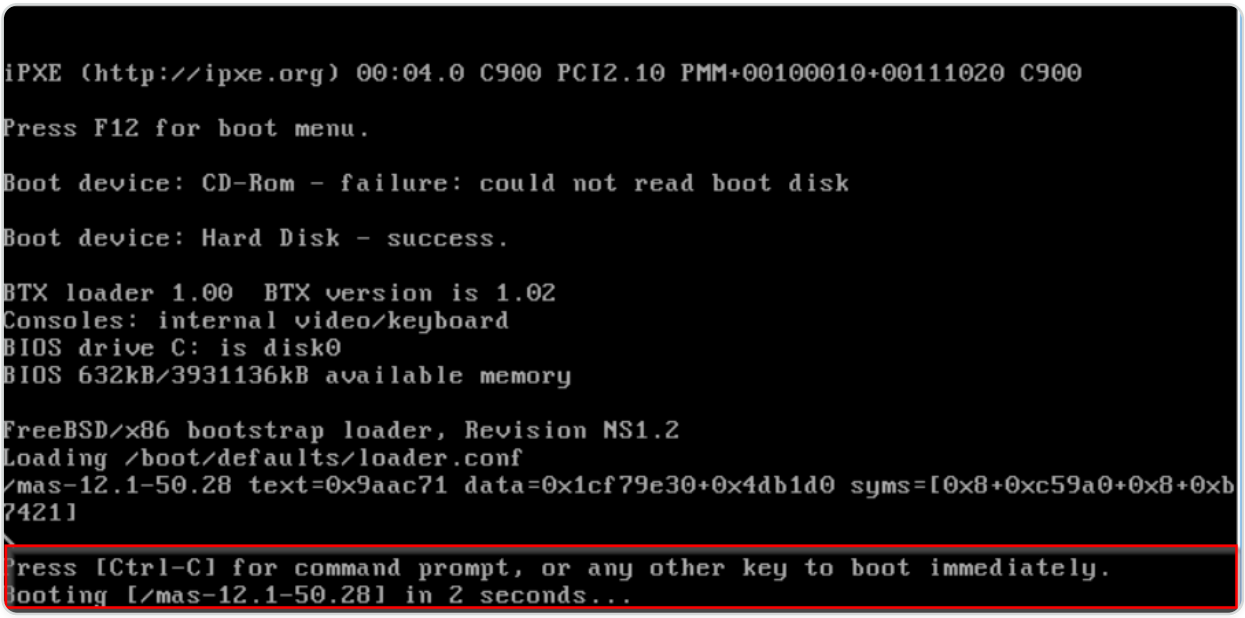
- `rm /flash/mpsconfig/master.passwd`
- `rm -rf /etc/passwd`

使用 vSphere 的 Esx：

1. 使用 vSphere 登录到 ESX。
2. 选择 NetScaler Console 节点，右键单击，然后选择 **Reboot**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在 **Console** 选项卡上，按 **CTL + C** 中断启动序列。



4. 在 OK 提示符下运行 **boot -s** 命令。

   NetScaler Console 重新启动。

5. 按 **Enter** 键获取 /u@ 提示符。
6. 使用以下命令挂载闪存分区：

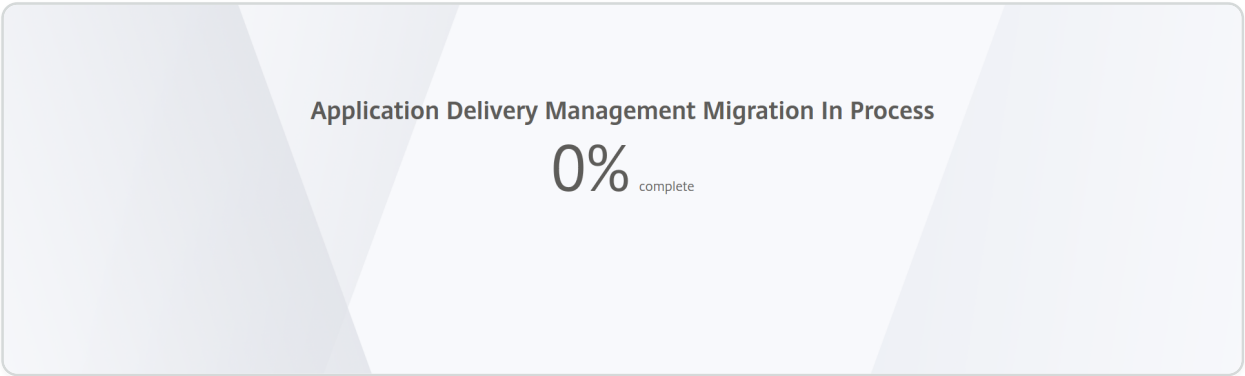
   `mount dev/da0s1a /flash`

7. 使用以下命令创建文件：

   `touch /flash/mpsconfig/.recover`

   密码现已重置为默认密码。

8. 运行 **Reboot** 命令以重新启动 NetScaler Console。
9. 访问 NetScaler Console GUI 并等待重新启动完成。



   您现在可以使用 *nsroot/nsroot* 凭据从 GUI 登录，并使用 *nsrecover/nsroot* 从 ESX 服务器登录。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

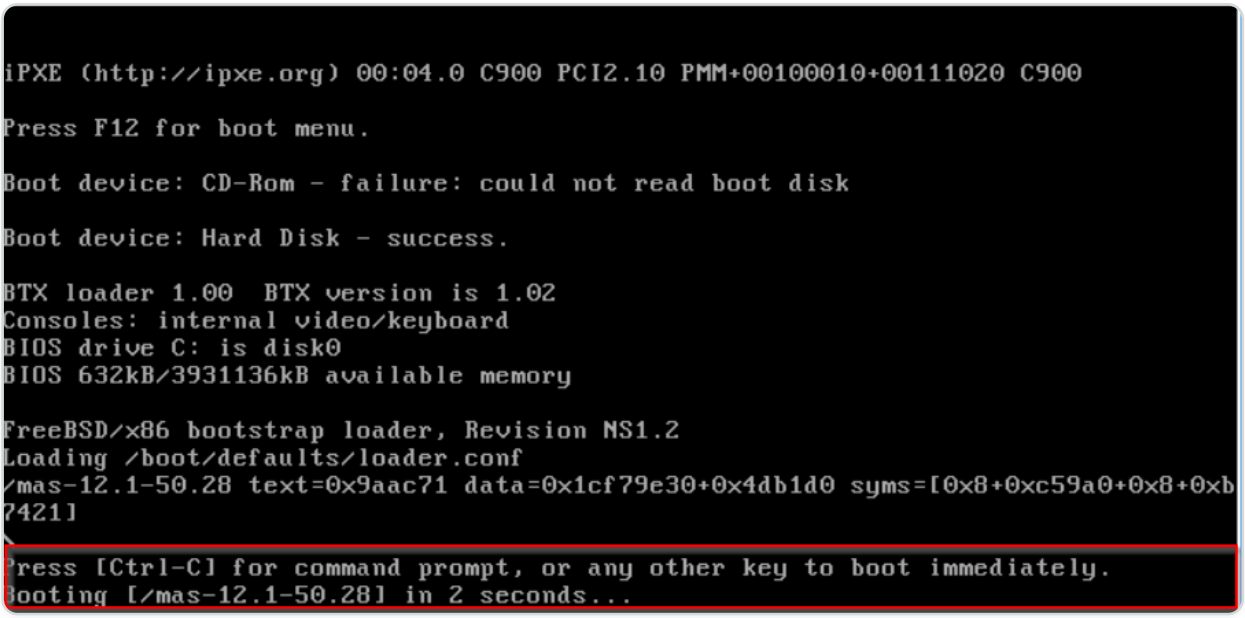
注意

> 重启后，如果密码未重置为默认密码，请重复相同的过程（步骤 1 到步骤 7）。然后，运行以下命令并重启 NetScaler Console：

- `rm /flash/mpsconfig/master.passwd`
- `rm -rf /etc/passwd`

使用 Hyper-v 管理器进行 Hyper-v 操作：

1. 使用 Hyper-v 管理器登录 Hyper-v。
2. 选择 NetScaler Console 节点，右键单击，然后选择 **Reboot**。
3. 在 **Console** 选项卡上，按 **CTL + C** 中断启动序列。



4. 在 OK 提示符下运行 **boot -s** 命令。

   NetScaler Console 重启。

5. 按 **Enter** 键获取 /u@ 提示符。
6. 使用以下命令挂载闪存分区：

   `mount dev/ad0s1a /flash`

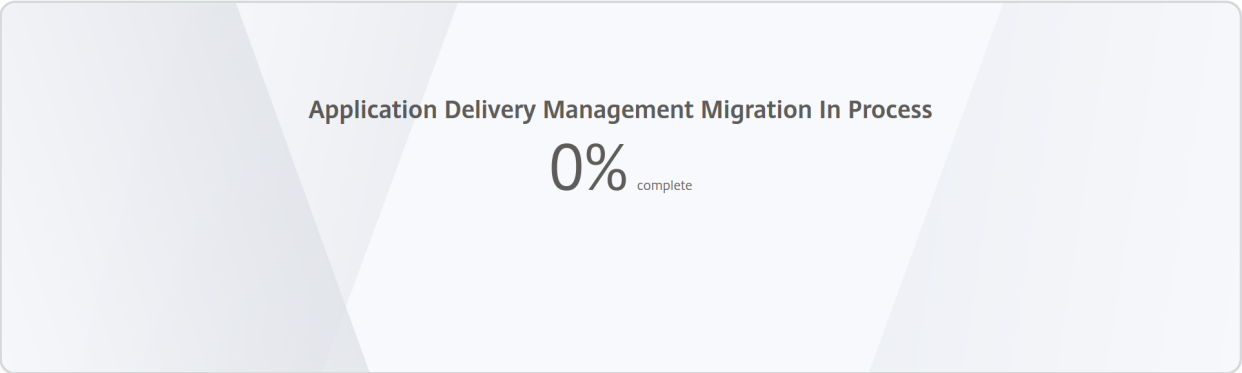
7. 使用以下命令创建文件：

   `touch /flash/mpsconfig/.recover`

   密码已重置为默认密码。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. 运行 **Reboot** 命令以重新启动 NetScaler Console。
9. 访问 NetScaler Console GUI 并等待重新启动完成。



您现在可以使用 *nsroot/nsroot* 凭据从 GUI 登录，并使用 *nsrecover/nsroot* 从 Hyper-V 管理器登录。

注意

> 重新启动后，如果密码未重置为默认密码，请重复相同的步骤（步骤 1 到步骤 7）。然后，运行以下命令并重新启动 NetScaler Console：

- `rm /flash/mpsconfig/master.passwd`
- `rm –rf /etc/passwd`

Linux KVM 服务器（使用任何 SSH 客户端通过 SSH 连接到 KVM 服务器）：

1. 使用 SSH 客户端登录到 KVM 服务器上的 NetScaler Console。
2. 重新启动 NetScaler Console。
3. 在显示 **Loading /boot/defaults/loader.conf** 消息后不久，按 **CTL + C** 中断启动序列。
4. 在 OK 提示符下，运行以下命令：

   `set console='comconsole,vidconsole'`
5. 运行 **boot -s** 命令以重新启动 NetScaler Console。
6. 在显示 **Enter full path of shell or RETURN for /bin/sh:** 消息后，按 **Enter** 键以获取 /u@ 提示符。
7. 使用以下命令挂载闪存分区：

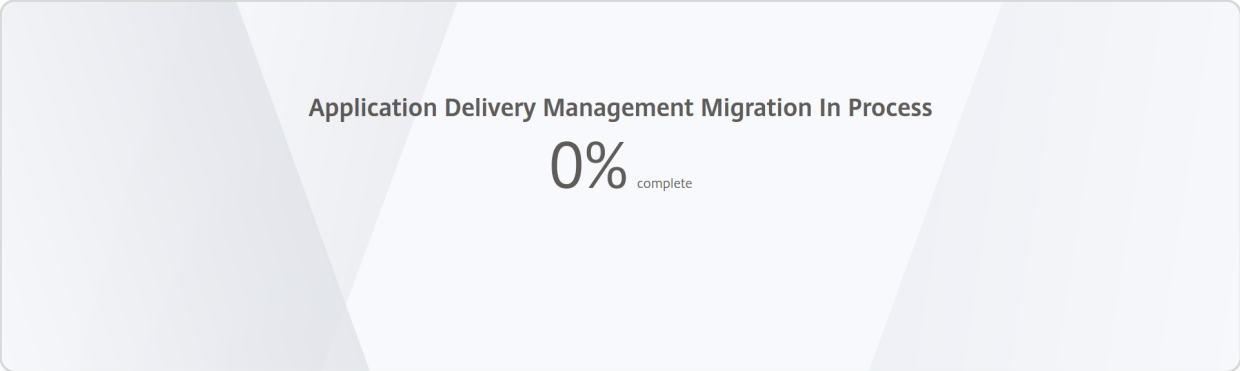
   `mount dev/vtbd0s1a /flash`
8. 使用以下命令创建文件：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`touch /flash/mpsconfig/.recover`

密码现已重置为默认密码。

9. 运行 **Reboot** 命令以重新启动 NetScaler Console。
10. 访问 NetScaler Console GUI 并等待重新启动完成。



您现在可以使用 *nsroot/nsroot* 凭据从 GUI 登录，并使用 *nsrecover/nsroot* 从 SSH 控制台登录。

注意

> 重新启动后，如果密码未重置为默认密码，请重复相同的步骤（步骤 1 到步骤 7）。然后，运行以下命令并重新启动 NetScaler Console：

- `rm /flash/mpsconfig/master.passwd`
- `rm -rf /etc/passwd`

配置辅助网卡以访问 NetScaler Console

您可以配置第二个网卡，用于隔离对 NetScaler Console 的管理访问。利用此第二个网卡功能，您可以根据需要选择如何隔离通过 NetScaler Console 接收和发送的流量。

考虑一个您希望隔离以下流量的场景：

- 将 NetScaler Console 及其管理的 NetScaler 实例之间的所有通信放在一个网络中。
- 将对 NetScaler Console 的管理访问放在另一个网络中。

在此场景中，作为管理员，您可以：

- 为 NetScaler Console 及其管理的 NetScaler 实例之间的流量配置一个 IP 地址。
- 配置另一个 IP 地址，用于管理 NetScaler Console 软件以在该软件中执行所有管理任务。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

如果 NetScaler Console 配置为 HA 对，则在第二个网卡上配置的管理 IP 地址将与主节点关联。

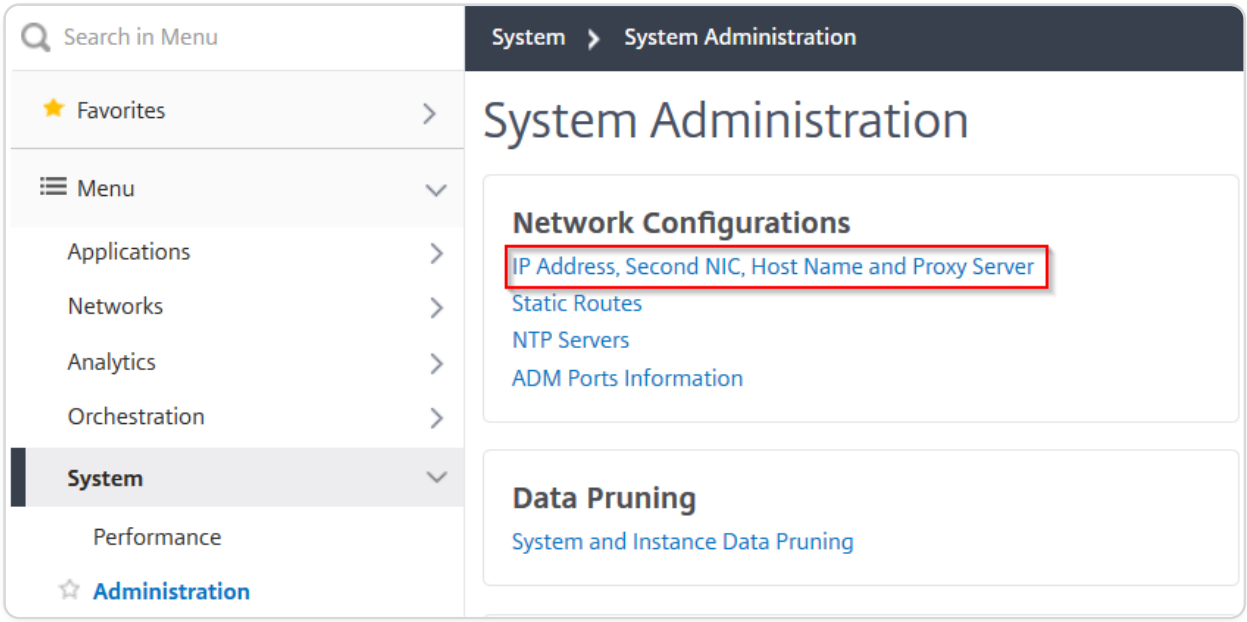
先决条件

- 确保您已在管理程序（Citrix Hypervisor、Microsoft Hyper-V、Linux KVM 或 VMware ESXi）上部署并配置 **NetScaler Console 13.0 Build 47.x 或更高版本**。
- 确保您已在管理程序（Citrix Hypervisor™、Microsoft Hyper-V、Linux KVM 或 VMware ESXi）上添加了第二个网卡。

要在 Citrix Hypervisor 上为网卡分配 IP 地址并创建辅助接口，请参阅 为网卡分配 IP 地址。

在 NetScaler Console 中配置第二个网卡

1. 登录到 NetScaler Console GUI。
2. 导航到 **设置 > 管理**。
3. 在 **网络配置** 下，单击 **IP 地址、第二网卡、主机名和代理服务器**。



显示 **Network Configuration** 页面。

4. 单击“Second NIC”选项卡并配置以下参数：

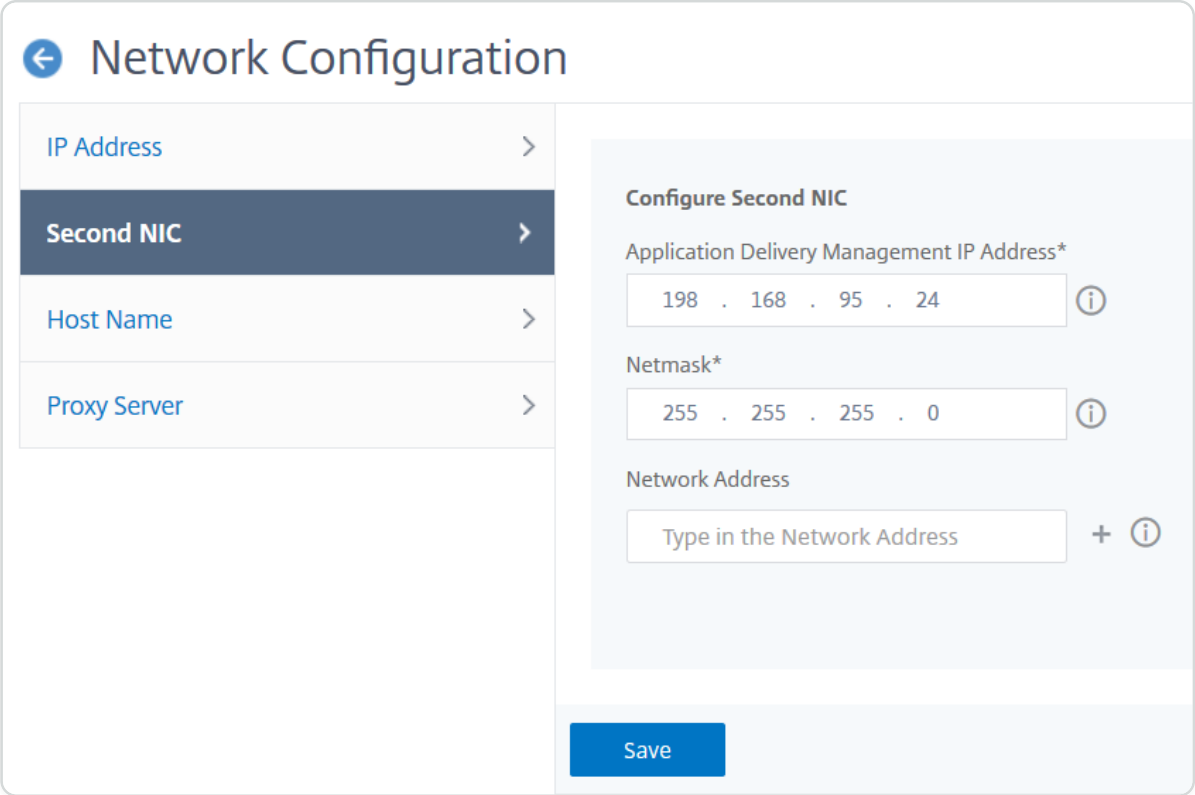
   a. **Application Delivery Management IP Address** – 输入有效的 IP 地址以访问 NetScaler Console。除了现有的管理 IP 地址之外，您还可以使用此 IP 地址访问 NetScaler Console。

   b. **Netmask** – 输入子网掩码地址以指定网络主机。默认地址为 255.255.255.0。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. **Network Address** – 输入 IP 地址以添加 NetScaler Console 的路由条目。单击 **+** 添加更多 IP 地址。此字段是可选的。

d. 单击 **Save**。



配置辅助网卡以访问 NetScaler® 代理

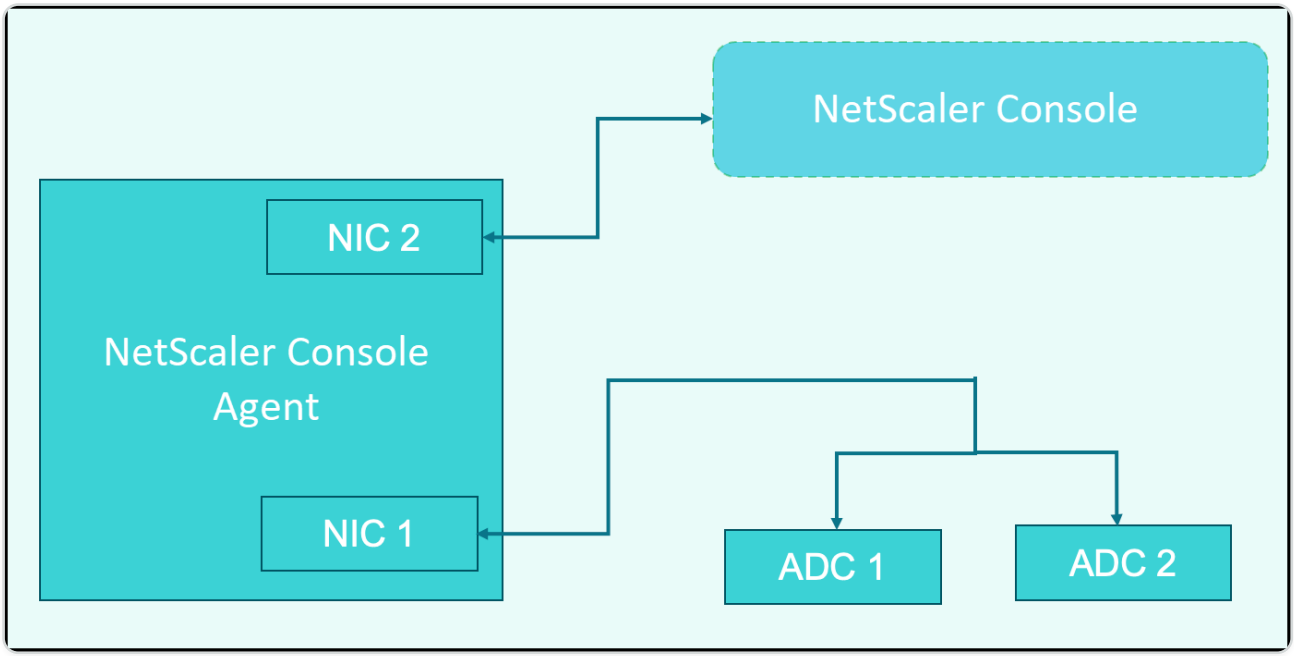
您可以在代理上配置两个网卡。使用双网卡架构，代理将能够：

- 建立代理与 NetScaler 实例之间的通信 - 您可以使用第一个网卡隔离通过 NetScaler Console 接收和发送的流量，并且还可以在另一个网络中，在 NetScaler Console 及其管理的 NetScaler 实例之间进行通信。
- 建立代理与 NetScaler Console 之间的通信 - 您可以使用第二个网卡管理网络上的 NetScaler Console 并执行管理任务

注意

您不能互换这两个网卡的功能和配置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



在此场景中，作为管理员，您可以：

- 配置 NetScaler Console 及其管理的 NetScaler 实例之间流量的 IP 地址。
- 配置用于管理 NetScaler Console 软件的 IP 地址，以在该软件中执行所有管理任务。

注意

并非强制要求为代理配置双网卡。它是可选的，并且仅当代理、NetScaler Console 和 NetScaler 实例之间的流量需要分离时才需要。

使用 CLI 修改 IPV4 网卡网络地址

1. 使用 SSH 客户端（例如 PuTTY）打开与 NetScaler 代理控制台的 SSH 连接。
2. 使用 **nsrecover/nsroot** 凭据登录并切换到 shell 提示符。
3. 运行命令 **ifconfig**。您可以看到已配置的两个网卡的详细信息 -
   - 网卡 1 – 用于代理与 NetScaler 之间的通信
   - 网卡 2 – 用于代理与 NetScaler Console 之间的通信

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bash-3.2# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
pflog0: flags=0<> metric 0 mtu 33152
        groups: pflog
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether a2:56:cd:d2:f8:8c
        hwaddr a2:56:cd:d2:f8:8c
        inet6 fe80::a056:cdff:fed2:f88c%1/1 prefixlen 64 scopeid 0x3
        inet 10.102.103.247 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
1/2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 32:89:fe:8c:8f:45
        hwaddr 32:89:fe:8c:8f:45
        inet6 fe80::3089:feff:fe8c:8f45%1/2 prefixlen 64 scopeid 0x4
        inet 10.102.103.250 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
```

4. 运行命令 **networkconfig**。将出现一个菜单，允许您设置或修改 IPV4 网络地址。

```
bash-3.2# /mps/networkconfig

--------------------------------------------------------------------------------
Citrix ADM Agent initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
--------------------------------------------------------------------------------
      1. Citrix ADM Agent Host Name [ns]:
      2. Citrix ADM Agent IPv4 address [10.102.103.247]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.103.1]:
      5. DNS IPv4 Address [10.102.166.70]:
      6. Second NIC IPv4 address [10.102.103.250]:
      7. Second NIC Netmask [255.255.255.0]:
      8. Second NIC Network address [10.102.103.251,10.102.103.252,10.102.103.252]:
      9. Second NIC Gateway IPv4 address [10.102.103.2]:
     10. Cancel and quit.
     11. Save and quit.
```

注意

\>

第二个网卡网络地址可以采用多个 IP 值。

5. 选择一个菜单项进行修改。保存并退出设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置 syslog 清除间隔

Syslog 是一种标准的日志记录协议。它包含两个组件：Syslog 审计模块，它运行在 Citrix NetScaler 实例上，以及 Syslog 服务器，它既可以运行在 NetScaler 实例的底层 FreeBSD 操作系统 (OS) 上，也可以运行在远程系统上。SYSLOG 使用用户数据报协议 (UDP) 进行数据传输。

Syslog 能够隔离生成信息的系统和存储信息的系统。您可以整合日志信息并从收集到的数据中获取洞察。您还可以配置 syslog 以记录不同类型的事件。

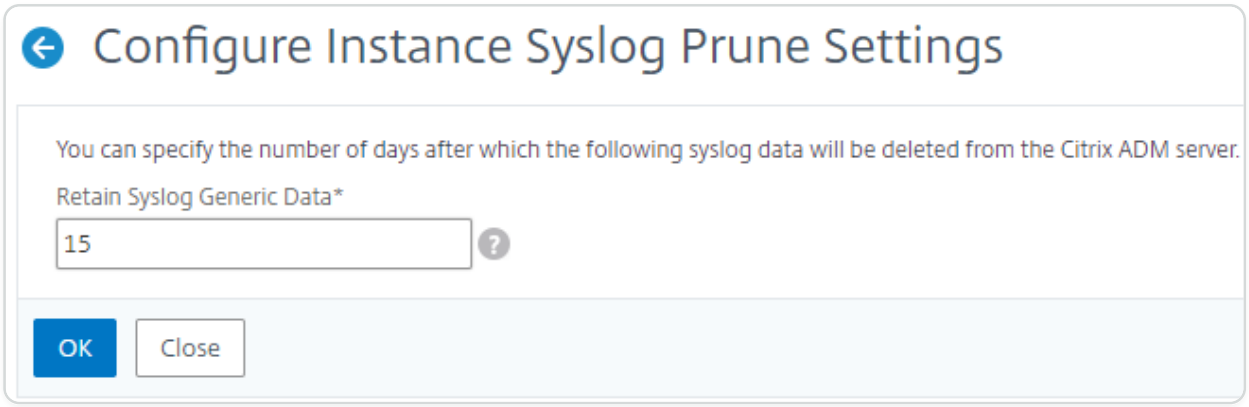
为了限制数据库中存储的 syslog 数据量，您可以指定清除 syslog 数据的间隔。您可以指定以下 syslog 数据将从 NetScaler Console 中删除的天数：

- 通用 Syslog 数据
- AppFirewall 数据
- NetScaler Gateway 数据

您还可以按 syslog 类型配置 NetScaler Gateway 清除间隔。此清除间隔优先于为保留 NetScaler Gateway 数据而配置的清除间隔。

配置 NetScaler Console 的 syslog 清除间隔设置：

1. 导航到 **设置 > 数据存储 > 数据保留策略**。**数据清除** 页面随即显示。单击 **实例 Syslog**。
2. 在 **配置实例 Syslog 清除设置** 页面中，指定 **保留 Syslog 通用数据（天）**。键入 NetScaler Console 保留通用 syslog 消息的天数。



配置系统修剪和事件修剪设置

为了限制存储在 NetScaler Console 软件数据库中的报告数据量，您可以对其进行修剪。您可以指定 NetScaler Console 保留网络报告数据、事件、审计日志和任务日志的时间间隔。默认情况下，此数据每 24 小时（00:00 时）修剪一次。

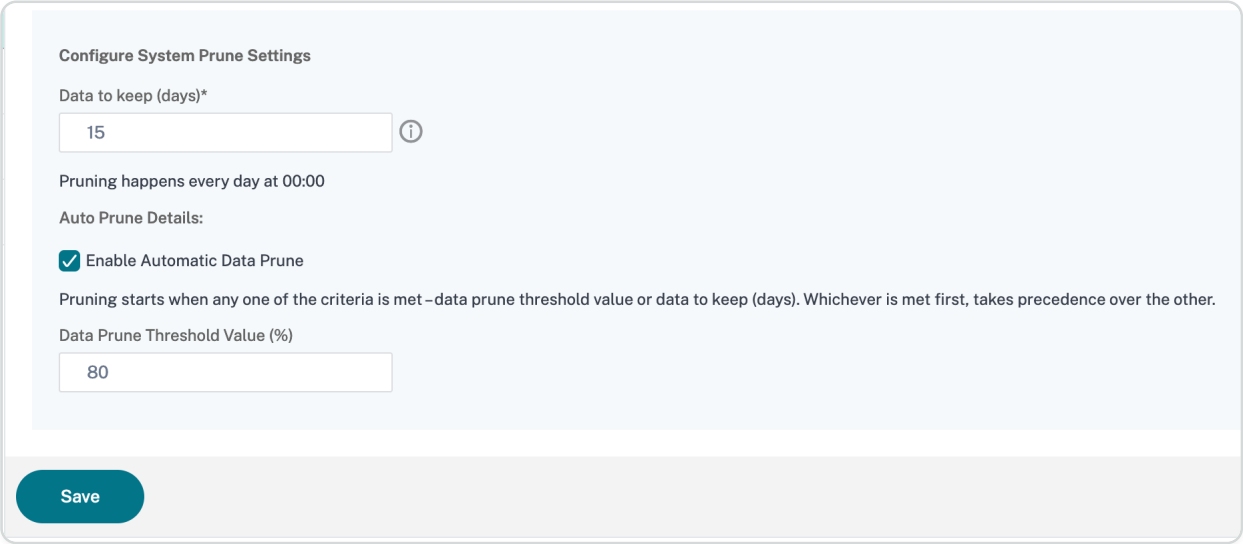
© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

您指定的值不能超过 30 天或少于 15 天。

配置性能报告的系统修剪设置：

1. 导航到 **设置** > **管理**。在 **数据修剪** 下，单击 **系统和实例数据修剪**。
2. 在 **配置系统修剪设置** 页面中，指定以下内容：
   - 保留数据的天数
   - 磁盘空间百分比（修剪阈值）
3. 单击 **确定**。



通过选择 **启用自动数据修剪** 复选框，可以启用自动修剪。当磁盘使用量超出配置的 **数据修剪阈值** 时，将触发警报并发送电子邮件。

注意

当满足以下任一条件时，修剪将开始：数据修剪阈值或要保留的数据（天数）。首先满足的条件优先于另一个条件。

配置和启用警报设置：

1. 导航到“**设置**”>“**SNMP**”。单击右上角的“**警报**”。
2. 选择要配置的警报（例如，diskUtilizationHigh），然后单击“**编辑**”。
3. 在“**配置警报**”页面中，指定以下内容：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **严重性**—选择严重性级别。
- **警报阈值**—键入用于计算事件严重性的值。
- **时间**—键入时间（以分钟为单位），在此时间之后要触发警报。

配置警报自动清除(/en-us/netscaler-application-delivery-management-software/media/configure-alarm-automatic-purging.png)

使用 NetScaler Console 配置事件清除设置

为了限制存储在 NetScaler Console 数据库中的事件消息数据量，您可以指定 NetScaler Console 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时（在 00:00 时）清除一次。

1. 导航到“**设置 > 管理 > 数据清除**”，然后单击“**系统和实例数据清除**”。单击“**实例事件**”。
2. 输入时间间隔（以天为单位），在此时间间隔内您希望将数据保留在 NetScaler Console 服务器上，然后单击“**保存**”。

为非默认用户启用 shell 访问

您可以在 NetScaler Console 中为非默认用户启用 shell 访问。您可以使用此功能启用并设置与实例的通信模式。

注意

默认情况下，非默认用户的 shell 访问已禁用。

在 NetScaler Console 中为非默认用户启用 shell 访问：

1. 在 NetScaler Console 中，导航到 **设置 > 管理**。
2. 在“**系统配置**”中，单击“**系统、时区、允许的 URL 和代理设置**”。
3. 在“**系统配置**”页面上，配置以下参数：
   - **与实例通信** - 选择通信协议。
   - **安全访问** - 为 NetScaler Console 启用安全访问。
   - **启用会话超时** - 指定保留非活动会话的时间段。
   - **允许基本身份验证** - 允许管理服务接受使用基本身份验证协议提供的凭据。
   - **启用 nsrecover 登录** - 在管理服务上启用 `nsrecover` 登录。
   - **启用证书下载** - 使您能够从添加的 NetScaler 下载证书。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **为非 nsroot 用户启用 Shell 访问** - 在 NetScaler Console 中为非默认用户启用 shell 访问。
- **提示用户凭据以登录实例** - 允许用户在从 NetScaler Console 登录实例时输入其用户凭据。
  - **提示凭据以进行 Stylebooks 操作** - 允许用户在 NetScaler 实例上使用 StyleBook 和配置包操作时输入其用户凭据。

> **注意：**
>
> 如果选中“**提示凭据以登录实例**”而未选中“**提示凭据以进行 Stylebook 操作**”，则不会提示用户为 NetScaler 实例上的 StyleBook 和配置包操作提供凭据。

4. 单击“**确定**”。

恢复无法访问的 NetScaler Console 服务器

NetScaler Console 现在提供了一个数据库维护工具，用于清理系统数据库。您现在可以启动 NetScaler Console 实用工具，连接到文件系统，删除一些组件，并使数据库可访问。NetScaler Console 恢复脚本是一个工具，通过清除旧的或未使用的数据库表和文件来帮助恢复文件系统中的空间。该工具可帮助您逐步浏览数据库表和文件，并显示文件系统中各个项目当前占用的空间。选择要删除的数据库表和文件后，该工具会在确认后从文件系统中删除它们。

如何在 NetScaler Console 独立部署中使用 NetScaler Console 数据库恢复脚本

在单服务器 NetScaler Console 部署中，使用以下过程连接到文件系统，删除一些组件，使数据库可访问，然后执行恢复操作。

1. 使用 SSH 客户端或您的虚拟机管理程序控制台，登录到 NetScaler Console 并键入以下命令：

```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

2. 当屏幕显示停止一些 NetScaler Console 进程的警告消息时，键入“y”并按 **Enter** 键。

   当系统确定可以删除数据库的哪些组件而不会影响系统的核心文件时，将显示以下屏幕。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
--------------------------------------------------------------------------------
************************** Citrix ADM Cleanup Utility **************************
--------------------------------------------------------------------------------

        This utility helps you gain disk space by performing cleanup.


                    Checking whether DB is accessible...

                              DB is accessible.

            Please wait. Gathering data. This will take some time.


                              <----------->
```

3. 屏幕显示数据库中的文件列表。键入“y”并按 Enter 键开始清理过程。

```
---------------------------------  SUMMARY  ----------------------------------

                  DB component                Current size
                  ------------                ------------

                  Analytics  ------------------  184.58 MB
                  Perf Reports  ----------------  43.73 MB
                  App Summary  -----------------  12.03 MB
                  App Health Summary  -----------  6.33 MB
                  App Counter Data  -------------  5.30 MB
                  Device Syslogs  --------------  56.00 KB
                  Device Events  ---------------  40.00 KB

                  Filesystem component        Current size
                  --------------------        ------------

                  Citrix ADM Images  -----------  15.51 GB
                  Core Files  -----------------  718.37 MB
                  Citrix ADC Images  ----------  453.32 MB
                  Techsupport Bundles  --------  439.35 MB
                  Device Backup  --------------  131.79 MB
                  Citrix ADM Backup  -----------  35.21 KB
                Citrix ADC VPX ESXi Images  -------  0.00 B
                  Citrix ADC SDX Images  ---------  0.00 B
                  Citrix ADC CPX images  ---------  0.00 B

--------------------------------------------------------------------------------

        Do you wish to proceed with cleanup?
        [y/n]:
```

4. 您可以选择需要清理的特定数据库组件并键入相应的数字。按 **Enter** 键。

   例如，要执行系统目录清理，请在 **DB 组件**选择菜单中选择选项 8，然后键入“y”并按 **Enter** 键以继续进行系统目录清理。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

NetScaler Console 包含称为系统目录的用户表。系统目录是 NetScaler Console 数据库中的一个位置，关系数据库管理系统在此存储架构元数据，例如有关表、列和内部记录的信息。系统目录中的表类似于常规表，它们会随着时间的推移积累膨胀和无效行，因此需要定期清理以获得最佳性能。定期维护这些表是一个好习惯。此活动不仅可以释放磁盘空间，还可以提高数据库的整体性能，从而提高 NetScaler Console 的性能。

```
-------------------------------------------------------------------------------
************************** Citrix ADM Cleanup Utility **************************
-------------------------------------------------------------------------------

                                DB components
                                -------------

        Enter the number corresponding to the menu entry.
        You can input multiple space separated numbers.
        E.g. '1 2 4' will select entries numbered 1, 2, and 4.

        [0]  Go back and start again
        [1]  Analytics --------------- 184.58 MB
        [2]  Perf Reports ------------ 41.84 MB
        [3]  App Summary ------------- 11.84 MB
        [4]  App Health Summary ------ 6.09 MB
        [5]  App Counter Data -------- 5.09 MB
        [6]  Device Syslogs ---------- 56.00 KB
        [7]  Device Events ----------- 40.00 KB
        [8]  Clean System Catalog
        [9]  Select all
        [10] Continue without selecting

        Your input: 8
        Are you sure you want to CLEAN SYSTEM CATALOG tables?

        [y/n]: y
```

清理实用程序提供清理数据库组件和文件组件的选项。您可以键入“1”到“9”之间的数字来选择任何文件组件，或者键入“11”并按 Enter 键来清理数据库组件。

注意

数字“11”表示您未选择任何要清理的文件组件，并且您将继续清理之前选择的数据库组件。在此示例中，它是“系统目录”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
--------------------------------------------------------------------------------
************************** Citrix ADM Cleanup Utility **************************
--------------------------------------------------------------------------------

                              Filesystem components
                              ---------------------

        Enter the number corresponding to the menu entry.
        You can input multiple space separated numbers.
        E.g. '1 2 4' will select entries numbered 1, 2, and 4.

        [0]  Go back and start again
        [1]  Citrix ADM Images ------- 15.51 GB
        [2]  Core Files -------------- 718.37 MB
        [3]  Citrix ADC Images ------- 453.32 MB
        [4]  Techsupport Bundles ----- 439.35 MB
        [5]  Device Backup ----------- 131.79 MB
        [6]  Citrix ADM Backup ------- 35.21 KB
        [7]  Citrix ADC VPX ESXi Images  0.00 B
        [8]  Citrix ADC SDX Images --- 0.00 B
        [9]  Citrix ADC CPX images --- 0.00 B
        [10] Select all
        [11] Continue without selecting

        Your input: 11
```

5. 在最终确认屏幕中再次键入“y”并按 **Enter** 键。

```
--------------------------------------------------------------------------------
************************** Citrix ADM Cleanup Utility **************************
--------------------------------------------------------------------------------
                              FINAL CONFIRMATION

                      These components will be cleaned.

                                DB components
                                -------------

                      >>  System Catalog

        No data has been deleted yet.

        If you choose to proceed, all ADM processes will be stopped
        for the remainder of the cleanup.

        Do you wish to proceed with cleanup?
        [y/n]:
```

系统目录已清理，这可能需要时间，具体取决于系统目录中表的大小。过程完成后，将显示摘要屏幕。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
--------------------------------------------------------------------------------
**************************** Citrix ADM Cleanup Utility ****************************
--------------------------------------------------------------------------------
----------------------------------  SUMMARY  ----------------------------------

                                DB components
                                -------------

          Component name              Present size     Size cleared
          --------------              ------------     ------------

          System Catalog  -------------  189.15 MB  -------  0.00 B
       Cleanup complete.
       Note that even empty tables in DB may appear to occupy some
       space, this is expected.


       To prevent potential unpredictable behavior, we STRONGLY recommend
       rebooting the ADM now.

       Do you want to REBOOT the ADM?
       [y/n]: 
```

6. 键入“y”并按 **Enter** 键以重新启动 NetScaler Console。

   确保在系统清理后重新启动 NetScaler Console。在 NetScaler Console 重新启动后，等待大约 30 分钟以完成内部数据库操作。然后您应该能够连接到 NetScaler Console 数据库。如果不能，请再次运行恢复脚本以释放更多空间。当 NetScaler Console 启动并运行时，它应该按预期工作。

> **注意**
>
> 清理后，系统目录表的当前大小永远不会等于零。这是因为只从表中删除了空行，即使清理后，表也可能包含一些有效条目。

如何将 NetScaler Console 数据库恢复脚本用于 NetScaler Console 高可用性部署

高可用性部署中 NetScaler Console 服务器的数据库系统处于连续同步模式。使用新的数据库恢复工具时，您无需在两台 NetScaler Console 服务器上重复此过程。

1. 使用 SSH 客户端或虚拟机管理程序的控制台登录到主节点。
2. 运行以下命令：

   `/mps/mas_recovery/mas_recovery.py`

3. 按照适用于 NetScaler Console 独立部署恢复脚本 的步骤 2 中的过程进行操作

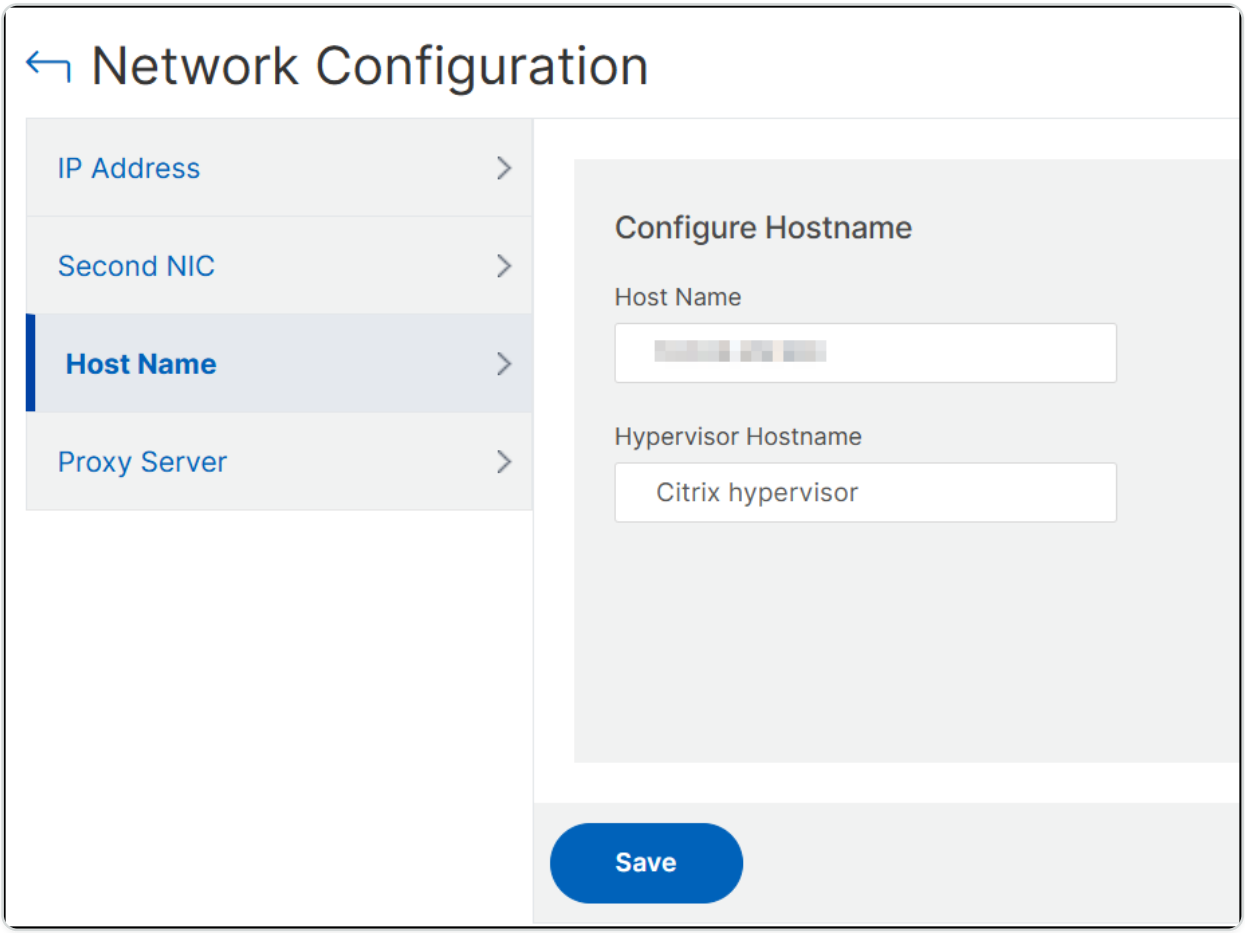
© 1997–2026 Citrix Systems, Inc. All rights reserved.

为 NetScaler Console 服务器分配主机名

为了识别 NetScaler Console 服务器，您可以为该服务器分配一个主机名。

为 NetScaler Console 服务器分配主机名：

1. 在 NetScaler Console 中，导航到**设置 > 管理**。
2. 在**网络配置**下，单击**IP 地址、第二块网卡、主机名和代理服务器**。
3. 选择**主机名**，输入主机名和管理程序主机名，然后单击**保存**。



注意：

您还可以在管理程序中使用 `networkconfig` 命令并更改主机名。

备份和恢复您的 NetScaler Console 服务器

您可以定期备份 NetScaler Console 服务器。您可以备份和恢复配置文件、实例详细信息、系统数据等。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要

Citrix 建议您使用相同版本的备份来恢复 NetScaler Console 服务器。例如，如果 NetScaler Console 版本为 13.0，请使用 13.0 NetScaler Console 备份来恢复服务器。

用户备份和恢复 NetScaler Console 服务器的权限是受限的。**设置 > 备份文件**页面仅对有权访问所有 NetScaler Console 功能的用户显示。用户只有在其访问策略具有所有权限时才能访问此页面。通常，超级用户有权访问所有 NetScaler Console 功能。
访问所有 NetScaler Console 功能(/en-us/netscaler-application-delivery-management-software/media/access-policy-for-all-adm-features.png)
有关详细信息，请参阅配置访问策略。
在升级之前，请出于预防目的备份 NetScaler Console 服务器配置文件。

备份包括以下组件：

- NetScaler Console 配置文件：
  - SNMP
  - Syslog 服务器配置文件
  - NTP 文件
  - SSL 证书
  - 控制中心文件
- NetScaler Console 服务器管理的 NetScaler 实例的备份。
- 配置审计模板。
- 存储在数据库中的系统数据：
  - 创建的租户和用户列表。
  - 外部身份验证服务器配置（LDAP、RADIUS 及其他）。
  - 创建的配置作业和作业模板。
- 存储在数据库中的基础设施和应用程序数据：
  - 来自已添加和已管理的 NetScaler 实例的数据。
  - 实例配置文件详细信息、版本详细信息、实例组详细信息等。
  - 管理员创建的静态应用程序（虚拟服务器组）。
- SNMP 设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

分析数据、事件、NetScaler Console 许可证和系统日志消息不包含在备份中。

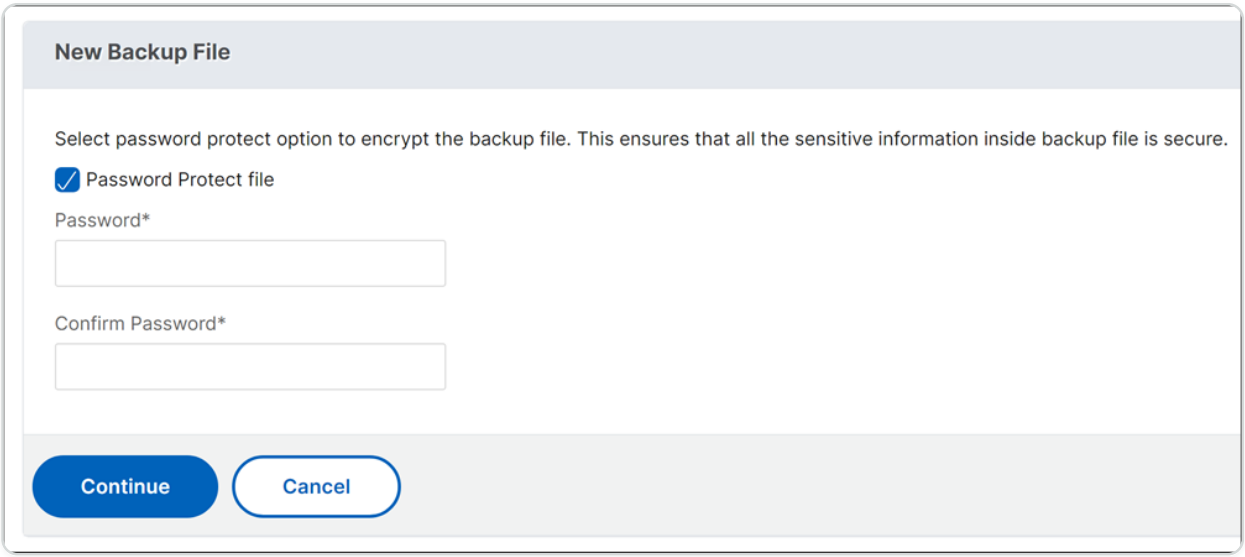
备份 NetScaler Console 配置

默认情况下，NetScaler Console 服务器每 24 小时（00:30）备份一次配置。您还可以安排和选择备份时间。此外，您可以将备份文件的副本移动到另一个系统。

备份以压缩的 TAR 文件形式存储，该文件也可以加密。默认情况下，服务器中保留三个备份文件。为避免磁盘空间不足问题，您可以在 NetScaler Console 服务器上最多存储 10 个备份文件。但是，我们建议您将备份文件的某些副本存储在服务器上或 (#transfer-a-citrix-adm-backup-file-to-an-external-system)，以作为预防措施。

备份 NetScaler Console 配置：

1. 导航到 **设置 > 备份文件**，然后单击 **备份**。
2. 要加密备份文件，请选中 **密码保护文件** 复选框，然后提供密码以加密文件。



将 NetScaler Console 备份文件传输到外部系统

您可以将备份文件的副本传输到另一个系统作为预防措施。当您要还原配置时，请先将文件上传到 NetScaler Console 服务器，然后执行 (#restore-the-citrix-adm-configuration-from-a-backup-file)。

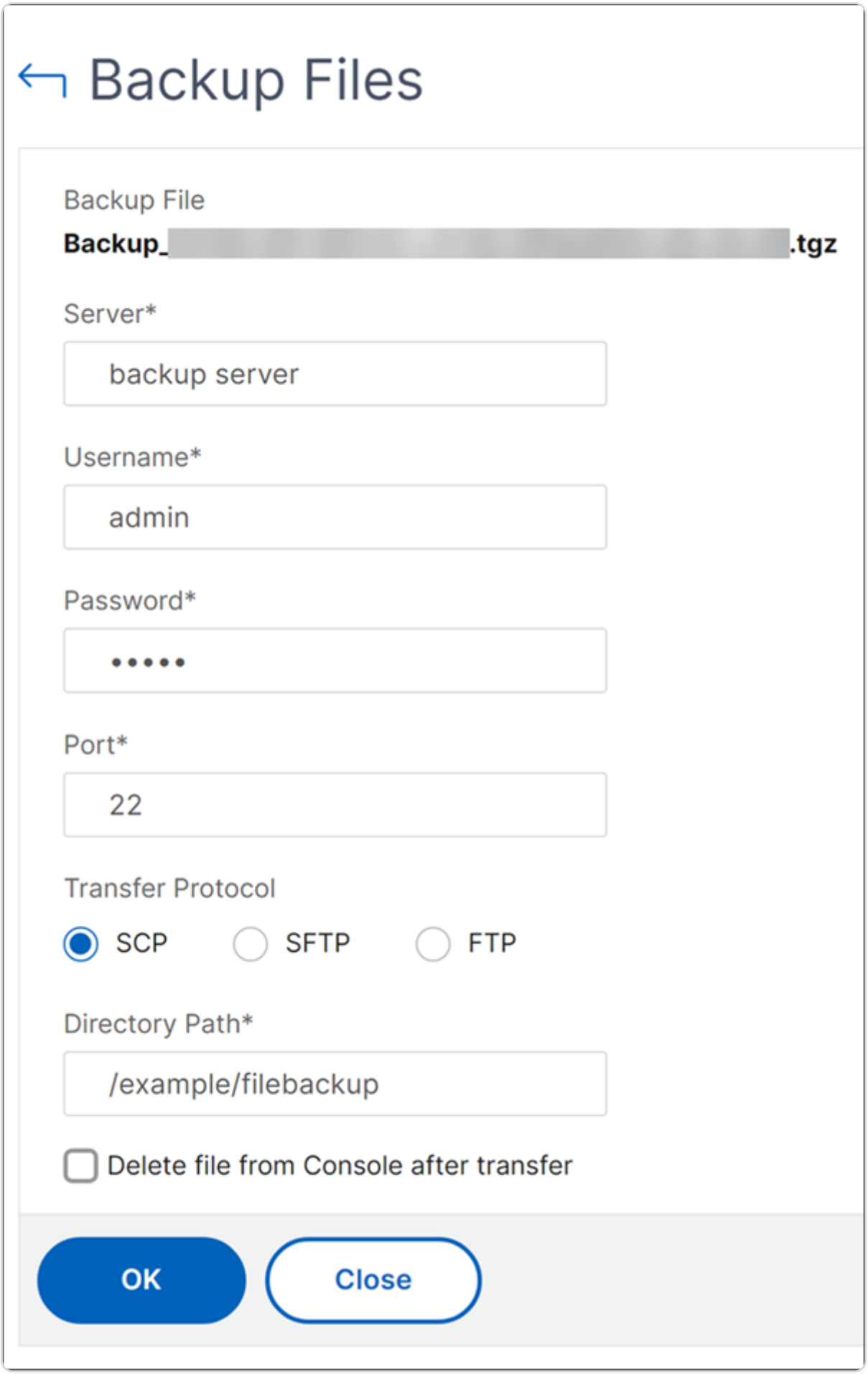
传输 NetScaler Console 备份文件：

1. 导航到 **设置 > 备份文件**。
2. 选择要移动到另一个系统的备份文件，然后单击 **传输**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在 **备份文件** 页面上，指定以下参数：
   - **服务器** - 要传输备份文件的系统的 IP 地址。
   - **用户名和密码** - 正在复制备份文件的新系统的用户凭据。
   - **端口** - 文件传输到的系统的端口号。
   - **传输协议** - 用于进行备份文件传输的协议。您可以选择 SCP、SFTP 或 FTP 协议来传输备份文件。
   - **目录路径** - 新系统上备份文件传输到的位置。
4. 传输后，通过选择**传输后从 Application Delivery Management 删除文件**复选框，可以从 NetScaler Console 中删除备份文件。
5. 单击**确定**以进行传输。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

要在本地系统保存备份文件的副本，请导航到**设置 > 备份文件**，选择要复制的文件，然后单击**下载**。

从备份文件还原 NetScaler Console 配置

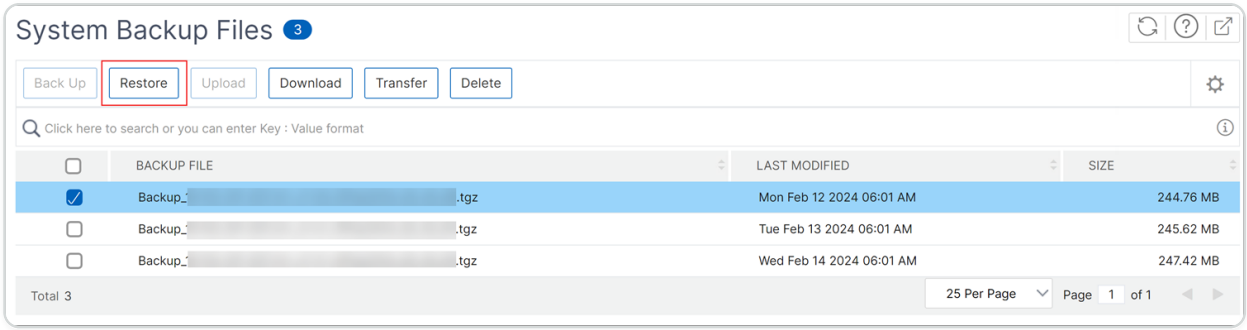
从以前备份的文件还原 NetScaler Console 配置时，还原操作会解压备份文件，然后还原配置。还原操作会删除现有配置，并将其替换为备份文件中的配置。

注意

- 如果备份文件被重命名或备份文件内容被修改，还原操作将失败。
- 在 NetScaler Console 上启动还原之前，将许可证文件复制到 `/mpsconfig/license/` 目录。目标设备的主机 ID 必须与复制的许可证文件中的主机 ID 匹配。

从备份文件还原 NetScaler Console 配置：

1. 导航到**设置 > 备份文件**。
2. 选择要还原的备份文件，然后单击**还原**。



3. 在确认对话框中，单击 **Yes**。

注意

要从外部系统中存储的备份文件恢复配置，请在执行恢复操作之前将备份文件上传到 NetScaler Console 服务器。要上传文件，请导航到 **Settings > Backup Files**，然后单击 **Upload**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高可用性部署中 NetScaler Console 的 VM 快照

您可以在开始升级之前，对 HA 部署中的 NetScaler Console 服务器进行快照。快照会捕获您拍摄时虚拟机的整个状态。

对 NetScaler Console 服务器进行快照

使用以下顺序对 NetScaler Console 服务器进行快照：

1. NetScaler Console 辅助服务器
2. NetScaler Console 主服务器

对 NetScaler Console 服务器进行快照：

1. 在您的虚拟机管理程序上，从虚拟机列表中选择 NetScaler Console 辅助服务器。
2. 拍摄 VM 快照。

   注意：

   我们建议您在拍摄快照时选择**拍摄 VM 内存**。

3. 为快照指定一个有意义的名称，并在需要时输入描述。

   快照存储在默认的 VM 目录中。

4. 对主服务器重复相同的步骤。

注意：

您在创建快照时无需关闭虚拟机电源。

恢复 NetScaler Console 服务器的快照

恢复快照时，会将虚拟机的内存、设置以及虚拟机磁盘的状态恢复到创建快照时的状态。

使用以下顺序恢复 NetScaler Console 服务器的快照：

1. NetScaler Console 主服务器
2. NetScaler Console 辅助服务器

恢复 NetScaler Console 服务器快照的步骤：

1. 在您的虚拟机管理程序上，从虚拟机列表中选择 NetScaler Console 主服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 右键单击虚拟机并还原快照。

   虚拟机将恢复到最新的快照。

3. 对 NetScaler Console 辅助服务器重复相同的步骤。

查看审计信息

审计日志包含特定时间段内的某些信息记录，例如用户详细信息、操作和执行的动作。您可以查看以下示例场景的系统日志消息：

- 如果您的 NetScaler® Console 是一个 HA 对，并且主节点和辅助节点之间的数据库复制存在任何延迟问题，您可以将详细信息作为事件查看。
- 如果存在任何无效登录尝试（用户名或密码错误）或成功登录，您可以将详细信息作为事件查看。

作为管理员，您可以使用这些日志来维护安全性并恢复丢失的事务。

在 NetScaler Console 上配置系统日志服务器：

1. 导航到 **设置 > 审计日志消息 > 系统日志服务器**。
2. 在 **系统日志服务器** 页面上，单击 **添加**。
3. 在 **创建系统日志服务器** 页面上，输入以下值：
   - **名称** - 系统日志服务器的名称。
   - **IP 地址** - 系统日志服务器的 IP 地址。
   - **端口** - 系统日志服务器端口。
4. 选择日志级别（全部、无或自定义）。
5. 单击 **创建**。

在 NetScaler Console 上配置系统日志日期和时间格式：

1. 导航到“**设置 > 审计日志消息 > Syslog 服务器**”。
2. 在“**Syslog 服务器**”页面上，选择一个 syslog 服务器，然后单击“**Syslog 参数**”。
3. 在“**配置 Syslog 参数**”页面上，指定日期和时间格式。
4. 单击“**确定**”。

要在 NetScaler Console 上查看 syslog 消息：

导航到“**设置 > 审计日志消息**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您还可以应用以下筛选器并查看系统日志消息：

- 事件
- 消息
- 模块
- 严重性
- 源

有关详细信息，请参阅 Syslog 消息参考。

配置 SSL 设置

SSL（安全套接字层）和 TLS（传输层安全）是常用的安全网络协议，它们在用户和服务器之间提供加密通信。您可以在 NetScaler Console 上配置 SSL 设置，并指定连接到系统的客户端类型。

配置 NetScaler Console 的 SSL 设置：

1. 导航到 **设置 > 管理**。在 **SSL 设置**下，单击 **配置 SSL 设置**。
2. 在 **SSL 设置**页面上，查看当前协议设置以及应用于系统的密码套件。
3. 要修改协议设置，请在 **编辑设置**下的 **协议设置**中单击 **+** 图标，并进行所需的更改。
4. 要修改应用的密码套件，请在 **编辑设置**下的 **密码套件**中单击 **+** 图标，并进行所需的更改。
5. 单击 **确定**，然后单击 **关闭**。

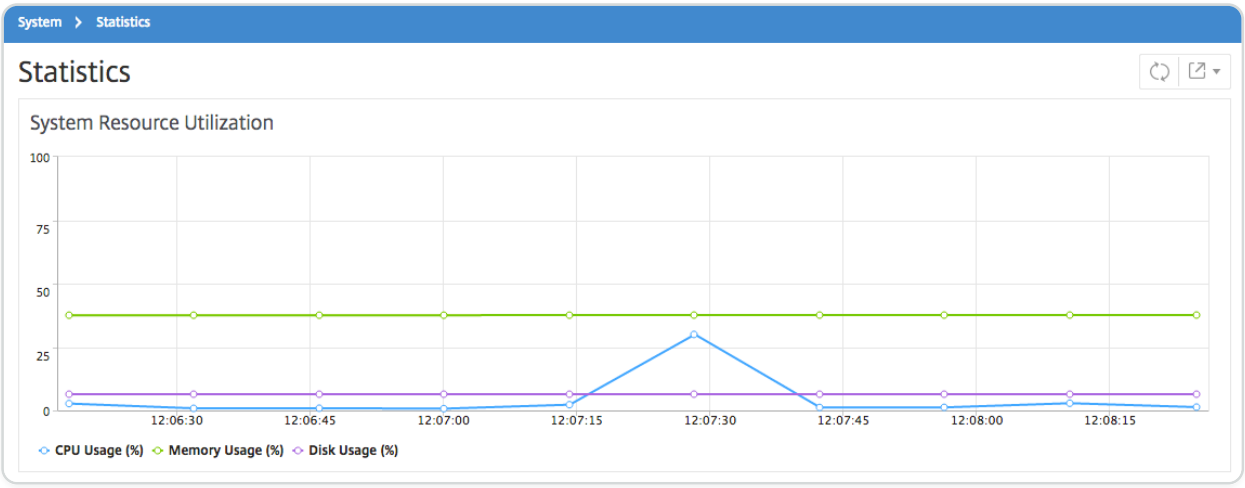
监控 CPU、内存和磁盘使用情况

您可以使用日志和统计信息中维护的信息。此信息也显示在报告中，可帮助您配置和维护 NetScaler Console。

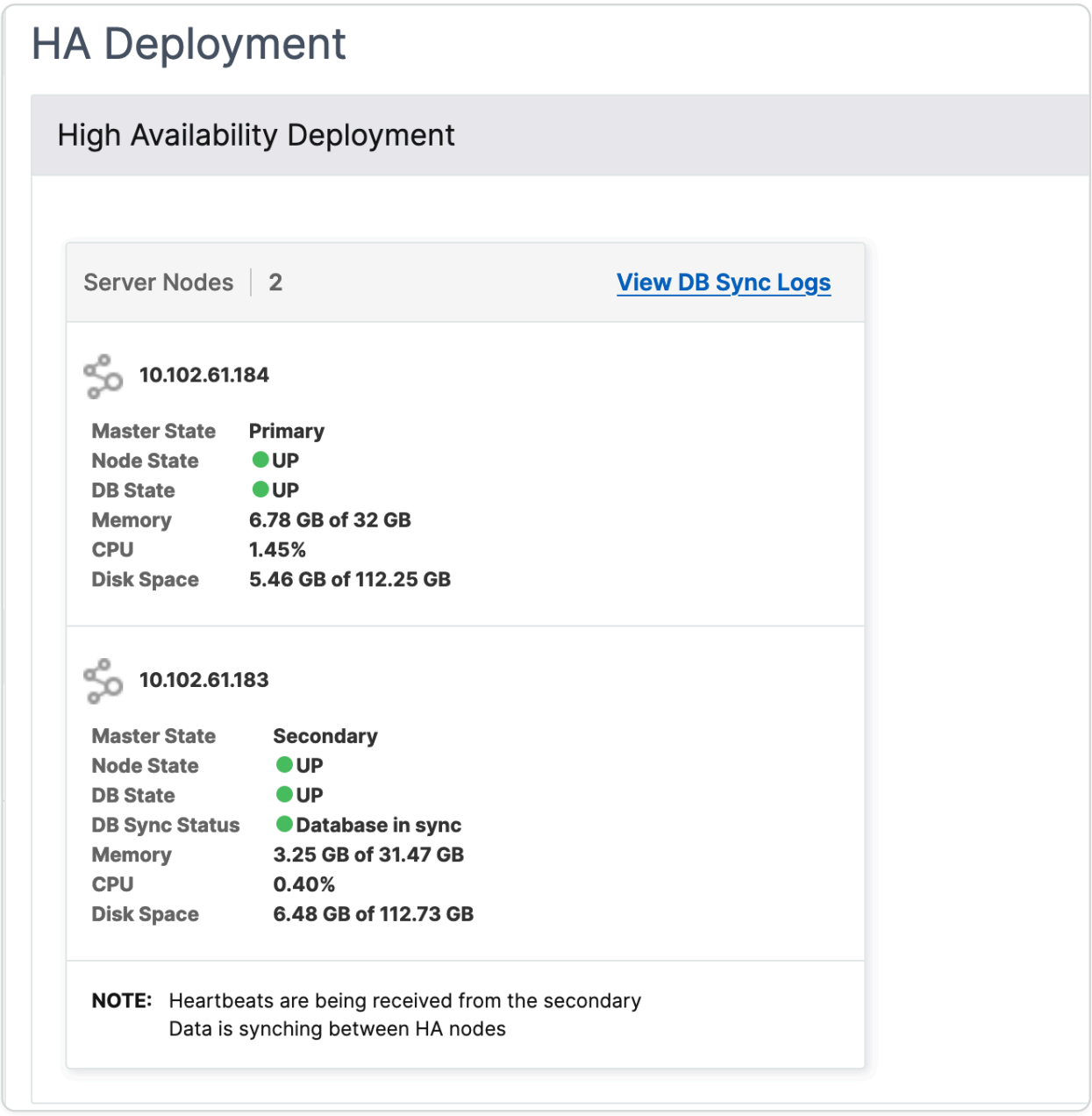
要监控 CPU、内存和磁盘使用情况，

- **独立部署。** 导航到 **系统** \> **统计信息**。您可以查看实时 CPU、内存和磁盘利用率图表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **高可用性部署。** 导航到 **设置 > 部署**。内存、CPU、磁盘空间和托管实例的统计信息以数字形式显示，如下图所示：



© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置通知设置

您可以选择通知类型以接收以下功能的通知：

- **事件** – 为 NetScaler 实例生成的事件列表。有关详细信息，请参阅 添加事件规则操作。
- **许可证** – 当前处于活动状态、即将到期等的许可证列表。有关详细信息，请参阅 NetScaler Console 许可证到期。
- **SSL 证书** – 添加到 NetScaler 实例的 SSL 证书列表。有关详细信息，请参阅 SSL 证书到期

NetScaler Console 支持以下通知类型：

- 电子邮件
- 短信
- 史拉克
- PagerDuty
- ServiceNow

对于每种通知类型，NetScaler Console GUI 都会显示已配置的分发列表或配置文件。NetScaler Console 会将通知发送到选定的分发列表或配置文件。

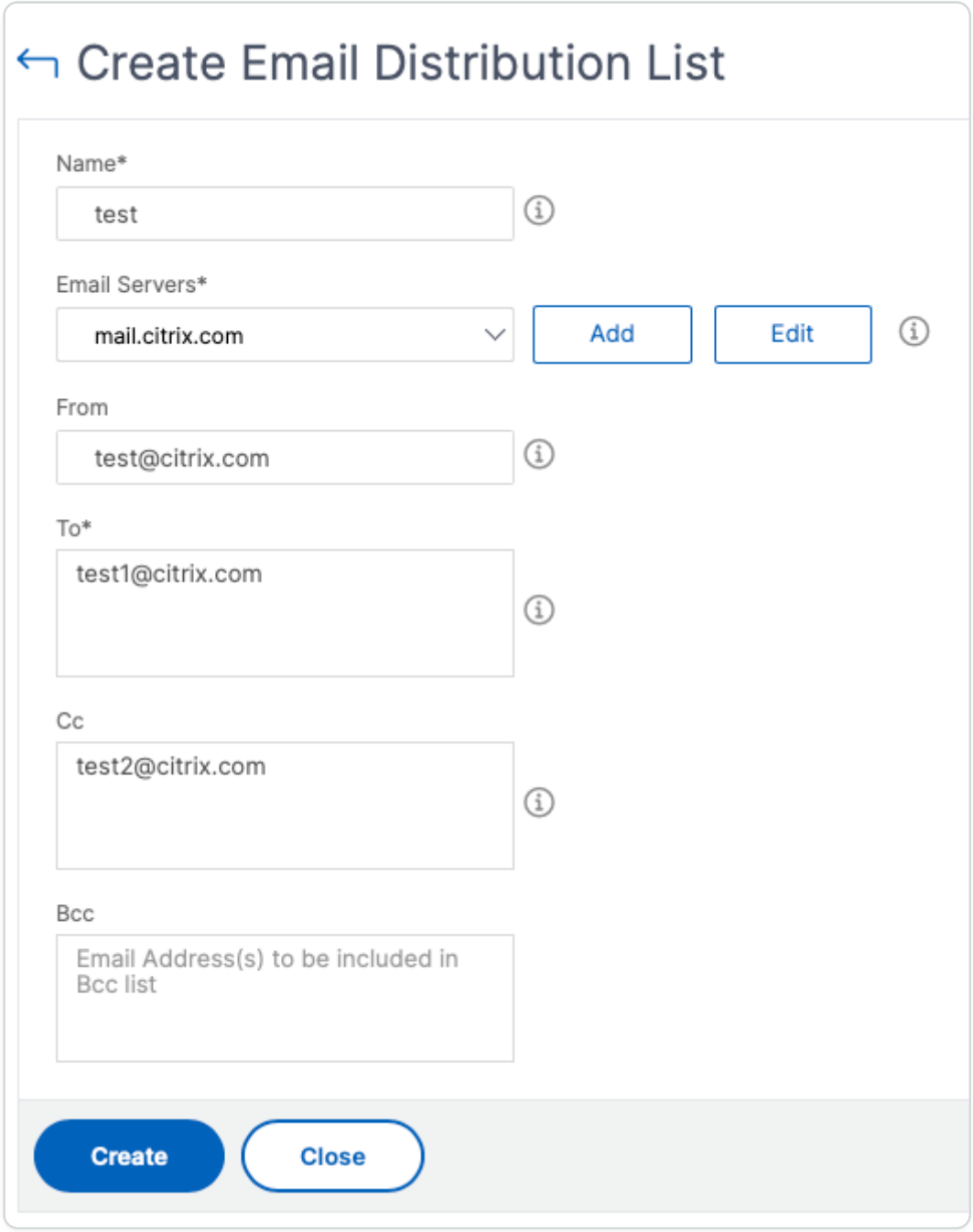
创建电子邮件分发列表

要接收 NetScaler Console 功能的电子邮件通知，您必须添加电子邮件服务器和分发列表。

执行以下步骤以创建电子邮件分发列表：

1. 导航到 **设置 > 通知**。
2. 在 **电子邮件** 中，单击 **添加**。
3. 在 **创建电子邮件分发列表** 中，指定以下详细信息：
    - **名称** - 指定分发列表名称。
    - **电子邮件服务器** - 选择发送电子邮件通知的电子邮件服务器。如果要添加电子邮件服务器，请单击 **添加**。
    - **发件人** - 指定 NetScaler Console 必须从中发送消息的电子邮件地址。
    - **收件人** - 指定 NetScaler Console 必须向其发送消息的电子邮件地址。
    - **抄送** - 指定 NetScaler Console 必须向其发送消息副本的电子邮件地址。
    - **密送** - 指定 NetScaler Console 必须向其发送消息副本而不显示地址的电子邮件地址。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 单击 **创建**。

重复此过程以创建多个电子邮件分发列表。**电子邮件** 选项卡显示 NetScaler Console 中存在的所有电子邮件分发列表。

创建短信分发列表

要接收 NetScaler Console 功能的短信通知，您必须添加短信服务器和电话号码。

执行以下步骤配置短信通知设置：

1. 导航到 **设置 > 通知**。
2. 在 **SMS** 中，单击 **Add**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在 **Create SMS Distribution List** 中，指定以下详细信息：
   - **Name** - 指定分发列表名称。
   - **SMS Server** - 选择发送短信通知的短信服务器。
   - **To** - 指定 NetScaler Console 必须发送消息的电话号码。
4. 单击 **Create**。

重复此过程以创建多个短信分发列表。**SMS** 选项卡显示 NetScaler Console 中存在的所有短信分发列表。

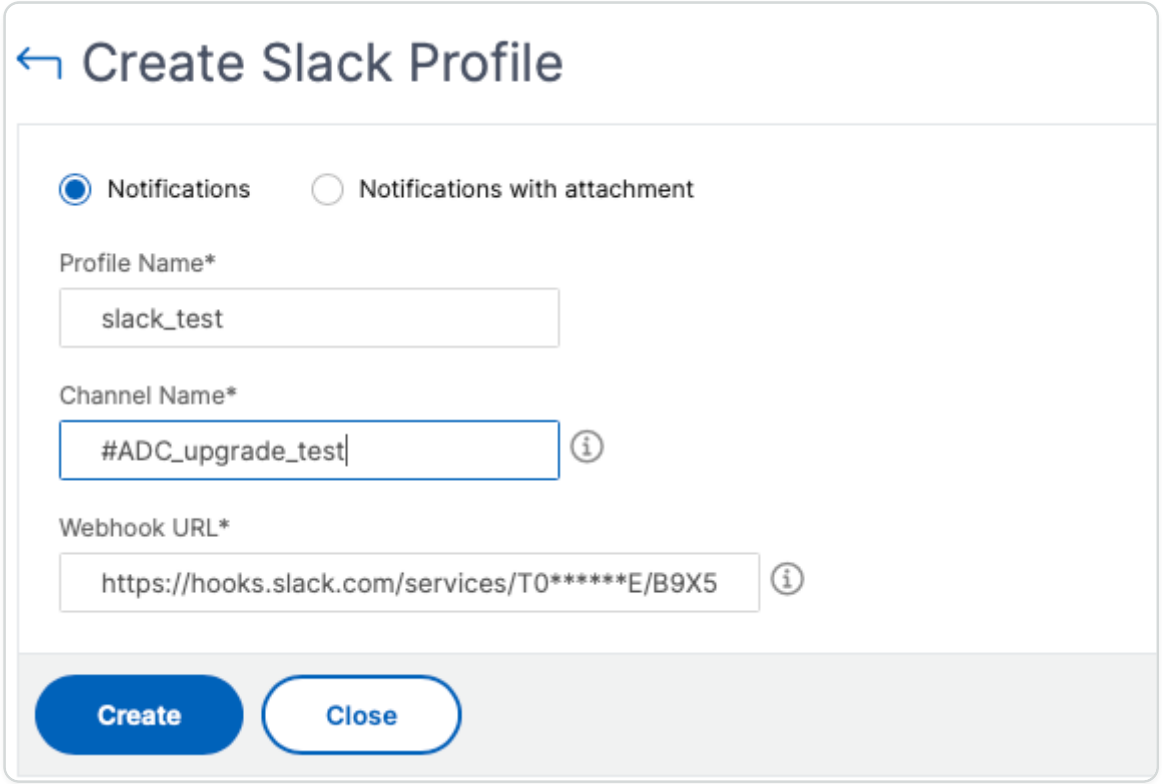
创建 Slack 配置文件

要接收 NetScaler Console 功能的 Slack 通知，您必须创建 Slack 配置文件。

执行以下步骤以创建 Slack 配置文件：

1. 导航到 **设置 > 通知**。
2. 在 **Slack** 中，单击 **Add**。
3. 在 **Create Slack Profile** 中，指定以下详细信息：
   - **Profile Name** - 指定配置文件名称。此名称将显示在 Slack 配置文件列表中。
   - **通道名称** - 指定 NetScaler Console 必须发送通知的 Slack 通道名称。
   - **Webhook URL** - 指定通道的 Webhook URL。传入 Webhook 是一种将外部源消息发布到 Slack 的简单方式。该 URL 在内部与通道名称关联。并且，所有发送到此 URL 的事件通知都会发布到指定的 Slack 通道。Webhook 示例如下：`<https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 单击“**创建**”。

重复此过程以创建多个 Slack 配置文件。**Slack** 选项卡显示 NetScaler Console 中存在的所有 Slack 配置文件。

创建 PagerDuty 配置文件

您可以添加 PagerDuty 配置文件，以根据 PagerDuty 配置监控事件通知。PagerDuty 使您能够通过电子邮件、短信、推送通知和注册号码上的电话呼叫来配置通知。

在 NetScaler Console 中添加 PagerDuty 配置文件之前，请确保您已在 PagerDuty 中完成所需的配置。要开始使用 PagerDuty，请参阅 PagerDuty 文档。

执行以下步骤以创建 PagerDuty 配置文件：

1. 导航到“**设置 > 通知**”。
2. 在“**PagerDuty**”中，单击“**添加**”。
3. 在“**创建 PagerDuty 配置文件**”中，指定以下详细信息：
   - **配置文件名称** - 指定您选择的配置文件名称。
   - **集成密钥** - 指定集成密钥。您可以从 PagerDuty 门户获取此密钥。在 PagerDuty 中创建用于集成的服务时，请使用“**通用事件 API 集成**”选项。
4. 单击“**创建**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关详细信息，请参阅 PagerDuty 文档中的 Services and Integrations。

重复此过程以创建多个 PagerDuty 配置文件。**PagerDuty** 选项卡显示 NetScaler Console 中存在的所有 PagerDuty 配置文件。

查看 ServiceNow 配置文件

当您要为 NetScaler 事件和 NetScaler Console 事件启用 ServiceNow 通知时，必须使用 ITSM 连接器将 NetScaler Console 与 ServiceNow 集成。有关详细信息，请参阅 将 NetScaler Console 与 ServiceNow 实例集成。

执行以下步骤以查看和验证 ServiceNow 配置文件：

1. 导航到 **设置 > 通知**。
2. 在 **ServiceNow** 中，从列表中选择 **Citrix_Workspace_SN** 配置文件。
3. 单击 **Test** 以自动生成 ServiceNow 票证并验证配置。

   如果您想在 NetScaler Console GUI 中查看 ServiceNow 票证，请选择 **ServiceNow Tickets**。

生成技术支持文件

我们建议您在联系技术支持以调试问题之前，生成 NetScaler Console 数据和统计信息的存档。该存档是一个 TAR 文件，您可以将其发送给技术支持团队。

注意

对于处于高可用性模式的 NetScaler Console 服务器，您可以从任一服务器生成技术支持文件。Citrix 建议您不要使用负载平衡虚拟服务器 IP 地址来生成技术支持文件。

从 NetScaler Console 配置和发送技术支持文件：

1. 导航到 **设置** \> **诊断** \> **技术支持**，然后单击 **生成技术支持文件**。
2. 在 **Generate Support File** 页面上，选择以下选项：

- **Collect Debug Logs** – 选择此选项以收集 `afdecoder` 日志。
- **Duration** – 输入必须收集调试日志的持续时间。只有启用 **Collect Debug Logs** 选项时，才会看到此选项。
- **Collect Data Distribution** – 选择此选项以从数据库中收集不同且多样的日志。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 The archive file is created as a TAR file.



 For example, the archive file that is created might be named as
follows:
Citrix_ADM_&lt;ADM_IP_address>_&lt;DDMMYY>_&lt;time_stamp>.tar.gz
```

1. 您可以通过两种方式将技术支持文件发送给支持团队：

   a. 您可以将文件从 NetScaler Console GUI 下载到本地存储，然后使用 Web 浏览器上传到 Citrix Insight Services(CIS)。

   b. 您还可以通过在 Console 上运行脚本将技术支持文件上传到 CIS 网站。

      i. 使用 SSH 登录到 Console。

      ii. 切换到 Shell 提示符并键入：

      /mps/collector_upload.pl

完整的命令及其所需属性如下所示：

```
/mps/collector_upload.pl [-proxy
[<proxy_user>:<proxy_password>@]<proxy_host>:<proxy_port>] [-user <user>]
[-password <password>] [-sr <sr>] [-description <description>] [-debug]
<file>
```

运行 Perl 脚本的优点是，您无需将技术支持文件从 NetScaler Console 下载到本地系统，然后再将其上传到 CIS。作为一种选择，您可以使用控制台中的代理直接将文件上传到 CIS。

确保您在 CIS 上拥有一个帐户。您可以使用您的 Citrix 帐户凭据将文件上传到 CIS。

如果您没有代理服务器怎么办？或者，如果您在使用 SSL 正向代理时遇到一些问题怎么办？（如果 Perl 脚本不信任代理服务器的根证书，则可能会发生这种情况。） 您仍然可以直接从 NetScaler Console shell 将文件上传到 CIS。

注意

如果 NetScaler Console 无法将文件从控制台上传到 CIS，您仍然可以下载文件并将其通过电子邮件发送给 Citrix 技术支持团队。或者，您可以将文件从 NetScaler Console 下载到本地存储，然后使用 Web 浏览器上传到 CIS。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

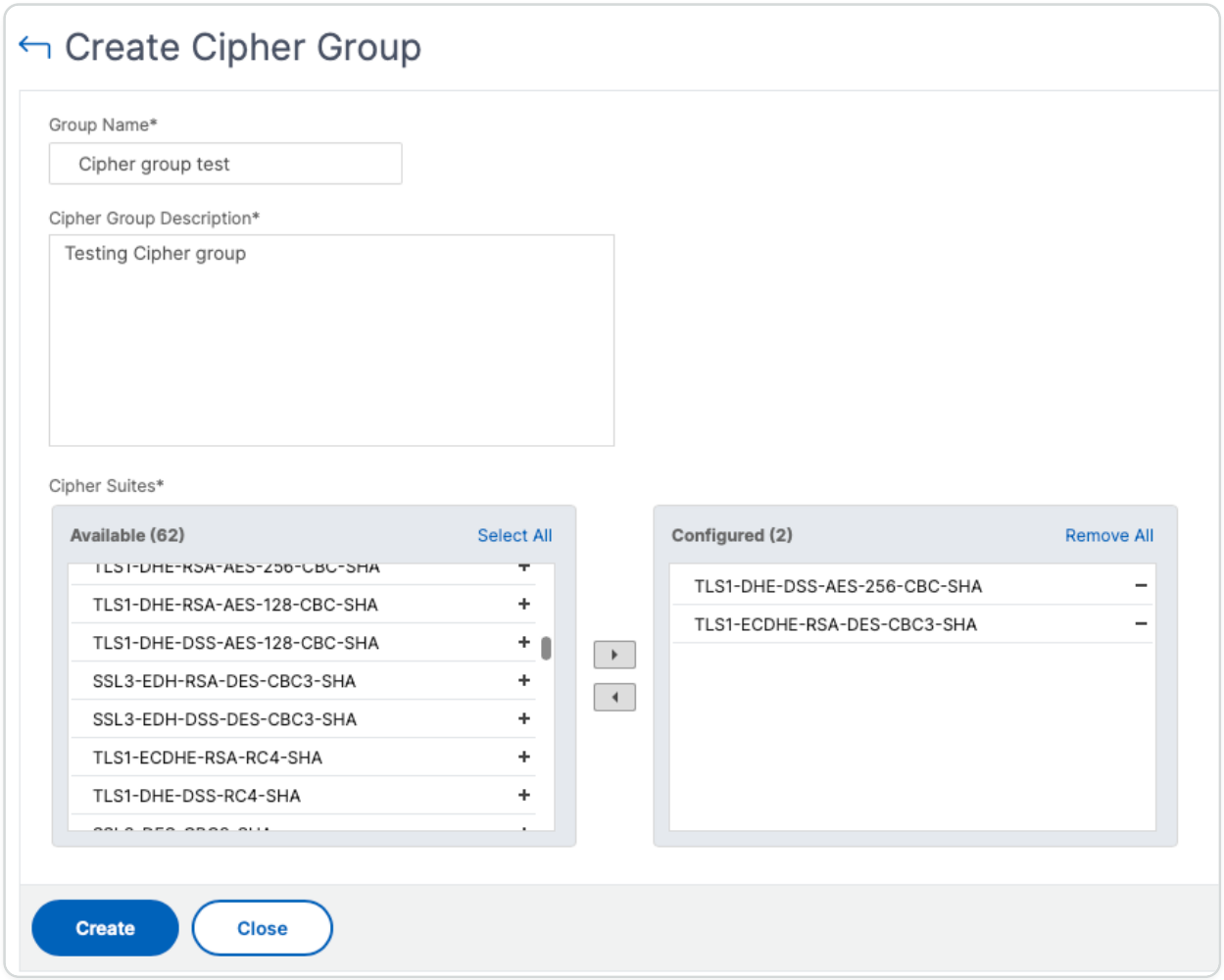
配置密码组

密码组是您绑定到 Citrix NetScaler 实例上的 SSL 虚拟服务器、服务或服务组的一组密码套件。密码套件包含一个协议、一个密钥交换 (`Kx`) 算法、一个身份验证 (`Au`) 算法、一个加密 (`Enc`) 算法和一个消息认证码 (`Mac`) 算法。

在 NetScaler Console 上添加密码组：

1. 导航到 **Settings > Administration**（设置 > 管理）
2. 在 **SSL Settings**（SSL 设置）下，单击 **Cipher Groups**（密码组）
3. 单击 **Add**（添加）
4. 在 **Create Cipher Group**（创建密码组）页面上，输入以下详细信息：
   - **Group Name**（组名称）- 密码组的名称。
   - **Cipher Group Description**（密码组描述）– 提供密码组的描述。
   - **Cipher Suites**（密码套件）– 单击“添加”从“可用”列表中选择密码套件，然后将选定（或所有）密码套件移动到“已配置”列表。
5. 单击 **Create**（创建）。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



创建 SNMP trap 目标、管理器社区和用户

每当 NetScaler Console 上出现异常情况时，就会生成一个 SNMP trap。然后，这些 trap 会发送到名为 trap 目标服务器或 *SNMP trap 目标*的远程设备。在此处，NetScaler Console 被配置为 trap 目标。您可以从名为 *SNMP 管理器*的远程设备查询 SNMP 代理以获取系统特定信息。然后，代理会在管理信息库 (MIB) 中搜索请求的数据，并将数据发送到 SNMP 管理器。

在 NetScaler Console 上创建 SNMP trap 目标：

1. 导航到 **系统** \> **SNMP** \> **陷阱目标**。
2. 在 **SNMP Traps** 下，单击 **Add** 以创建 SNMP trap，然后指定以下详细信息：
   - **版本。**选择要使用的 SNMP 版本。
   - **目标服务器。**trap 目标的名称或 IP 地址。
   - **端口。**输入 trap 目标的端口。默认情况下，端口设置为 162。
   - **社区。**指定向 trap 侦听器发送 trap 时要使用的社区字符串。
3. 单击 **Create**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

如果您正在创建 SNMP v3 trap 目标，请指定要绑定 trap 的 SNMP 用户凭据。要添加 SNMP 用户凭据，请单击 **Insert**，然后从可用 SNMP 用户列表中添加用户。

创建 SNMP 管理器社区：

1. 导航到 **System** \> **SNMP** \> **Managers**。
2. 在 **SNMP Manager** 下，单击 **Add** 以创建 SNMP 管理器社区，然后指定以下详细信息：
   - **SNMP 管理器。** 输入 SNMP 管理器的名称或 IP 地址。
   - **社区。** 指定向陷阱侦听器发送陷阱时要使用的社区字符串。
3. （可选）您可以选中“**启用管理网络**”复选框，以指定 **网络掩码**，即 SNMP 管理器网络的子网掩码。
4. 单击“**创建**”。

创建 SNMP 用户：

1. 导航到“**系统**”>“**SNMP**”>“**用户**”。
2. 在“**SNMP 用户**”下，单击“**添加**”。
3. 输入用户名，并从菜单中为用户分配安全级别。
4. 根据您为用户分配的安全级别，提供额外的身份验证协议（例如身份验证协议、隐私密码）并分配 SNMP 视图。

配置和查看系统警报

您可以启用和配置一组警报，以监控 NetScaler Console 服务器的运行状况。您必须配置系统警报，以确保您了解任何严重或主要的系统问题。例如，您可能希望在 CPU 使用率过高或服务器登录失败次数过多时收到通知。对于某些警报类别，例如 cpuUsageHigh 或 memoryUsageHigh，您可以设置阈值并为每个类别定义严重性（例如“严重”或“主要”）。对于某些类别，例如 inventoryFailed 或 loginFailure，您只能定义严重性。当警报类别（例如 memoryUsageHigh）的阈值被突破，或者当发生与警报类别（例如 **loginFailure**）对应的事件时，系统会记录一条消息，您可以将该消息视为 syslog 消息。您可以进一步设置通知，以接收与您的警报设置相对应的电子邮件或短信。

您可以分配或修改警报的严重性。您可以分配的严重性级别包括“严重”、“主要”、“次要”、“警告”和“信息”。

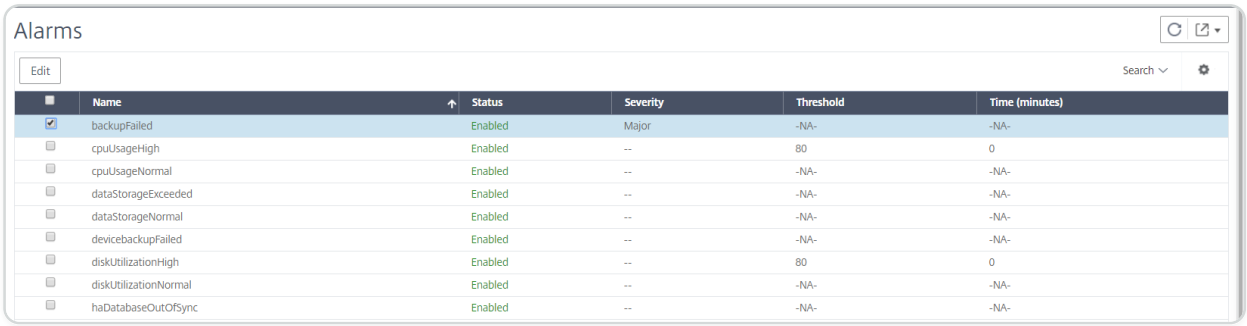
© 1997–2026 Citrix Systems, Inc. All rights reserved.

假设您希望在备份尝试失败时进行监控。您可以启用 backupFailed 警报并为其分配严重性，例如“主要”。每当 NetScaler Console 尝试备份系统文件且尝试失败时，就会触发警报。您可以在 NetScaler Console 上查看消息，或通过电子邮件或短信获取通知。

要配置警报，您必须选择 backupFailed 警报并将严重性级别指定为“主要”。警报默认处于启用状态。

使用 NetScaler Console 配置和查看系统警报：

1. 导航到 **Settings > SNMP**。单击右上角的 **Alarms**。



2. 选择要配置的警报（例如 backupFailed），然后单击 **Edit** 以修改其设置。
3. 警报默认处于启用状态。分配严重性级别（例如：“主要”），然后单击 **OK**。

注意

对于某些警报，您无法设置阈值。 触发警报时，您可以将生成的事件视为 syslog 消息。

使用 NetScaler Console 查看 backupFailed 警报生成的事件：

1. 导航到 **System** > **Auditing**。
2. 在 **Auditing** 页面中，在 **Audit Messages** 下，选择 **Syslog Messages**。
3. 在搜索字段中，输入警报的名称。

   在此示例中，您可以看到已为失败的备份尝试生成了一个事件。

   备份失败警报(/en-us/netscaler-application-delivery-management-software/media/backup-failure-message.png)

   您还可以设置通知，以便在触发警报时向您发送电子邮件或短信（Short Message Service）。有关如何配置系统通知的信息，请参阅如何配置 NetScaler Console 的系统通知设置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

为磁盘利用率警报添加阈值限制

当 NetScaler Console 服务器上使用的磁盘空间量超过预定义阈值时，会触发磁盘利用率警报。

作为管理员，当您收到警报时，可以选择删除不必要的数据或分配额外的存储资源，以防止服务中断或性能下降。

从版本 14.1-25.x 开始，您还可以为磁盘利用率警报添加一个较低级别的阈值。通过此阈值，您可以设置一个较低级别的限制，以便在达到上限阈值之前接收警报。

要配置较低级别的阈值：

1. 导航到 **设置 > SNMP > 警报**，并在搜索字段中输入 diskUtilizationHigh 以查看磁盘利用率警报。
2. 选择警报并单击 **编辑**。
3. 在 **配置警报** 页面中，选择 **配置较低级别的阈值**。输入较低级别的阈值限制。

   备份失败警报(/en-us/netscaler-application-delivery-management-software/media/snmp-alarms-lower-threshold.png)

例如，如果您将较低的磁盘利用率阈值设置为 60，将较高的阈值设置为 80，则当磁盘使用量超过磁盘容量的 60% 时，您会收到警报。此设置允许您在磁盘利用率达到 80% 之前采取纠正措施。

为 NetScaler 代理创建 SNMP 管理器和用户

您可以从称为 SNMP 管理器的远程设备查询 SNMP 代理以获取系统特定信息。然后，代理会在管理信息库 (MIB) 中搜索请求的数据，并将数据发送给 SNMP 管理器。

您可以添加 SNMP 管理器来查询 NetScaler 代理。该管理器符合 SNMP V2 和 V3 标准。如果您指定一个或多个 SNMP 管理器，则 NetScaler 代理将不接受来自指定 SNMP 管理器以外的任何主机的 SNMP 查询。

添加 SNMP v2 管理器

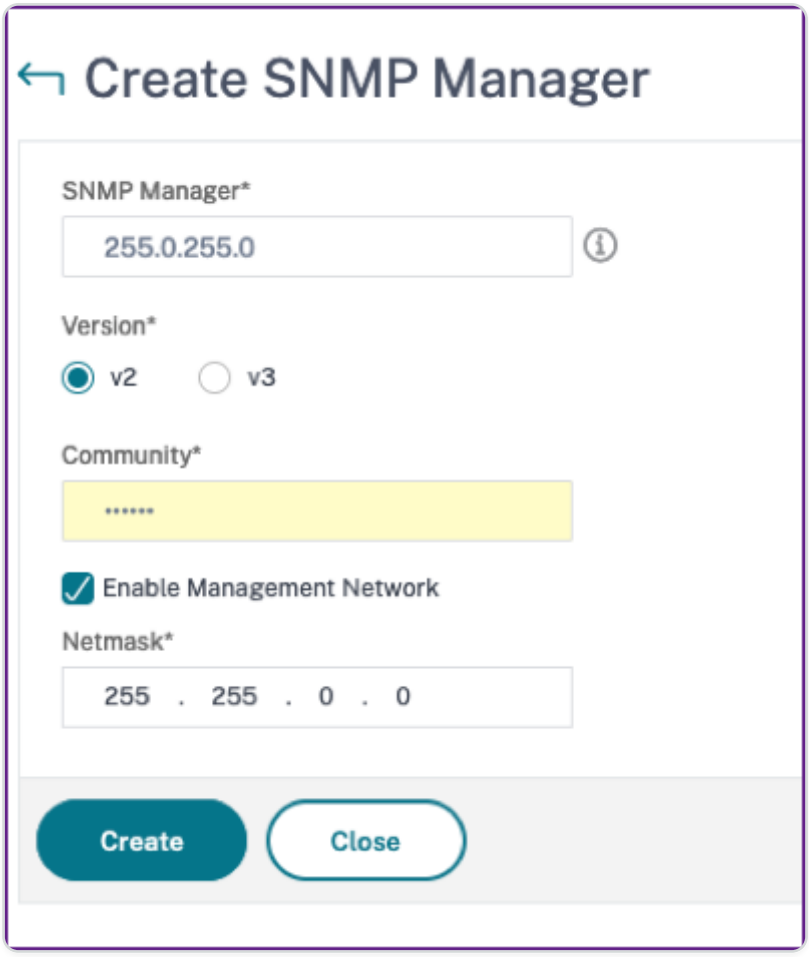
要为 NetScaler 代理添加 SNMP v2 管理器，请执行以下操作：

1. 导航到 **Infrastructure > Agents**，选择一个 NetScaler 代理，然后单击 **Select Action> Manage SNMP**。
2. 在 **SNMP> SNMP Manager** 选项卡中，单击 **Add**。
3. 在 **Create SNMP Manager** 页面中，指定以下详细信息：
   - **SNMP 管理器**。输入 SNMP 管理器的名称或 IP 地址。
   - **版本**。选择 v2。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **社区**。输入社区名称。SNMP 社区配置可对来自 SNMP 管理器的 SNMP 查询进行身份验证。
- **启用管理网络**：选中此复选框以指定 SNMP 管理器网络的网络掩码。
- **网络掩码**：输入与 IP 地址关联的子网掩码。

4. 单击 **Create**。



添加 SNMP v3 管理器

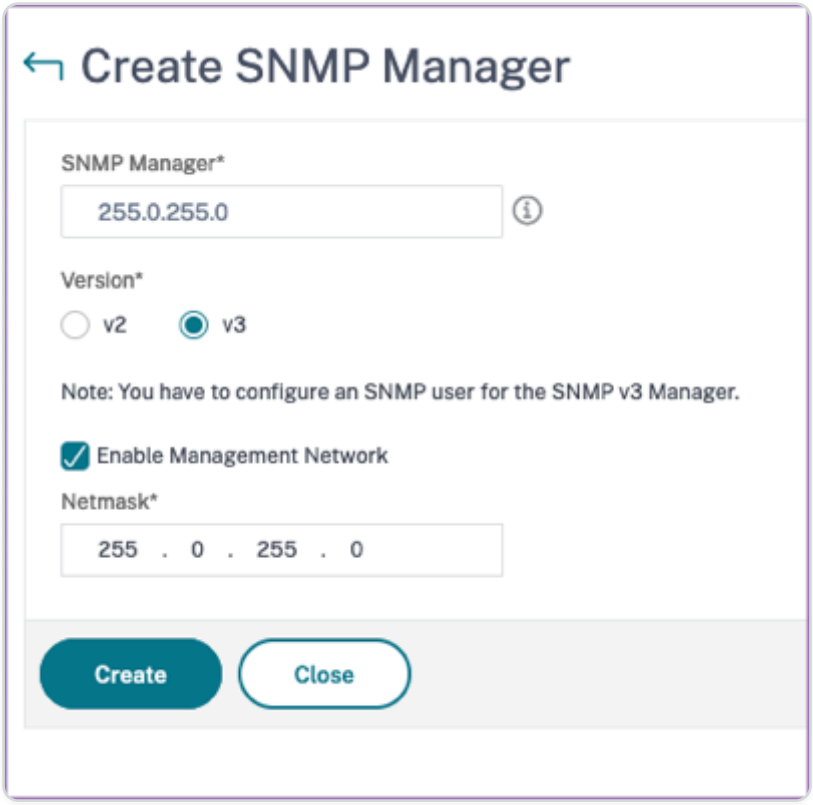
要为 NetScaler 代理添加 SNMP v3 管理器，请执行以下操作：

1. 导航到 **Infrastructure > Agents**，选择一个 NetScaler 代理，然后单击 **Select Action> Manage SNMP**。
2. 在 **SNMP> SNMP Manager** 选项卡中，单击 **Add**。
3. 在 **Create SNMP Manager** 页面中，指定以下详细信息：
   - **SNMP Manager**。输入 SNMP 管理器的名称或 IP 地址。
   - **Version**。选择 v3。
   - **Enable Management Network**：选中此复选框以指定 SNMP 管理器网络的网络掩码。

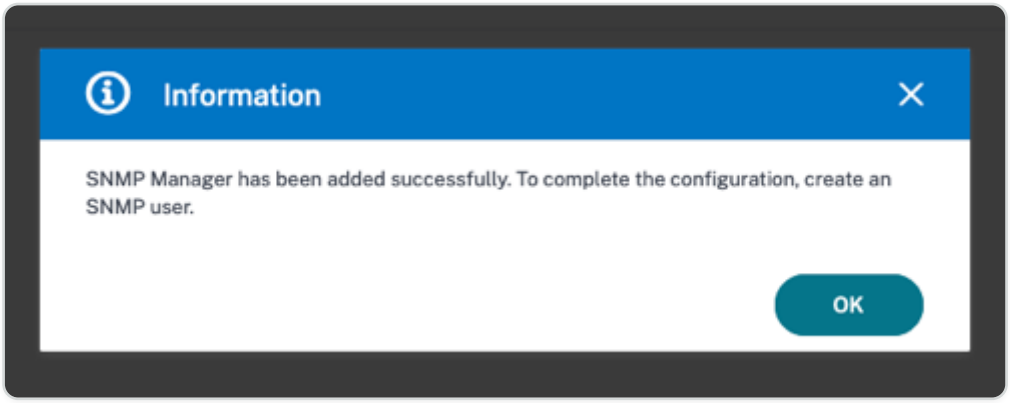
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Netmask**：输入与 IP 地址关联的子网掩码。

4. 单击 **Create**。



将出现一个对话框，确认已创建 SNMP 管理器并提示您配置 SNMP 用户。



注意

您必须为 SNMP v3 管理器配置 SNMP 用户。要配置 SNMP 用户，请转到 **SNMP > SNMP User**。

添加 SNMP 用户

添加 SNMP 用户以响应来自 SNMP 管理器的 SNMP v3 查询。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

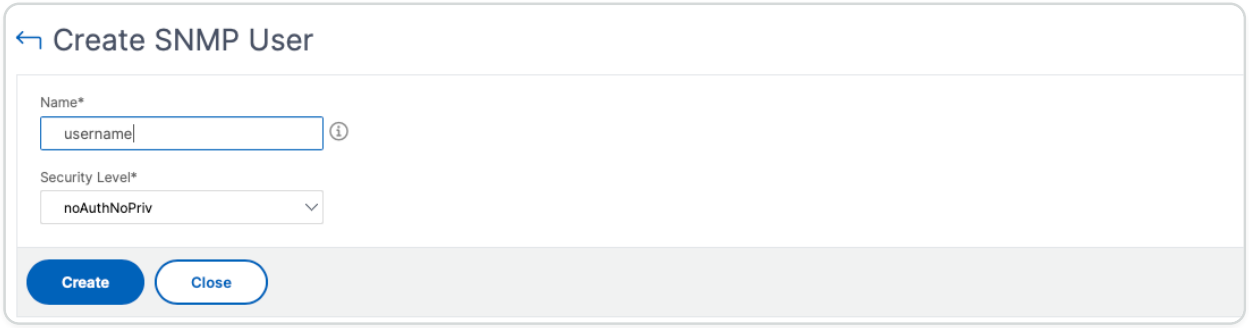
为 NetScaler 代理添加 SNMP 用户：

1. 导航到 **Infrastructure > Agents**，选择一个 NetScaler 代理，然后单击 **Select Action> Manage SNMP**。
2. 在 **SNMP> SNMP User** 选项卡中，单击 **Add**。
3. 在 **Create SNMP User** 页面中，添加以下详细信息：

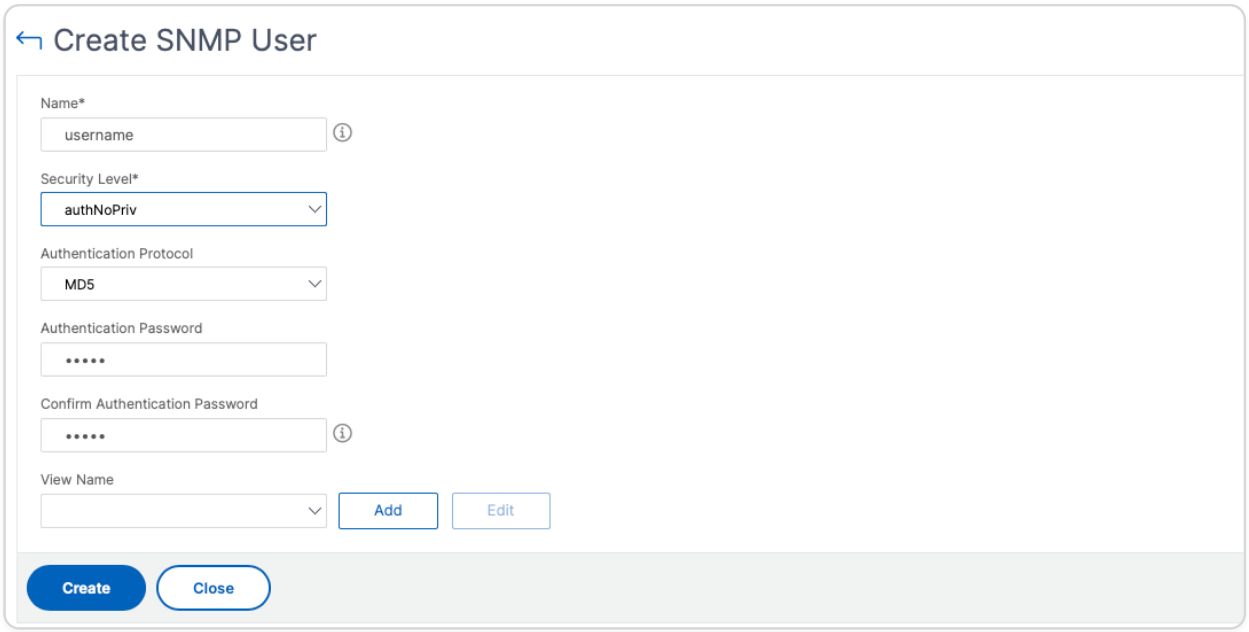
   - **名称**。输入用户名。
   - **安全级别**。NetScaler 代理与 SNMP 管理器之间通信所需的安全级别。

     选择以下安全级别之一：

   - **noAuthNoPriv**。既不需要身份验证也不需要加密。

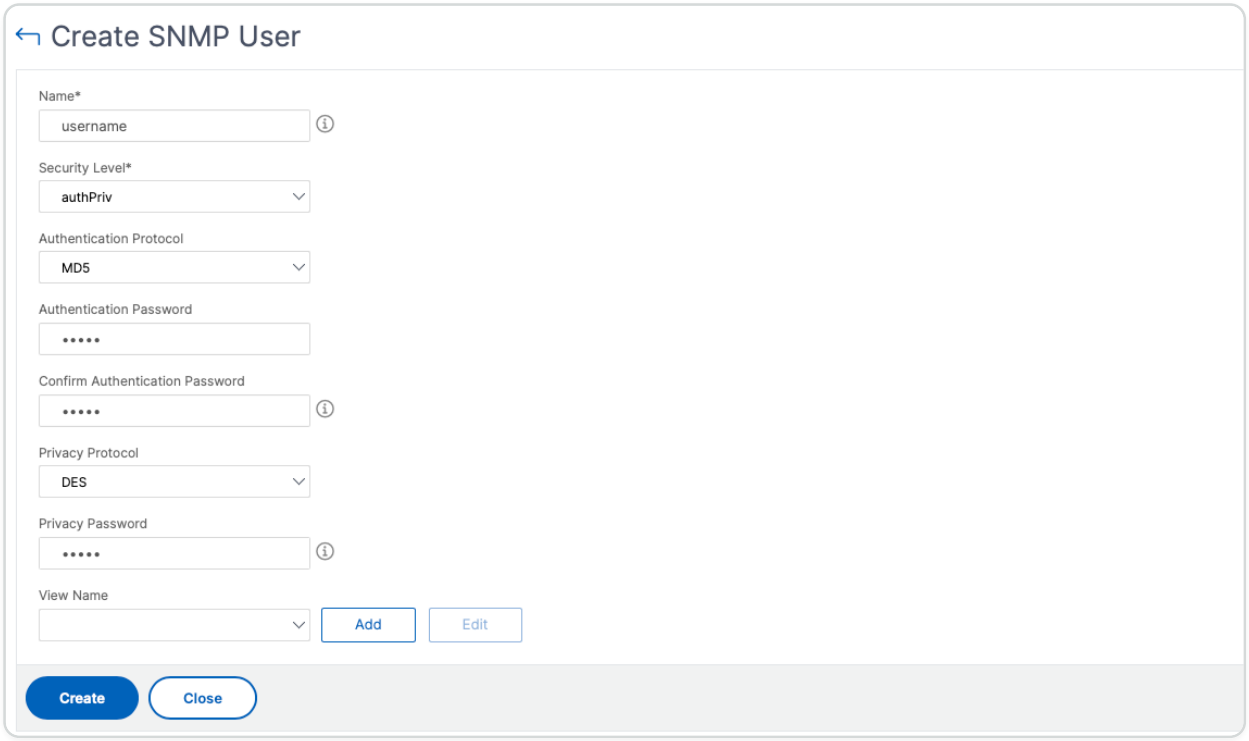


   - **authNoPriv**。需要身份验证但不需要加密。



   - **authPriv**。需要身份验证和加密。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



根据您为用户分配的安全级别，提供额外的身份验证协议，例如身份验证协议、隐私密码，并分配 SNMP 视图。

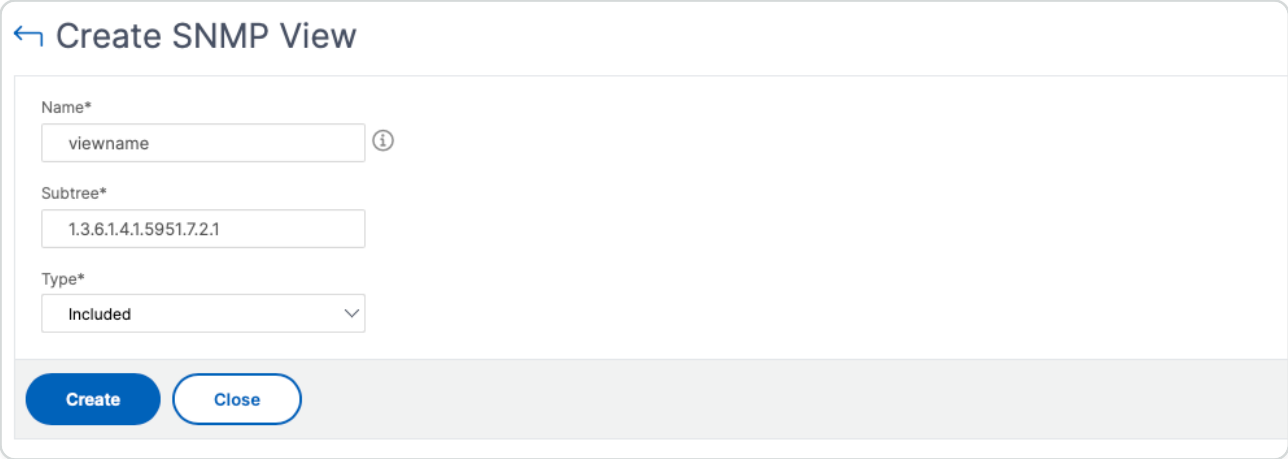
管理 SNMP 视图

SNMP 视图用于为 SNMP 用户实施访问控制。SNMP 视图将用户访问限制在 MIB 的特定部分。

允许或限制 NetScaler 代理的 SNMP OID：

1. 导航到“**基础架构 > 代理 > 管理 SNMP**”，然后在“**SNMP 视图**”选项卡中，单击“**添加**”。
2. 在“**创建 SNMP 视图**”中，输入以下详细信息：
   - **视图名称**：SNMP 视图的名称。一个实例可以有多个同名的 SNMP 视图，通过子树参数设置进行区分。
   - **子树**：您希望与此 SNMP 视图关联的 MIB 树的特定分支（子树）。您必须将子树指定为 SNMP OID。
   - **类型**：此字段允许您从视图中包含或排除子树。
3. 单击“**创建**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



配置代理设置

您可以修改 NetScaler Console 代理的保持活动间隔和密码更改要求。

设置代理的保持活动间隔

NetScaler Console 服务器和代理在指定的保持活动间隔内保持相同的 TCP 连接。代理使用此连接将托管实例数据发送到 NetScaler Console 服务器。

1. 导航到 **Settings > Administration**（设置 > 管理）。
2. 在 **System Configurations**（系统配置）下，选择 **System, Time zone, Allowed URLs and Agent Settings**（系统、时区、允许的 URL 和代理设置）。
3. 在 **Basic Settings > Agent Settings**（基本设置 > 代理设置）中，将保持活动间隔指定为 30–120 秒。
4. 单击 **Save**（保存）。

在没有当前密码的情况下更改代理密码

您可以允许在没有当前密码的情况下更改代理密码。

1. 导航到 **Settings > Administration**（设置 > 管理）。
2. 在 **System Configurations**（系统配置）下，选择 **System, Time zone, Allowed URLs and Agent Settings**（系统、时区、允许的 URL 和代理设置）。
3. 在 **Basic Settings > Agent Settings > Remove current password prerequisite for agent password change**（基本设置 > 代理设置 > 移除代理密码更改的当前密码先决条件）复选框中，您可以执行以下操作：
   - 选中该复选框以移除 **Change Agent Password**（更改代理密码）页面中的 **Current password**（当前密码）字段。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 清除该复选框以保留 **Change Agent Password**（更改代理密码）页面中的 **Current password**（当前密码）字段。

4. 点击 **保存**。

> **注意**
>
> 要查看 **更改代理密码** 页面，请导航到 **基础架构 > 实例 > 代理**，选择一个代理，然后点击 **选择操作 > 更改密码**。

使用数据存储管理仪表板

了解 NetScaler Console 中使用了哪些功能以及每个功能的数据使用情况非常重要。**数据存储管理**仪表板正是为此目的而设，并作为您的可视化工具，使您能够了解 NetScaler Console 数据库中跨各种功能存储的总数据量。仪表板还会指示已用存储是否在指定限制内，或者是否超过了授权存储。

作为管理员，您可以在**数据存储管理**仪表板中执行以下任务：

- 查看过去 30 天的数据存储消耗 - 数据存储趋势在 NetScaler Console 数据库中存储了最近 30 天。这些趋势以图形或表格形式提供。这些趋势显示了有多少数据进入以及在 NetScaler Console 中经过计划的修剪周期后存储了多少数据。
- 查看数据摄取状态 - 只要已用存储在授权存储的限制内，数据摄取活动就会进行。当已用存储超过授权存储时，数据活动将暂停。
- 发送通知 - 您可以设置在已用存储达到授权存储的 75% 或 100% 时发送通知，从而允许用户管理其存储。
- 灵活管理数据存储空间 - 您可以通过修剪您认为适合删除或减少的数据，在已存储数据中创建更多空间。

导航到**设置 > 数据存储**以查看您的数据存储仪表板。

以下部分概述了如何使用**数据存储管理**仪表板进行有效的数据存储管理：

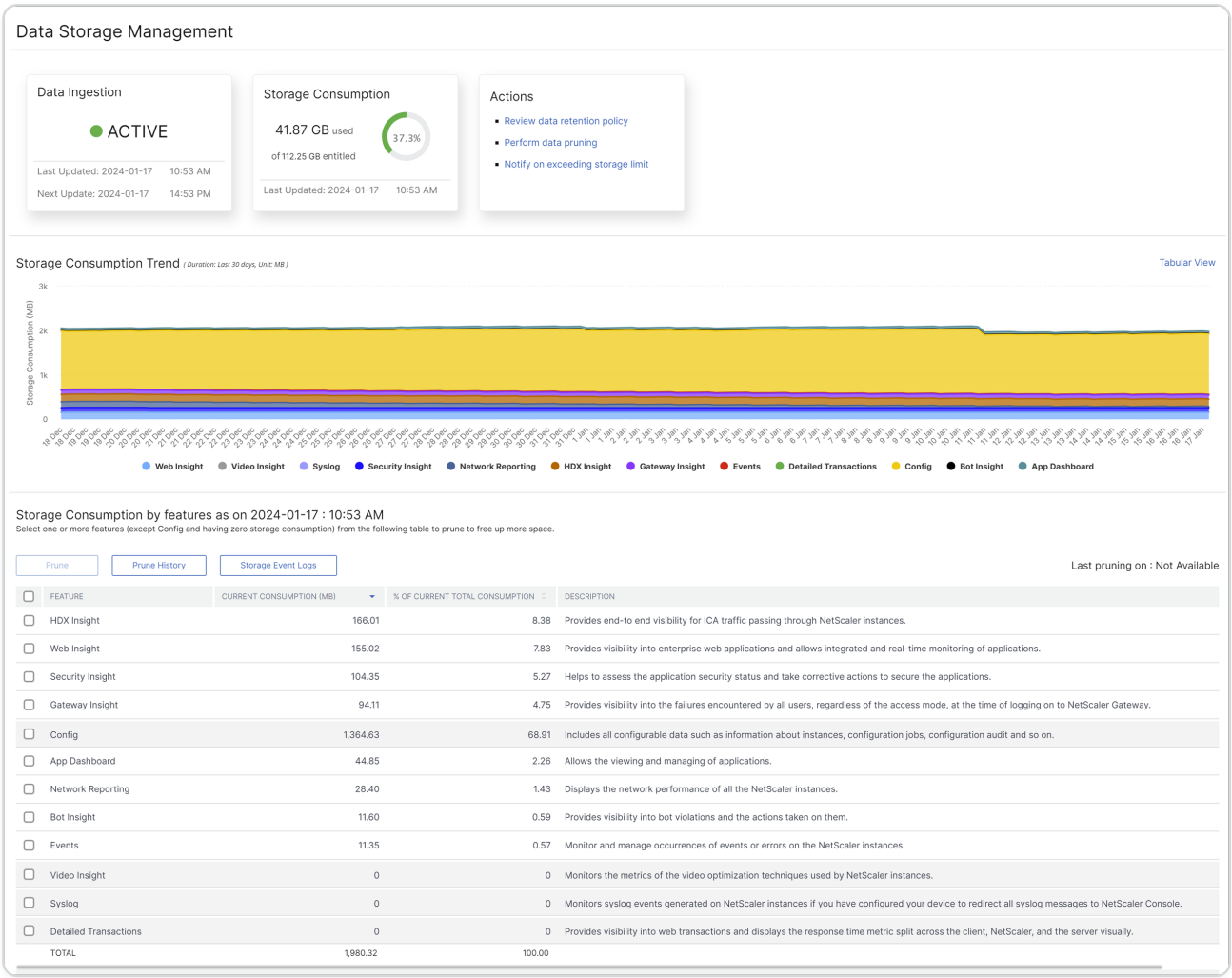
- 了解您的数据存储 - 本节帮助您了解如何使用仪表板查看有关数据存储的信息。
- 管理您的数据存储 - 本节提供了有关您可以在仪表板中采取哪些操作来管理您的数据存储的信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

了解您的数据存储

您可以使用 NetScaler Console 中的“**数据存储管理**”仪表板来查看数据和图表，以帮助您跟踪数据存储使用情况。

要监控您的数据存储消耗，请导航到“**设置 > 数据存储**”。



数据存储管理仪表板显示以下信息：

- 数据摄取活动状态
- 总存储消耗
- 存储消耗趋势
- 按功能划分的存储消耗

数据摄取活动状态

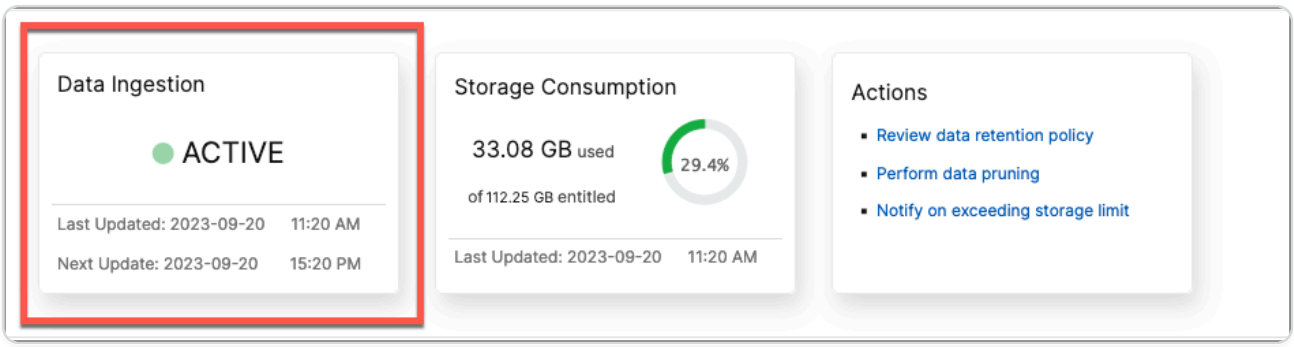
数据摄取是指将来自所有托管 NetScaler 实例的大量各种数据（例如事件、系统日志、网络报告等）导入到 NetScaler Console 存储中的过程。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

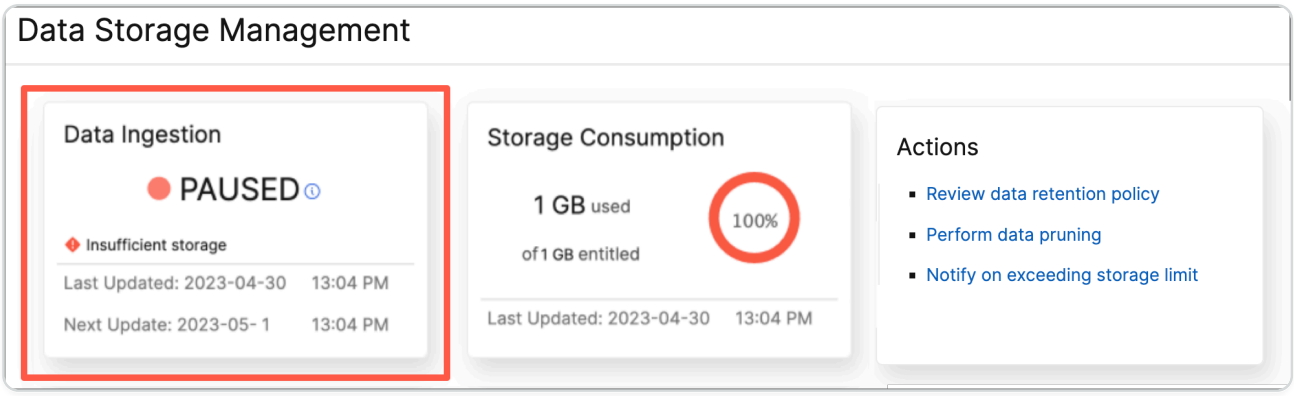
数据摄取状态指示 NetScaler Console 是否正在从 NetScaler 实例收集统计信息。只要消耗的存储空间在授权存储空间内，数据摄取活动就会继续。当消耗量超过授权存储空间时，数据摄取将暂停。

查看“**数据摄取**”磁贴以了解数据摄取的当前状态。此磁贴显示以下两种状态之一：

- “**活动**” - 数据摄取活动正在进行中。



- **已暂停** - 由于已用存储超出授权存储，数据摄取活动已暂停。

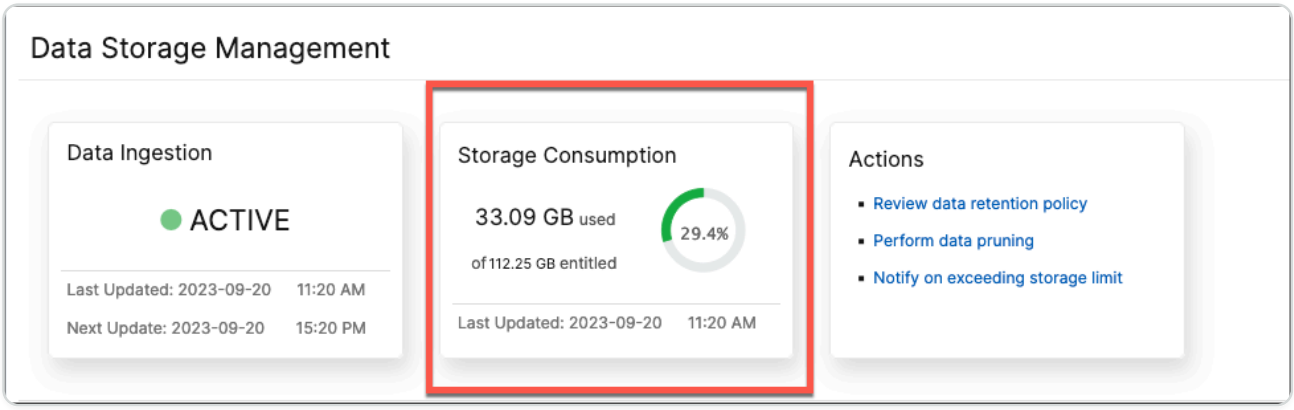


如何恢复已暂停的数据摄取

要恢复数据摄取活动，您可以执行数据清理。有关详细信息，请参阅执行数据清理。

总存储消耗

要快速概览数据存储，请查看“**存储消耗**”磁贴。



“**存储消耗**”磁贴显示部署中所有功能使用的总存储空间。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

将鼠标悬停在圆环图上可查看以下内容：

授权存储

授权存储是根据您的许可证可供您使用的总存储空间。如果您拥有 Express 许可证，您将获得 500 MB 的授权存储。如果您拥有 Advanced 许可证，您将获得每个购买的 VIP 500 MB 存储空间的总和，以及任何未购买 VIP 而直接购买的额外存储空间。

请考虑以下情况：

- 您购买了 20 个 VIP。每个 VIP 可获得 500 MB 的免费存储空间。您的授权存储空间为 20*500 = 10 GB。
- 您购买了 20 个 VIP 和 5 GB 的附加存储。每个 VIP 可获得 500 MB 的免费存储空间。您的授权存储空间为 20*500 + 5 = 15 GB。

已用存储

已用存储空间是部署中所有功能使用的总存储空间。以下颜色编码标准指定了功能使用的存储空间量：

- **绿色** - 已用存储空间小于授权存储空间的 75%。
- **琥珀色** - 已用存储空间介于授权存储空间的 75% 到 99% 之间。
- **红色** - 已用存储空间限制已达到或超过当前授权存储空间。

存储消耗趋势

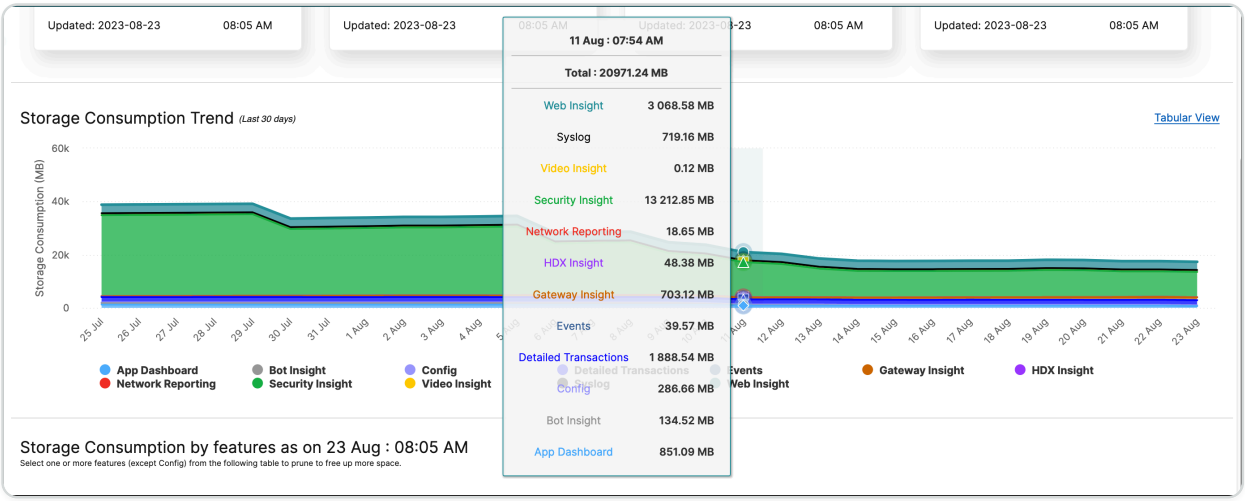
要了解过去 30 天的数据消耗情况，请查看“**存储消耗趋势**”部分。

“**存储消耗趋势**”提供了关于哪些功能在一段时间内使用最多或最少存储空间的见解，并帮助您有效管理数据存储消耗。

您可以以下列任一形式查看存储数据趋势：

- **图形视图** – 显示数据存储如何在不同的 NetScaler Console 功能之间分布。将鼠标悬停在时间轴上，可查看该月中任何一天的数据存储信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

"**图形视图**"是默认视图。

- **表格视图** – 单击"**表格视图**"以表格形式显示数据存储信息。

FEATURE	25 JUL	26 JUL	27 JUL	28 JUL	29 JUL	30 JUL	31 JUL	1 AUG	2 AUG	3 AUG	4 AUG
Security Insight	30415.05	30478.90	30535.21	30596.05	30648.76	25069.69	25222.26	25380.30	25552.37	25551.91	2570
Web Insight	3193.42	3200.39	3207.48	3213.02	3219.95	3226.22	3231.98	3238.30	3246.83	3252.87	3258
Detailed Transactions	2007.07	1998.34	1985.43	2046.68	2031.71	2014.52	1995.44	1985.16	2039.65	2025.91	2014
Gateway Insight	248.15	279.05	310.27	342.74	373.78	403.89	434.83	466.64	499.50	499.01	529.
Syslog	775.05	775.54	776.50	686.32	697.56	708.37	719.57	720.30	721.24	721.61	721.5
App Dashboard	1240.54	1237.85	1238.79	1238.08	1238.98	1238.13	1238.94	1238.66	1239.17	1239.24	1238
Config	269.76	270.68	272.41	273.02	274.16	275.49	275.18	272.52	271.13	271.70	271.8
HDX Insight	52.95	52.72	52.49	52.53	52.45	52.64	52.75	52.83	52.80	53.23	52.9
Events	45.06	45.27	44.85	44.49	43.96	43.63	43.24	43.08	43.16	42.95	42.5
Network Reporting	21.80	21.78	21.77	21.77	21.77	21.77	21.77	21.77	21.75	22.07	22.2
Bot Insight	544.23	543.98	544.09	544.32	544.10	544.01	544.10	544.05	544.10	544.10	544.
Video Insight	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25
TOTAL	38813.31	38904.75	38989.54	39059.27	39147.42	33598.61	33780.30	33963.85	34231.95	34224.85	3439

注意：

表格视图允许您使用搜索字段筛选数据。

下表描述了"**存储消耗趋势**"部分中显示的字段：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

功能	描述
配置	包括所有可配置数据，例如有关实例、配置作业、配置审计等信息。
HDX 洞察	为通过 NetScaler 的 ICA 流量提供端到端可见性。
网络报告	显示所有 NetScaler 实例的网络性能。
Web 洞察	提供企业 Web 应用程序的可见性，并允许对应用程序进行集成和实时监控。
安全洞察	帮助评估应用程序安全状态并采取纠正措施以保护应用程序。
网关洞察	提供对所有用户在登录 NetScaler Gateway 时遇到的故障的可见性，无论其访问模式如何。
事件	监视和管理 NetScaler 实例上事件或错误的发生。
应用程序仪表板	允许查看和管理应用程序。
机器人洞察	提供对机器人违规及其所采取操作的可见性。
系统日志	如果您已将设备配置为将所有系统日志消息重定向到 NetScaler Console，则监视 NetScaler 实例上生成的系统日志事件。
视频洞察	监视 NetScaler 实例使用的视频优化技术的指标。
详细事务	提供对 Web 事务的可见性，并以可视化方式显示客户端、NetScaler 和服务器之间的响应时间指标。

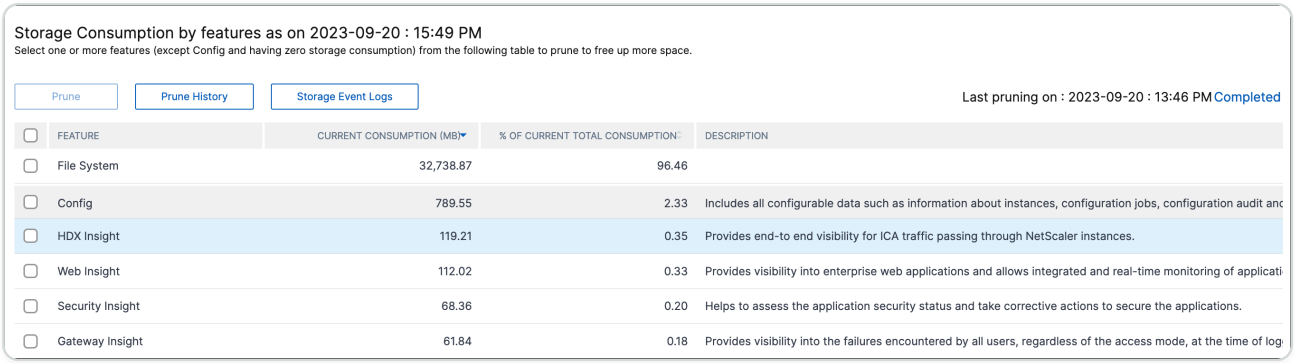
按功能划分的存储消耗

要详细了解数据存储如何在不同功能之间分布，请查看 **按功能划分的存储消耗，截至 *dd mmm*** 部分。

按功能划分的存储消耗，截至 *dd mmm* 帮助您了解：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Console 中所有不同功能使用的存储空间
- 功能在特定日期消耗的空间百分比

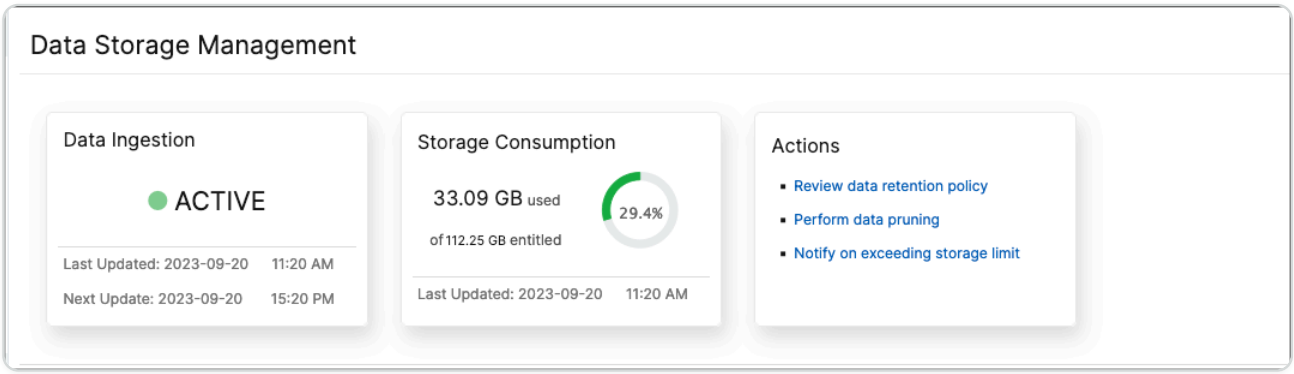


如果要对表条目进行排序，请点击表头。NetScaler Console 会根据所选列中的数据，按字母数字从上到下对表进行排序。要以倒序对表进行排序，请再次单击列标题。

有关修剪数据、修剪历史记录和存储事件日志的信息，请参阅 管理数据存储

管理您的存储空间

您可以使用“**数据存储管理**”仪表板来观察您的数据存储使用情况，并在数据存储超出许可限制时采取必要措施来清理空间或增加存储。



“**操作**”磁贴显示了您可以采取的建议步骤列表，以管理您的存储容量：

- 查看数据保留策略
- 执行数据修剪
- 超出存储限制时通知

执行数据修剪

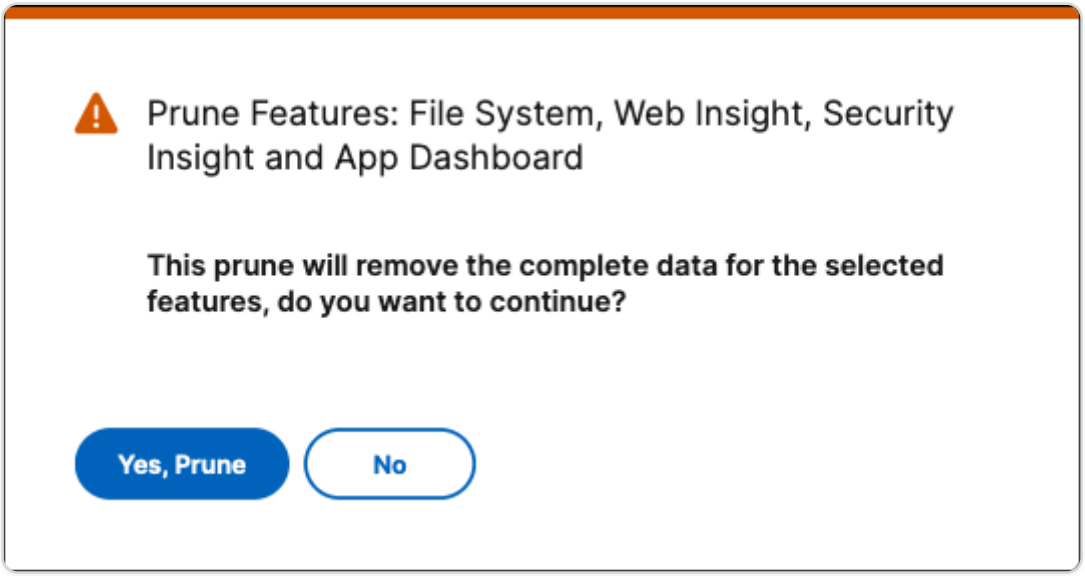
修剪数据以优化存储资源并获得更多存储空间。除了释放空间外，数据修剪还能提高数据质量并加快处理时间。我们建议您定期审查和清除不必要的数据。此过程可确保您的资源得到合理利用，并且 NetScaler Console 保持敏捷和响应迅速。

要修剪数据：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

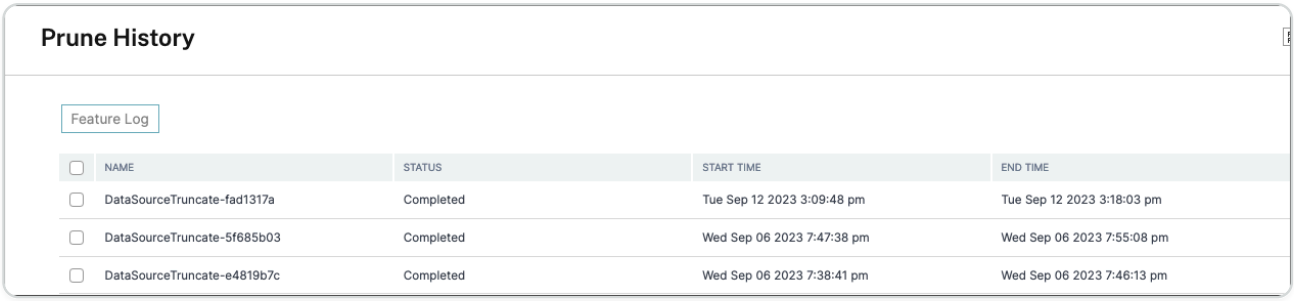
1. 在“**数据存储管理**”页面中，向下滚动到“***截至 yyyy-mm-dd 的功能存储消耗***”部分。
2. 选择一个或多个功能，然后单击“**修剪**”。您不能选择“**配置**”，因为它包含所有系统配置。

   弹出一个窗口，提示您确认是否要删除所选功能的所有数据。单击“**是，修剪**”。



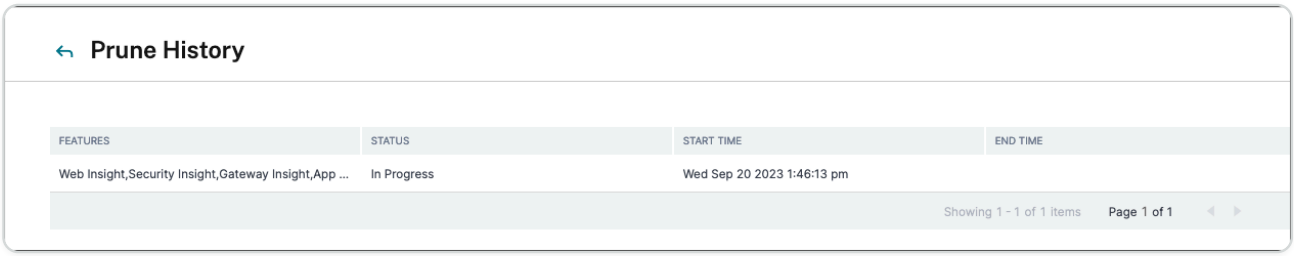
查看修剪历史记录

点击 **查看清除历史记录** 以获取您在 NetScaler Console 中执行的所有清除活动的详细信息。



清除日志: 任务日志 页面显示所有清除任务的列表，包括它们各自的状态、开始时间和结束时间。

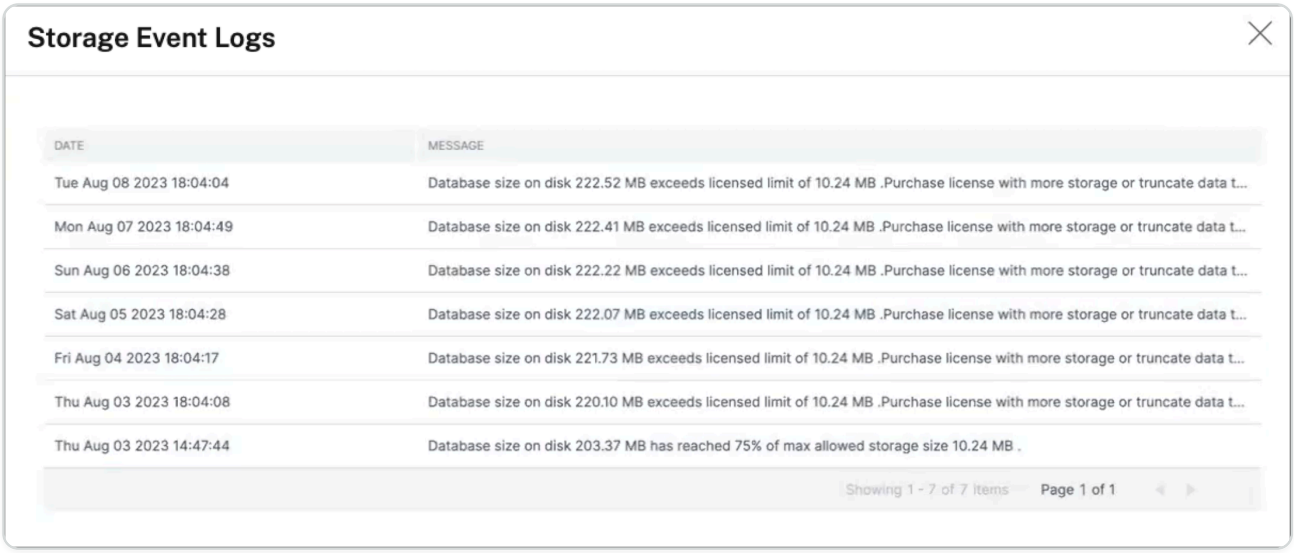
要了解在每次清除操作中删除了哪些功能，请选择一个任务并点击 **功能日志**。



查看存储事件日志

点击 **存储事件日志** 以了解您的数据超出或达到许可限制的 75% 的所有时间。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



查看数据保留策略

数据保留策略是指一组规则和配置，用于确定 NetScaler Console 如何随时间管理和维护历史数据。此策略概述了数据在自动删除之前存储多长时间。

如果您想减少所有不同功能使用的存储空间，可以更改数据在 NetScaler Console 中保留的时间。

使用 **数据保留策略** 页面编辑以下数据存储设置：

- 事件消息
- 系统日志消息
- 网络报告数据

有关数据存储设置的更多信息，请参阅 数据保留策略。

超出存储限制时通知

您可以为 NetScaler Console 设置通知，以便在您的数据存储容量超出指定限制时向您发送警报。

要查看和配置系统通知：

1. 在 **操作** 磁贴中，单击 **超出存储限制时通知**。
2. 在 **配置系统通知** 页面中，在 **系统事件类别** 下，确保选中 **DataStorageExceeded** 类别以接收通知。

您可以指定与通知发送给您或其他用户的方式和时间相关的各种参数。选择首选的通信方法（例如，电子邮件、Slack、PagerDuty 和 ServiceNow 通知），并定义通知的接收者。

有关如何设置配置文件和发送通知的更多信息，请参阅 配置通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

数据保留策略

为了限制 NetScaler Console 服务器数据库中存储的报告数据量，您可以指定 NetScaler Console 保留网络报告数据、事件、审计日志和任务日志的时间间隔。默认情况下，此数据每 24 小时（00:00 时）清除一次。

配置系统清除设置

要配置系统清除设置，请执行以下操作：

1. 导航到 **Settings（设置）> Data Storage（数据存储）> Data Retention Policy（数据保留策略）**。
2. 在 **Data Pruning（数据清除）**页面中，单击 **System（系统）**。
3. 在 **System（系统）**页面中，输入以下详细信息：
   - **Data to keep(days)（数据保留天数）** - 输入数据必须保留的天数。您必须指定一个介于 1 到 30 之间的值。
   - **Data Prune Threshold Value (%)（数据清除阈值 (%)）** - 输入一个阈值限制（百分比），作为数据清除或数据清理过程的条件。当数据库中的数据达到存储容量的指定百分比时，将触发数据清除过程以删除数据并释放空间。
   - **Auto Prune Details（自动清除详细信息）** - 如果您希望在满足以下任一条件时开始数据清除，请选择**Enable Automatic Data Prune（启用自动数据清除）**：
     - 达到**数据清除阈值 (%)** 中指定的数据阈值。
     - 达到**数据保留天数**中指定的天数。
   - **Data Ingestion Setting（数据摄取设置）** - 输入一个阈值限制（百分比），作为数据摄取的条件。当数据库中的数据达到此指定百分比时，数据摄取活动将暂停。您必须指定一个介于 50% 到 80% 之间的限制。
4. 单击 **Save（保存）**以保存设置。

配置实例事件清除设置

为了限制存储在 NetScaler Console 服务器数据库中的事件消息数据量，您可以指定 NetScaler Console 保留网络报告数据、事件、审计日志和任务日志的时间间隔。默认情况下，此数据每 24 小时（00:00 时）修剪一次。

配置实例事件修剪设置：

1. 导航到 **设置 > 数据存储 > 数据保留策略**。
2. 在 **Data Pruning** 页面中，单击 **Instance Events**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 在 **Data to keep (days)** 字段中，输入您希望 NetScaler Console 服务器保留数据的时间间隔（以天为单位），然后单击 **Save**。

配置实例 syslog 修剪设置

为了限制数据库中存储的 syslog 数据量，您可以指定清除 syslog 数据的时间间隔。您可以指定通用 syslog 数据从 NetScaler Console 中删除的天数。

配置实例 syslog 清除设置：

1. 导航到 **设置 > 数据存储 > 数据保留策略**。
2. 在 **Data Pruning** 页面中，单击 **Instance Events**。
3. 在 **Retain Syslog Generic Data** 字段中，指定 1 到 180 之间的天数。
4. 单击 **Save**。

配置网络报告修剪设置

为了限制 NetScaler Console 中存储的网络报告数据，您可以指定希望保留网络报告历史数据的时间间隔。

配置实例事件修剪设置：

1. 导航到 **设置 > 数据存储 > 数据保留策略**。
2. 在 **Data Pruning** 页面中，单击 **Network Reporting**。
3. 在 **Data to keep (days)** 字段中，指定 1 到 30 之间的天数。
4. 单击 **Save**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console 作为 API 代理服务器

除了能够接收用于自身管理和分析功能的 NITRO REST API 请求之外，NetScaler Application Delivery Management (NetScaler Console) 还可以作为其托管实例的 REST API 代理服务器。REST API 客户端无需直接向托管实例发送 API 请求，而是可以将 API 请求发送到 NetScaler Console。NetScaler Console 可以区分它必须响应的 API 请求和必须原封不动地转发给托管实例的 API 请求。

作为 API 代理服务器，NetScaler Console 为您提供以下优势：

- **API 请求验证**。NetScaler Console 根据配置的安全和基于角色的访问控制 (RBAC) 策略验证所有 API 请求。NetScaler Console 还具有租户感知能力，可确保 API 活动不会跨越租户边界。
- **集中审计**。NetScaler Console 维护与其托管实例相关的所有 API 活动的审计日志。
- **会话管理**。NetScaler Console 使 API 客户端无需维护与托管实例的会话。

作为 API 代理服务器，NetScaler Console 支持管理员分区。

NetScaler Console 如何作为 API 代理服务器工作

当您希望 NetScaler Console 将请求转发到托管实例时，您可以配置 API 客户端，使其在 API 请求中包含以下任一 HTTP 标头：

标头值	描述
MPS-API-PROXY-MANAGED-INSTANCE-NAME	托管实例的名称。
MPS-API-PROXY-MANAGED-INSTANCE-IP	托管实例的 IP 地址。
MPS-API-PROXY-MANAGED-INSTANCE-ID	受管实例的 ID。
MPS-API-PROXY-TIMEOUT	NITRO API 请求的超时值。以秒为单位设置超时值。当您设置代理超时时，NetScaler Console 会等待指定的持续时间，然后请求才会超时。
MPS-API-PROXY-MANAGED-INSTANCE-USERNAME	访问受管 NetScaler 实例的用户名。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

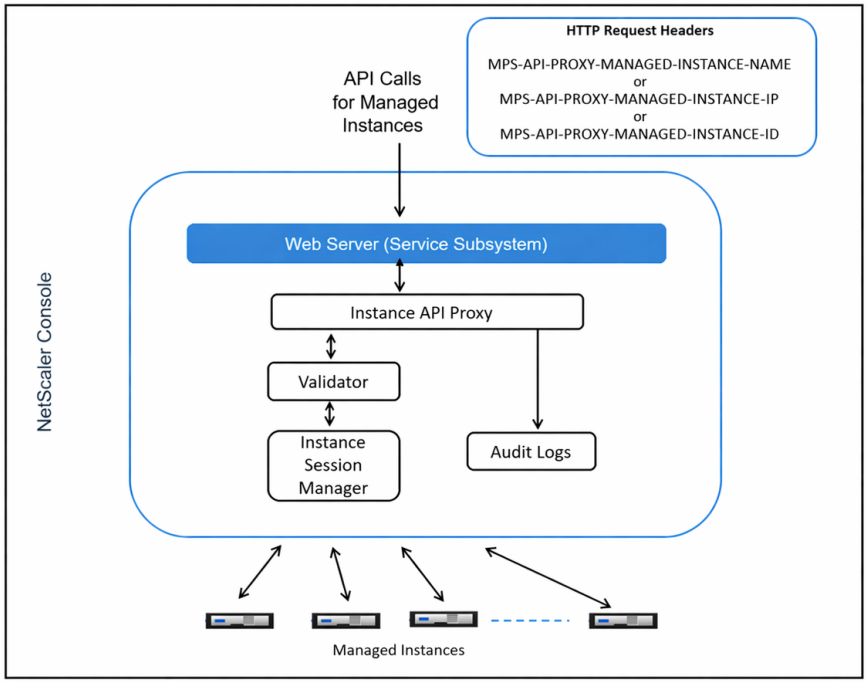
标头值	描述
MPS-API-PROXY-MANAGED-INSTANCE-PASSWORD	访问受管 NetScaler 实例的密码。
MPS-API-PROXY-MANAGED-INSTANCE-SESSID	访问受管实例的会话 ID。

注意

在 **设置 > 管理 >** 系统配置 **> 基本设置** 中，如果选择 **提示实例登录凭据**，请确保配置受管实例的用户名和密码。或者，您也可以指定实例会话 ID。

任何这些 HTTP 标头的存在都有助于 NetScaler Console 将 API 请求识别为必须转发到受管实例的请求。标头的值有助于 NetScaler Console 识别必须转发请求到的受管实例。

下图描述了此流程：



如上图所示，当请求中出现这些 HTTP 标头之一时，NetScaler Console 会按如下方式处理请求：

1. NetScaler Console 不修改请求，直接将请求转发到实例 API 代理引擎。
2. 实例 API 代理引擎将 API 请求转发给验证器，并在审计日志中记录 API 请求的详细信息。
3. 验证器确保请求不违反配置的安全策略、RBAC 策略、租户边界等。它还会执行额外检查，例如检查托管实例是否可用。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

如果 API 请求有效且可以转发到托管实例，NetScaler Console 会识别由实例会话管理器维护的会话，然后将请求发送到托管实例。

注意

确保**提示实例登录凭据**选项已禁用。为此，请执行以下操作：

1. 导航到**设置 > 管理**。
2. 在**系统配置**中，选择**系统、时区、允许的 URL 和每日消息**。

如何将 NetScaler Console 用作 API 代理服务器

以下示例显示了 API 客户端发送到 IP 地址为 192.0.2.5 的 NetScaler Console 服务器的 REST API 请求。NetScaler Console 需要将请求原封不动地转发到 IP 地址为 192.0.2.10 的托管实例。所有示例都使用 MPS-API-PROXY-MANAGED-INSTANCE-IP 标头。

在向 NetScaler Console 发送 API 请求之前，API 客户端必须：

- 登录 NetScaler Console
- 获取会话 ID
- 在后续 API 请求中包含会话 ID。

登录 API 请求格式如下：

```
POST /nitro/v1/config/login

Content-Type: application/json



{

    "login": {

        "username":"nsroot",

        "password":"nsroot"

     }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    }
```

NetScaler Console 会响应登录请求，响应中包含会话 ID。以下示例响应正文显示了一个会话 ID：


```
{

  "errorcode": 0,

  "message": "Done",

  "operation": "add",

  "resourceType": "login",

  "username": "***********",

  "tenant_name": "Owner",

  "resourceName": "nsroot",

  "login": [

    {
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "tenant_name": "Owner",

        "permission": "superuser",

        "session_timeout": "36000",

        "challenge_token": "",

        "username": "",

        "login_type": "",

        "challenge": "",

        "client_ip": "",

        "client_port": "-1",

        "cert_verified": "false",

        "sessionid":
"##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
```


© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
      "token": "b2f3f935e93db6a"
    }

  ]

}
```

示例 1：检索负载均衡虚拟服务器统计信息

客户端必须向 NetScaler Console 发送以下格式的 API 请求：

```
GET /nitro/v1/stat/lbvserver

Content-type: application/json

MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

其中 Cookie Header 的值是登录 API 调用返回的会话 ID。MPS-API-PROXY-MANAGED-INSTANCE-IP 的值是 NetScaler 的 IP 地址。

示例 2：创建负载均衡虚拟服务器

客户端必须向 NetScaler Console 发送以下格式的 API 请求：

```
    POST /nitro/v1/config/lbvserver/sample_lbvserver

    Content-type: application/json

    Accept-type: application/json
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D



{

     "lbvserver":{

         "name":"sample_lbvserver",

         "servicetype":"HTTP",

         "ipv46":"10.102.1.11",

         "port":"80"

     }

}
```

示例 3：修改负载均衡虚拟服务器

客户端必须向 NetScaler Console 发送以下格式的 API 请求：

```
PUT /nitro/v1/config/lbvserver

Content-type: application/json

Accept-type: application/json

MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10

SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D



{

   "lbvserver":{
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "name":"sample_lbvserver",

            "appflowlog":"DISABLED"

        }

    }
```

示例 4：删除负载均衡虚拟服务器

客户端必须向 NetScaler Console 发送以下格式的 API 请求：

```
    DELETE /nitro/v1/config/lbvserver/sample_lbvserver

    Accept-type: application/json

    MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10

    SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

示例 5：下载 NetScaler 上的 CLI 运行配置

客户端必须向 NetScaler Console 发送以下格式的 API 请求：

```
    GET /nitro/v1/config/nsrunningconfig

    Accept-type: application/json

    MPS-API-PROXY-MANAGED-INSTANCE-IP: 192.0.2.10

    SESSID: ##D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

常见问题

本节提供有关以下 NetScaler Application Delivery Management (NetScaler Console) 功能的常见问题解答。单击下表中的功能名称可查看该功能的常见问题列表。

分析	身份验证	配置管理
证书管理	部署	部署（灾难恢复）
事件管理	实例管理	StyleBooks
系统管理		

分析

是否需要在以单跳模式部署的 NetScaler Gateway 实例上启用 EUEM 虚拟通道?

EUEM 虚拟通道数据是 NetScaler Console 从 Gateway 实例接收的 HDX Insight 数据的一部分。EUEM 虚拟通道提供有关 ICA RTT 的数据。如果未启用 EUEM 虚拟通道，则剩余的 HDX Insight 数据仍会在 NetScaler Console 上显示。

EUEM 虚拟通道是 Citrix Virtual Desktop 应用程序 (VDA) 上运行的默认服务。如果它未运行，请在 VDA 服务中启动“Citrix End User Experience Monitoring”进程。

如何启用 NetScaler Console 来监控 Web 应用程序和虚拟桌面流量?

1. 导航到 **Infrastructure** \> **Instances** \> **NetScaler**，然后选择要启用分析的 NetScaler 实例。
2. 从 **Select Action** 列表中，选择 **Configure Analytics**。
3. 在 **Configure Analytics** 页面中，选择要启用分析的所有虚拟服务器，然后单击 **Enable AppFlow**。有关更多详细信息，请参阅 How to Enable Analytics on Instances。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

对于 11.0 版本、65.30 版本及更高版本的 NetScaler 实例，NetScaler Console 上没有明确启用 Security Insight 的选项。请确保在 NetScaler 实例上配置 AppFlow 参数，以便 NetScaler Console 开始接收 Security Insight 流量以及 Web Insight 流量。有关如何在 NetScaler 实例上设置 AppFlow 参数的更多信息，请参阅 To set the AppFlow parameters by using the configuration utility。

添加 NetScaler 实例后，NetScaler Console 会自动开始收集分析信息?

否。在 NetScaler Console 管理的 NetScaler 实例中托管的虚拟服务器上启用分析。有关更多详细信息，请参阅 How to Enable Analytics on Instances。

是否需要访问单个 NetScaler 设备才能启用分析?

否。所有配置均通过 NetScaler Console 用户界面完成，该界面列出了特定 NetScaler 实例上托管的虚拟服务器。有关更多详细信息，请参阅 How to Enable Analytics on Instances。

可以在 NetScaler 实例上列出哪些类型的虚拟服务器以启用分析?

目前，NetScaler Console 用户界面列出了以下用于启用分析的虚拟服务器：

- 负载平衡虚拟服务器
- 内容交换虚拟服务器
- VPN 虚拟服务器
- 缓存重定向虚拟服务器

如何将额外磁盘附加到 NetScaler Console?

要将额外磁盘附加到 NetScaler Console，请执行以下操作：

1. 关闭 NetScaler Console 虚拟机。
2. 在虚拟机管理程序中，将所需磁盘大小的额外磁盘附加到 NetScaler Console 虚拟机。

   例如，假设您想将一个 120 GB 的 NetScaler Console 虚拟机中的磁盘空间增加到 200 GB。在这种情况下，您必须附加 200 GB 的磁盘空间，而不是 80 GB。新附加的 200 GB 磁盘空间将用于存储数据库数据和 NetScaler Console 日志文件。现有的 120 GB 磁盘空间用于存储核心文件、操作系统日志文件等。
3. 启动 NetScaler Console 虚拟机。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler 实例上未配置收集器是什么意思?

收集器接收由 NetScaler 设备生成的 AppFlow 记录。

当启用 AppFlow 功能时，NetScaler Console 从 NetScaler 实例接收 Security Insight 和 Web Insight 流量。当您在 NetScaler 实例上启用 AppFlow 功能时，您必须指定至少一个收集器来接收 AppFlow 记录。如果未在 NetScaler 实例上配置收集器，NetScaler Console 将不会从这些实例接收流量。

例如，有五个 NetScaler 实例已添加到 NetScaler Console。如果未为其中两个实例指定收集器，则没有流量流向 NetScaler Console。自助诊断会检测到此问题，并将其显示为“未在 2 个实例上配置收集器”。

有关如何配置 AppFlow 功能的更多信息，请参阅 配置 AppFlow 功能。

启用客户端测量有什么作用?

启用客户端测量后，NetScaler Console 通过 HTML 注入捕获 HTML 页面的加载时间和渲染时间指标。管理员可以使用这些指标来识别 L7 延迟问题。

身份验证

什么是身份验证请求的负载均衡?

身份验证服务器负载均衡功能使 NetScaler Console 能够对指向外部身份验证服务器的身份验证请求进行负载均衡。对身份验证服务器进行负载均衡可确保身份验证负载分散到多个身份验证服务器，从而避免身份验证服务器过载。您可以使用 LDAP、RADIUS 或 TACACS 等身份验证协议创建身份验证服务，以连接到现有外部身份验证服务器并从中获取用户信息。

为什么需要级联外部身份验证服务器?

级联的外部身份验证服务器提供不间断的身份验证处理，允许在身份验证服务器发生故障时合法用户仍可访问。对可级联的身份验证服务器类型没有限制。您可以拥有所有 RADIUS 服务器、所有 LDAP 服务器，或者 RADIUS 和 LDAP 服务器的组合。

我可以级联多少个外部身份验证服务器?

您可以在 NetScaler Console 中级联最多 32 个外部身份验证服务器。

当外部身份验证失败时，我是否有替代方案?

即使您已级联了多个服务器，也可能出现外部身份验证完全失败的情况。例如，外部服务器可能无法访问，或者新用户的凭据可能尚未输入到任何外部身份验证服务器中。为防止在这种情况下将用

© 1997–2026 Citrix Systems, Inc. All rights reserved.

户锁定在系统之外，您可以启用回退本地身份验证。有关更多详细信息，请参阅 回退本地身份验证。

什么是回退本地身份验证?

回退本地身份验证是一种在外部身份验证失败时本地验证用户身份的选项。如果外部身份验证失败，NetScaler Console 会访问本地用户数据库以验证您的用户身份。

在 NetScaler Console 中，导航到 **设置 > 身份验证 > 身份验证配置**。在此页面上，您可以级联添加多个外部身份验证服务器，并选择“**启用回退本地身份验证**”选项。

什么是外部用户组的提取?

如果您已添加外部服务器来验证用户身份，则可以将现有用户组导入（提取）到 NetScaler Console 中。您只需导入一次用户组并为用户组提供组权限，而无需导入单个用户并为其授予单独权限。您无需在 NetScaler Console 上重新创建用户。

为什么需要分配组权限?

当您使用 NetScaler 的负载平衡功能时，可以将 NetScaler Console 与外部身份验证服务器集成，并从身份验证服务器导入用户组信息。登录到 NetScaler Console，并在 NetScaler Console 中手动创建相同的组信息，然后为这些组分配权限。用户和用户组权限在 NetScaler Console 中管理，而不是在外部服务器中管理。用户在外部服务器上具有不同的基于角色的访问权限。也要在 NetScaler Console 中为用户配置相同的权限。您可以配置组级别权限，而不是为每个用户单独配置权限，这样用户组成员就可以访问负载平衡虚拟服务器上的特定服务。您可以分配的典型权限是管理 NetScaler 实例、NetScaler SDX 实例、虚拟服务器等的权限，以便该组的用户只能管理这些实例或虚拟服务器。您以后可以在组级别编辑授予用户的权限。您甚至可以删除一个或多个用户组；其他组用户仍可在 NetScaler Console 上运行。

配置管理

我可以使用 NetScaler Console 同时在多个 NetScaler 实例上执行配置吗?

是的，您可以使用配置作业在多个 NetScaler 实例上执行配置。

NetScaler Console 上的配置作业是什么?

作业是您可以在一个或多个托管实例上创建和运行的一组配置命令。您可以创建作业以跨实例进行配置更改，在网络上的多个实例上复制配置，以及使用 NetScaler Console GUI 录制和回放配置任务。您还可以将录制的任务转换为 CLI 命令。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您可以使用 NetScaler Console 的“配置作业”功能来创建配置作业、发送电子邮件通知以及检查所创建作业的执行日志。

我可以使用 NetScaler Console 中的内置模板来安排作业吗?

是的！您可以使用内置模板选项来安排作业。作业是您可以在一个或多个托管实例上运行的一组配置命令。例如，您可以使用内置模板选项来安排配置 syslog 服务器的作业。您可以选择立即运行作业，也可以安排作业稍后运行。

您可以保存以前创建的作业配置，并在修改命令、参数、配置源和目标实例后再次运行该作业。当需要在不同的实例上运行同一组命令时，或者当作业遇到错误并停止进一步执行时，这非常有用。

证书管理

从 NetScaler Console 中删除 SSL 证书会导致从 NetScaler 实例中删除证书吗?

否

部署

默认用户名和密码是什么?

- 完成初始网络配置后，您可以使用默认用户名和密码 (nsrecover/nsroot) 从管理程序或 SSH 控制台登录到 NetScaler Console。
- 从 GUI 登录的默认用户名和密码是 *nsroot/nsroot*。

如何更改默认密码?

注意：

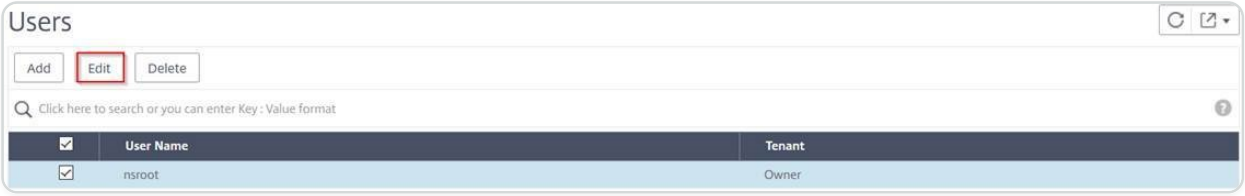
从版本 14.1-8x 开始，首次使用默认凭据登录 NetScaler Console GUI 或 API 后，系统会提示您更改默认密码。

要更改密码：

1. 在 NetScaler Console 中，导航到 **设置 > 用户管理 > 用户**。

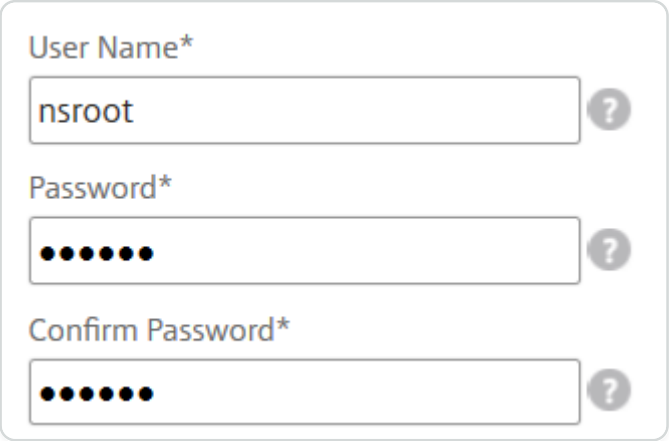
   此时将显示 **Users page**。
2. 选择用户名 **nsroot**，然后单击 **Edit**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



此时将显示 **Configure System User** 页面。

3. 选择 **Change Password** 并创建您选择的密码。



4. 单击 **OK**。

   您现在可以使用新密码从 GUI、管理程序或 SSH 控制台登录。

> **注意：**
>
> 您无法修改用户名。

如何重置密码?

您可以参阅此文档来重置密码。

在 HA 对中，如果主节点中的密码已更改，并且稍后选择了“中断 HA 对”选项，行为会是怎样?

您可以使用新密码登录到两个独立节点。

如果两台独立服务器的密码不同，将这两台服务器部署到 HA 对中会有什么影响?

建议在将两台独立服务器部署到 HA 对时，为这两台服务器设置默认密码。

HA 配置已完成，但主节点 GUI 无法访问。原因可能是什么?

配置生效需要几分钟。您可以在几分钟后尝试再次访问。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HA 配置已完成，但浮动 IP 地址 GUI 无法访问。原因可能是什么?

完成 HA 配置后，您需要首先访问主节点 GUI 并完成部署。有关详细信息，请参阅将主节点和辅助节点部署为高可用性对。部署完成后，服务器将重新启动并准备好进行高可用性部署。然后，您可以访问浮动 IP 地址 GUI。

NetScaler Console 独立版和 NetScaler Console HA 支持哪些数据库?

NetScaler Console 独立版和 NetScaler Console HA 都支持 PostgreSQL。

辅助节点可能存在哪些数据丢失?

辅助节点侦听主节点通过 NetScaler Console 数据库发送的心跳消息。如果辅助节点在 180 秒内未收到心跳，则辅助节点会对主节点执行基于 SSH 的检查。如果心跳和基于 SSH 的检查失败，则认为主节点已宕机。

在这种情况下，辅助节点将接管成为主节点，并且 180 秒的时间范围可视为辅助节点可能的数据丢失量。

如果主节点宕机，会发生什么?

辅助节点将接管并成为主节点。

如何重新安装故障节点?

建议安装全新的虚拟机版本。重新安装步骤如下：

1. 解除 HA 对。导航到 **Settings > Deployment**

   显示部署页面。单击 **Break HA**
2. 从虚拟机管理程序中删除故障节点。
3. 将 .XVA 映像文件导入到虚拟机管理程序。
4. 在“控制台”选项卡中，使用初始网络配置配置 NetScaler Console。有关详细信息，请参阅 注册和部署第一个服务器（主节点） 和 注册和部署第二个服务器（辅助节点）。
5. 重新部署 HA 对。

NetScaler Console 是否支持 SAN 存储?

我们建议您将 NetScaler Console VHD 托管在本地存储上。当托管在 SAN 中的存储设备上时，NetScaler Console 可能无法按预期工作。因此，不支持在 SAN 上部署 NetScaler Console。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console 是否支持额外磁盘?

是的。NetScaler Console HA 对的新安装默认分配 120 GB 存储空间。对于超过 120 GB 的存储空间，您可以添加一个额外磁盘，最大可达 3 TB 存储空间。不支持添加多个额外磁盘。

禁用 HA 对后，配置的浮动 IP 地址会发生什么?

浮动 IP 地址不再可访问，您需要重新部署高可用性对。

重新部署时可以提供不同的浮动 IP 地址吗?

是的。您可以配置新的浮动 IP 地址。

为什么辅助节点 GUI 无法访问?

辅助节点只是一个只读副本服务器，仅当主节点因任何原因宕机时才充当主节点。我们建议访问主节点 GUI 或浮动 IP 地址 GUI。

如果主节点长时间宕机，是否仍可以使用浮动 IP 地址 GUI 进行配置?

是的。您仍然可以继续进行配置，并且配置会保存在辅助节点中。主节点恢复后，所有配置都会同步。

如果将来需要更改主节点 IP 地址、辅助节点 IP 地址或浮动 IP 地址（例如，更改为 IPv6），建议遵循哪些解决方案?

在不中断 HA 对的情况下，不支持更改 HA 对中的 IP 地址。

要更新主节点或辅助节点 IP 地址：

1. 中断 HA 对。导航到 **Settings > Deployment**。

   显示“部署”页面。单击 **Break HA**

   a. 使用 SSH 客户端或从管理程序登录到主节点。
   b. 使用 `nsrecover` 作为用户名，并输入您设置的密码。
   c. 输入 **networkconfig**。按照 注册并部署第一个服务器（主节点） 中提供的**步骤 3** 执行操作。

      在初始网络配置期间，您可以提供不同的 IP 地址。
   d. 对辅助节点执行相同的过程，并按照 注册并部署第二个服务器（辅助节点） 中提供的**步骤 3** 继续操作。

要更新浮动 IP 地址：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 导航到 **设置 > 部署**。

   将显示“部署”页面。

   a. 单击 **HA Settings**。

   b. 单击 **配置高可用性模式的浮动 IP 地址**。

   c. 输入浮动 IP 地址，然后单击 **OK**。

NetScaler Console 是否支持 AMD 处理器?

AMD 处理器支持以下版本：

- **NetScaler Console 13.1 build 4.43 或更高版本**。
- **NetScaler agent 13.1 build 17.42 或更高版本**。

部署（灾难恢复）

主站点和灾难恢复站点之间的复制频率如何?

主站点和灾难恢复站点之间的复制是实时的。

在灾难恢复站点启动备份脚本后，灾难恢复站点是否会成为临时主站点，直到主站点恢复并完全运行?

否。灾难恢复站点现在将成为主站点。要将 HA 对恢复为主站点，请参阅将配置恢复到原始主站点

如果选择了“中断 HA 对”选项，则两个节点都将作为独立服务器运行。由于灾难恢复不支持独立服务器，如果选择了“中断 HA 对”，灾难恢复站点会发生什么?

如果您选择“中断 HA 对”选项，则主站点和灾难恢复站点之间的复制将终止。您需要重新配置灾难恢复站点，作为重新部署 HA 对的一部分。

事件管理

如何使用 NetScaler Console 跟踪我的托管 NetScaler 实例上生成的所有事件?

作为网络管理员，您可以查看 NetScaler 实例上的详细信息，例如配置更改、登录条件、硬件故障、阈值违规和实体状态更改，以及特定实例上的事件及其严重性。您可以使用 NetScaler Console 事件仪表板查看为所有 NetScaler 实例上的关键事件严重性详细信息生成的报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

什么是事件规则?

使用 NetScaler Console，您可以配置规则来监视特定事件。事件规则使监视 NetScaler Console 基础架构中生成的许多事件变得更加容易。

您可以通过配置具有特定条件的规则并将操作分配给这些规则来筛选一组事件。当生成的事件符合规则中的筛选条件时，将运行与该规则关联的操作。

您可以创建筛选器的条件包括严重性、NetScaler 实例、类别和故障对象。您可以分配给事件的操作包括发送电子邮件通知、将 SNMP 陷阱从托管 NetScaler 实例转发到 NetScaler Console 以及发送短信通知。

实例管理

当您使用 NetScaler 池容量许可时，如果在分配带宽后 NetScaler 实例无法连接到 NetScaler Console，会发生什么?

如果 NetScaler 实例与 NetScaler Console 之间的心跳失败，实例将进入 30 天的宽限期。重新建立通信后，池化容量许可将开始工作。在宽限期内，NetScaler 功能不受影响。宽限期 30 天后，NetScaler 实例将启动热重启并取消许可。

NetScaler Console 中的数据中心是什么?

NetScaler Console 数据中心是特定地理位置中 NetScaler 实例的逻辑分组。每个服务器都可以监视和管理数据中心内的多个 NetScaler 实例。您可以使用 NetScaler Console 服务器管理来自受管实例的数据，例如 syslog、应用程序流量流和 SNMP 陷阱。有关配置数据中心的更多详细信息，请参阅《如何在 NetScaler Console 中为地理地图配置数据中心》。

NetScaler Console 支持哪些不同的 NetScaler 设备?

实例是您希望从 NetScaler Console 发现、管理和监视的 NetScaler 设备或虚拟设备。您必须将这些实例添加到 NetScaler Console 服务器。您可以将以下 NetScaler 设备和虚拟设备添加到 NetScaler Console：

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler 网关

您可以首次设置 NetScaler Console 服务器时添加实例，也可以稍后添加。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

什么是实例配置文件?

NetScaler Console 使用实例配置文件来访问实例。

实例配置文件包含用于访问一个或多个实例的用户名和密码。每种实例类型都有一个默认配置文件。例如，ns-root-profile 是 NetScaler 实例的默认配置文件。它包含默认的 NetScaler 管理员凭据。当您更改访问实例所需的凭据时，可以为这些实例定义自定义实例配置文件。

我可以在 NetScaler Console 中重新发现多个 NetScaler VPX 实例吗?

是，您可以在 NetScaler Console 中重新发现多个 Citrix **VPX** 实例，以了解这些实例的最新状态和配置。

导航到 **Infrastructure > Instances > NetScaler > VPX**，选择要重新发现的实例，然后在 **Action** 列表中单击 **Rediscover**。有关详细信息，请参阅 如何重新发现多个 VPX 实例。

NetScaler Console 可以安装在 NetScaler SDX 上吗?

否

我可以使用公共 IP 地址在 NetScaler Console 软件上添加 NetScaler 实例吗?

可以，您可以使用网络地址转换 (NAT)。

- 对于添加单个实例：使用 NetScaler 实例的公共 IP 地址的 NAT IP。
- 对于添加 NetScaler HA 对：按此格式添加 HA 对的 NAT IP 地址：

  `<NAT public IP of the primary instance>#<NAT public IP of the secondary instance>`
- 对于添加 NetScaler 群集：添加群集中所有实例的所有 NAT 公共 IP 地址，每个地址用逗号分隔，并将群集 IP 的 NAT IP 添加到括号或圆括号内。示例格式：NAT1, NAT2, NAT3, (CLUSTERIP 的 NATIP)。

有关详细信息，请参阅以下主题：

- 将实例添加到 NetScaler Console
- 配置网络地址转换

如果 DR 节点凭据已更改，如何注册灾难恢复节点?

使用以下命令将灾难恢复 (DR) 节点凭据重置为 `nsrecover` / `nsroot`：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
./mps/change_freebsd_password.sh <username> <password>
```

要注册 DR 节点，请按照 使用 DR 控制台部署和注册 NetScaler Console DR 节点 中的步骤操作。

StyleBooks

StyleBook 能否用于配置运行不同版本 NetScaler 软件的不同 NetScaler 实例?

可以，如果不同版本之间的命令没有差异，您可以使用 StyleBook 配置运行不同版本的不同 NetScaler 实例。

当 StyleBook 同时用于配置多个 NetScaler 实例时，如果其中一个 NetScaler 实例的配置失败，会发生什么?

如果将配置应用于某个 NetScaler 实例失败，则该配置将不再应用于任何其他实例，并且已应用的配置将回滚。

通过 NetScaler 进行的备份是否包含通过 StyleBook 应用的配置?

是

系统管理

我可以为我的 NetScaler Console 服务器分配主机名?

可以，您可以分配主机名来标识您的 NetScaler Console 服务器。要分配主机名，请导航到 **系统**\> **系统管理** \> **系统设置**，然后单击 **更改主机名**。

主机名显示在 NetScaler Console 的通用许可证上。有关详细信息，请参阅 如何为 NetScaler Console 服务器分配主机名。

我可以备份和恢复我的 NetScaler Console 配置?

可以，您可以备份配置文件（NTP 文件和 SSL 证书）、系统数据、基础设施和应用程序数据以及所有 **SNMP** 设置。如果您的 NetScaler Console 变得不稳定，您可以使用备份文件将其恢复到稳定状态。

要备份和恢复 NetScaler Console 配置，请导航到 **系统** > **高级设置** > **备份文件**，然后根据需要单击 **备份** 或 **恢复**。有关详细信息，请参阅 如何在 NetScaler Console 上备份和恢复配置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

建议您在执行升级之前或出于预防目的使用此功能。

NetScaler Console 中的阈值和警报是什么?

您可以设置阈值和警报来监控 NetScaler 实例的状态以及受管实例上的实体。

当计数器值超过阈值时，NetScaler Console 会生成警报以表示性能相关问题。当计数器值返回到阈值中指定的清除值时，事件将被清除。

我可以为 NetScaler Console 生成技术支持文件吗?

是的。我们建议您在联系技术支持调试问题之前，生成 NetScaler Console 数据和统计信息的存档。该存档是一个 TAR 文件，您可以将其发送给技术支持团队。

您可以生成一个技术支持文件，其中包含调试日志、调试日志的收集时长以及来自 NetScaler Console 数据库的独特且多样化的日志。

要配置和发送技术支持文件，请导航到 **System** \> **Diagnostics** \> **Technical Support**，然后单击 **Generate Technical Support File**。有关详细信息，请参阅 How to Generate a Tech Support File for NetScaler Console。

syslog 清除是什么?

Syslog 是一种标准的日志记录协议。Syslog 能够将生成信息的系统与存储信息的系统隔离开来。您可以整合日志信息并从收集的数据中获取见解。您还可以配置 syslog 以记录不同类型的事件。

为了限制数据库中存储的 syslog 数据量，您可以指定清除 syslog 数据的间隔。您可以指定在多少天后，所有通用 Syslog 数据、AppFirewall 数据和 NetScaler Gateway 数据将从 NetScaler Console 中删除。

我可以在 NetScaler Console 上配置 NTP 服务器吗?

您可以在 NetScaler Console 中配置网络时间协议 (NTP) 服务器，以使 NetScaler Console 时钟与 NTP 服务器同步。配置 NTP 服务器可确保 NetScaler Console 时钟与网络上的其他服务器具有相同的日期和时间设置。

要配置 NTP 服务器，请导航到 **System** \> **NTP Servers**，然后单击 **Add**。有关详细信息，请参阅 How to Configure NTP Server on NetScaler Console。

NetScaler Console 主动-被动 HA 部署从哪个版本开始支持?

NetScaler Console 主动-被动 HA 部署模式从 NetScaler Console 12.0 build 51.24 版本开始支持。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

我有一个 NetScaler Console 主动-主动 HA 设置，并且在其上配置了带有负载平衡虚拟服务器的 NetScaler 设备，用于统一 GUI 访问。如何更新此配置?

将 NetScaler Console HA 对升级到主动-被动模式后，您必须在 NetScaler 设备上运行以下命令以更新负载平衡配置：

添加负载均衡监视器 MAS_Monitor **TCP-ECV -send "GET /mas_health HTTP/1.1\\r\\nAccept-Encoding: identity\\r\\nUser-Agent: NetScaler-Monitor\\r\\nConnection: close\\r\\n\\r\\n\\"" -recv "{\\"statuscode\\":0, \\"is_passive\\":0}" -LRTM DISABLED**

我可以在 NetScaler 实例上使用端口 443 配置 NetScaler Console HA 对的负载平衡吗?

不可以，您不能在 NetScaler 实例上使用端口 443 配置 NetScaler Console HA 对的负载平衡。

当您在 NetScaler 上配置 `http-ecv` 和 `https-ecv` 监视器时，它无法正确监视 NetScaler Console HA 节点。

NetScaler Console 服务器备份文件可用于恢复另一个 NetScaler Console 服务器的配置吗?

是

NetScaler Console 备份 NetScaler 实例后，该备份文件是否可以通过 NetScaler Console 用于恢复另一个 NetScaler 实例的配置?

是。下载 NetScaler Console 备份文件，将其上传到另一个 NetScaler 实例的备份存储库中，并恢复该实例。确保网络信息和身份验证信息不冲突。例如，检查 IP 地址或端口冲突、密码配置文件不匹配等问题。此外，请确保恢复的 VPX 实例具有与备份实例相同的 NSIP 地址和 NetScaler 许可证。

在恢复高可用性对中的实例之前，请确保备份文件中存储的 IP 地址和状态（主或辅助）与原始 HA 配置中的信息匹配。此外，请验证新的主节点和辅助节点是否具有相同类型的 NetScaler 许可证。

我们可以强制 NetScaler Console 使用 SNIP 地址与 NetScaler 实例通信，而不是使用 NetScaler Console 服务器的 NSIP 地址吗?

是，您可以在 NetScaler Console 中添加 SNIP 地址（启用管理）用于与 NetScaler 实例通信。

当我在 NetScaler Console 中备份 NetScaler 实例时，结果是完全备份还是基本备份?

NetScaler Console 对 NetScaler 实例的备份是完整备份。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Console 是否有故障排除指南?

是的。请参阅 `<https://support.citrix.com/article/CTX224502>`。

NetScaler Console HA 故障转移发生时 NetScaler 实例的管理?

如果心跳和基于 SSH 的检查失败，则主节点被视为已关闭，辅助节点将接管作为主节点。默认情况下，所有 NetScaler 实例都会使用最新的主节点详细信息作为其 SNMP trap 目标进行更新。

新的主（活动）NetScaler Console 节点会检查以确定先前活动的节点是否配置为 AppFlow 收集器或 syslog 服务器；如果是，则新的主节点会将 AppFlow 收集器或 syslog 服务器详细信息添加到发送到实例的信息中。

对于 syslog，它会替换旧的服务器详细信息。

NetScaler Console HA 节点故障后恢复时的处理?

恢复服务后，NetScaler Console 节点将保持被动状态，除非活动节点发生故障转移

NetScaler 实例如何在 NetScaler Console HA 节点之间分布?

所有 NetScaler 实例均由主 NetScaler Console 节点管理。

如果发生 NetScaler Console HA 故障转移，如何管理虚拟服务器许可证?

如果应用了虚拟服务器许可证的 NetScaler Console 主节点发生故障，新的主节点将在 30 天的宽限期内管理虚拟服务器许可证。请在宽限期结束前在新主节点上重新应用许可证。有关替代方案，请联系 NetScaler 支持。

NetScaler Console HA 设置是否强制要求负载均衡器?

否，但如果没有负载均衡器，则必须通过其自身的 IP 地址访问 NetScaler Console 节点。被动节点标有“Passive”标签，我们建议不要在被动节点上创建任何配置。

被动节点(/en-us/netscaler-application-delivery-management-software/media/netscaler-mas-faq.png)

NetScaler Console 是否支持外部数据库?

否

© 1997–2026 Citrix Systems, Inc. All rights reserved.

由 NetScaler Console 管理的 NetScaler 实例能否用作 NetScaler Console HA 的负载均衡器?

是

NetScaler Console HA 节点之间同步哪些数据?

完整的 NetScaler Console 数据库已同步，并同步以下文件夹：

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/
- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/

© 1997–2026 Citrix Systems, Inc. All rights reserved.

index

- 配置自适应阈值
- 配置数据库汇总
- 配置 SLA 管理
- 创建阈值和警报
- 禁用 URL 数据收集
- Logstream 概述
- 仪表板
- 所有违规
- 应用程序概览
- 网络违规详情
- SSL 洞察
- 排查 Web Insight 问题
- 查看 Web 事务分析
- 设置双层或服务网格精简拓扑的详细步骤
- 设置服务网格拓扑的详细步骤
- 数据治理（适用于 14.1-8.x 到 14.1-21.x 版本之间的 NetScaler Console）
- 数据治理（适用于 NetScaler ADM 14.1-4.42 或更早版本）
- 用于 Cloud Connect 的可选遥测数据
- NetScaler® 遥测程序的可选遥测数据
- Cloud Connect 所需的遥测数据
- NetScaler® 遥测程序所需的遥测数据
- 许可
- 备份和恢复 HA 对中的 NetScaler Console 配置
- 配置系统通知设置
- 为地理地图配置站点

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置自适应阈值

自适应阈值功能设置每个 URL 的最大命中数阈值。如果 URL 的最大命中数大于为该 URL 设置的阈值，则会将 syslog 消息发送到外部 syslog 服务器。阈值间隔可以是天或周。

阈值计算方法如下：

阈值 = **最大命中数 * 阈值乘数**

其中：

- 最大命中数是 URL 的最大命中数。
- 阈值乘数是您定义的整数值（默认值：2）。

使用 NetScaler Console 创建自适应阈值

1. 导航到 **系统** \> **分析设置** \> **自适应阈值**，然后单击 **添加**。
2. 在 **创建自适应阈值** 页面上，指定以下参数：
   - **名称** - 阈值名称
   - **实体** - URL
   - **持续时间** - 阈值持续时间（天或周）
   - **阈值乘数** - 一个用户定义的整数，该整数与指定 URL 的最大命中数相乘，以获取该 URL 的自适应阈值。

配置数据库汇总

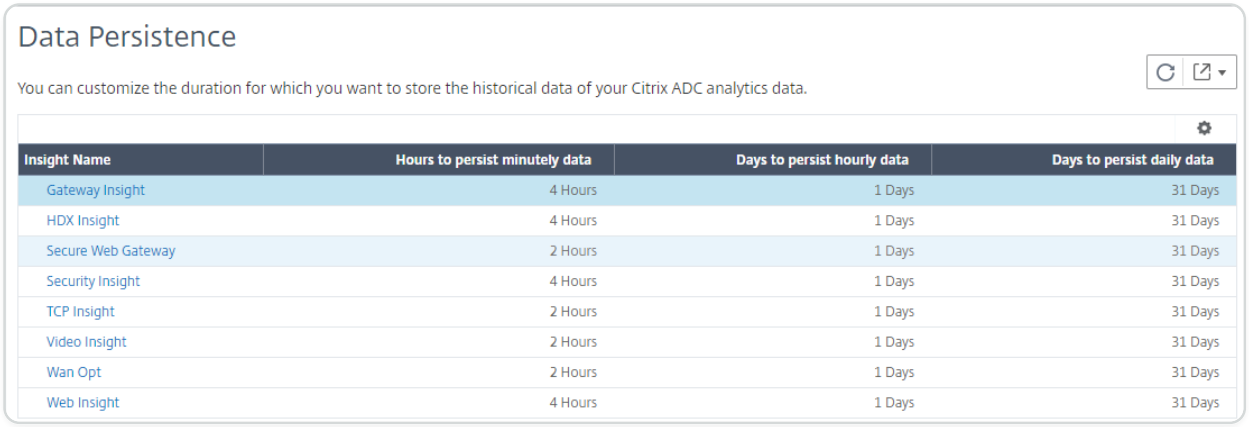
在 NetScaler Console 中配置数据库汇总允许您自定义存储 NetScaler 分析数据的历史数据的持续时间。您可以为分析的历史数据选择以下数据库汇总类型：

- 分钟数据的保留小时数
- 小时数据的保留天数
- 每日数据的保留天数

配置数据库汇总

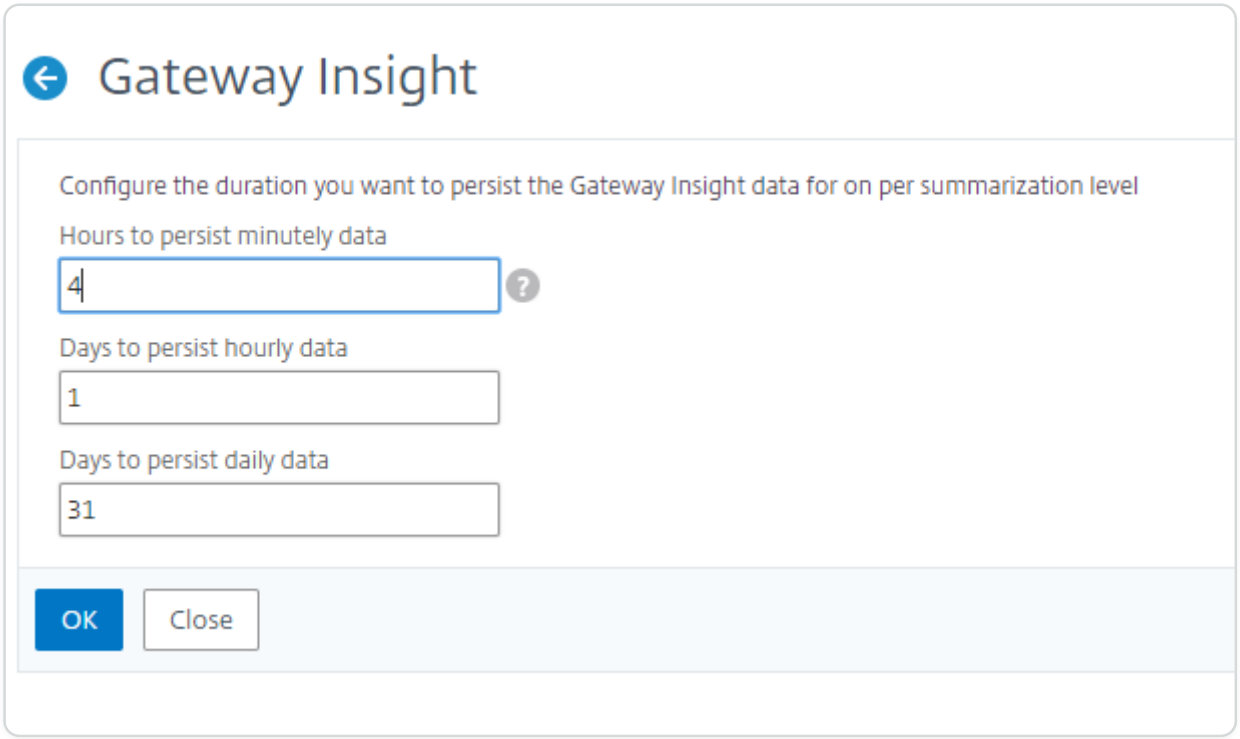
1. 导航到 **系统** \> **分析设置** \> **数据库汇总**。
2. 单击要配置数据库汇总的 Insight 类型。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Insight Name	Hours to persist minutely data	Days to persist hourly data	Days to persist daily data
Gateway Insight	4 Hours	1 Days	31 Days
HDX Insight	4 Hours	1 Days	31 Days
Secure Web Gateway	2 Hours	1 Days	31 Days
Security Insight	4 Hours	1 Days	31 Days
TCP Insight	2 Hours	1 Days	31 Days
Video Insight	2 Hours	1 Days	31 Days
Wan Opt	2 Hours	1 Days	31 Days
Web Insight	4 Hours	1 Days	31 Days

3. 指定要在 NetScaler Console 上保留 Insight 数据的持续时间。例如，对于 Gateway Insight，您可以将分析的分钟历史数据存储 2 小时，或将小时数据存储 1 天。



配置 SLA 管理

服务级别协议管理功能将帮助您管理服务器响应时间、每秒点击次数和带宽使用方面的 SLA，涵盖您的域使用。针对各种违规配置 SLA，可让您轻松监控 NetScaler 基础设施中生成的许多事件。

您可以配置以下各项的 SLA 违规：

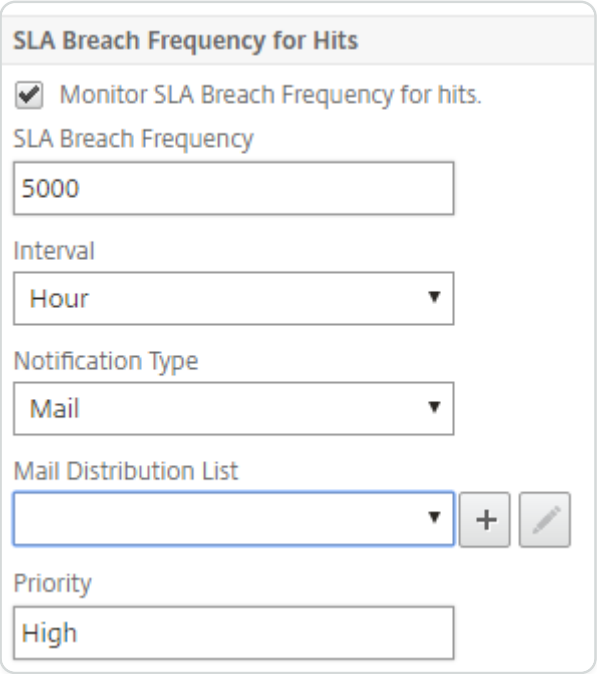
- 服务器响应时间
- 针对带宽的 SLA 违规频率
- 针对点击次数的 SLA 违规频率
- 针对响应时间的 SLA 违规频率

© 1997–2026 Citrix Systems, Inc. All rights reserved.

每当您的设备遇到 SLA 违规时，您可以为其配置通知。您可以将通知类型配置为邮件、短信或系统日志，并分别配置分发列表。

配置 NetScaler 实例的 SLA 违规

1. 导航到 **系统** \> **分析设置** \> **SLA 管理**。
2. 从显示的列表中，选择您要在其上管理 SLA 的设备的 NetScaler® IP 地址。
3. 如果您想添加新的“**SLA 组**”并向其中添加违规定义，请单击“**添加**”。或者，如果您已经添加了 SLA 组，则可以从列表中选择一个 SLA 组。
4. 在“**SLA 组**”字段中，输入新 SLA 组的名称。
5. 选择相应的复选框以启用或禁用 SLA 监视器。
6. 为所选选项选择相应的违规值。例如，最大服务器响应时间 (ms)* = 22 毫秒。
7. 从**通知类型**和**间隔**列表中选择通知类型和通知间隔。
8. 您可以从“邮件/短信/Syslog 分发列表”菜单中选择用于发送通知的分发列表。
9. 单击“**创建**”，以创建并将 SLA 组添加到您的 NetScaler 设备。



创建阈值和警报

您可以设置阈值和警报来监控 NetScaler 实例的状态。您可以在计数器上设置阈值，并监控托管实例上的实例和实体。

当计数器值超过阈值时，NetScaler Console 会生成一个事件，表示存在与性能相关的问题。当计数器值与阈值中指定的清除值匹配时，事件将被清除，这意味着该特定阈值已恢复正常状态。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

您还可以将操作与阈值关联。操作包括发送警报、电子邮件或短信通知。当阈值被突破时，NetScaler Console 会自动执行您定义的操作，例如启用警报并发送电子邮件或短信通知。

使用 NetScaler Console 创建阈值和警报

1. 导航到 **系统** \> **分析设置** \> **阈值**。在 **阈值** 下，单击 **添加**。
2. 在 **Create Thresholds and Alerts** 页面上，指定以下详细信息：
   - **Name** – 用于配置阈值的名称。
   - **Traffic Type** – 您要为其配置阈值的流量类型。
   - **Entity** – 您要为其配置阈值的类别或资源类型。
   - **Reference Key** – 根据所选流量类型和实体自动生成的值。
   - **Duration** - 您要为其配置阈值的间隔。
   - **Community** – 要发送到陷阱侦听器的每个陷阱的社区字符串。
3. （可选）配置警报、电子邮件通知和短信通知等操作。
4. 单击 **Create**。

对于 HDX™ insight，您还可以设置多个阈值，只有当配置的阈值中的所有实体都被突破时，才会生成警报。

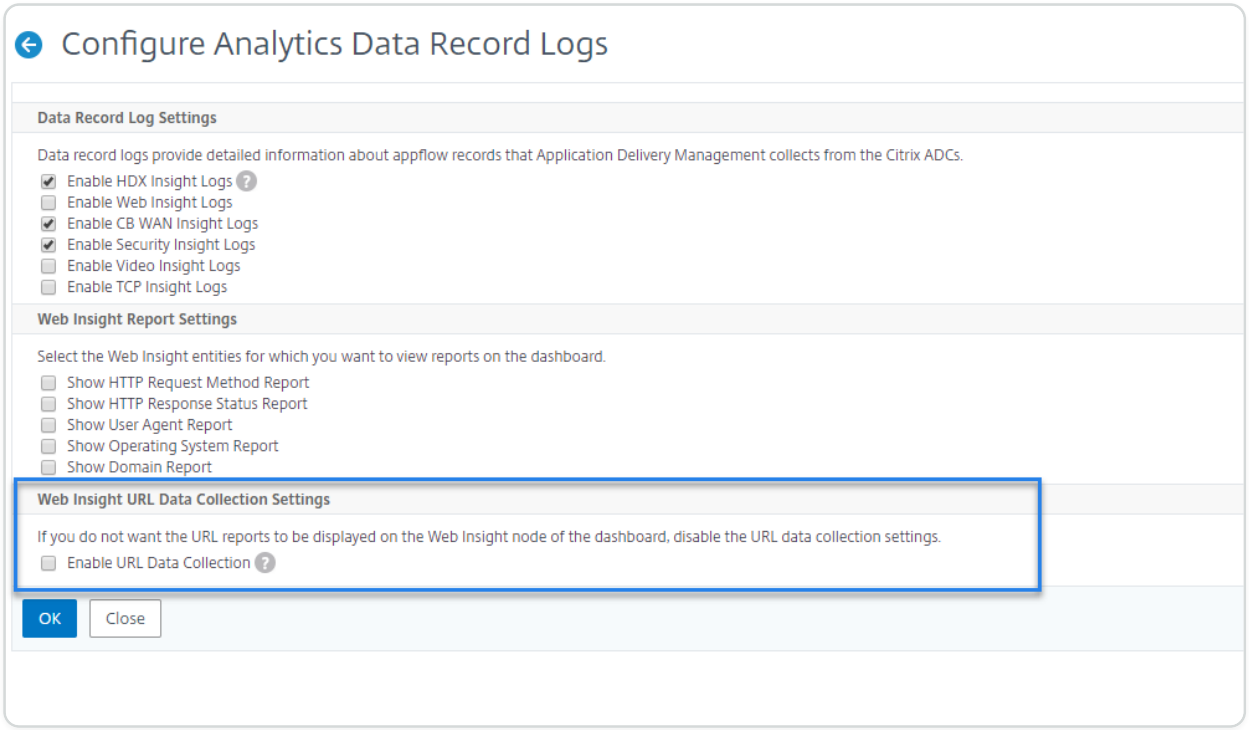
禁用 URL 数据收集

如果您不希望 URL 报告显示在 NetScaler Console 控制板的 Web Insight 节点上，可以禁用 URL 数据收集。

从 NetScaler Console 禁用 URL 数据收集

1. 导航到 **系统** \> **分析设置**，然后单击 **配置数据记录设置**。
2. 在 **Web Insight URL Data Collection Settings** 部分中，如果选中了 **Enable URL Data Collection** 选项，请清除该复选框。
3. 单击 **OK**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Logstream 概述

NetScaler 实例生成 AppFlow 记录，并且是数据中心所有应用程序流量的中心控制点。IPFIX 和 Logstream 是将这些 AppFlow 记录从 NetScaler 实例传输到 NetScaler Console 的协议。有关更多信息，请参阅 AppFlow。

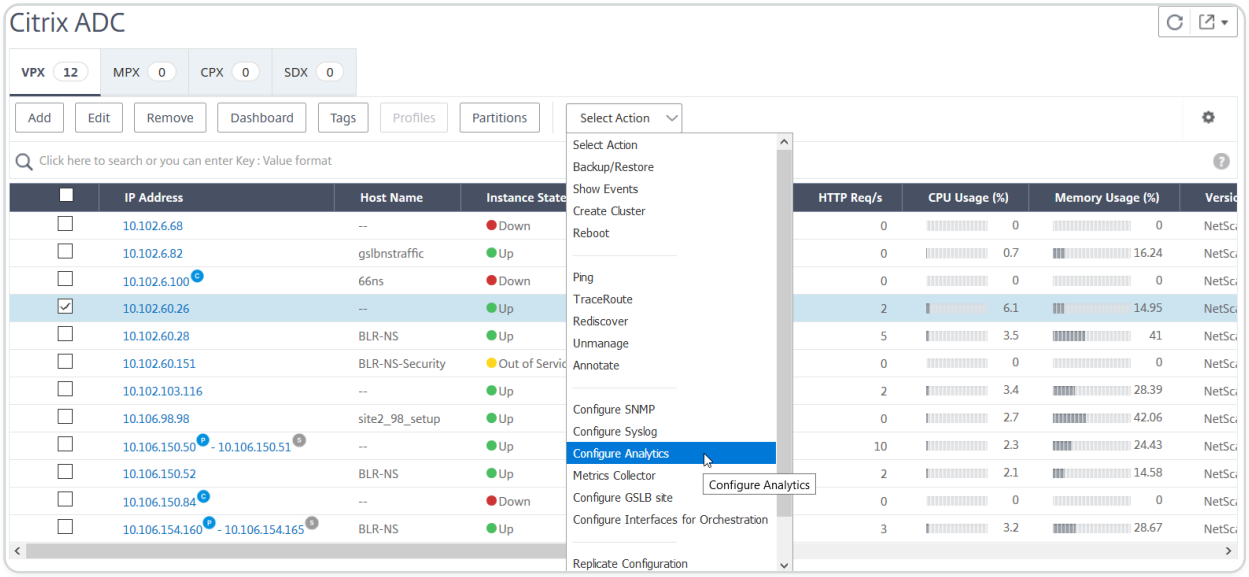
- IPFIX 是 RFC 5101 中定义的开放式互联网工程任务组 (IETF) 标准。IPFIX 使用 UDP 协议，这是一种用于单向数据流的不可靠传输协议。由于 IPFIX 使用 UDP 协议，因此遵循 IPFIX 标准会导致 NetScaler Console 中处理更多资源。
- Logstream 是 Citrix 专有协议，用作将分析日志数据从 NetScaler 实例高效传输到 NetScaler Console 的传输模式之一。Logstream 使用可靠的 TCP 协议，并且在处理数据时需要较少的资源。

对于 NetScaler **11.1 Build 47.14 到 11.1 Build 62.8** 之间的版本，Logstream 是启用 Web Insight (HTTP) 的默认传输模式，而 IPFIX 是启用其他洞察的唯一传输模式。对于从 **12.0 到最新版本**的 NetScaler 版本，您可以选择 **Logstream** 或 **IPFIX** 作为传输模式。

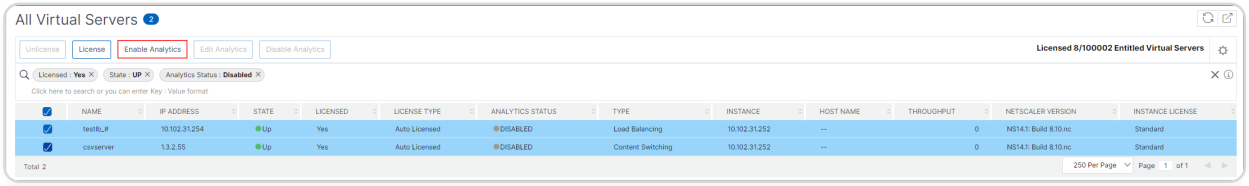
启用 Logstream 作为传输模式

1. 导航到 **基础结构 > 实例**，然后选择要启用分析的 NetScaler 实例。
2. 从“**选择操作**”列表中，选择“**配置分析**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 选择虚拟服务器，然后单击“**启用分析**”。



4. 在“**启用分析**”窗口中：

   a. 选择洞察类型（Web Insight 或 WAF 安全违规）

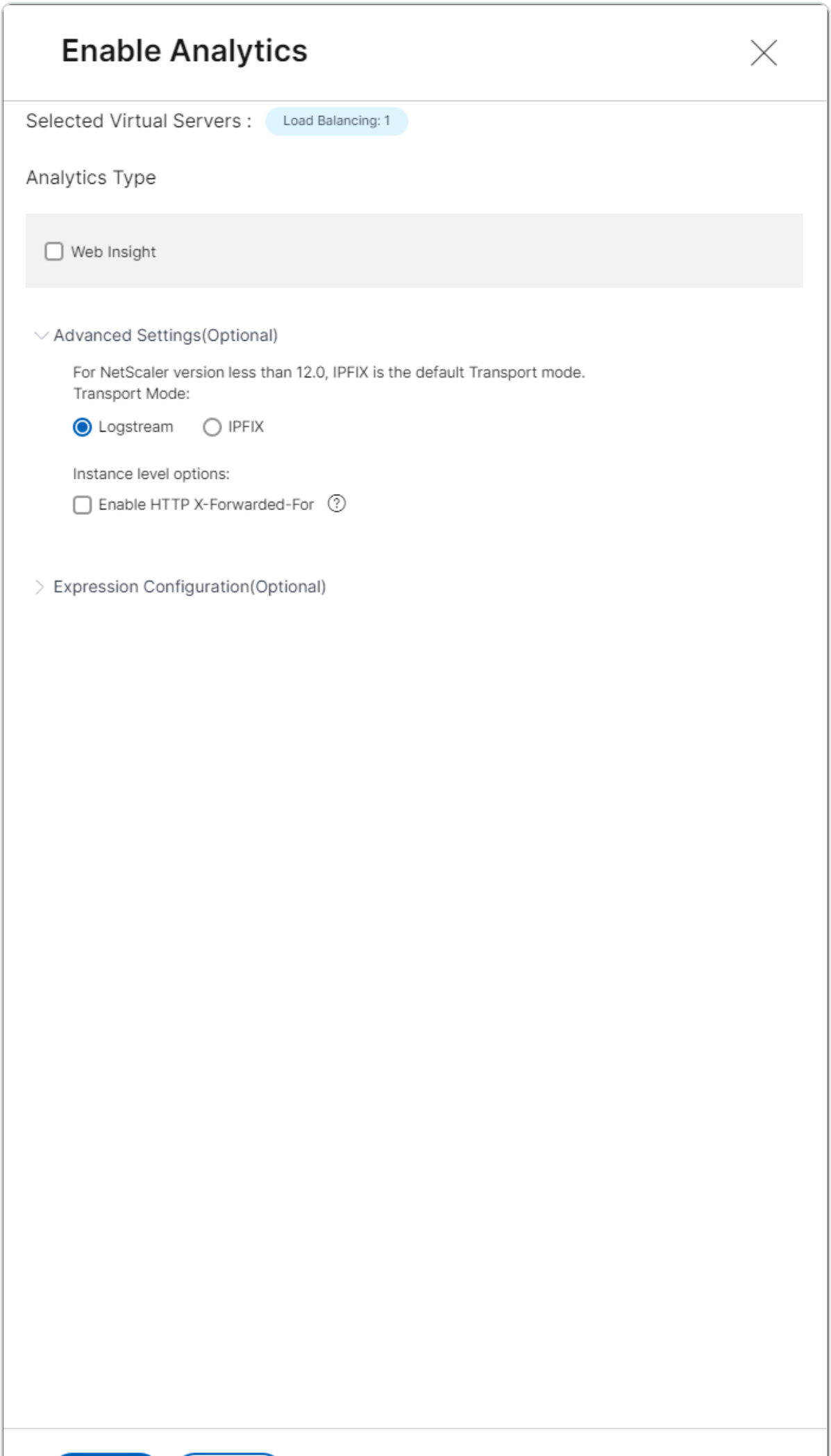
   b. 选择 **Logstream** 作为传输模式

   > **注意**
   >
   > 对于 NetScaler **11.1 Build 47.14 到 11.1 Build 62.8** 版本之间，Logstream 是启用 Web Insight (HTTP) 的默认传输模式，而 IPFIX 是启用其他洞察的唯一传输模式。对于 NetScaler **12.0 到最新版本**，您可以选择 **Logstream** 或 **IPFIX** 作为传输模式。

   c. 表达式默认为 true

   d. 单击 **确定**

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Enable Analytics
Selected Virtual Servers :
Load Balancing: 1
Analytics Type
Web Insight
Advanced Settings(Optional)
For NetScaler version less than 12.0, IPFIX is the default Transport mode.
Transport Mode:
Logstream
IPFIX
Instance level options:
Enable HTTP X-Forwarded-For
Expression Configuration(Optional)

注意

- 如果您选择未获得许可的虚拟服务器，则 NetScaler Console 会首先许可这些虚拟服务器，然后启用分析功能
- 对于管理分区，仅支持 **Web Insight**
- 对于缓存重定向、身份验证和 GSLB 等虚拟服务器，您无法启用分析。将显示错误消息

下表描述了 NetScaler Console 支持 Logstream 作为传输模式的功能：

功能	IPFIX	日志流
Web 洞察	•	•
WAF 安全违规	•	•
网关洞察	•	•
HDX 洞察	•	•
SSL 洞察	不支持	•
CR 洞察	•	•
IP 信誉	•	•
AppFirewall	•	•
客户端测量	•	•
Syslog/审计日志	•	•

仪表板

NetScaler Console 提供两个仪表板：**出站流量仪表板**和**用户仪表板**。这些仪表板显示多个图表，总结了从企业网络访问的网站或应用程序以及网络用户执行的活动。

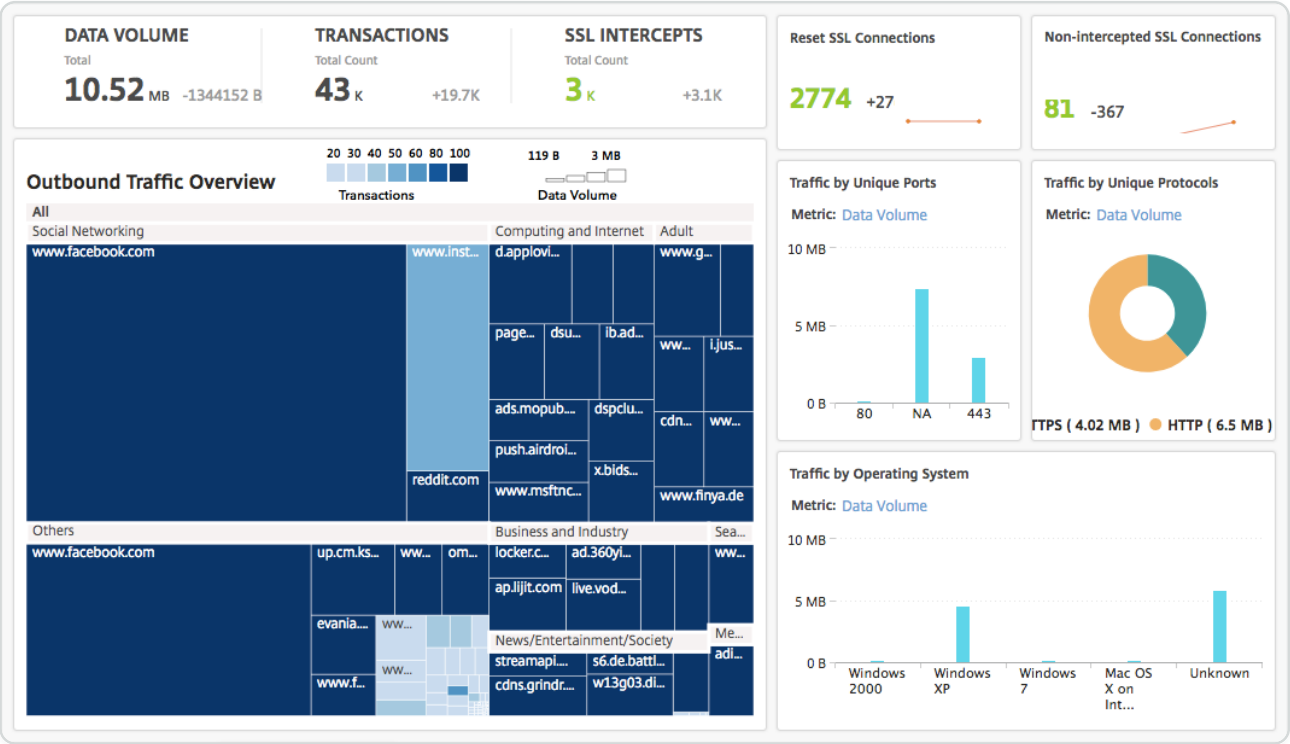
© 1997–2026 Citrix Systems, Inc. All rights reserved.

出站流量仪表板

“**出站流量仪表板**”提供了从您的网络访问的 URL 或域的摘要。它通过事务数或 URL 或域消耗的数据量，提供所有 URL 或域的整体视图。 它还提供以下详细信息：

1. 从您的网络访问的 URL 或域消耗的带宽量。
2. 从您的网络访问 URL 和域时发生的事务数。
3. 事务期间 NetScaler 设备拦截的 SSL 连接数。
4. 事务期间 NetScaler 设备未拦截的 SSL 连接数。
5. 事务期间 NetScaler 设备重置的 SSL 连接数。
6. 根据用于传输流量的端口、Web 流量使用的协议以及用于传输流量的客户端操作系统，传输的 Web 流量量。

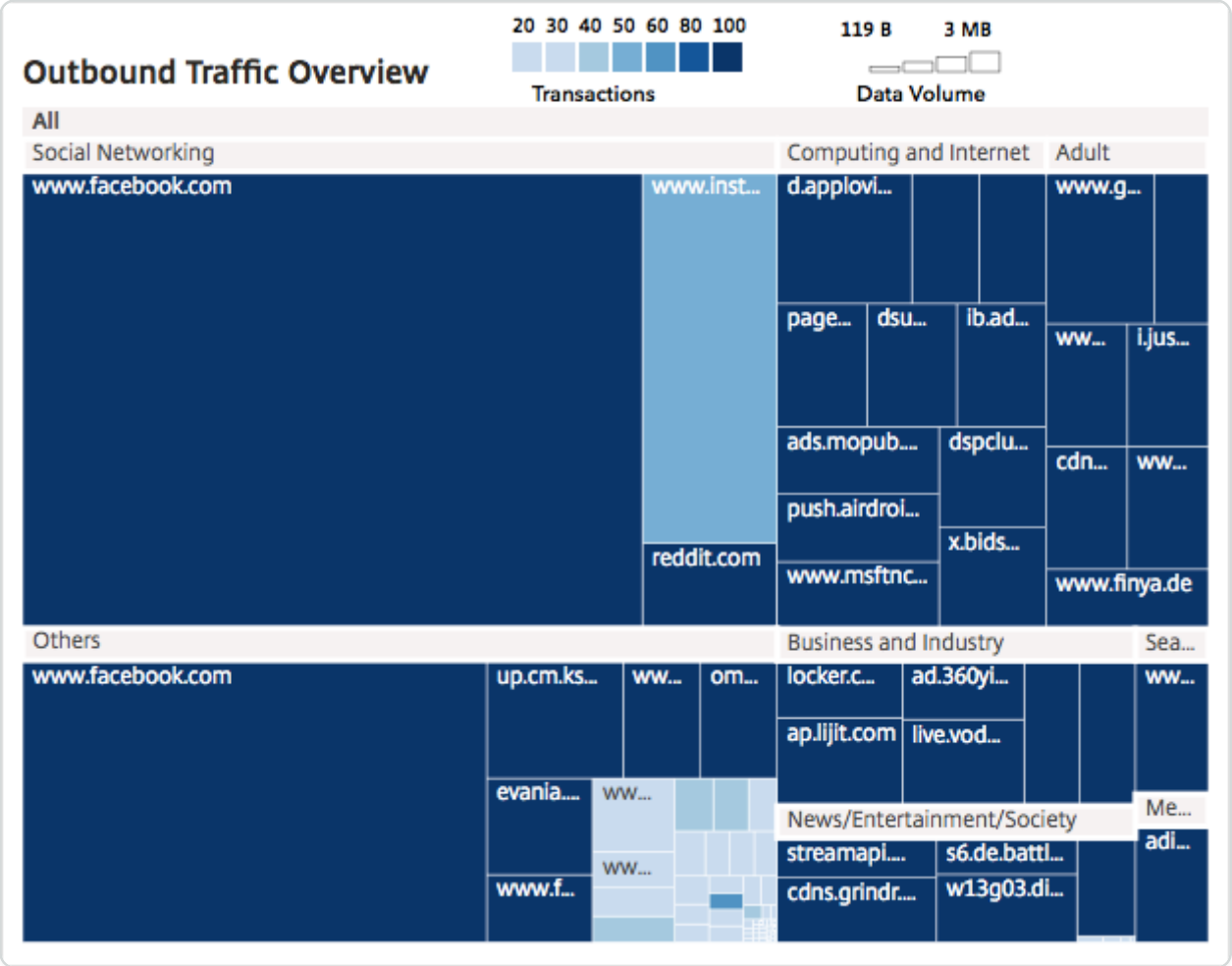
要访问出站流量仪表板，请导航到 **应用程序 \> 出站流量仪表板**。



查看网络中的出站流量

“**出站流量仪表板**”包括一个“**出站流量概览**”窗格。在“**出站流量概览**”窗格中，NetScaler Console 将访问的 URL 或域分组到类别中，例如购物、新闻、社交网络等。“**出站流量概览**”窗格将从您的网络访问的 URL 或域显示为 URL 类别中的节点。节点大小根据访问 URL 或域所消耗的数据量确定。节点的颜色表示访问 URL 或域时发生的事务数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您可以点击一个类别来筛选图表，以显示指定时间范围内与该类别相关的详细信息。

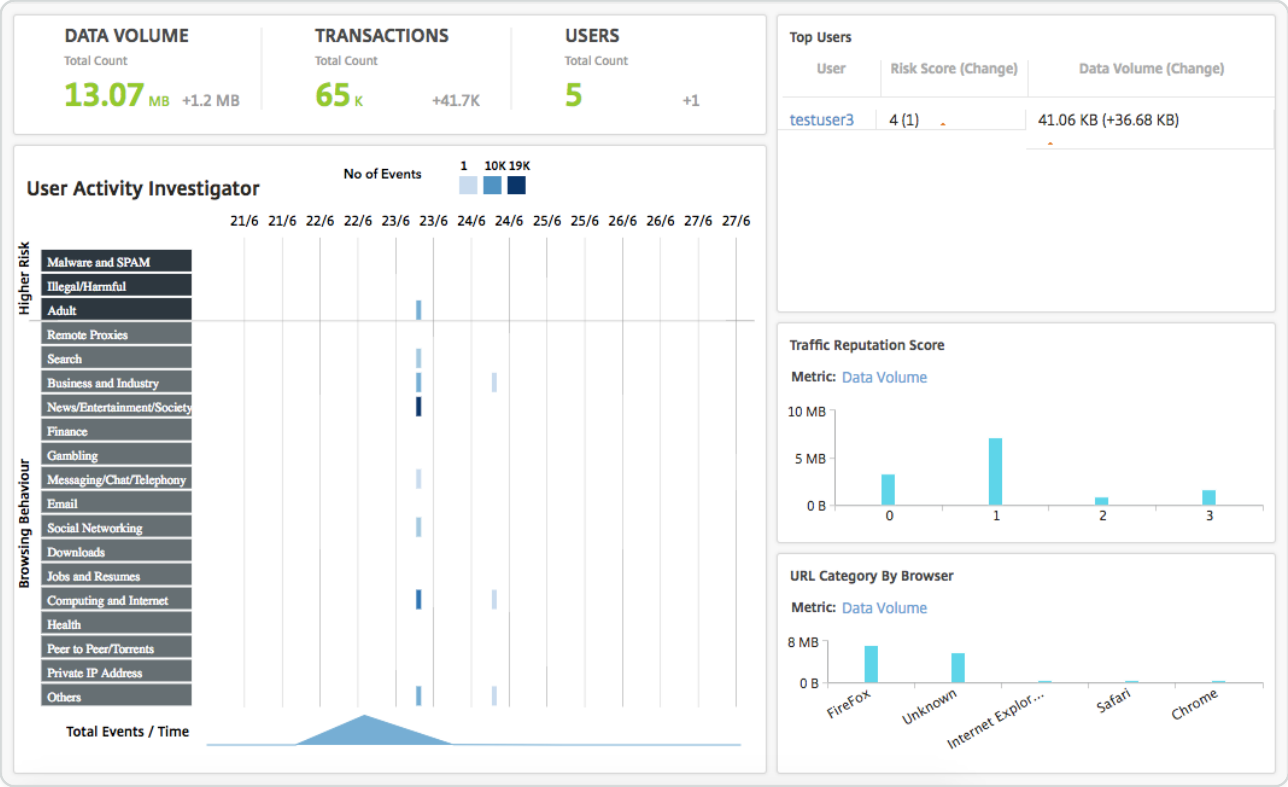
用户仪表板

用户仪表板显示了企业中用户所执行活动的摘要。它提供了关键指标，您可以使用这些指标来确定以下内容：

1. 企业中用户的浏览行为。
2. 企业中用户访问的 URL 类别。
3. 根据风险评分和消耗的带宽排名前五的用户。有关风险评分的更多信息，请参阅风险评分。
4. 用于访问 URL 或域的浏览器。
5. 根据流量信誉评分，用户生成的网络流量量。

要访问**用户仪表板**，请导航到**用户 \> 仪表板**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



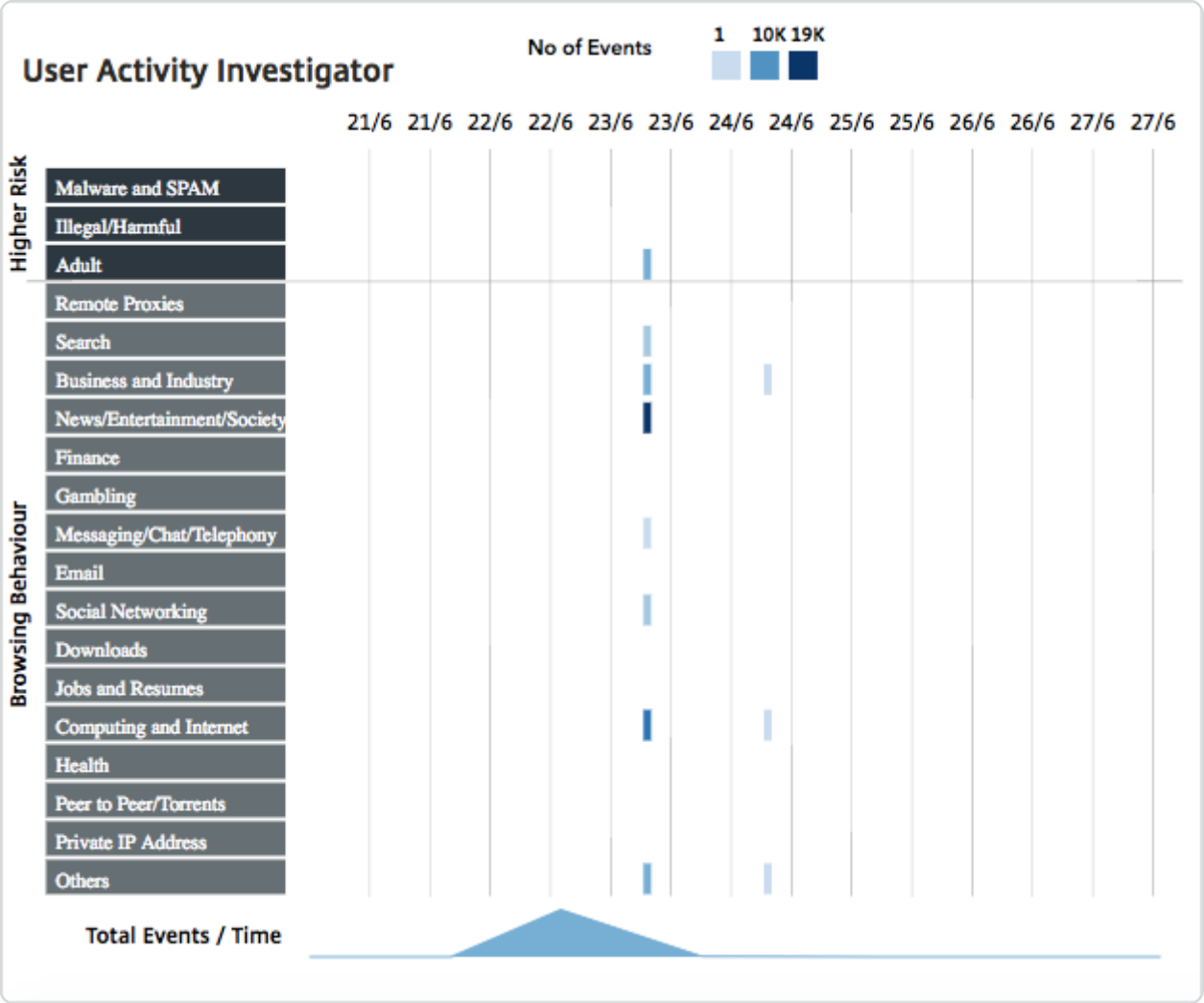
您可以点击**热门用户**窗格中的用户，以筛选图表，显示该用户在指定时间范围内执行的网络活动的详细信息。

用户活动调查器

用户仪表板包含一个**用户活动调查器**窗格，显示用户执行的各种网络活动。它显示了用户在选定时间范围内访问的 URL 类别，以及每个 URL 类别触发的各种事件。您可以点击事件以获取事务级别详细信息。

用户活动调查器显示关键信息，例如用户的浏览行为、用户的高风险活动以及每个 URL 类别触发的事件。事件在图表上显示为矩形图例。如果选定持续时间为一小时，则每个图例按一分钟间隔聚合；如果选定持续时间为一天，则按一小时间隔聚合。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



这些图例是聚合的，并根据发生的事件数量进行颜色编码。您可以将鼠标指针悬停在图例上，以显示所选图例的详细信息，例如时间和聚合的事件数量。您可以通过从时间段列表中选择时间来自定义图表的时间段。

您可以单击事件以进一步深入查看事务的详细信息。

用户事务

“用户事务”页面显示网络中用户事务的详细信息。它提供事务级别的详细信息，例如：

1. 事务发生的时间
2. 事务使用的协议
3. 用户名
4. 用户访问的域
5. URL 类别
6. 用于拦截事务的代理服务器
7. 客户端端口详细信息

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. 入站字节数
9. 出站字节数

用户事务(/en-us/netscaler-application-delivery-management-software/media/swg-analytics-5.png)

摘要面板

“**摘要面板**”显示在“**事务详细信息**”窗格中可见的所有事务指标。此面板允许您通过选择或取消选择指标来对“**事务详细信息**”窗格中的事务进行排序和查看。“**摘要面板**”显示以下指标：

指标	描述
协议	事务中使用的协议
端口	事务使用的端口
URL 信誉	URL 信誉评分
浏览器	事务使用的浏览器
操作系统	事务使用的操作系统
入站字节数	通过 NetScaler 设备接收的数据量。
出站字节	通过 NetScaler 设备发送的数据量。

风险评分

风险评分是 NetScaler Console 中使用的一种评分系统，用于确定企业中与用户相关的风险。NetScaler Console 根据 NetScaler 设备为网络中用户访问的 URL 分配的 URL 信誉评分来分配风险评分。有关 URL 信誉评分的信息，请参阅 URL 信誉评分。下表描述了 NetScaler Console 分配的风险评分。

风险评分	描述
1	用户的 Web 活动没有感知到的威胁，也不是异常的。
2	用户的 Web 活动没有感知到的威胁，也不是异常的，但用户正在访问“未知站点”，这些站点没有 URL 信誉评分。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

风险评分	描述
3	用户的 Web 活动中未检测到威胁，但用户曾尝试访问可能存在漏洞的站点或与可能存在漏洞的站点相关联的站点。
4	可能已受感染的用户。
5	用户的网络活动异常，且用户访问了已知的恶意网站。

所有违规

所有违规页面显示基于**网络**、**WAF** 和 **Bot** 类别的应用程序安全违规详情。

违规类别

NetScaler Console 允许您查看以下违规。在**违规详情**下，您可以单击每个违规选项卡以查看违规详情。

网络	WAF	BOT
HTTP 慢速 Loris	CSRF 表单标记	营销
DNS 慢速 Loris	拒绝 URL	爬虫
HTTP 慢速 Post	表单字段一致性	屏幕截图创建器
NXDomain 洪水攻击	字段格式	搜索引擎
HTTP 脱同步攻击	Cookie 劫持	订阅源获取器
布莱兴巴赫攻击	推断内容类型 XML	链接检查器
分段猛击攻击	缓冲区溢出	服务代理
SYN 洪水攻击	内容类型	站点监控器
小窗口攻击	Cookie 一致性	速度测试器
	安全对象	工具
	HTML SQL 注入	未分类

© 1997–2026 Citrix Systems, Inc. All rights reserved.

网络	WAF	BOT
	起始 URL	病毒扫描器
	跨站脚本	漏洞扫描器
	XML DoS	DeviceFP 等待超时
	XML 格式	无效设备指纹
	XML WSI	无效验证码响应
	XML SSL	验证码尝试次数超出限制
	XML 附件	有效验证码响应
	XML SOAP 故障	验证码客户端静默
	XML 验证	验证码等待时间超出限制
	其他	请求大小超出限制
	IP 信誉	速率限制超出限制
	HTTP DOS	阻止列表（IP、子网、策略表达式）
	TCP 小窗口	允许列表（IP、子网、策略表达式）
	签名违规	零像素请求
	文件上传类型	源 IP
	JSON 跨站点脚本	主机
	JSON SQL	地理位置
	JSON DOS	URL
	命令注入	爬虫
	最大上传数	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

网络	WAF	BOT
	Referrer 标头	
	安全商务	

安全违规仪表板

在安全违规仪表板中，您可以查看：

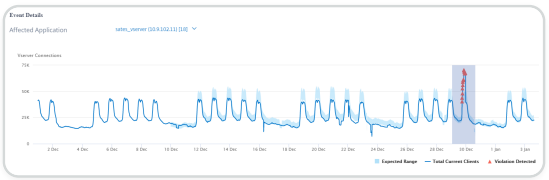
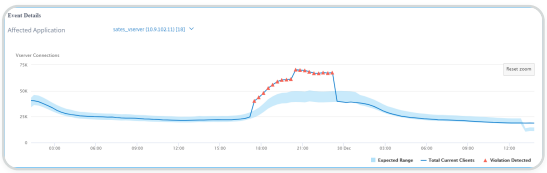
- 所有 NetScaler 实例和应用程序中发生的总违规。总违规数根据选定的时间段显示。
- 总违规数。
- 受影响的 NetScaler 实例总数、受影响的应用程序总数，以及根据总发生次数和受影响应用程序排名的主要违规。

违规详情

对于每个违规，NetScaler Console 会在特定时间段内监控行为，并检测异常行为的违规。单击每个选项卡可查看违规详情。您可以查看以下详细信息：

- 总发生次数、上次发生时间以及受影响的应用程序总数。
- 在事件详情下，您可以查看：
  - 受影响的应用程序。如果两个或更多应用程序受到违规影响，您还可以从列表中选择应用程序。
  - 显示违规的图表。

    在列出违规的图表上拖动并选择，以缩小违规搜索范围。

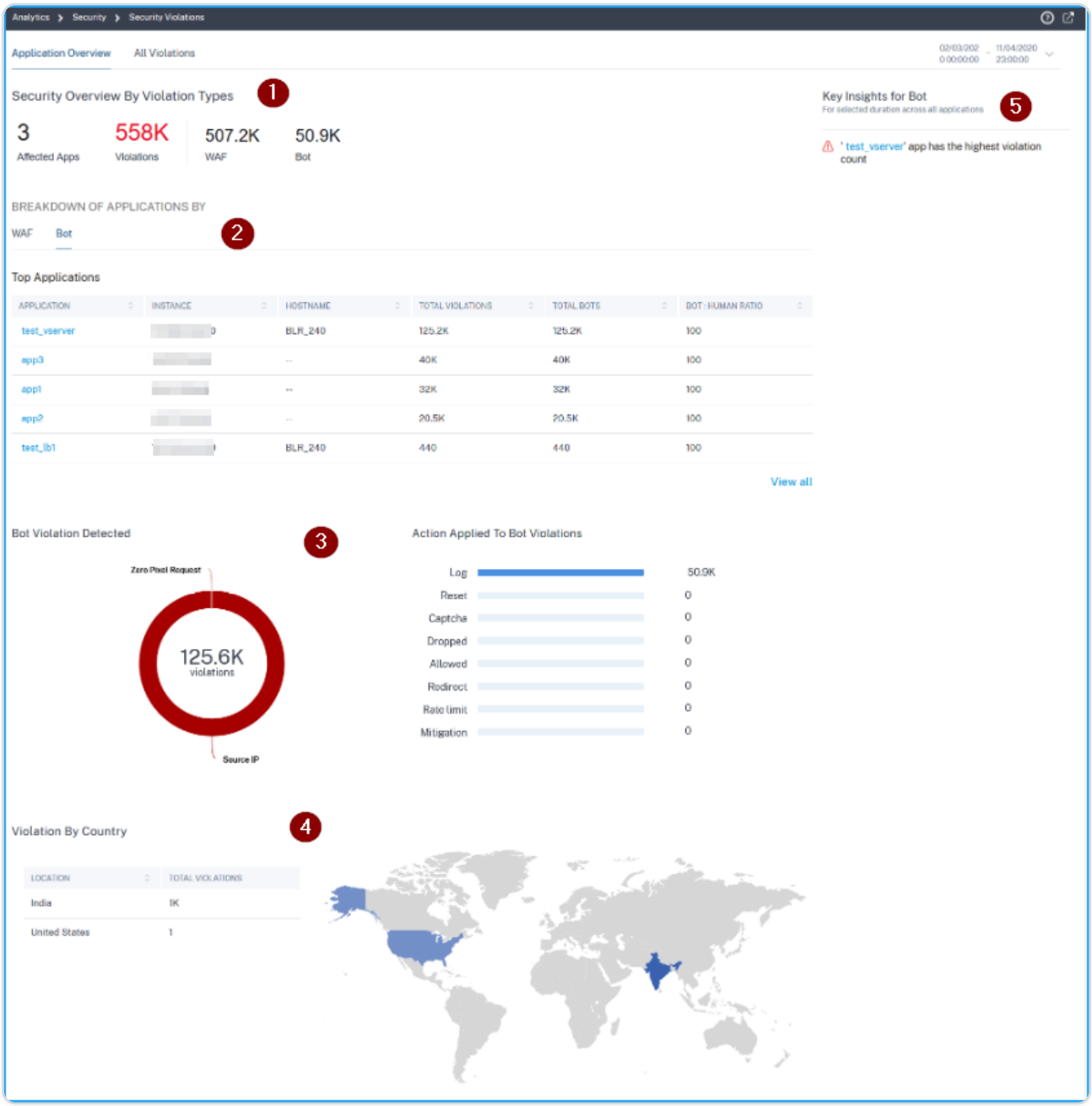
在图表上拖动并选择	搜索结果
	

    单击**重置缩放**以重置缩放结果。
  - **建议操作**，建议您排查问题。
  - 其他违规详细信息，例如违规发生时间和检测消息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

应用程序概览

“**应用程序概览**”页面显示应用程序，并全面了解 WAF 安全违规和 Bot 安全违规中关联的威胁详细信息。您还可以查看总违规数、WAF 和 Bot 违规总数、按国家/地区划分的违规等信息。



1 – 显示选定持续时间内受影响的应用程序总数、总违规数、WAF 违规总数和 Bot 违规总数。

2 – 显示 WAF 和 Bot 违规详情。单击“**WAF**”和“**Bot**”选项卡可查看根据发生的违规总数排名前 5 的应用程序。单击“**查看所有**”可查看所有应用程序详情。

3 – 显示根据发生次数和已应用的操作排名前列的违规。

4 – 显示地理地图视图，提供违规发生位置的可视性。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5 – 根据违规情况提供信息。

违规类别

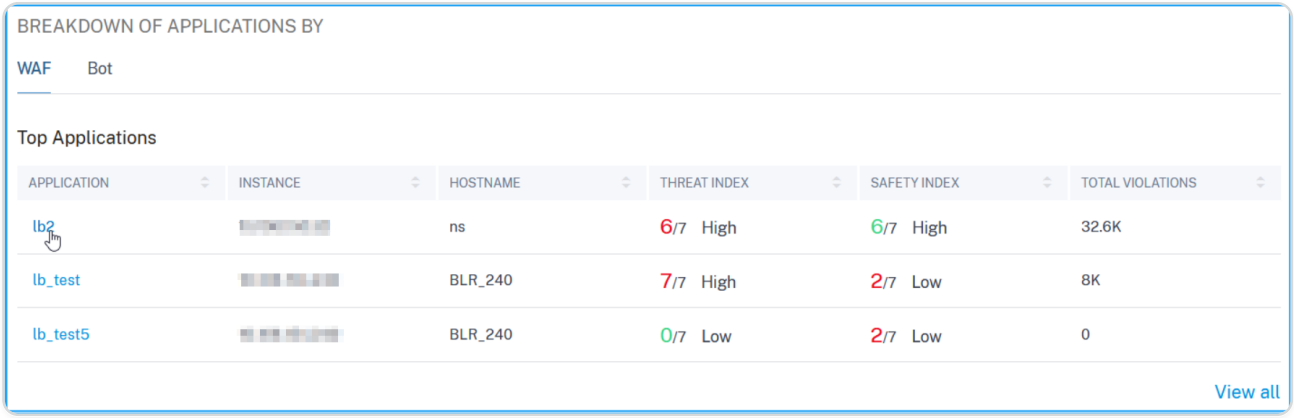
WAF	BOT
Cookie 劫持	订阅源抓取器
推断内容类型 XML	链接检查器
CSRF 表单标记	营销
拒绝 URL	抓取器
表单字段一致性	屏幕截图创建器
字段格式	搜索引擎
最大上传数	服务代理
引用者标头	站点监视器
安全商务	速度测试器
安全对象	工具
HTML SQL 注入	未分类
启动 URL	病毒扫描程序
跨站点脚本	漏洞扫描程序
XML DoS	DeviceFP 等待超时
XML 格式	无效 DeviceFP
XML WSI	无效验证码响应
XML SSL	验证码尝试次数超出限制
XML 附件	有效的验证码响应
XML SOAP 故障	验证码客户端已静音

© 1997–2026 Citrix Systems, Inc. All rights reserved.

WAF	BOT
XML 验证	验证码等待时间超出
其他	请求大小超出限制
IP 信誉	速率限制超出
HTTP DOS	阻止列表（IP、子网、策略表达式）
TCP 小窗口	允许列表（IP、子网、策略表达式）
签名违规	零像素请求
文件上传类型	源 IP
JSON 跨站脚本	主机
JSON SQL	地理位置
JSON DOS	URL
命令注入	爬虫
缓冲区溢出	
内容类型	
Cookie 一致性	

查看 WAF 违规详情

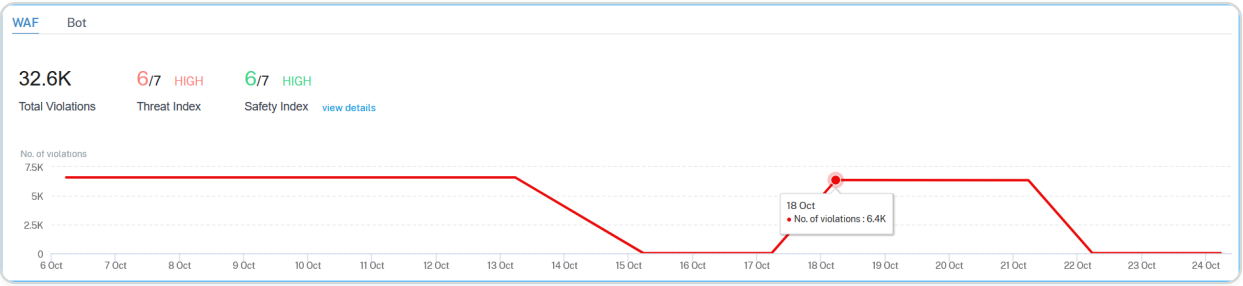
从 **热门应用程序** 或 **查看所有** 选项中点击一个应用程序以查看 WAF 详细信息。



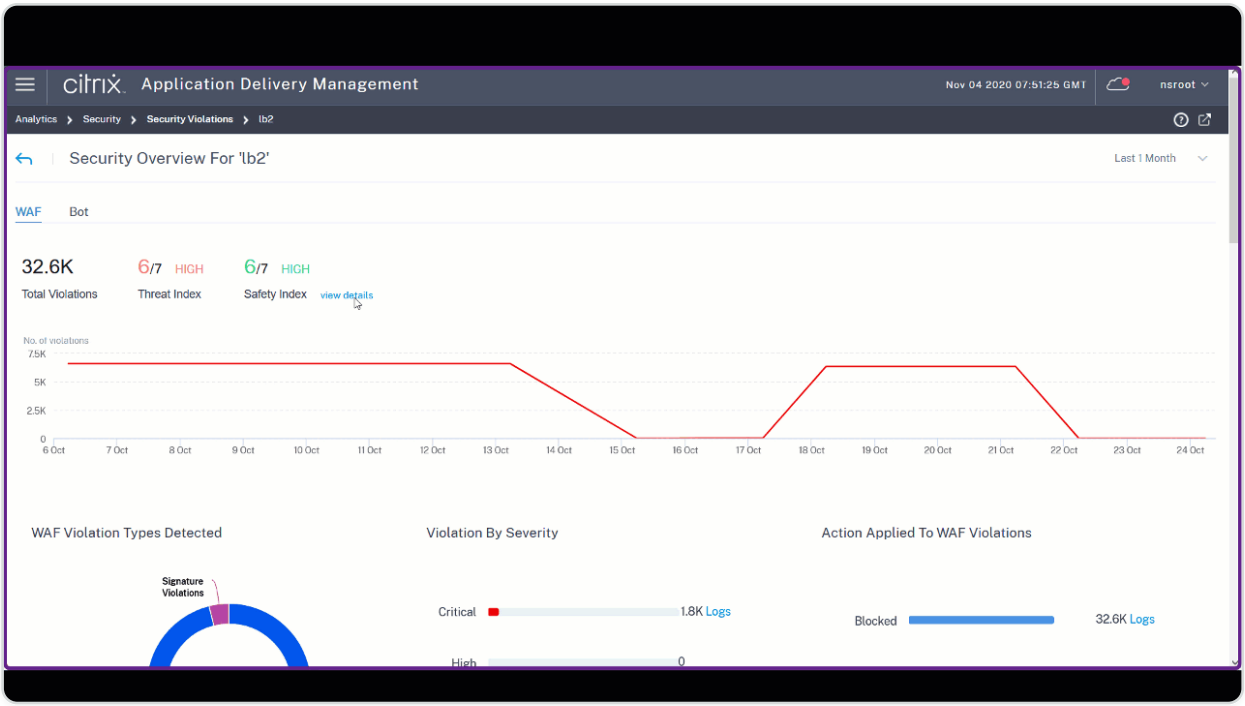
显示所选应用程序的 **安全概览** 页面。在 **WAF** 下，您可以查看：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

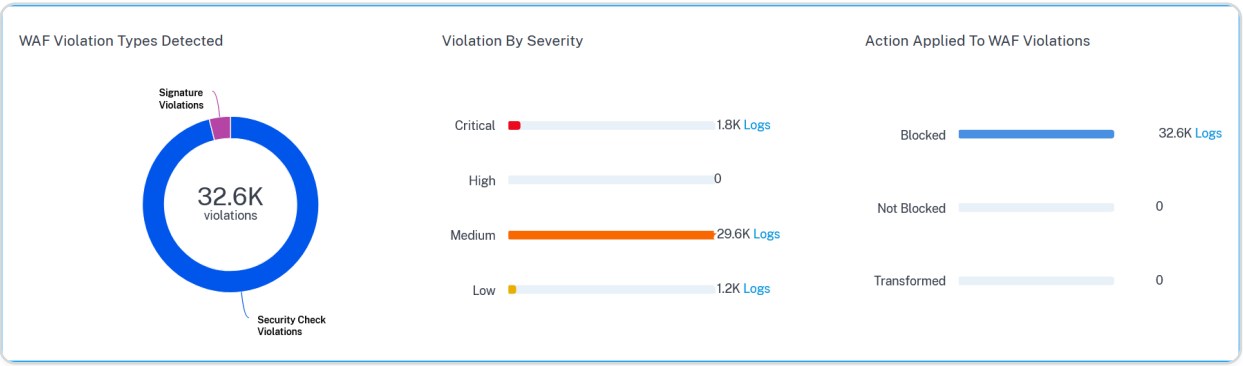
- 一个图表视图，显示应用程序的总违规次数、威胁指数分数和安全指数分数。



点击 **查看详细信息** 以查看应用程序防火墙和 NetScaler 系统安全配置详细信息。

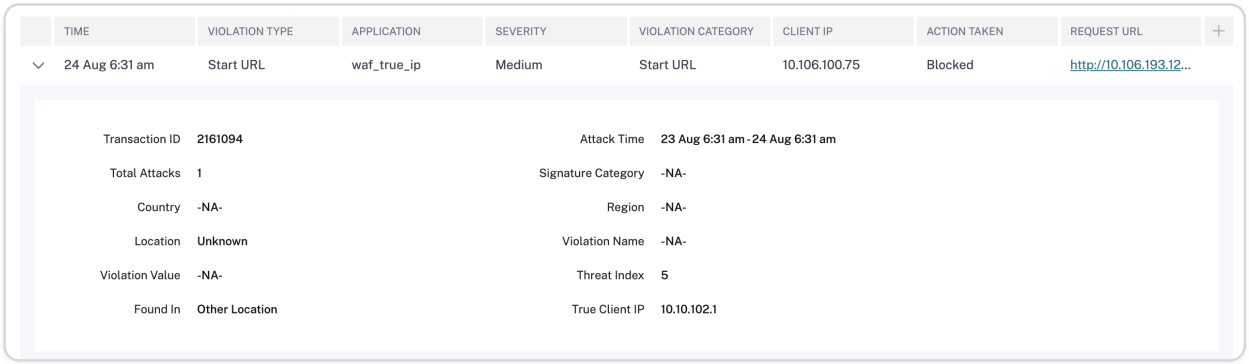


- 基于类型、严重性和所采取操作的违规行为。

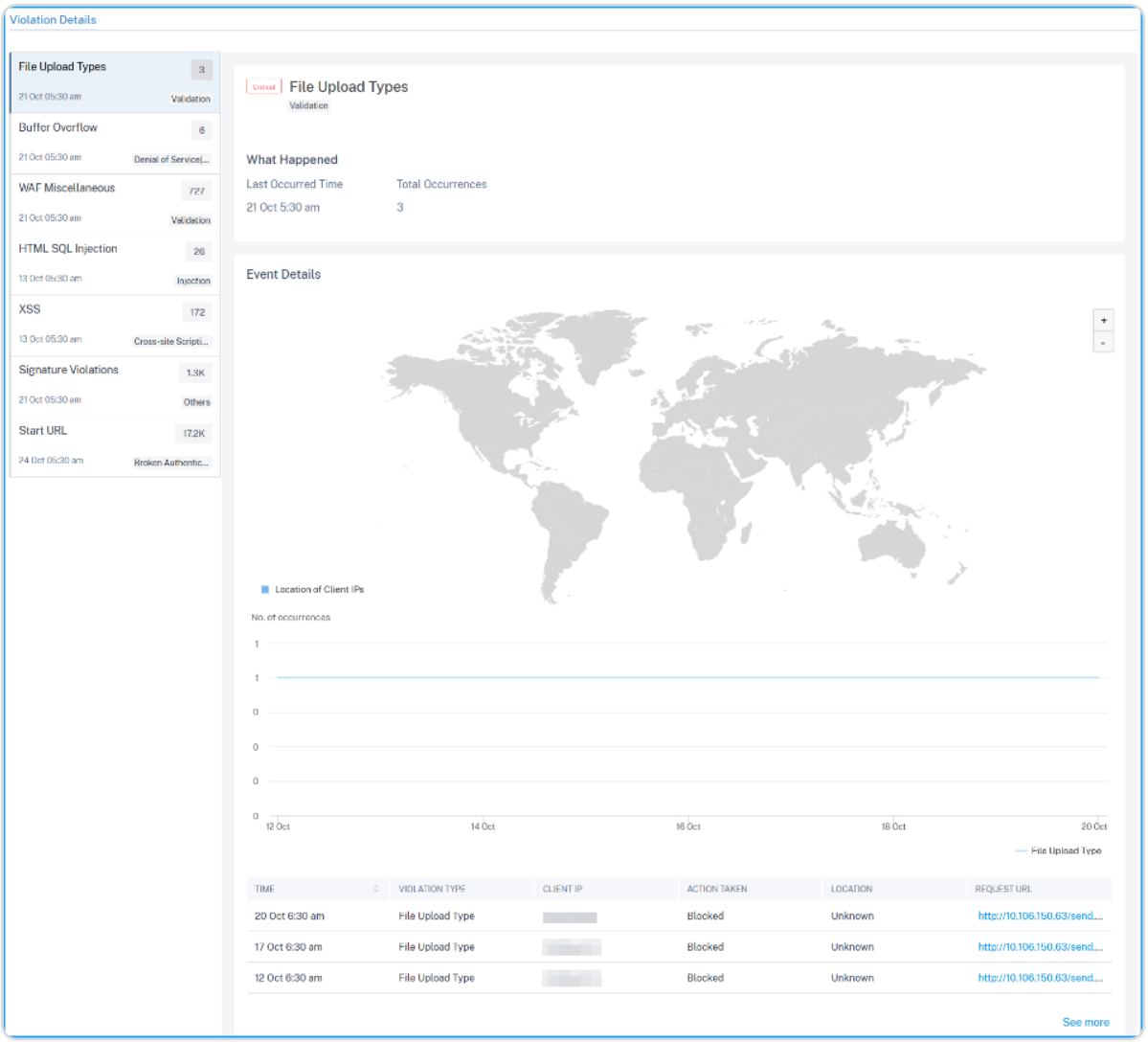


点击 **日志** 以查看基于严重性或所采取操作的详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- 影响应用程序的违规行为。在 **违规详细信息** 下，您可以查看受影响的违规详细信息。点击每个违规行为以查看以下详细信息：
  - **发生了什么** – 指示总发生次数和最后发生日期和时间。
  - **事件详细信息** – 显示一个地理地图，指示客户端 IP 和其他违规详细信息，例如违规类型、客户端 IP、位置等。



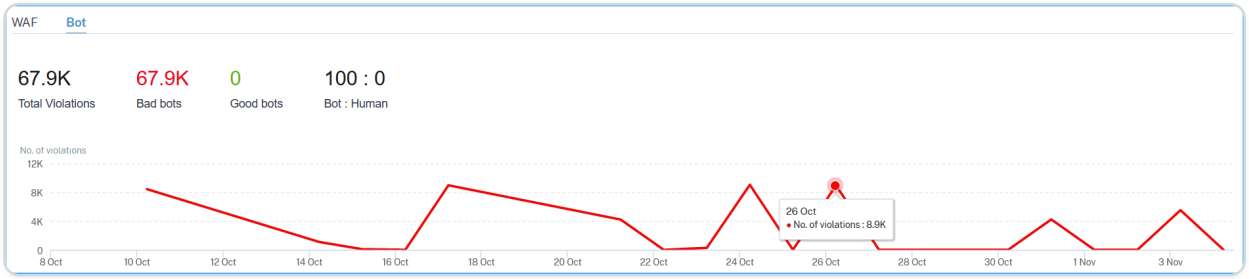
© 1997–2026 Citrix Systems, Inc. All rights reserved.

查看机器人违规详情

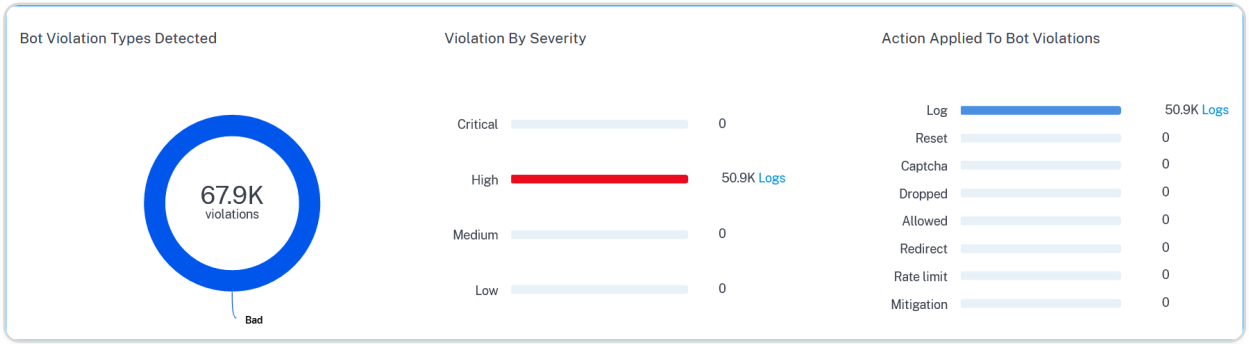
在**机器人**选项卡中，从“热门应用程序”或“**查看全部**”选项中单击一个应用程序以查看机器人详情。

将显示所选应用程序的**安全概览**页面。在**机器人**下，您可以查看：

- 一个图表，显示访问应用程序的机器人总数、恶意机器人总数、良好机器人总数以及人类用户与机器人之间的总比例。

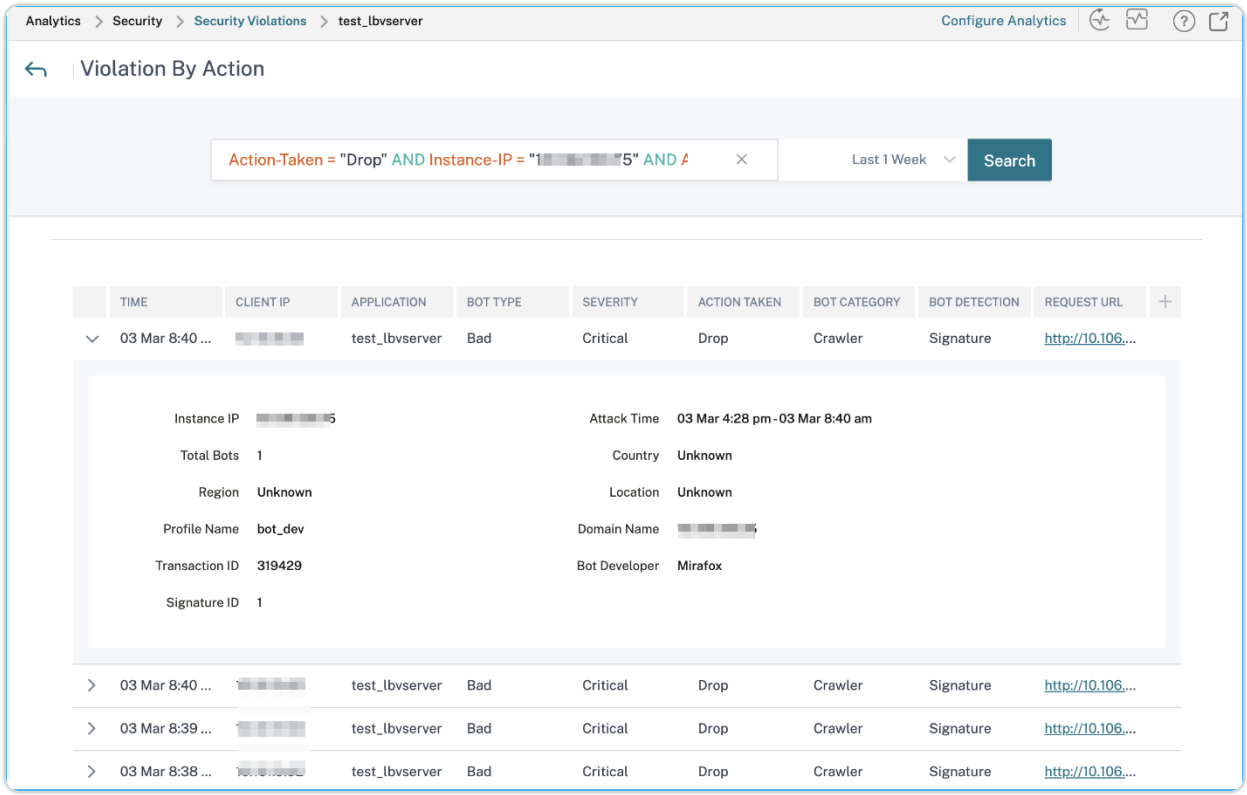


- 基于机器人类型、严重性和所采取操作的违规行为。



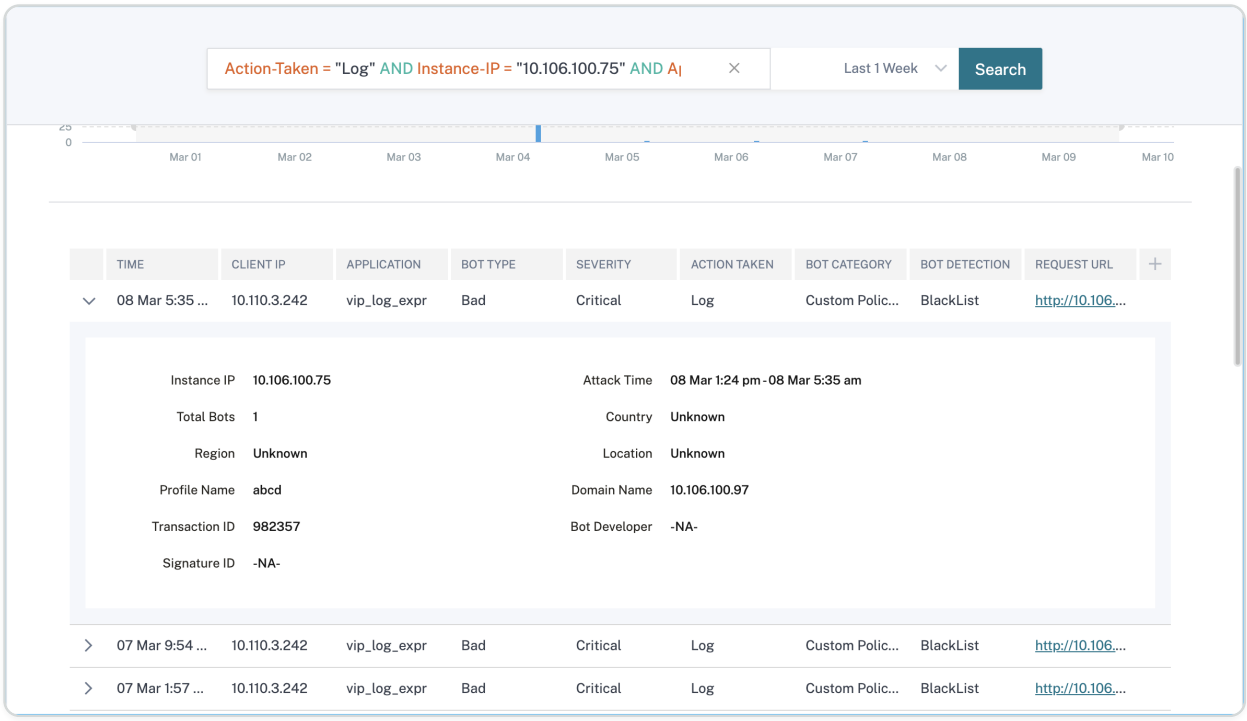
单击**日志**以根据严重性或所采取的操作查看详细信息。如果检测到的机器人是签名类型机器人，您可以查看更多详细信息，例如机器人开发者和签名 ID。签名 ID 使您能够识别检测到的机器人是良好机器人还是恶意机器人。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意

> 如果检测到的机器人是除签名机器人之外的任何其他机器人类型，则签名 ID 和机器人开发者将显示为 N/A。



- 应用程序上受影响的违规行为。在“违规详情”下，您可以查看受影响的违规详情。单击每个违规行为以查看详细信息，例如：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **发生了什么** – 指示总发生次数以及最后发生日期和时间。
- **事件详情** – 显示地理地图，其中指示客户端 IP 和其他违规详情，例如违规类型、客户端 IP、位置等。

  Bot 违规详情(/en-us/netscaler-application-delivery-management-software/media/bot-violation-details.png)

> **注意**
>
> 在 **WAF** 和 **Bot** 下，您可以查看绑定了负载平衡虚拟服务器的内容交换虚拟服务器的分析。单击内容交换虚拟服务器，并在 **绑定的负载平衡服务器** 下，您可以查看绑定到内容交换虚拟服务器的负载平衡服务器列表。

带有负载平衡服务器的内容交换服务器(/en-us/netscaler-application-delivery-management-software/media/cs-lb-analytics.png)

查看事件历史记录

单击 **事件** 选项卡以查看 Bot 和 WAF 事件。

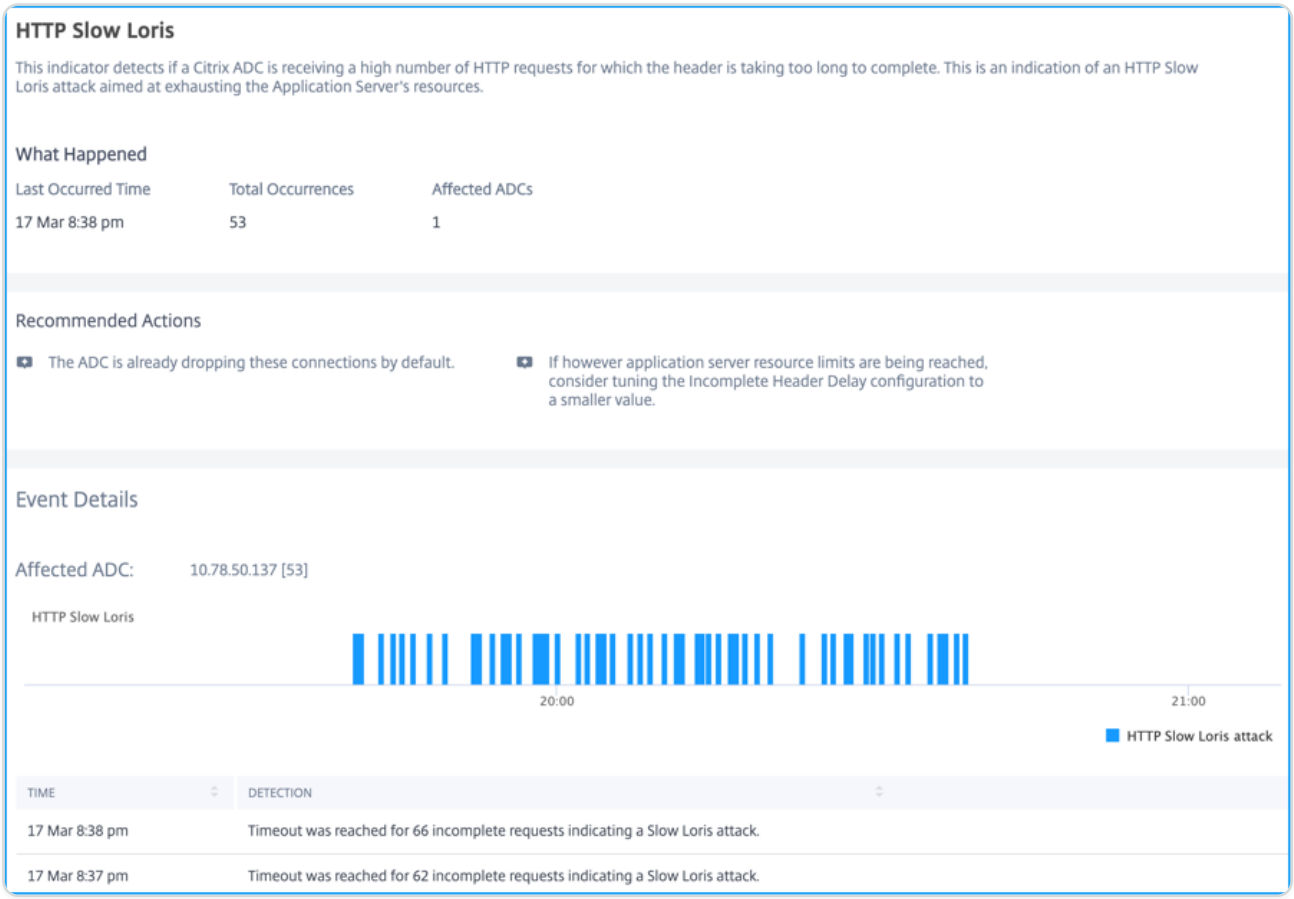
网络违规详情

HTTP 慢速洛里斯

Slow Loris 是一种拒绝服务攻击，它能以尽可能慢的速度向目标应用程序发送 HTTP 标头。目标应用程序被迫等待标头到达，如果打开多个类似连接，它也可能很快变得无法处理请求。当 NetScaler 实例接收到大量 HTTP 请求时，HTTP 标头会增加，并且需要很长时间才能完成请求。此过程会耗尽应用程序服务器资源，并导致 HTTP **Slow Loris** 攻击。

使用 **HTTP Slow Loris** 指标，您可以分析导致 **Slow Loris** 攻击的请求。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



解决此问题的**建议操作**：

- 考虑将不完整标头延迟 (incompHdrDelay) 配置调整为较小的值。
- 默认情况下，NetScaler 实例会丢弃这些不完整的请求。

在**事件详细信息**下，您可以查看：

- 受影响的应用程序。如果两个或更多应用程序受到违规影响，您还可以从列表中选择应用程序。
- 指示所有违规的图表
- 违规发生时间
- 指示总不完整请求为 **Slow Loris** 攻击的检测消息

DNS 慢速洛里斯

DNS Slow Loris 指标检测到 NetScaler 接收到跨越多个数据包的大量 DNS 请求。此过程会耗尽 DNS 服务器资源，并导致 **DNS Slow Loris** 攻击。默认情况下，NetScaler 实例会丢弃这些 **DNS Slow Loris** 请求，无需采取进一步措施来解决此问题。

DNS 攻击(/en-us/netscaler-application-delivery-management-software/media/dns-slow-loris.png)

在**事件详细信息**下，您可以查看：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 受影响的应用程序。如果两个或更多应用程序受到违规影响，您还可以从列表中选择该应用程序。
- 指示所有违规的图表
- 违规发生时间
- 检测消息，指示总 DNS 请求为**慢速洛里斯**攻击

HTTP 慢速 POST

慢速 POST 是一种拒绝服务攻击，可以将 HTTP POST 标头发送到目标应用程序。在标头中，正文消息大小指定正确，但消息正文以低速发送。如果打开多个类似的连接，目标应用程序将被迫等待，并且也可能很快变得无法处理请求。

此过程会耗尽应用程序服务器资源，并导致 HTTP 慢速 POST 攻击。

使用**HTTP 慢速 POST**指示器，您可以分析导致慢速 POST 攻击的请求。

HTTP 慢速 POST(/en-us/netscaler-application-delivery-management-software/media/http-slow-post.png)

解决此问题的**建议操作**是在 NetScaler HTTP 配置文件中启用和配置请求超时。有关更多信息，请参阅HTTP 配置。

在**事件详细信息**下，您可以查看：

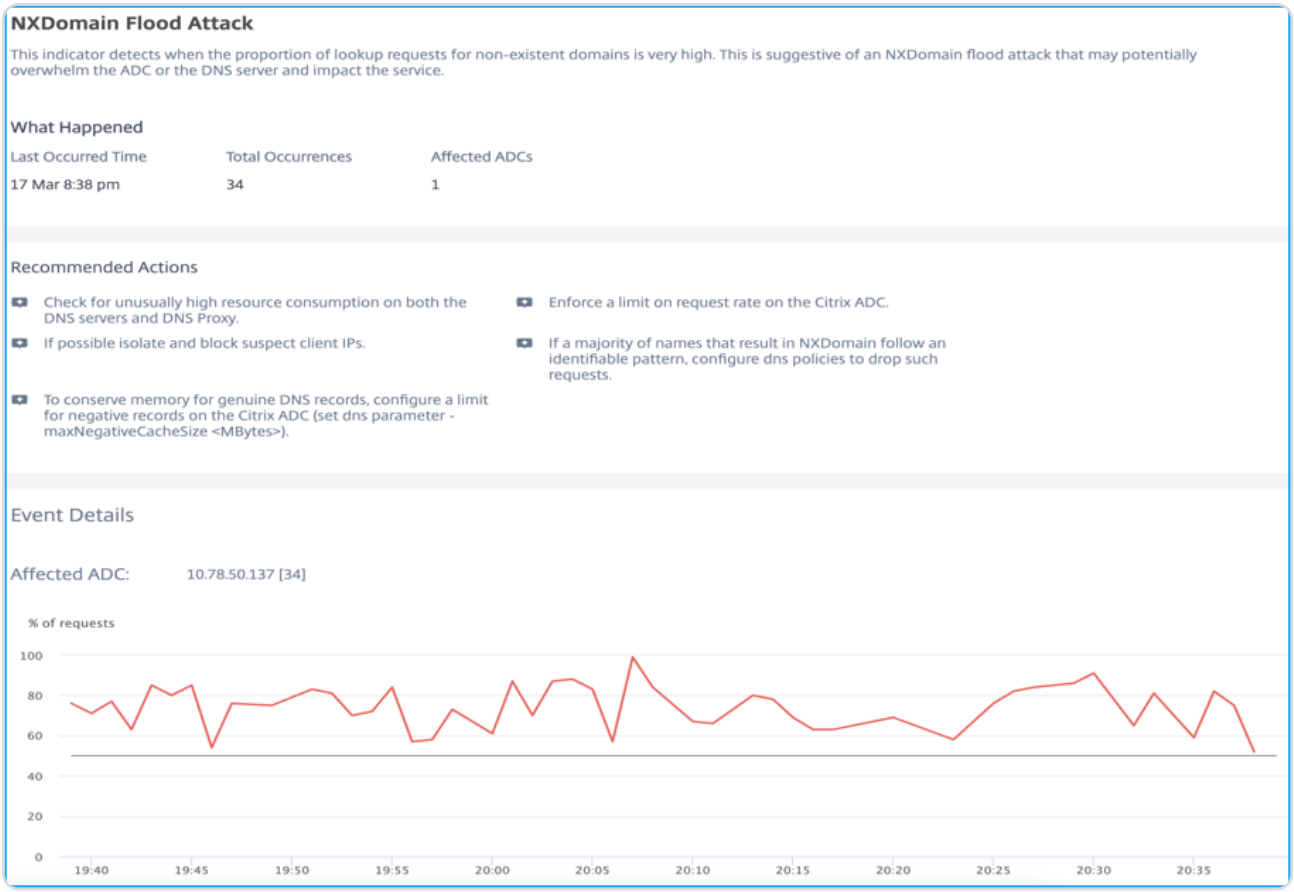
- 受影响的应用程序。如果两个或更多应用程序受到违规影响，您还可以从列表中选择该应用程序。
- 指示所有违规的图表
- 违规发生时间
- 指示总 POST 请求为 **Slow Loris** 攻击的检测消息

NXDOMAIN 洪水攻击

NXDOMAIN 洪水攻击是一种分布式拒绝服务 (DDoS) 攻击，它可针对 DNS 服务器或 NetScaler 实例（配置为 DNS 代理服务器），并发送大量不存在或无效的请求。此攻击会影响 DNS 服务器或 NetScaler 实例，导致速度变慢或请求无法获得响应。

使用 **NXDOMAIN 洪水攻击** 指标，您可以分析导致 NXDOMAIN 攻击的请求。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



解决此问题的**建议操作**：

- 检查 DNS 服务器和 DNS 代理服务器上是否存在异常高的资源消耗。
- 对 NetScaler 实例上的请求速率强制执行限制
- 隔离并阻止可疑客户端 IP 地址
- 如果大多数名称导致 NXDOMAIN，请遵循可识别的模式并配置 DNS 策略以丢弃此类请求
- 为了节省真实 DNS 记录的内存，请在 NetScaler 实例上配置负记录的限制。有关更多信息，请参阅缓解 DNS DDoS 攻击。

在**事件详细信息**下，您可以查看：

- 受影响的应用程序。如果两个或更多应用程序受到违规影响，您还可以从列表中选择该应用程序。
- 指示所有违规的图表

HTTP 解同步攻击

在 HTTP 解同步攻击中，单个 HTTP 请求被解释为：

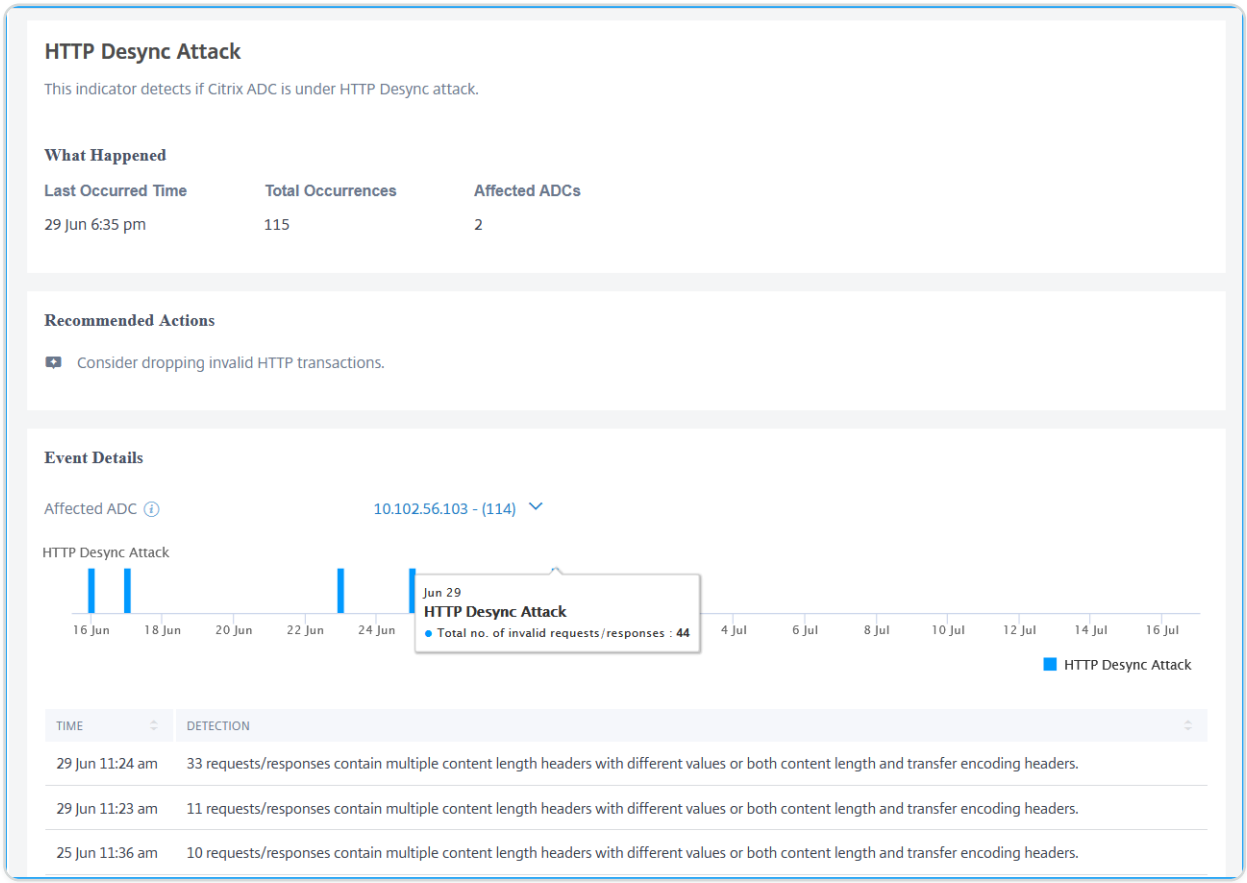
- 对前端服务器（虚拟服务器）的单个请求
- 对后端服务器的 2 个请求

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在此场景中，后端服务器将第二个请求解释为来自不同的客户端。虚拟服务器和后端服务器之间的连接会重复用于不同的请求。如果第一个客户端请求由恶意客户端处理并包含一些恶意数据，则下一个客户端请求可能是一个自定义请求。这种活动可能通过滥用两个标头（内容长度和传输编码）的组合来导致攻击。

使用 **HTTP 解同步攻击** 指标，您可以分析 NetScaler 实例是否可能因存在以下情况而遭受 HTTP 解同步攻击：

- 单个 HTTP 事务中包含内容长度和传输编码标头
- 单个 HTTP 事务中包含多个具有不同值的 Content-Length 标头



建议操作建议您考虑丢弃无效的 HTTP 事务。

在 **事件详细信息**下，您可以查看：

- 受影响的应用程序。如果两个或更多应用程序受到此违规的影响，您还可以从列表中选择应用程序。
- 指示违规详细信息的图表。将鼠标指针悬停在条形图上可查看无效请求/响应的总数。
- 违规的检测消息，指示请求/响应总数：
  - 包含多个具有不同值的 Content-Length 标头

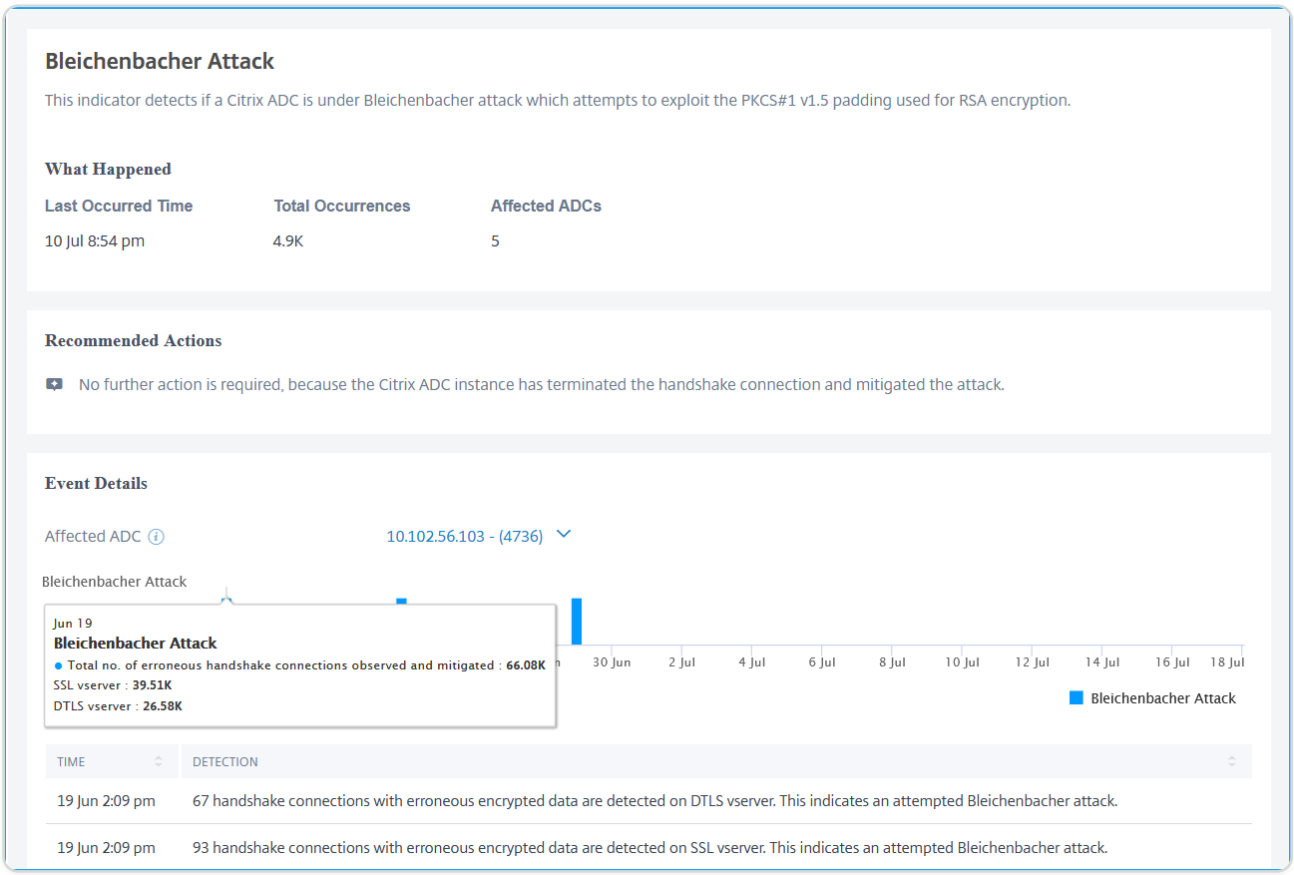
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 包含内容长度和传输编码标头

布莱兴巴赫攻击

NetScaler 实例会检测加密消息的给定字节序列在解密后是否具有正确的填充格式。

使用 **Bleichenbacher 攻击** 指标，您可以分析 NetScaler 实例是否接收到任何包含错误加密数据的 SSL/TLS 握手连接。



建议操作 指示无需进一步操作，因为 NetScaler 实例会终止握手连接并缓解此攻击。

在 **事件详细信息** 下，您可以查看：

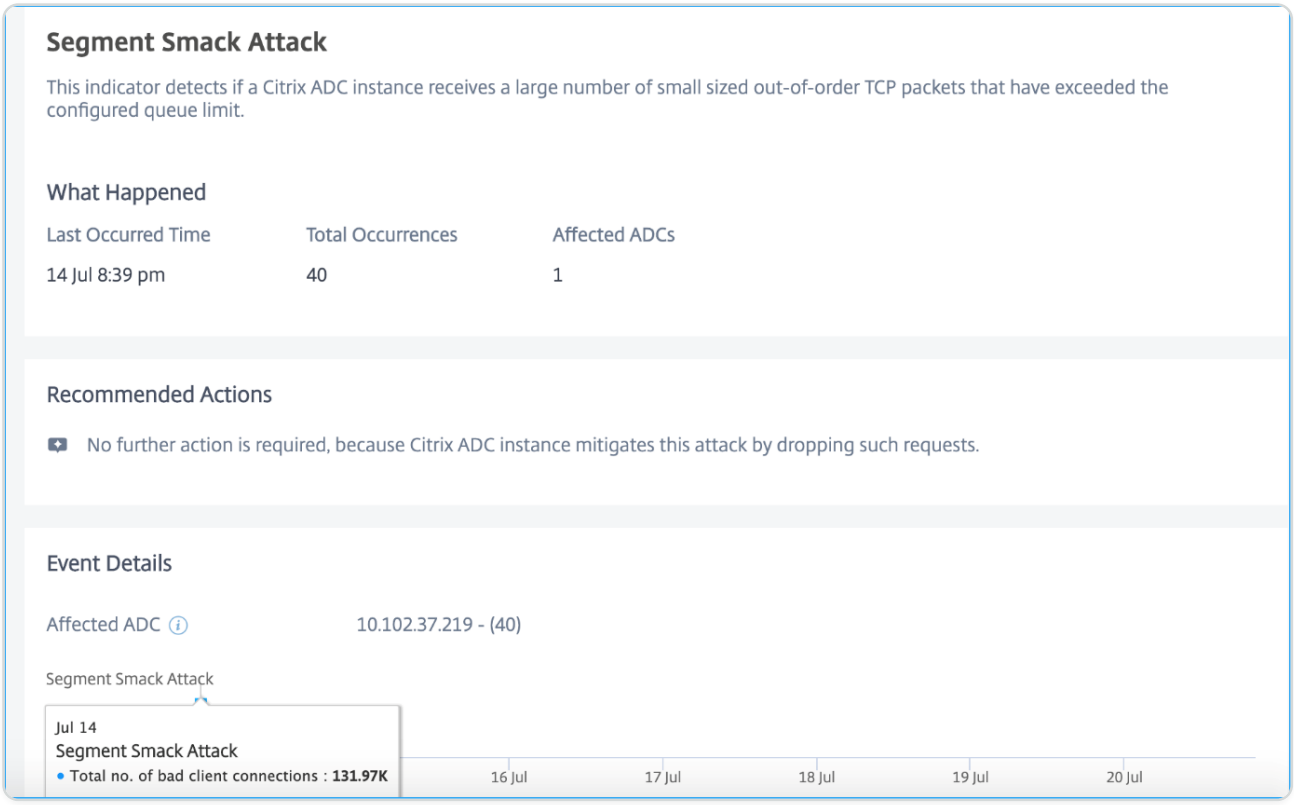
- 受影响的应用程序。如果两个或更多应用程序受到此违规的影响，您还可以从列表中选择该应用程序。
- 指示违规详细信息的图表。将鼠标指针悬停在条形图上，可查看检测到的错误握手连接总数。
- 违规检测消息，指示虚拟服务器上包含错误加密数据的握手连接总数。

分段粉碎攻击

分段粉碎攻击 是一种拒绝服务 (DoS) 攻击，攻击者可以在 TCP 会话期间发送无序的小尺寸数据包。这些定制的 TCP 数据包会影响 CPU 和内存，并导致 NetScaler 实例上的拒绝服务。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 **分段粉碎攻击** 指标，您可以分析 NetScaler 实例是否接收到大量超出配置队列限制的 TCP 数据包。有关更多信息，请参阅 TCP 配置。

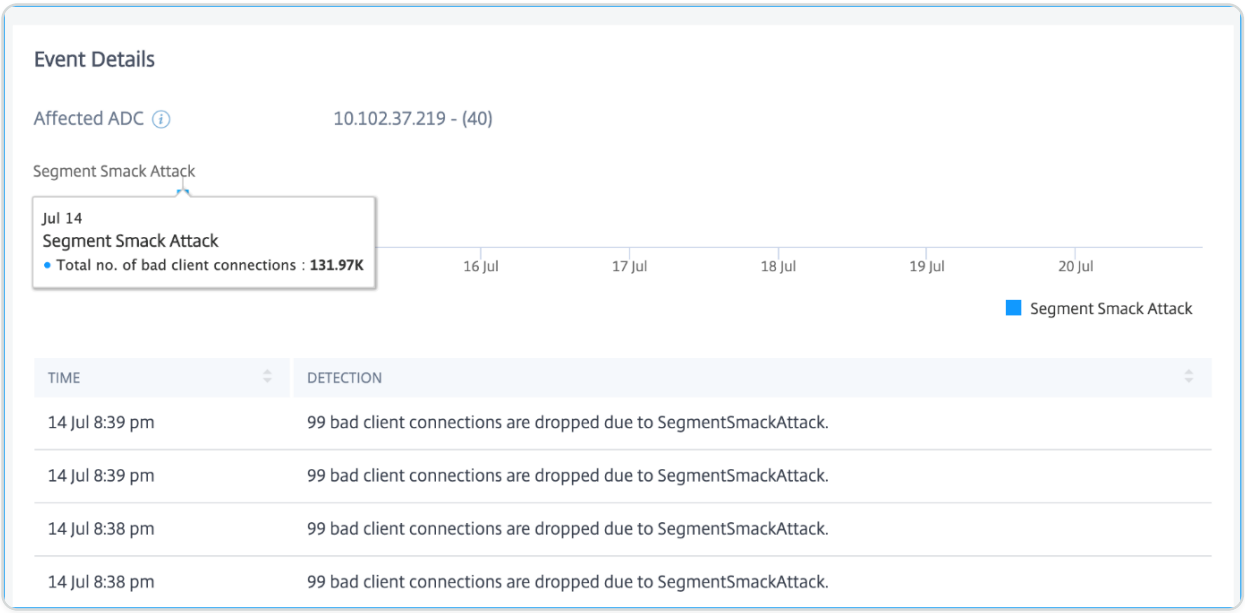


作为管理员，无需进一步操作，因为 NetScaler 实例通过丢弃所有这些多余的 TCP 数据包来缓解此攻击。

在 **事件详细信息** 下，您可以查看：

- 受影响的 NetScaler 实例
- 指示违规详细信息的图表。将鼠标指针悬停在条形图上，可查看检测到的不良客户端连接总数。
- 违规检测消息，指示已丢弃的客户端连接总数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



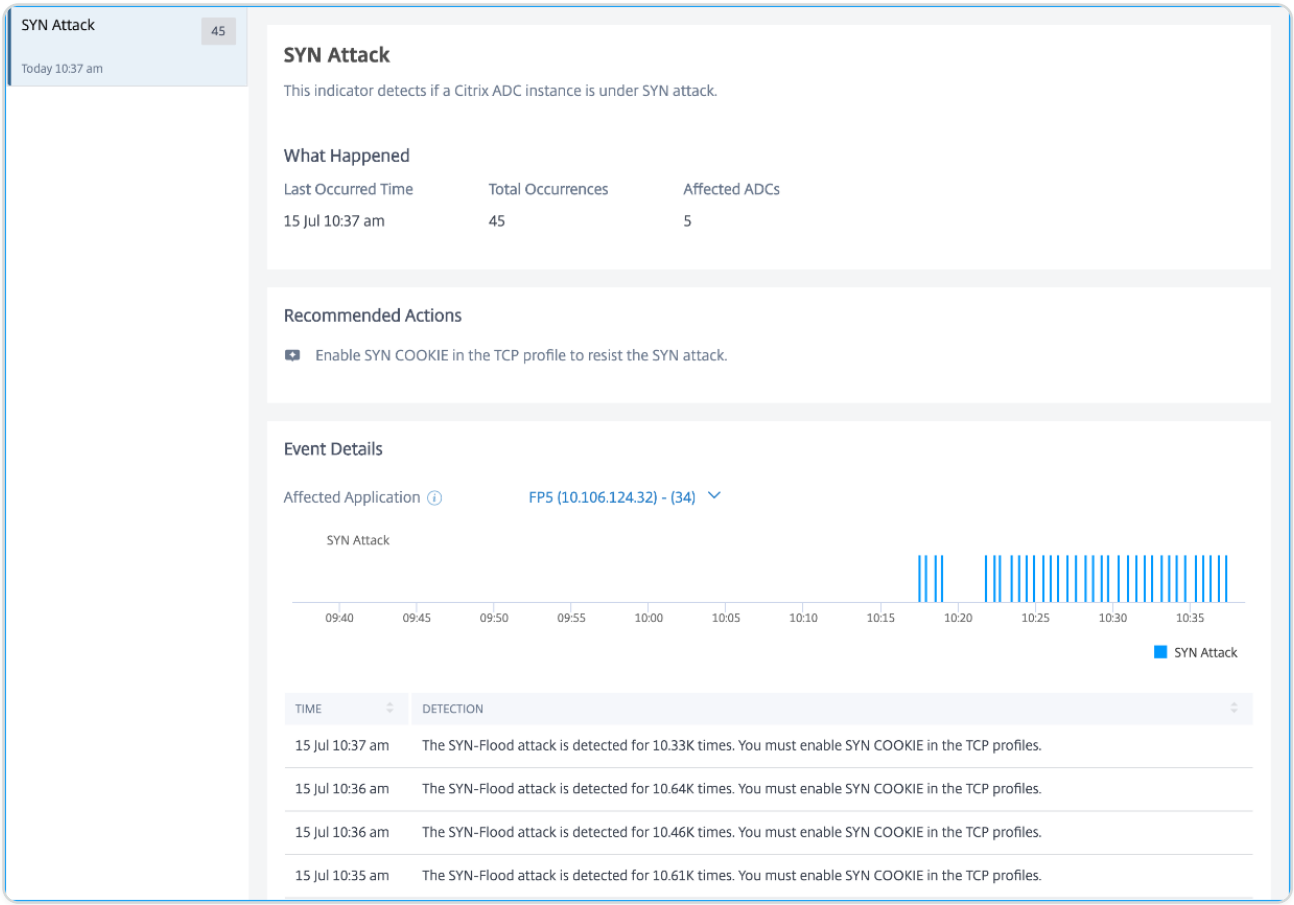
SYN 洪水攻击

SYN 洪水攻击是一种拒绝服务 (DoS) 攻击，它通过使用欺骗性 IP 地址发送数千个连接请求来影响目标计算机。当 NetScaler 实例受到 SYN 洪水攻击时，该实例会尝试为每个恶意请求打开一个连接，然后等待永远不会到达的确认数据包。

TCP 配置文件中的 **SYNCOOKIE** 可防止 NetScaler 设备上的 SYN 攻击。默认情况下，NetScaler 实例上的 **SYNCOOKIE** 已启用。只有在禁用 SYNCOOKIE 时，NetScaler 实例遭受 SYN 洪水攻击的可能性才高。

使用 **SYN 洪水攻击** 指标，您可以分析 NetScaler 实例是否受到 SYN 攻击。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



作为管理员，**建议操作** 建议您在 TCP 配置文件中启用 SYN COOKIE。

在 **事件详细信息** 下，您可以查看：

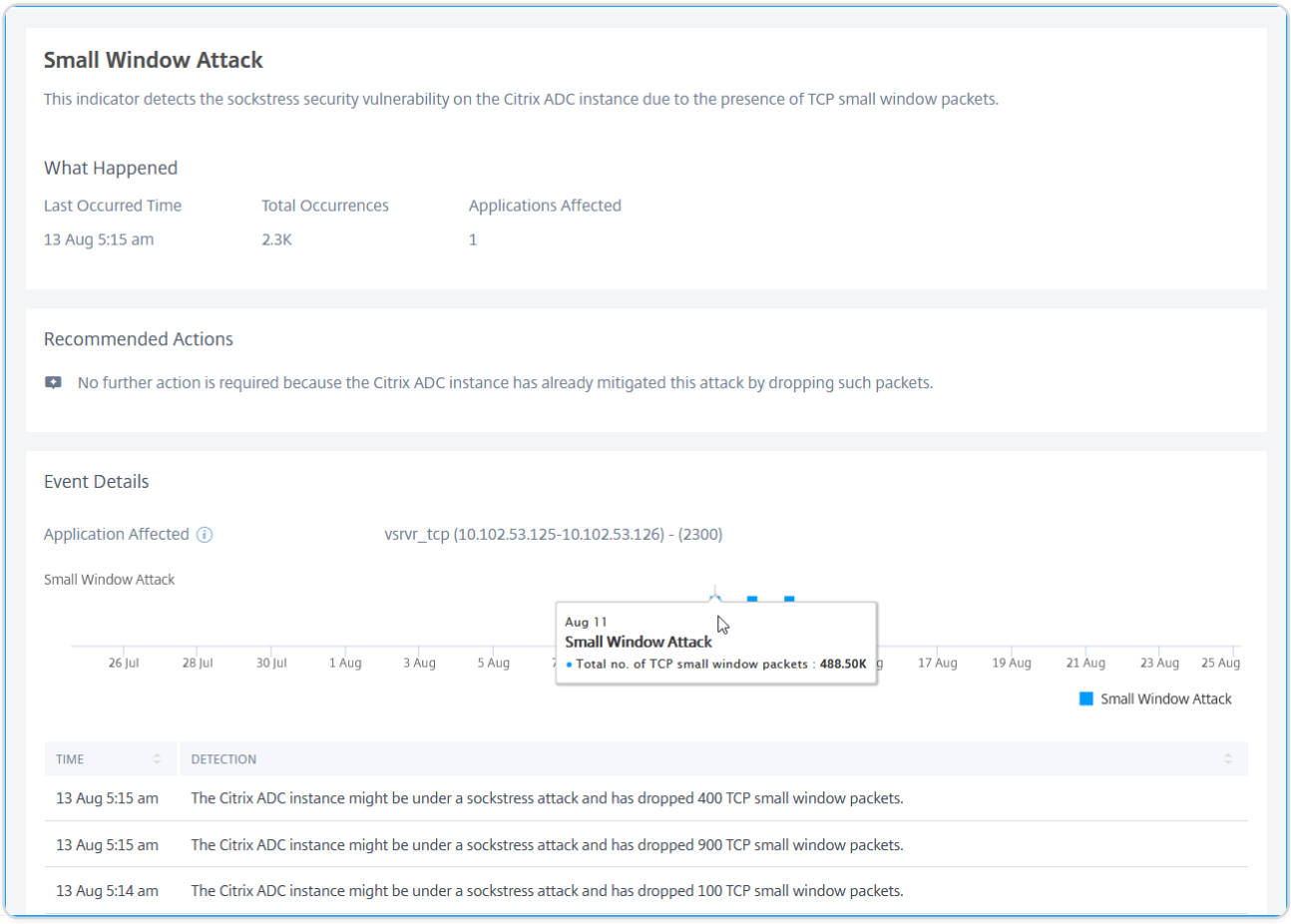
- 受影响的应用程序。如果两个或更多应用程序受到此违规的影响，您还可以从列表中选择该应用程序
- 指示 SYN 攻击详细信息的图表
- 检测消息，指示应用程序被检测到 SYN 攻击的总次数

小窗口攻击

小窗口攻击是一种拒绝服务 (DoS) 攻击，它通过发送数千个窗口大小较小或窗口大小为 0 的 TCP 数据包来影响目标计算机。窗口大小为 0 表示目标计算机必须在另行通知之前停止发送任何数据。通过向目标计算机发送尽可能多的类似连接，目标计算机的内存会被最大程度地利用，并变得无响应。

使用 **小窗口攻击** 指示器，您可以分析 NetScaler 实例是否受到 sockstress 攻击。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



默认情况下，NetScaler 实例通过丢弃所有此类 TCP 小窗口数据包来缓解此攻击。因此，作为管理员，无需采取进一步操作。

在 **事件详细信息** 下，您可以查看：

- 受影响的应用程序。如果两个或更多应用程序受到此违规的影响，您还可以从列表中选择应用程序。
- 指示攻击详细信息的图表。将鼠标指针悬停在条形图上，以查看检测到的 TCP 小窗口数据包总数。
- 检测消息，指示丢弃的 TCP 小窗口数据包总数。

SSL 洞察

SSL Insight 提供对安全 Web 事务 (HTTPS) 的可见性，并允许 IT 管理员通过提供对安全 Web 事务的集成式实时和历史监控来监视 NetScaler 提供的所有安全 Web 应用程序。通过这种可见性，管理员可以评估以下内容：

- **确定配置更改对客户使用的影响**：管理员可以了解进行配置更改（例如关闭 SSLv3 或删除 RC4-MD5 等密码）对客户端的影响。这可以通过评估此协议和密码的历史事务数据来完成。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **量化客户端性能**：管理员可以根据使用的 SSL 密码/协议或协商的证书来了解对应用程序响应时间的影响。
- **应用程序安全性**：评估是否有任何应用程序的事务正在低安全性协议、密码或弱密钥强度下运行。

当在 NetScaler 实例上启用 SSL Analytics 时，会记录并日志化每个 SSL 事务的 SSL 统计信息。这些统计信息显示了 SSL 流的详细信息。此外，每个成功的连接都会由 NetScaler Console Analytics 记录并显示。

SSL Insight 提供以下关键信息，这些信息由 NetScaler Console Analytics 显示：

- 协商的 SSL 协议版本
- 协商的密码和密码强度
- 所用证书的签名哈希算法
- 证书类型和大小
- SSL 前端和后端错误

注意

对于成功的 SSL 连接，SSL AppFlow® 日志记录在每个事务结束时发生。

先决条件

- 您打算配置 SSL Insight 的 NetScaler 实例必须运行 NetScaler 软件版本 11.1 51.21 及更高版本。在运行 11.1 51.21 的 ADC 实例上运行以下命令，以启用 Logstream 作为 SSL Insight 的传输类型。

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the Console>`

   对于运行版本 12.0 及更高版本的 ADC 实例，在通过 NetScaler Console 启用 AppFlow 时，选择 Logstream 作为传输类型。

- NetScaler Console 的版本和内部版本号必须等于或高于 NetScaler 的版本和内部版本号。例如，如果您安装了 NetScaler Console 11.1 build 61.7，则请确保您安装了 NetScaler 11.1 build 60.14 或更早版本。

配置 SSL Insight

如果您启用以下元素，SSL Insight 指标将包含在 Web Insight 报告中：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 在每个 NetScaler 实例上为 Web Insight 启用 AppFlow。
- 在每个 NetScaler 实例上启用 ULFD 模式。
- 在每个 NetScaler 实例上启用所需的 AppFlow 参数。

启用 AppFlow 功能

注意

您可以从 NetScaler Console 或从每个 NetScaler 实例启用 AppFlow 功能。

要从 NetScaler Console 启用 AppFlow 功能：

如果您的 NetScaler Console 为 **13.0 Build 41.x 或更高版本**：

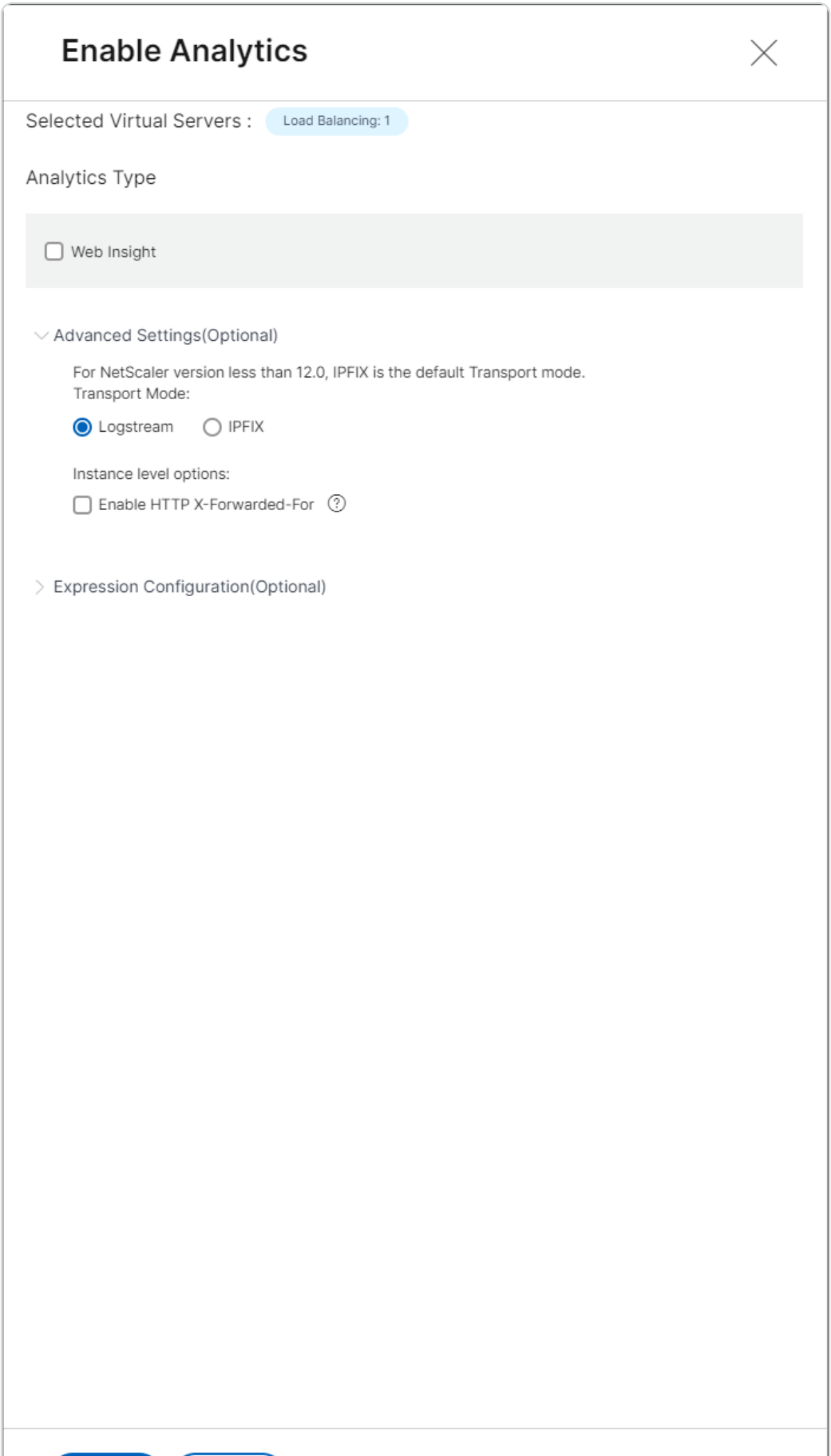
1. 导航到 **Infrastructure > Instances > NetScaler**，然后选择实例类型。例如，VPX。
2. 选择实例，然后从 **Select Action** 列表中单击 **Configure Analytics**。
3. 在 **Configure Analytics on Virtual Server(s)** 页面上，选择虚拟服务器，然后单击 **Enable Analytics**。
4. 在 **Enable Analytics** 窗口中：
   a. 选择 **Web Insight**
   b. 选择 **Logstream** 作为传输模式

      注意

      对于 NetScaler 12.0 或更早版本，**IPFIX** 是传输模式的默认选项。对于 NetScaler 12.0 或更高版本，您可以选择 **Logstream** 或 **IPFIX** 作为传输模式。

      有关 IPFIX 和 Logstream 的更多信息，请参阅 Logstream 概述。
   c. 表达式默认为 true
   d. 单击 **OK**

© 1997–2026 Citrix Systems, Inc. All rights reserved.


Enable Analytics
Selected Virtual Servers :
Load Balancing: 1
Analytics Type
Web Insight
Advanced Settings(Optional)
For NetScaler version less than 12.0, IPFIX is the default Transport mode.
Transport Mode:
Logstream
IPFIX
Instance level options:
Enable HTTP X-Forwarded-For
Expression Configuration(Optional)

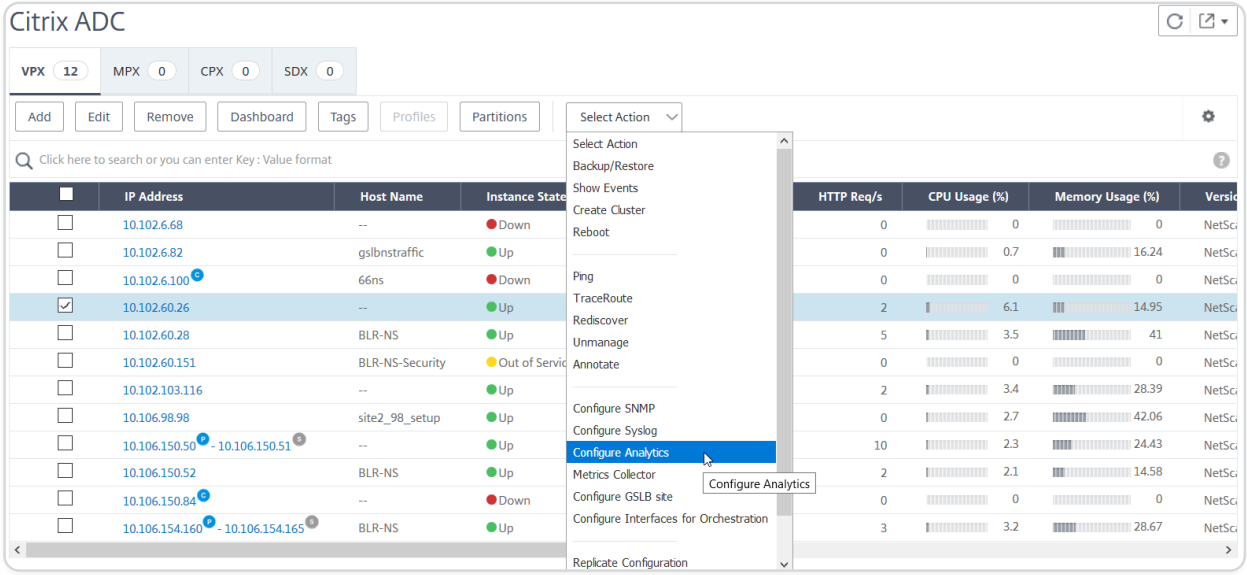
注意

- 如果您选择未获得许可的虚拟服务器，则 NetScaler Console 会首先许可这些虚拟服务器，然后启用分析
- 对于管理分区，仅支持 **Web Insight**
- 对于缓存重定向、身份验证和 GSLB 等虚拟服务器，您无法启用分析。将显示错误消息。

单击 **确定** 后，NetScaler Console 将处理以在选定的虚拟服务器上启用分析。

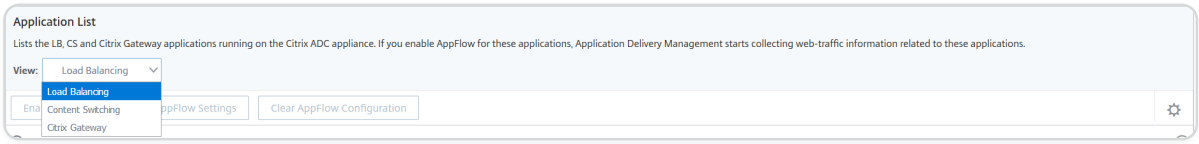
如果您的 NetScaler Console 版本为 **13.0 Build 36.27 或更早版本**：

1. 导航到 **基础架构 > 实例 > NetScaler**，然后选择要启用分析的 NetScaler 实例。
2. 从 **选择操作** 列表中，选择 **配置分析**。



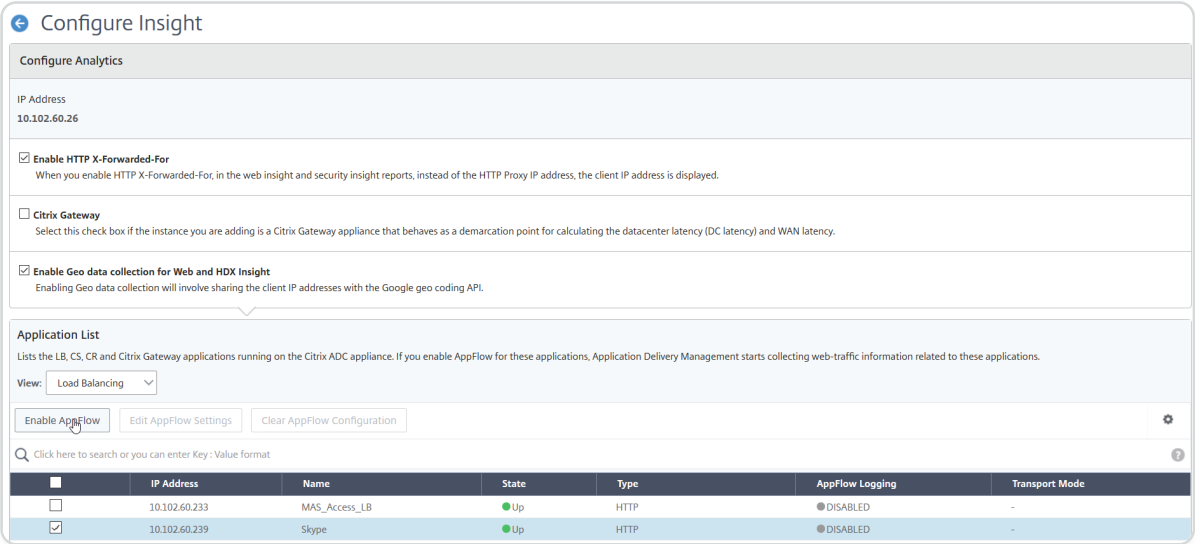
3. 在 **配置 Insight** 页面上：

   a. 选择用于负载平衡或内容切换的 **应用程序列表**。



   b. 选择虚拟服务器，然后单击 **启用 AppFlow**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



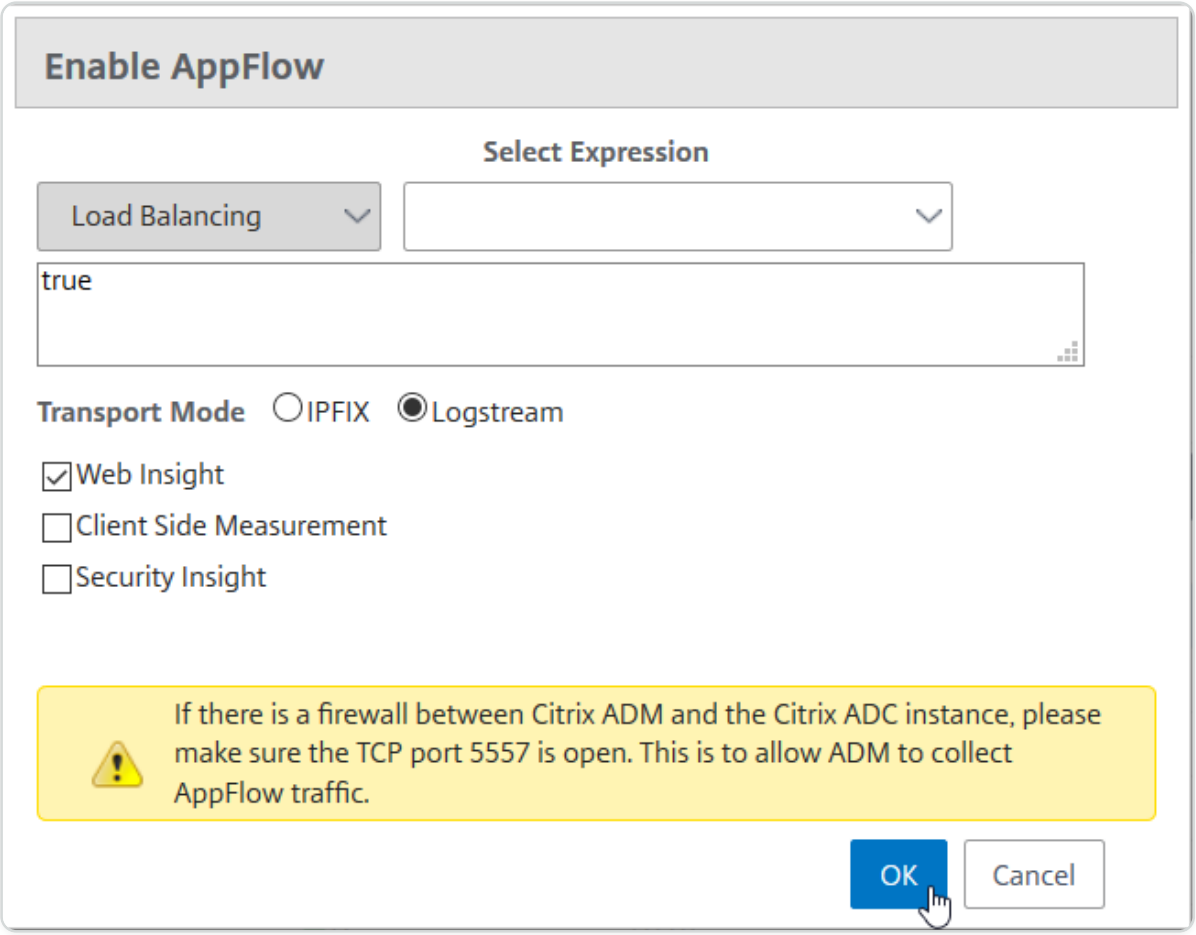
4. 在“启用 AppFlow”对话框中：

   - 在文本框中输入 **true**
   - 选择 **Logstream** 作为传输模式

注意：

建议您选择 Logstream 作为传输模式

   - 选择 **Web Insight** 并单击 **OK**。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用 NetScaler GUI 启用 AppFlow 功能：

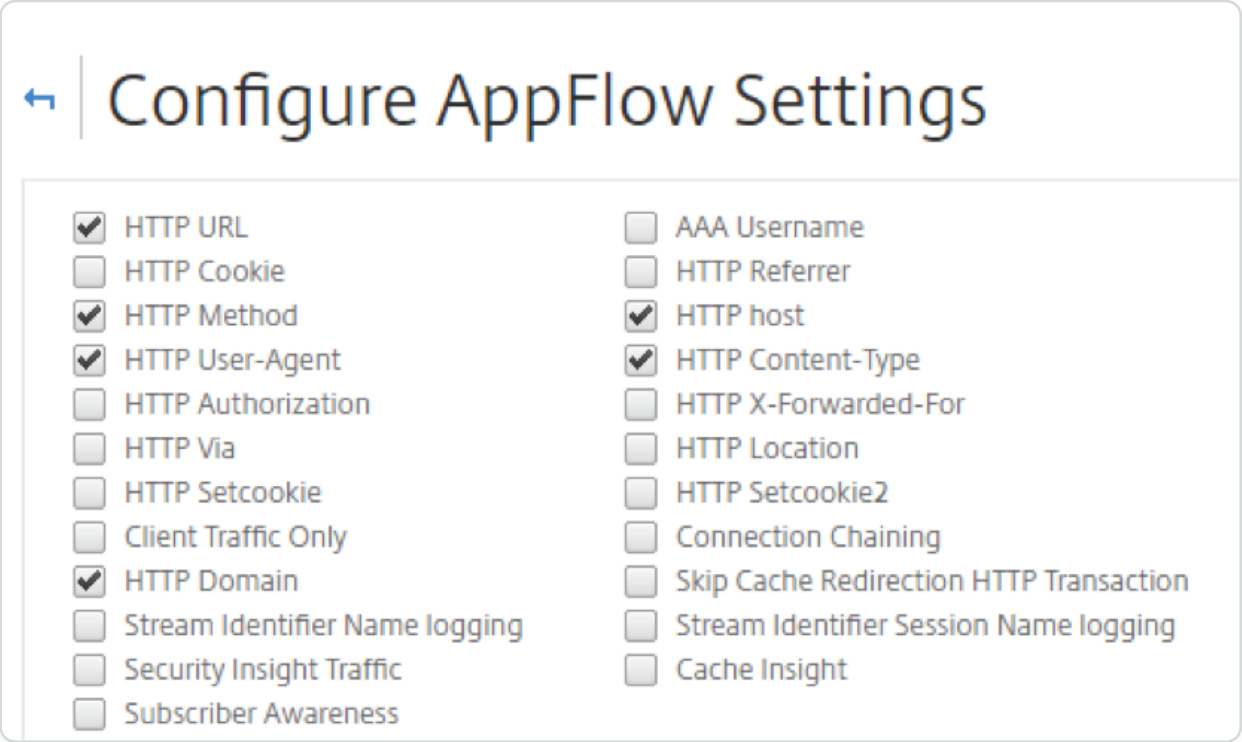
在 NetScaler 实例的 GUI 中，导航到 **Configuration** \> **System** \> **Settings**，单击 **Configure Advanced Features**，然后选择 **AppFlow**。

启用 SSL Insight 参数

在每个 NetScaler 实例上，您必须启用一些 HTTP 参数才能在 NetScaler Console 中显示 SSL Insight 记录。

通过 NetScaler 配置实用程序启用 SSL Insight 参数：

1. 导航到 **Configuration** \> **System** \> **AppFlow**，然后单击 **Change AppFlowSettings**。
2. 选择以下复选框：**HTTP Domain**、**HTTP Host**、**HTTP Method**、**HTTP URL**、**HTTP User-Agent**、**HTTP Content-Type**。
3. 单击 **OK**。



查看 SSL Insight 指标

NetScaler Console 中的 SSL Insight 指标提供了 NetScaler 实例所服务的 SSL 事务性能的详细视图。您可以在客户端、服务器或应用程序级别查看 SSL Insight 指标，以及 SSL 成功和失败事务的指标。借助这些指标，您可以分析和优化 **NetScaler HTTPS** 设置和 SSL 证书设置，并跟踪性能问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

创建组时，您可以为组分配角色、为组提供应用程序级访问权限，并将用户分配给组。NetScaler Console 分析现在支持基于虚拟 IP 地址的授权。您的用户现在可以查看所有 Insight 的报告，但仅限于他们有权访问的应用程序（虚拟服务器）。有关组以及如何将用户分配给组的更多信息，请参阅 配置组。

在 NetScaler Console 中监控 SSL Insight 指标：

您可以查看以下各项的 SSL 指标：

- 某个应用程序。导航到 **Applications > Dashboard**，单击某个应用程序，然后选择 **Web Insight** 选项卡以查看详细指标。有关详细信息，请参阅 应用程序使用情况分析。
- 所有应用程序。导航到 **Applications > Web Insight**，然后单击 **Applications** 和 **Clients** 选项卡以查看 SSL 指标。

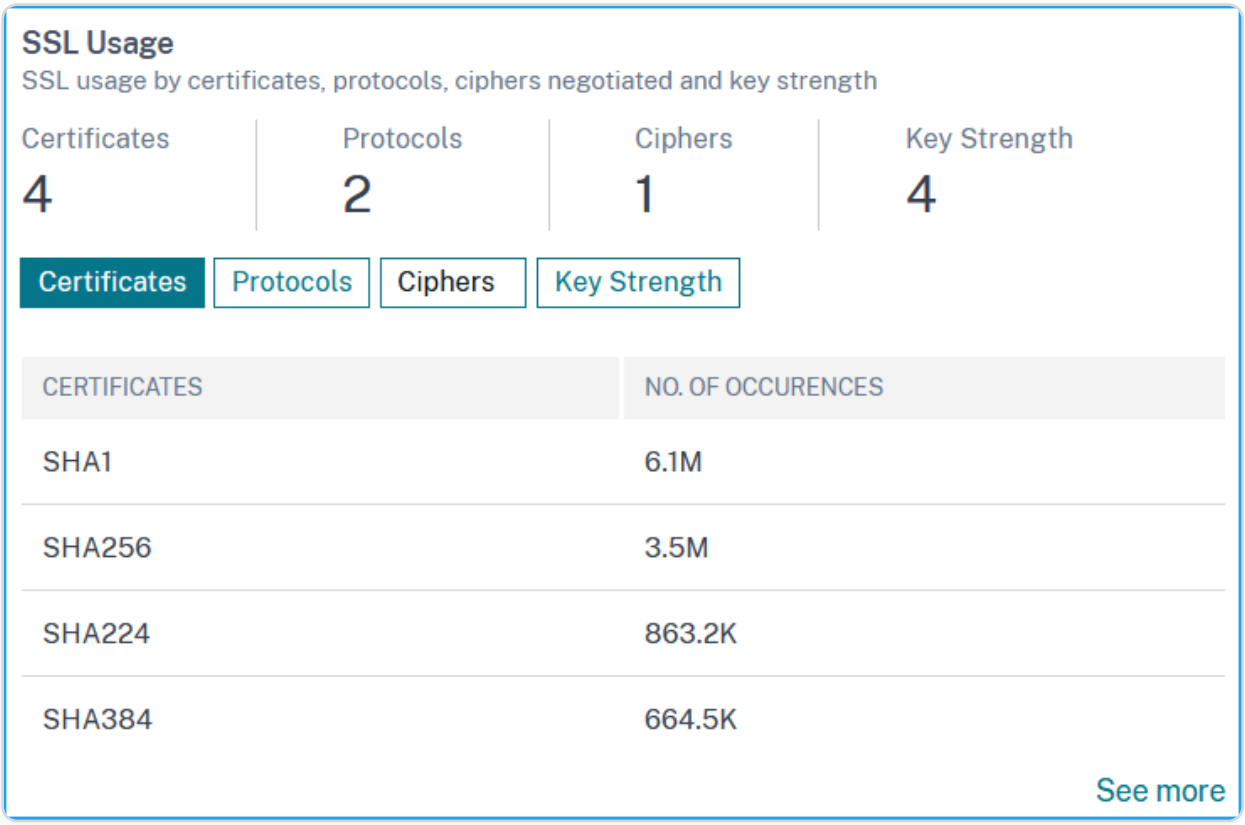
用例：获取 SSL 事务概述

以下用例描述了如何使用 SSL Insight 评估各种 SSL 参数的使用情况并改进安全措施。

假设您有一组应用程序使用 SSL 事务 (HTTPS) 进行通信，并且您已配置 NetScaler Console 来监控 SSL 组件。您可能需要经常审查这些应用程序，以便首先关注最需要关注的应用程序。应用程序或所有应用程序的 **Web Insight** 控制板在 **SSL Errors** 和 **SSL Usage** 下提供了以下 SSL 参数的摘要：

- SSL 证书
- SSL 协议
- SSL 密码
- SSL 密钥强度
- SSL 故障 – 前端
- SSL 故障 – 后端

© 1997–2026 Citrix Systems, Inc. All rights reserved.



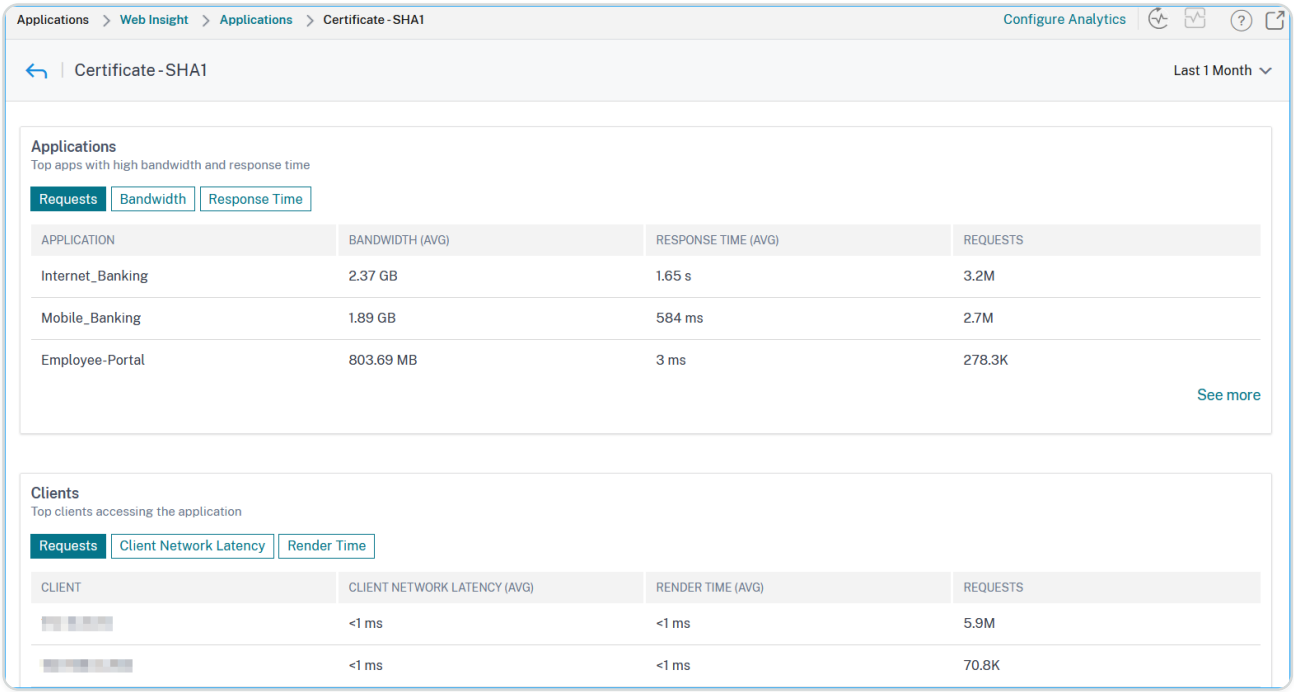
您可以单击每个选项卡以查看详细信息。

用例：客户端的 SSL 指标

您可以查看客户端列表（通过其 IP 地址识别）以及每个客户端的总出现次数。导航到 **应用程序 > Web Insight**，然后选择 **客户端** 选项卡以查看 **SSL 使用情况** 下的详细信息。

单击指标以查看详细信息，并在 **客户端** 下，单击任何客户端 IP 地址以查看所选客户端的 SSL 指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



排查 Web Insight 问题

在 Web Insight 控制板中，您可以可视化您的应用程序使用情况并监控 NetScaler 提供的所有应用程序。使用 Web Insight，NetScaler 将 HTTP 和 SSL 事务数据发送到配置为 AppFlow 收集器的 NetScaler Console。AppFlow 是用于识别和收集网络基础设施中应用程序和事务数据的流导出标准。

本文档可帮助您排查常见的 Web Insight 部署问题。

无数据诊断

如果 Web Insight 未显示任何数据，请确保已为虚拟服务器启用 **Web Insight**。有关详细信息，请参阅管理许可并在虚拟服务器上启用分析。

如果 Web Insight 中没有数据，还会显示一个包含 **无数据诊断** 的通知。您可以单击以查看详细信息进行故障排除。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

与 Web Insight 控制板报告相关的问题

如果 NetScaler Console Web Insight 控制板 (**应用程序> Web Insight**) 未能显示报告，问题可能属于以下情况之一：

- Web Insight 配置问题
- NetScaler 与 NetScaler Console 之间的连接问题
- 未从 NetScaler 收到 AppFlow 数据
- 许可证问题
- 观察点 ID 问题
- AppFlow® 参数缺失问题

配置问题

完成以下步骤以解决此问题：

1. 确保在 NetScaler 实例中启用了 AppFlow 功能。有关详细信息，请参阅启用 AppFlow。
2. 检查 NetScaler 中的 Web Insight 配置：
   a. 运行 `show running | grep -i <appflow_policy>` 命令以检查策略上的 Web Insight 配置。确保绑定类型为 `REQUEST`。例如：`bind lb vserver afsanity -policy afp -priority 100 -type REQUEST`
   b. 运行 `show appflow action` 命令以检查操作上的 Web Insight 配置。确保启用了 `-webinsight` 选项
   c. 检查 LB/CS/CR 虚拟服务器中的 `appflowlog` 参数，以及绑定的服务和服务组。确保在虚拟服务器以及绑定的服务和服务组中都启用了此参数。

NetScaler 与 NetScaler Console 之间的连接问题

完成以下步骤以解决此问题：

1. 检查 NetScaler 中的 AppFlow 收集器状态。有关详细信息，请参阅如何检查 NetScaler 与 AppFlow 收集器之间的连接状态。
2. 在 NetScaler GUI 上，检查 AppFlow 策略是否收到命中。运行命令 `show appflow policy <policy_name>` 以检查 AppFlow 策略命中。您还可以导航到 GUI 中的 **Settings > AppFlow > Policies**（设置 > AppFlow > 策略）以检查 AppFlow 策略命中。
3. 确保防火墙未阻止从 NetScaler 到 NetScaler Console 的 AppFlow 数据。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

未从 NetScaler® 接收到 AppFlow 数据

完成以下步骤以解决此问题：

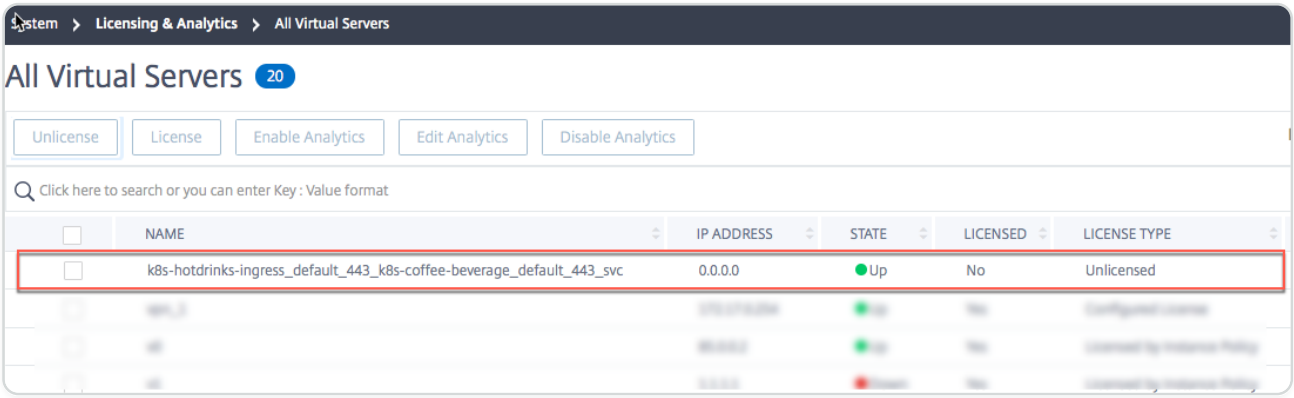
1. 确保没有 AppFlow 配置和连接问题。有关详细信息，请参阅本主题中关于配置问题 和NetScaler 与 NetScaler Console 之间的连接问题 的解决方案部分。
2. 在 NetScaler 上，在 shell 提示符下，运行 `nsconmsg -g appflow_tmpl -d current` 命令并检查以下计数器：

   - `appflow_tmpl_v4_l7_clt2ns_complete`
   - `appflow_tmpl_v4_l7_srvr2ns_complete`
   - `appflow_tmpl_v46_ulfd_client_eot`
   - `appflow_tmpl_v46_ulfd_server_eot`

   如果缺少任何计数器，请在 NetScaler 上进行跟踪。接下来，确认事务已完成且响应正从源服务器提供。如果事务已完成但缺少某些计数器，请联系支持团队。

许可证问题

出现此问题时，您要查看 Web Insight 报告的特定虚拟服务器的许可证在 **Settings > Licensing & Analytics Configuration > Configure License** 下显示为“否”。



完成以下步骤以解决此问题：

1. 在 NetScaler 中，确保 AppFlow 策略命中数正在增加，并且实例正在将 AppFlow 记录发送到 NetScaler Console。
2. 检查相应的虚拟服务器是否已获得许可。如果虚拟服务器未获得许可，NetScaler Console 将丢弃 AppFlow 记录。因此，Web Insight 报告不会显示。

观察点 ID 问题

出现此问题是因为观察点 ID 不唯一。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

观察点 ID 是导出 AppFlow 记录的 NetScaler 的标识符。默认情况下，NetScaler IP 是观察点 ID。

完成以下步骤以排查此问题：

1. 在 NetScaler 中，确保 AppFlow 策略命中数正在增加，并且实例正在将 AppFlow 记录发送到 NetScaler Console。
2. 检查相应的虚拟服务器是否已获得许可。
3. 确保配置未从一个 NetScaler 复制到另一个。复制时，配置可能会导致导出器 ID 问题，从而导致 NetScaler Console 无法处理 AppFlow 记录。
4. 登录到 NetScaler 并运行 `unset appflow param -observationpointId` 命令。

AppFlow 参数缺失问题

出现此问题是因为 NetScaler Console 由于数据缺失而丢弃了 AppFlow 记录。

完成以下步骤以排查此问题：

1. 确保在 NetScaler 中，AppFlow 策略命中数正在增加，并且实例正在将 AppFlow 记录发送到 NetScaler Console。
2. 检查相应的虚拟服务器是否已获得许可。
3. 确保配置未从一个 NetScaler 复制到另一个。复制时，配置可能会导致导出器 ID 问题，从而导致 NetScaler Console 无法处理 AppFlow 记录。
4. 确保在 NetScaler 上启用了以下 AppFlow 参数：
   - `HTTP method logging`
   - `HTTP domain name logging`
   - `HTTP URL logging`
   - `HTTP host logging`
   - `HTTP Content-Type header logging`

使用计数器进行故障排除

检查以下 AppFlow 计数器，以查找任何 AppFlow 或 Web Insight 相关问题。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

计数器	描述
`appflow_tot_record_drop`	由于收集器无效而丢弃的 AppFlow 记录。通常发生在收集器配置更改，并且现有连接使用旧收集器配置时。
`lstream_tot_trans_written`	此计数器必须针对每个要记录的事务递增。
`lstream_sent`	此计数器针对每个发送的事务日志递增。

查看 Web 事务分析

Web 事务分析使您能够查看以下详细事务：

- 响应时间 > 500 毫秒
- 5xx 错误

注意：

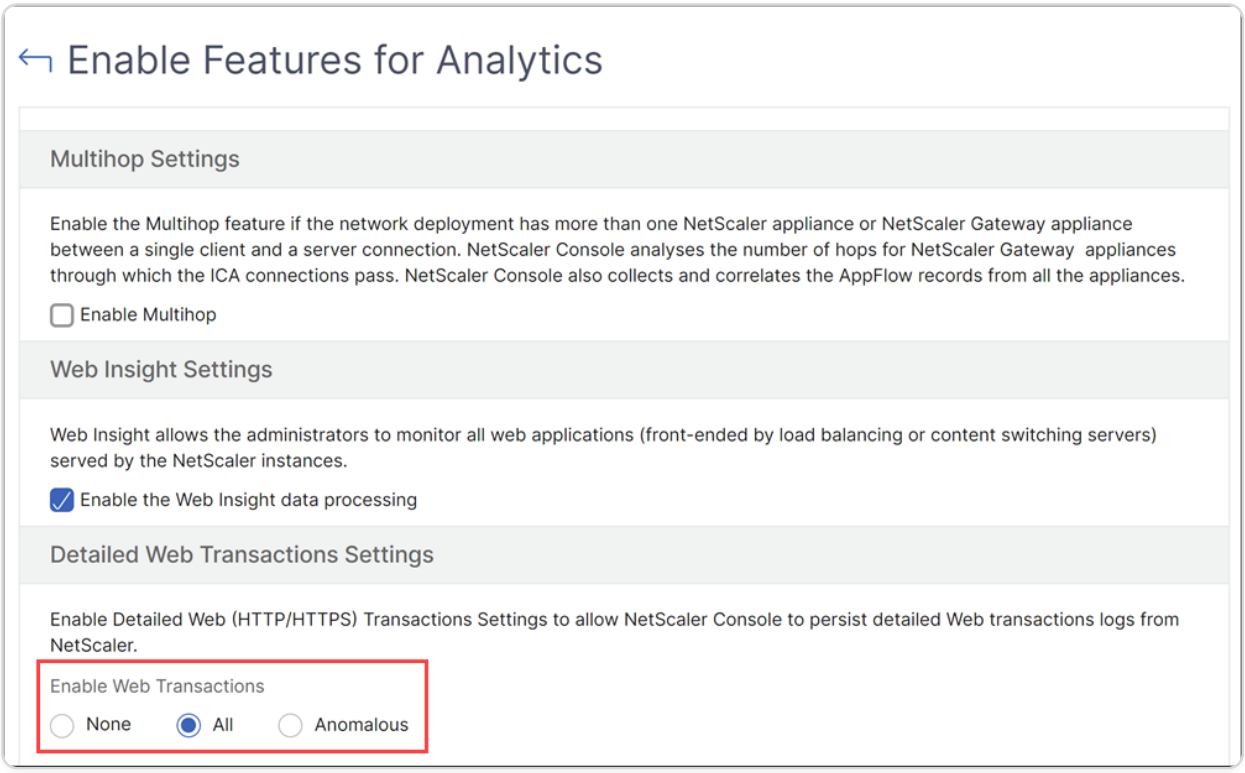
> 您只能查看所选应用程序的少量 2xx 事务示例。

先决条件：

要查看 Web 事务分析，您必须：

- 启用 分析。
- 更改 **Web 事务设置** 以显示 2xx。导航到 **设置** > **分析设置**，选择 **启用分析功能**，然后选择 **全部**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



详细的 Web 事务

此功能不仅使您能够深入查看详细事务，还能直观地了解客户端、NetScaler 和服务器之间的响应时间指标分布。

注意

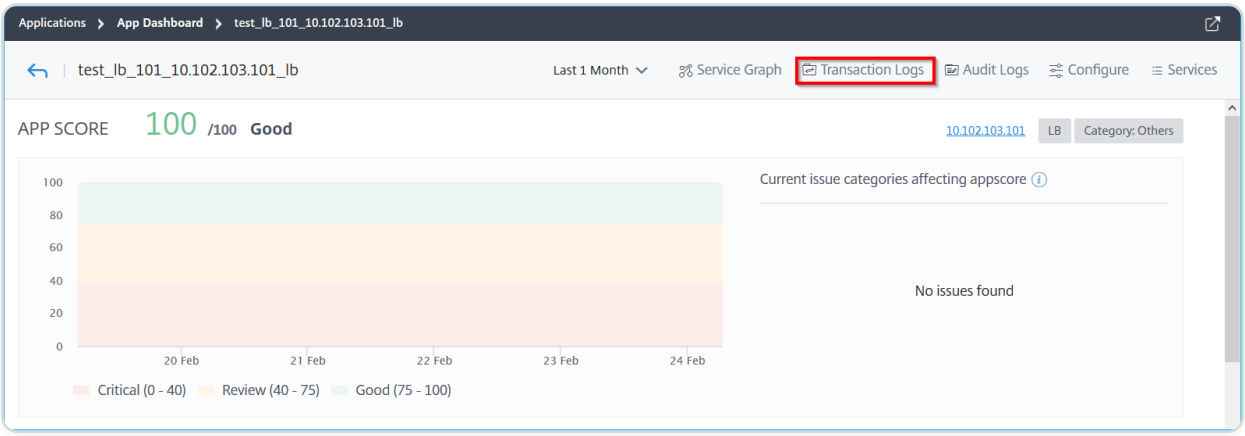
> 在某些情况下，NetScaler 可能无法计算某些事务的 RTT 值。对于此类事务，NetScaler Console 将 RTT 值显示为

- **NA** – 当 NetScaler 实例无法计算 RTT 时显示。
- **< 1ms** – 当 NetScaler 实例计算的 RTT 为 0 毫秒到 1 毫秒之间的小数时显示。例如，0.22 毫秒。

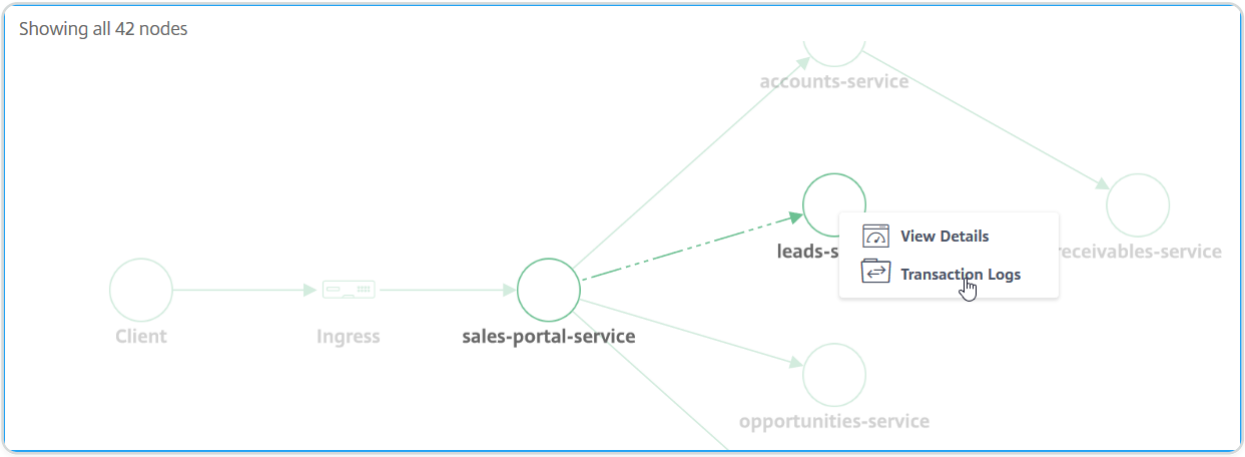
您可以访问以下内容的**事务摘要**：

- **应用程序** - 导航到**应用程序** > **仪表板**，选择一个应用程序，然后单击**事务日志**。

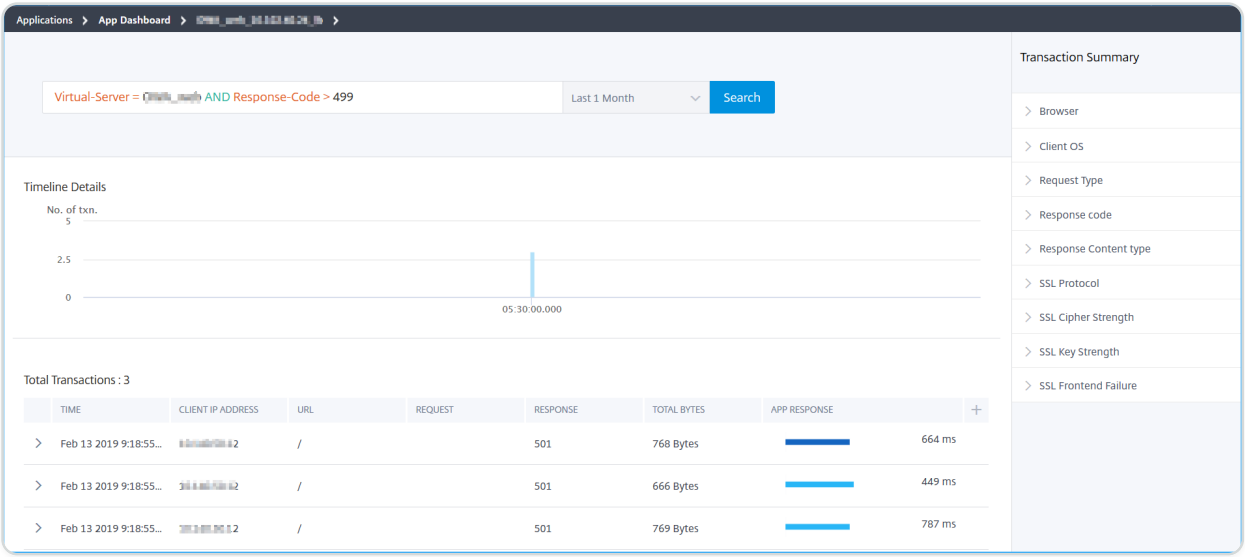
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Kubernetes 应用程序** - 导航到**应用程序** > **服务图**，然后单击一个服务并选择**事务日志**。



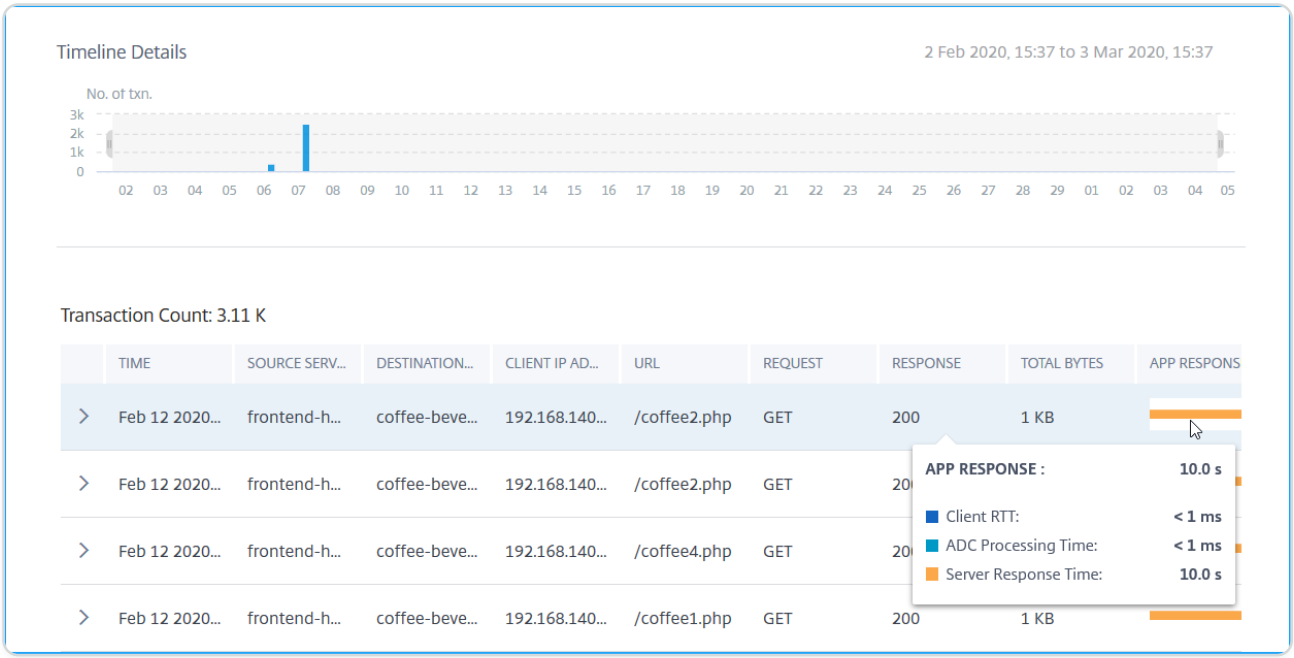
所选应用程序的**事务摘要**页面随即显示。



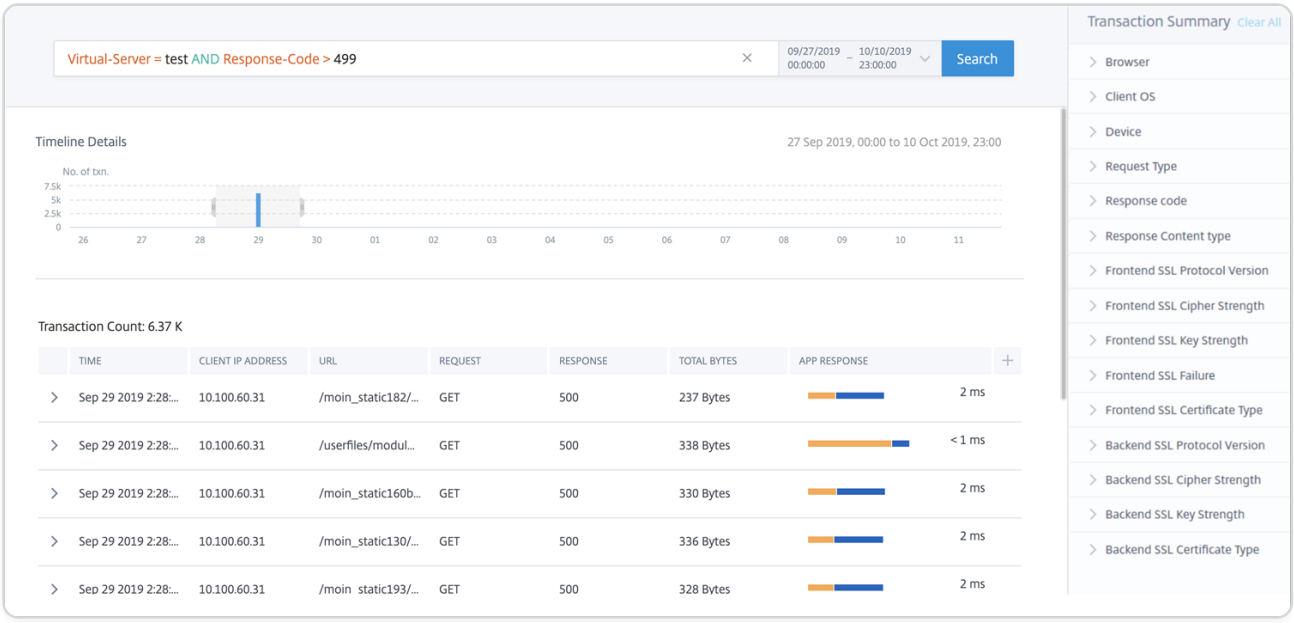
将鼠标指针悬停在**应用程序响应**中，以查看来自 NetScaler 实例和服务器的 RTT 和处理时间等详细信息。

以下示例可帮助您分析问题来自服务器。服务器响应时间显示为 10 秒。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



您还可以拖动并选择以查看特定持续时间的事务。



查看事件

您可以查看特定事件的详细信息。在**事务摘要**面板上，您可以通过从每个指标中选择选项来筛选结果。

例如，假设您要查看 4xx 事务。

在**事务摘要**面板上，单击**响应代码**，然后选择**404**以查看结果。

查看事件(/en-us/netscaler-application-delivery-management-software/media/view-event.png)

单击事务以查看显示从客户端到服务器的指标信息的详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

详细事务(/en-us/netscaler-application-delivery-management-software/media/detailedevent.png)

对于存在 SSL 错误的事务，将显示客户端和服务器的详细信息。将显示以下 SSL 指标：

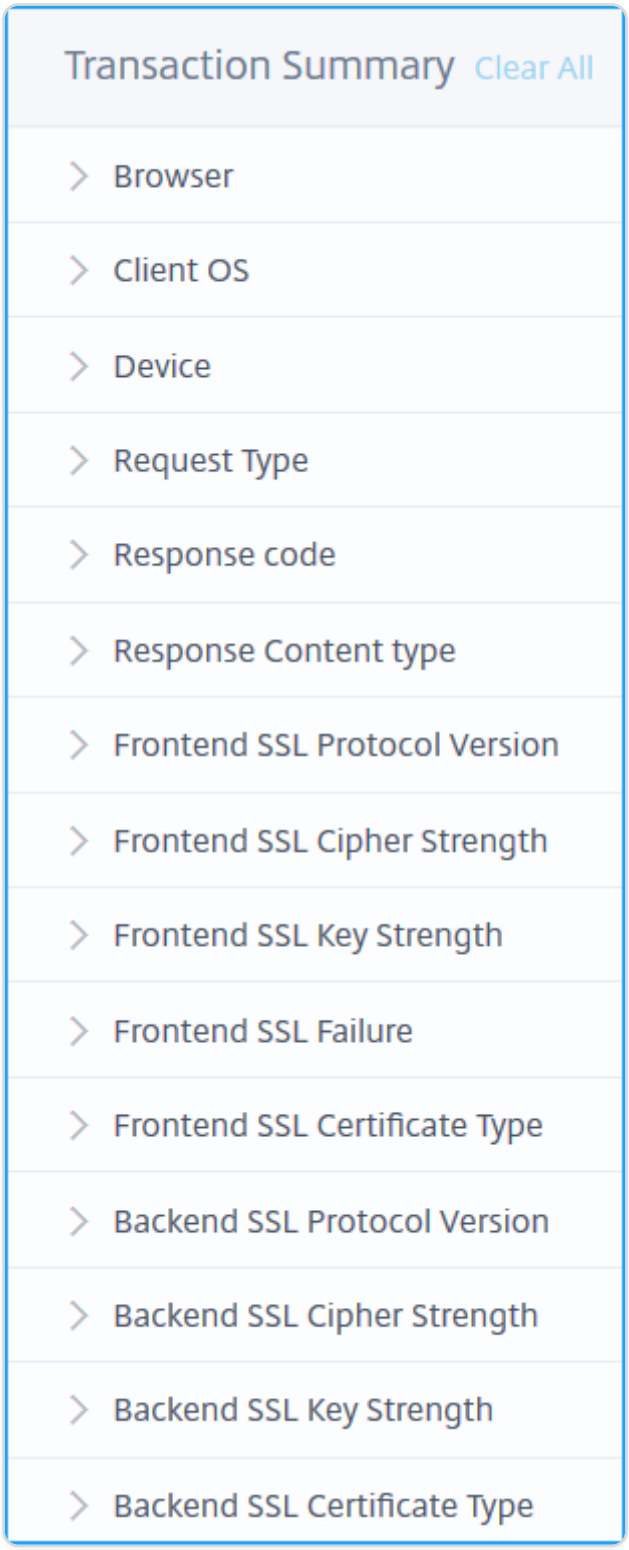
- SSL 协议版本
- SSL 前端故障
- SSL 密码强度
- SSL 密钥强度
- SSL 证书类型

  SSL(/en-us/netscaler-application-delivery-management-software/media/ssl-detailed-metrics.png)

您还可以从**事务摘要**面板中单击**SSL 前端**和**SSL 后端指标**来筛选结果。

要筛选结果，请选择**事务摘要**下可用的选项。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **浏览器**：客户端使用的浏览器类型。例如：Chrome、Firefox。
- **客户端操作系统**：基于浏览器用户代理详细信息的客户端操作系统。例如：Windows
- **设备**：基于浏览器用户代理详细信息的设备。例如：平板电脑、移动设备。
- **请求类型**：事务请求类型。例如：GET。
- **响应代码**：从服务器接收到的响应代码。例如：501、404、200。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

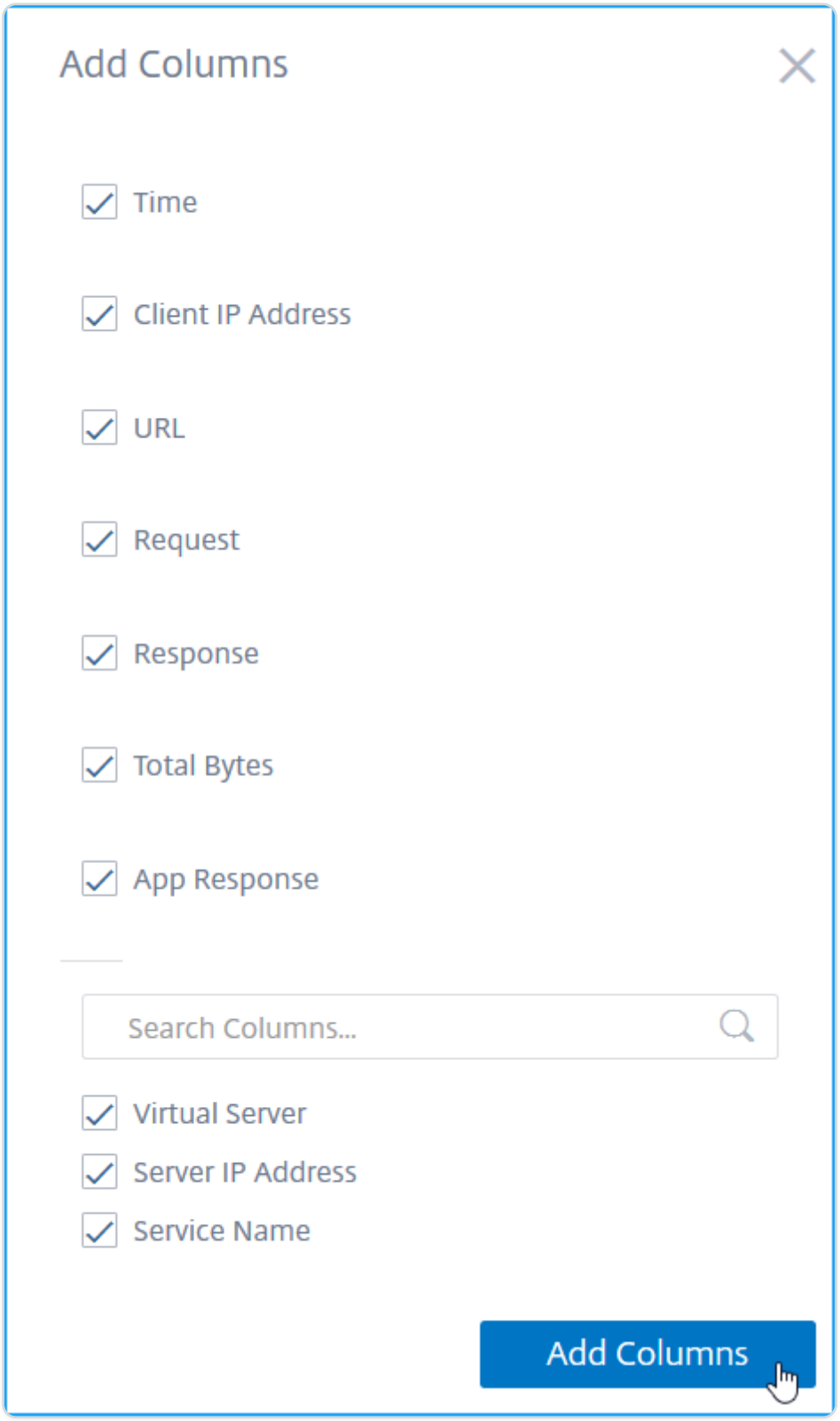
- **响应内容类型**：事务内容类型。如果客户端请求的是 text/html，则服务器的响应也必须是 text/html。
- **前端 SSL 协议版本**：客户端使用的 SSL 协议版本。例如：SSLv3。
- **前端 SSL 密码强度**：基于 SSL 证书密钥大小的密码强度，例如高、中、低。
- **前端 SSL 密钥强度**：SSL 密码强度根据 SSL 证书密钥大小计算。密钥长度定义了 SSL 算法的安全性。例如：2048
- **前端 SSL 故障**：前端 SSL 握手错误消息。例如：SSL CLIENTAUTH FAILURE
- **前端 SSL 证书类型**：客户端使用的证书类型。例如：RSA、DSA、ECDSA、DH。
- **后端 SSL 协议版本**：服务器使用的 SSL 协议。例如：SSLv3
- **后端 SSL 密码强度**：基于 SSL 证书密钥大小的密码强度，例如高、中、低。
- **后端 SSL 密钥强度**：SSL 密码强度根据 SSL 证书密钥大小计算。密钥长度定义了 SSL 算法的安全性。例如：2048
- **后端 SSL 证书类型**：服务器使用的证书类型。例如：RSA、DSA、ECDSA、DH。

在事件列表中添加列

您可以单击

按钮选择选项列表，然后单击**添加列**以显示详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



高级搜索

事务摘要还包含一个搜索文本框和时间范围列表，您可以在其中根据需要查看事件。当您将光标置于搜索框中时，搜索框会为您提供搜索建议列表。您还可以在搜索查询中使用运算符来缩小搜索范围。

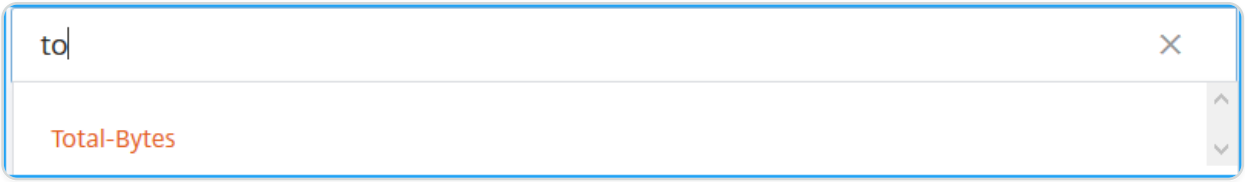
© 1997–2026 Citrix Systems, Inc. All rights reserved.

以下是您可以在搜索查询中使用的运算符：

运算符	描述	示例	输出
=	等于某个值	虚拟服务器 = 测试	显示名称为“test”的虚拟服务器的事件。
>	大于某个值	应用程序响应时间 > 500	显示应用程序中响应时间大于 500 毫秒的事件
<	小于某个值	应用程序响应时间 < 300	显示应用程序中响应时间小于 300 毫秒的事件
>=	大于或等于某个值	总字节数 >= 1024	显示大于或等于 1 KB 的事务事件
<=	小于或等于某个值	总字节数 <= 1024	显示小于或等于 1 KB 的事务事件
!=	不等于某个值	响应代码 != 200	显示所有事务的事件，但失败的事务除外。
~	包含某个值	虚拟服务器 ~ mas	显示名称为 mas 的虚拟服务器的事件。

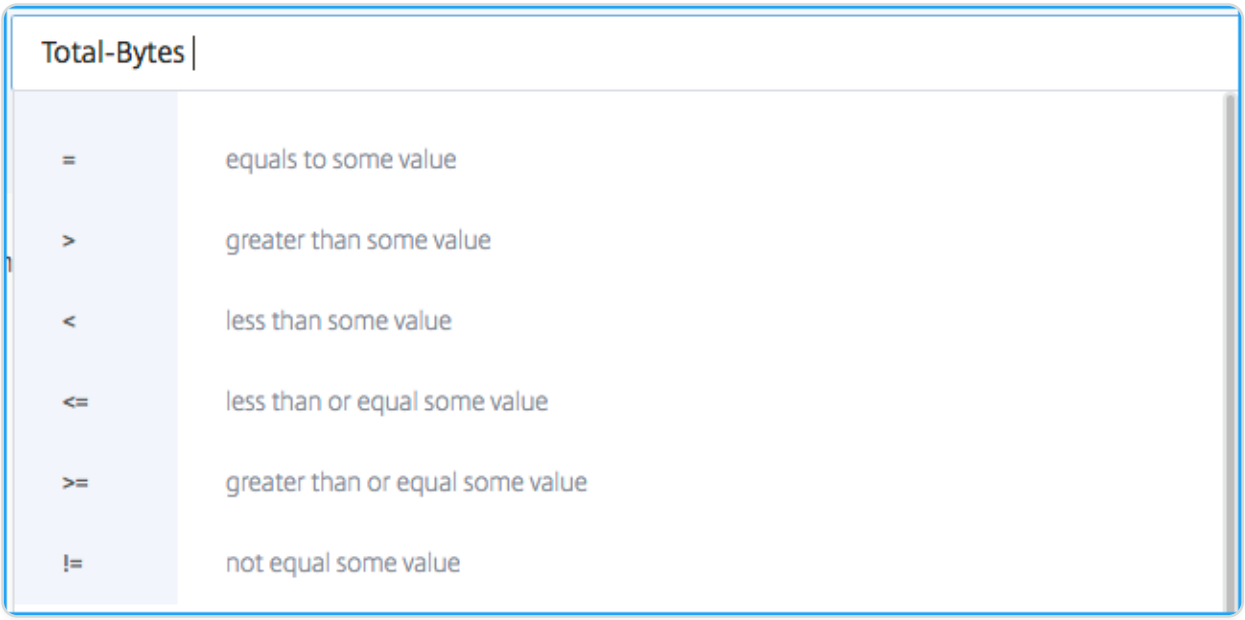
例如，假设您想为小于 300 字节的总字节数生成事件。您必须按如下方式指定搜索查询：

1. 在搜索框中指定所需的词语以获取相关建议。



2. 选择 **Total-Bytes**，然后再次单击搜索文本框，并选择 **<**。

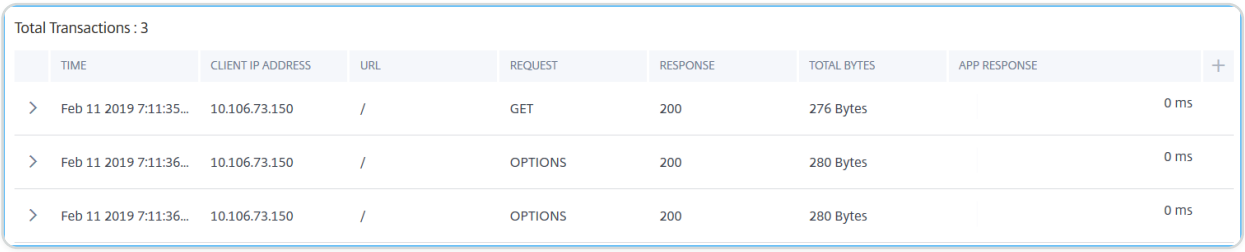
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. 输入值 300。

4. 选择时间段，然后点击 **搜索** 以根据您的搜索查询查看事件。

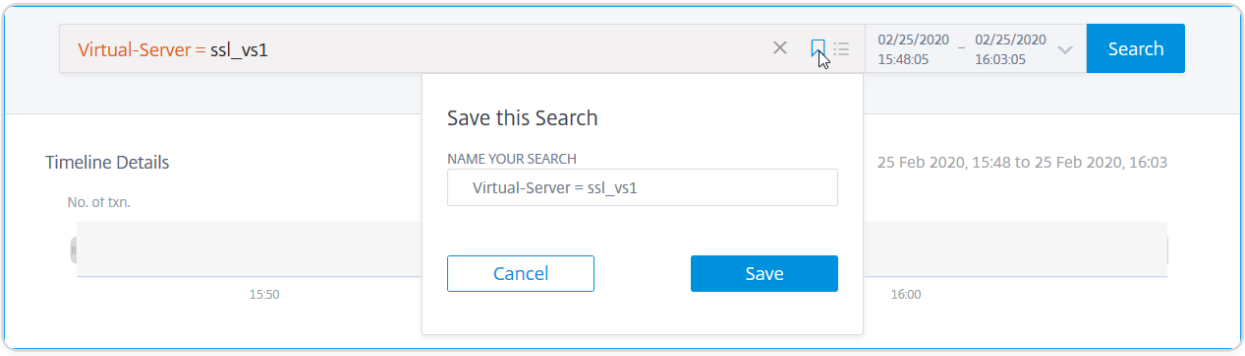
   搜索结果已显示。



保存搜索

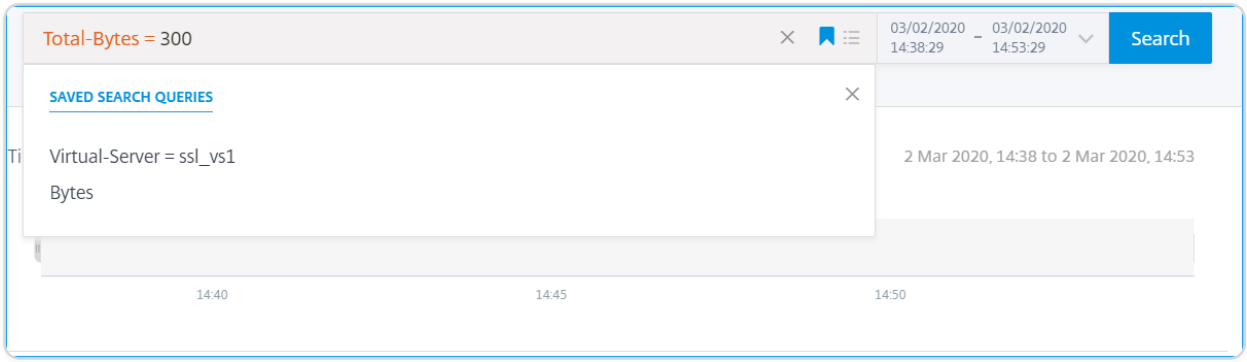
在使用建议和运算符后，您可以保存搜索查询。然后，您可以从列表中使用它，而无需再次使用建议和运算符。

- 要保存搜索查询，请点击书签图标，指定一个您选择的名称，然后点击 **保存**。

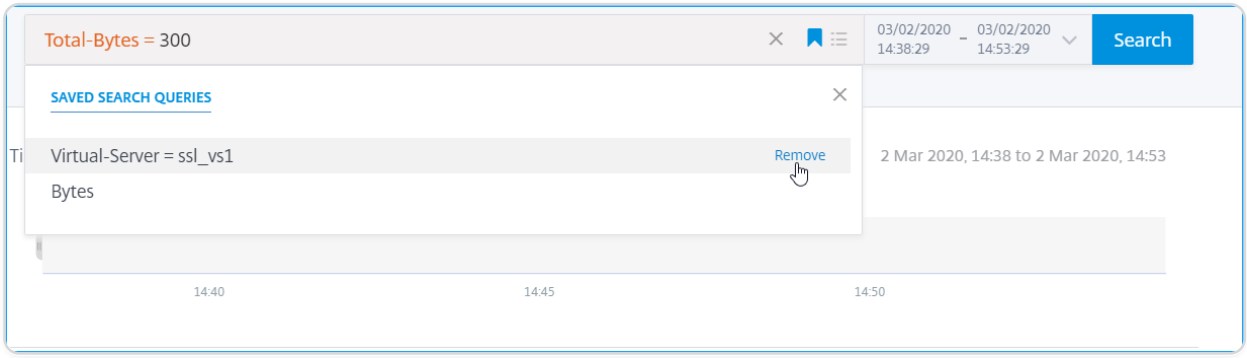


© 1997–2026 Citrix Systems, Inc. All rights reserved.

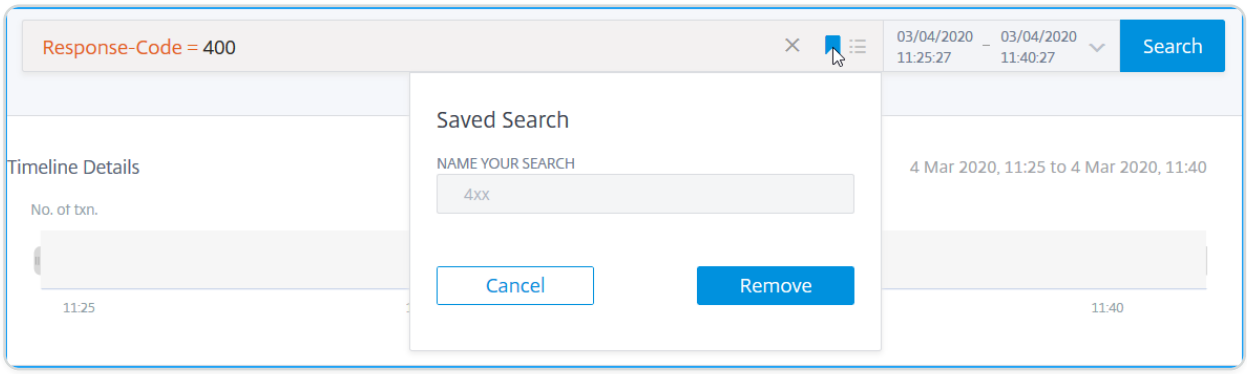
- 要从列表中使用搜索查询，请点击图标并从列表中选择搜索查询以显示结果。



- 要删除搜索查询，请点击图标，将鼠标指针悬停在已保存的搜索查询上，然后点击 **删除**。



您也可以点击书签图标并点击 **删除**。



导出数据

您可以通过单击“**导出**”图标，导出选定持续时间内的 Web 事务分析数据。您可以导出为 PDF、PNG、JPEG 和 CSV 格式。“**导出**”选项使您能够执行以下操作之一：

- 选择“**立即导出**”以查看并将报告导出为 PDF、JPEG、PNG 或 CSV 格式。
- 选择“**计划导出**”选项卡以每天、每周或每月计划报告，并通过电子邮件或 Slack 消息发送报告。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

设置双层或服务网格精简拓扑的详细步骤

软件要求

KUBERNETES 分发版	KUBERNETES 版本	容器网络接口 (CNI)	CPX 版本	CIC 版本	NETSCALER CONSOLE 版本	NETSCALER 代理版本
开源	v1.16.3	法兰绒	13.0–41.28	1.5.25	13.0–47.22	13.0–47.22

开始之前

您可以使用以下场景查看服务图：

- NetScaler Console 和 Kubernetes 集群位于同一网络（例如，NetScaler Console 和 Kubernetes 集群托管在 Citrix Hypervisor 上）。
- NetScaler Console 和 Kubernetes 集群位于不同的网络。在这种情况下，您必须配置一个 本地代理 并在托管 Kubernetes 集群的网络上注册该代理。

要在 NetScaler Console 中使用服务图，请确保您已完成以下操作：

- Kubernetes 集群以 NetScaler CPX 作为代理。有关更多信息，请参阅 NetScaler Ingress Controller。
- 在 NetScaler Console 上配置了 静态路由，以启用 NetScaler Console 和 NetScaler CPX 之间的通信
- 从 GitHub 存储库 下载了示例部署文件。
- 在 CPX YAML 文件 中添加了所需参数，以确保 CPX 成功注册到 NetScaler Console。
- 在 NetScaler Console 中添加了 Kubernetes 集群。
- 部署了 示例微服务应用程序。
- 部署了 NetScaler CPX 并将 CPX 注册到 NetScaler Console。
- 启用了 **自动选择虚拟服务器** 以许可虚拟服务器。
- 将 **Web 事务设置** 更改为 **All**，以便 NetScaler 代理获取 HTTP 事务。
- 更新了 **lstream.conf** 文件，并将 TCP 设置更改为 **All**，以便 NetScaler 代理获取 TCP 指标。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

软件要求

KUBERNETES 分发版	KUBERNETES 版本	容器网络接口 (CNI)	CPX 版本	CIC 版本	NETSCALER CONSOLE 版本	NETSCALER 代理版本
开源	v1.16.3	法兰绒	13.0–41.28	1.5.25	13.0–47.22	13.0–47.22

开始之前

您可以使用以下场景查看服务图：

- NetScaler Console 和 Kubernetes 集群位于同一网络上（例如，NetScaler Console 和 Kubernetes 集群托管在 Citrix Hypervisor 上）。
- NetScaler Console 和 Kubernetes 集群位于不同的网络上。在这种情况下，您必须配置一个 本地代理，并在托管 Kubernetes 集群的网络上注册该代理。

要在 NetScaler Console 中使用服务图，请确保您已完成以下操作：

- 将 NetScaler CPX 作为代理的 Kubernetes 集群。有关更多信息，请参阅 NetScaler Ingress Controller。
- 在 NetScaler Console 上配置 静态路由，以启用 NetScaler Console 和 NetScaler CPX 之间的通信
- 从 GitHub 存储库下载了示例部署文件。
- 在 CPX YAML 文件中添加了所需参数，以确保 CPX 成功注册到 NetScaler Console。
- 在 NetScaler Console 中添加了 Kubernetes 集群。
- 部署了 示例微服务应用程序。
- 部署了 NetScaler CPX 并将 CPX 注册到 NetScaler Console。
- 启用了 **自动选择虚拟服务器**以许可虚拟服务器。
- 将 **Web 事务设置**更改为 **All**，以便 NetScaler 代理获取 HTTP 事务。
- 更新了 **lstream.conf** 文件，并将 NetScaler 代理的 TCP 设置更改为 **All** 以获取 TCP 指标。

在 NetScaler Console 中配置静态路由

在 Kubernetes 集群内部，所有容器化 Pod 都使用覆盖网络。无法直接使用这些私有 IP 地址建立通信。要启用从 NetScaler Console 到 Kubernetes 集群的通信，您必须在 NetScaler Console 中配置静态路由。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

> 如果您使用的是本地代理，请确保在代理上配置静态路由。使用 SSH 客户端登录到 NetScaler 代理并配置静态路由。

假设您的 Kubernetes 集群具有以下 IP 地址：

- Kubernetes 主节点 – 101.xx.xx.112
- Kubernetes 工作节点 1 – 101.xx.xx.111
- Kubernetes 工作节点 2 – 101.xx.xx.110

在 Kubernetes 主节点上，运行以下命令以识别用于静态路由的 Pod 网络：

```
kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}{.status.addresses[0].address}{'\n'}{end}"
```

以下是运行命令后的示例输出：

```
root@master:~# kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}
{.status.addresses[0].address}{'\n'}{end}"
podNetwork: 1[illegible]  gateway: 1[illegible]0
podNetwork: 1[illegible]  gateway: 1[illegible]1
podNetwork: 1[illegible]  gateway: 1[illegible]2
```

1. 使用 SSH 客户端登录到 NetScaler Console
2. 使用命令 `route add -net <public IP address range> <Kubernetes IP address>` 配置静态路由

   例如：

   `route add -net 192.168.0.0/24 101.xx.xx.112`

   `route add -net 192.168.1.0/24 101.xx.xx.111`

   `route add -net 192.168.2.0/24 101.xx.xx.110`
3. 使用 `netstat -rn` 验证配置

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bash-3.2# netstat -rn
Routing tables

Internet:
Destination        Gateway            Flags    Refs      Use  Netif Expire
default            10.[redacted].1    UGS         0 20224745    1/1
10.[redacted].0/24 link#3             U           0  7002455    1/1
10.[redacted].115  link#3             UHS         0        0    lo0
127.0.0.1          link#1             UH          0  7421390    lo0
192.168.0.0/24     10.[redacted].12   UGS         0        0    1/1
192.168.1.0/24     10.[redacted].11   UGS         0   319315    1/1
192.168.2.0/24     10.[redacted].10   UGS         0    41712    1/1
```

4. 将这些路由命令附加到 `/mpsconfig/svm.conf` 文件中。

   a. 在 NetScaler Console 中，使用以下命令访问 **svm.conf** 文件：

   `vim /mpsconfig/svm.conf`

   b. 在 **svm.conf** 文件中添加静态路由。

   例如，`route add -net 192.168.0.0/24 101.xx.xx.112`。

从 GitHub 下载示例部署文件

1. 使用命令 **git clone** `https://github.com/citrix/citrix-k8s-ingress-controller.git` 将 GitHub 存储库克隆到主节点。
2. 要访问 YAML 文件：

   `cd citrix-k8s-ingress-controller/example/servicegraph-demo/`

在 CPX YAML 文件中添加参数

注意

如果您使用的是 CPX 58.x 或更高版本，则在注册到代理时必须使用非 nsroot 密码。为确保安全，NetScaler 代理 61.x 或更高版本需要强制更改密码。如果您的 NetScaler 代理已升级到 61.x 或最新版本，则必须确保使用 **CPX 58.x 或更高版本**的构建。

您必须在 `cpx.yaml` 文件中包含以下参数，以确保 CPX 注册到 NetScaler Console：

```
- name: "NS_MGMT_SERVER"

  value: "xx.xx.xx.xx"

- name: "NS_MGMT_FINGER_PRINT"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    value: "xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx"

  - name: "NS_HTTP_PORT"

    value: "9080"

  - name: "NS_HTTPS_PORT"

    value: 9443"

  - name: "NS_MGMT_USER"

    value: "nsroot"

  - name: "NS_MGMT_PASS"

    value: <your password>

  - name: "LOGSTREAM_COLLECTOR_IP"

    value: "xx.xx.xx.xx"
```

- **NS_MGMT_SERVER** – 指示 NetScaler Console IP 地址

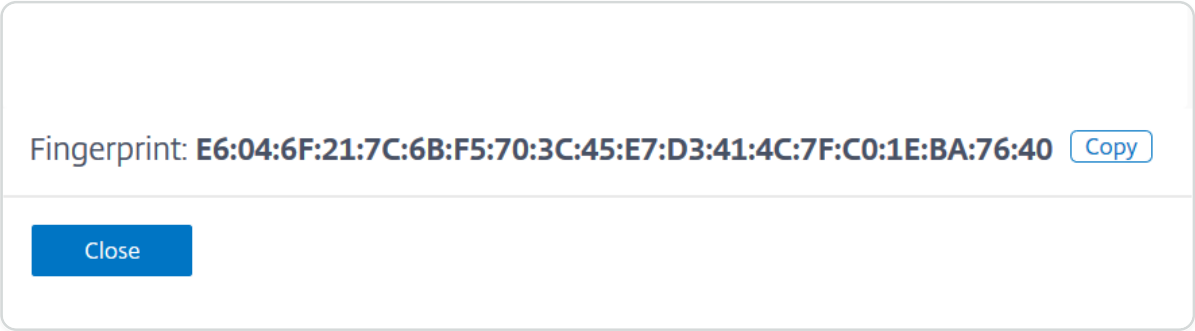
  注意

  如果使用了代理，则这表示代理的 IP 地址。

- **NS_MGMT_FINGER_PRINT** – 指示 NetScaler Console 中 CPX 的身份验证。要获取指纹：

  a. 在 NetScaler Console 中，导航到 **设置 > 管理**

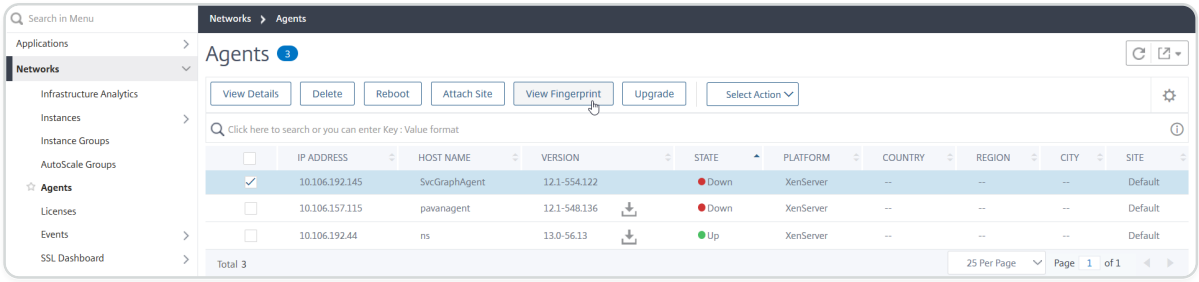
  b. 在 **系统配置** 下，单击 **查看 ADM 指纹**



© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

> 如果您已配置本地代理，请导航到 **Infrastructure > Instances > Agents**，选择代理，然后单击 **View Fingerprint**。



- **NS_HTTP_PORT** – 指示用于通信的 HTTP 端口
- **NS_HTTPS_PORT** – 表示用于通信的 HTTPS 端口
- **NS_MGMT_USER** - 表示用户名
- **NS_MGMT_PASS** - 表示密码。指定您选择的密码
- **LOGSTREAM_COLLECTOR_IP** – 表示 NetScaler 代理 IP 地址，其中必须启用 **Logstream** 协议才能将日志数据从 CPX 传输到 NetScaler Console

在 NetScaler Console 中添加 VPX、SDX、MPX 或 BLX 实例

要在服务图中获取第 1 层 NetScaler 实例分析，您必须在 NetScaler Console 中添加 VPX/SDX/MPX/BLX 实例并启用 **Web Insight**。

1. 导航到 **基础架构 > 实例 > NetScaler**
2. 单击“**添加**”选项以添加实例。有关详细信息，请参阅在 NetScaler Console 中添加实例
3. 添加实例后，选择虚拟服务器并启用 **Web Insight**。有关详细信息，请参阅管理许可并在虚拟服务器上启用分析

在 NetScaler Console 中添加 Kubernetes 集群

要添加 Kubernetes 集群：

1. 使用管理员凭据登录到 NetScaler Console。
2. 导航到 **Orchestration** > **Kubernetes** > **Cluster**。 此时将显示“集群”页面。
3. 单击“**添加**”。
4. 在“**添加集群**”页面中，指定以下参数：
   a. **名称** - 指定一个您选择的名称。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **API 服务器 URL** - 您可以从 Kubernetes 主节点获取 API 服务器 URL 详细信息。

   i. 在 Kubernetes 主节点上，运行命令 `kubectl cluster-info`。

   ```
   root@kmaster:[redacted]# kubectl cluster-info
   Kubernetes master is running at https://10.[redacted]:6443
   KubeDNS is running at https://10.[redacted]:6443/api/v1/namespaces/kube-system/
   services/kube-dns:dns/proxy

   To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
   ```

   ii. 输入显示为 **“Kubernetes 主节点正在运行于。”** 的 URL。

c. **身份验证令牌** - 指定身份验证令牌。身份验证令牌用于验证 Kubernetes 集群与 NetScaler Console 之间通信的访问权限。要生成身份验证令牌：

   在 Kubernetes 主节点上：

   i. 使用以下 YAML 创建服务帐户：

   ```
   apiVersion: v1

   kind: ServiceAccount

   metadata:

     name: <name>

     namespace: <namespace>
   ```

   ii. 运行 `kubectl create -f <yaml file>`。

   服务帐户已创建。

   iii. 运行 `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` 以将集群角色绑定到服务帐户。

   服务帐户现在具有集群范围的访问权限。

   在创建服务帐户时会自动生成一个令牌。

   iv. 运行 `kubectl describe sa <name>` 以查看令牌。

   v. 要获取密钥字符串，请运行 `kubectl describe secret <token-name>`。

   生成令牌(/en-us/netscaler-application-delivery-management-software/media/sg-generate-token.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. 从列表中选择代理。

注意

> 如果您使用的是本地代理，请确保选择您在 CPX YAML 中添加的同一代理。

e. 单击 **创建**。

添加集群(/en-us/netscaler-application-delivery-management-software/media/add-cluster.png)

部署示例微服务应用程序

在主节点上：

1. 运行 `kubectl create -f namespace.yaml` 以创建命名空间。
2. 使用以下命令部署 `hotdrink` 微服务、入口和密钥：

   `kubectl create -f team_hotdrink.yaml -n sg-demo`

   `kubectl create -f hotdrink-secret.yaml -n sg-demo`

部署 CPX 并在 NetScaler Console 中注册 CPX

1. 运行 `kubectl create -f rbac.yaml` 以部署集群角色和集群绑定。
2. 运行 `kubectl create -f cpx.yaml -n sg-demo` 以部署 CPX。

部署后，CPX 注册会自动完成。

启用许可证的虚拟服务器自动选择

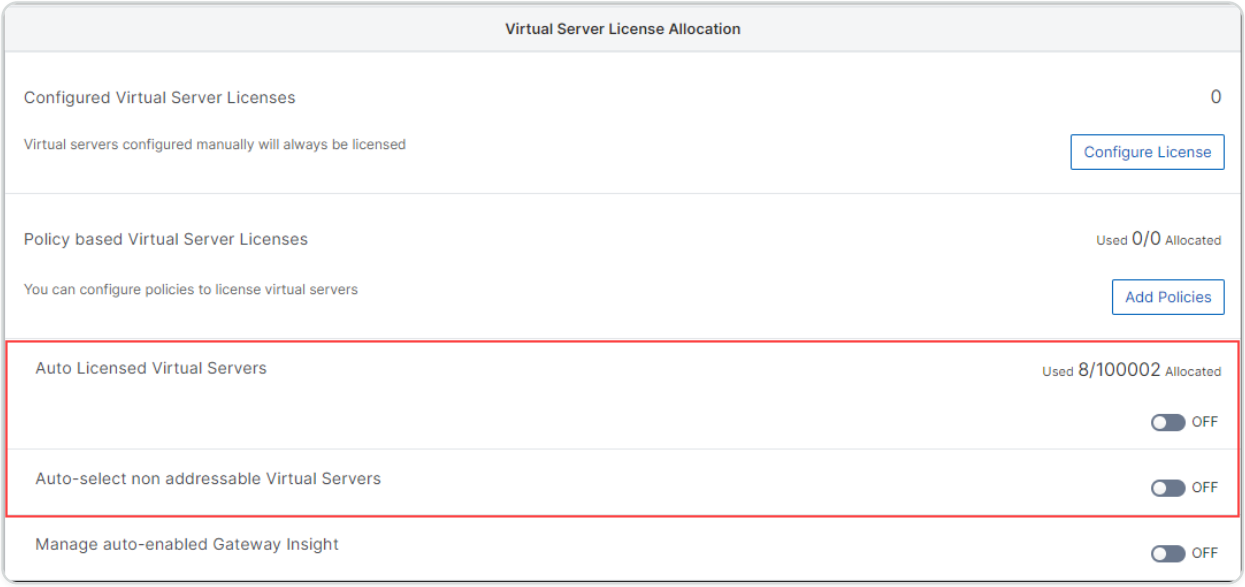
注意

> 确保您有足够的虚拟服务器许可证。有关更多信息，请参阅许可

在 NetScaler Console 中添加 Kubernetes 集群后，您必须确保自动选择虚拟服务器以进行许可。虚拟服务器必须获得许可才能在服务图表中显示数据。要自动选择虚拟服务器：

1. 导航到 **设置 > 许可和分析配置**。
2. 在 **虚拟服务器许可证摘要** 下，启用 **自动选择虚拟服务器** 和 **自动选择不可寻址虚拟服务器**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



启用 Web 事务和 TCP 事务设置

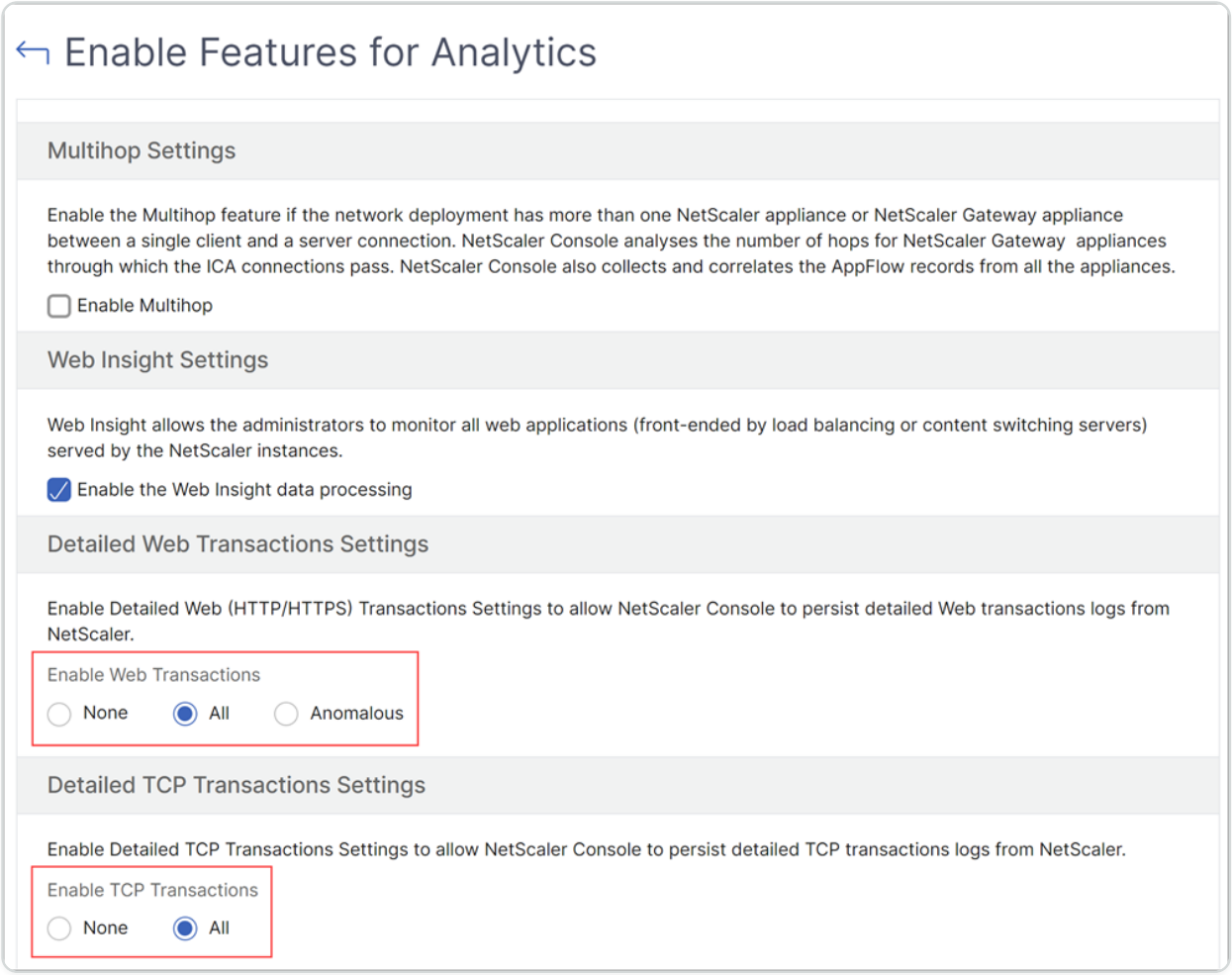
添加 Kubernetes 集群并启用自动选择虚拟服务器后，将 **Web 事务设置** 和 **TCP 事务设置** 更改为 **所有**。

1. 导航到 **设置 > 分析设置**。

   将显示 **分析设置** 页面。

2. 单击 **为分析启用功能**。
3. 在 **Web 事务设置** 下，选择 **所有**。
4. 在 **TCP 事务设置** 下，选择 **所有**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 单击 **确定**。

向微服务发送流量

接下来，您必须向微服务发送流量，以便在 NetScaler Console 中填充服务图。

1. 运行 `kubectl get svc -n sg-demo` 以通过 NodePort 暴露 CPX。

```
root@adm-cic-master:~/adm# kubectl get svc -n sg-demo
NAME                    TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)
 AGE
coffee                  ClusterIP   10.102.13.37    <none>        80/TCP,443/TCP
 83s
coffee-beverage         ClusterIP   None            <none>        80/TCP,443/TCP
 83s
cpx-service             NodePort    10.98.190.208   <none>        80:30402/TCP,443:32042/TCP
 34s
frontend-hotdrinks      ClusterIP   None            <none>        80/TCP,443/TCP
 83s
lb-service-hotdrinks    ClusterIP   None            <none>        80/TCP,443/TCP
 33s
tea                     ClusterIP   10.103.233.53   <none>        80/TCP,443/TCP
 83s
tea-beverage            ClusterIP   None            <none>        80/TCP,443/TCP
 83s
```

2. 编辑 **etc/host** 文件，并为 `hotdrink.beverages.com` 创建一个域 IP 条目

   您现在可以使用 `https://hotdrink.beverages.com` 访问微服务

© 1997–2026 Citrix Systems, Inc. All rights reserved.

设置服务网格拓扑的详细步骤

部署服务网格拓扑的先决条件可在 设置服务图 中找到。

在 NetScaler Console 中配置静态路由

在 Kubernetes 集群中，所有容器化 Pod 都使用覆盖网络。无法直接使用这些私有 IP 地址建立通信。要启用从 NetScaler Console 到 Kubernetes 集群的通信，您必须在 NetScaler Console 中配置静态路由。

注意

> 如果您使用的是本地代理，请确保在代理上配置静态路由。使用 SSH 客户端登录到 NetScaler 代理并配置静态路由。

假设您的 Kubernetes 集群具有以下 IP 地址：

- Kubernetes 主节点 – 101.xx.xx.112
- Kubernetes 工作节点 1 – 101.xx.xx.111
- Kubernetes 工作节点 2 – 101.xx.xx.110

在 Kubernetes 主节点上，运行以下命令以识别 Pod 网络以进行静态路由：

```
kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}{.status.addresses[0].address}{'\n'}{end}"
```

以下是运行命令后的示例输出：

```
root@master:~# kubectl get nodes -o jsonpath="{range .items[*]}{'podNetwork: '}{.spec.podCIDR}{'\t'}{'gateway: '}
{.status.addresses[0].address}{'\n'}{end}"
podNetwork: 1[illegible]  gateway: 1[illegible]0
podNetwork: 1[illegible]  gateway: 1[illegible]1
podNetwork: 1[illegible]  gateway: 1[illegible]2
```

1. 使用 SSH 客户端登录到 NetScaler Console
2. 使用命令 `route add -net <public IP address range> <Kubernetes IP address>` 配置静态路由

   例如：

   `route add -net 192.168.0.0/24 101.xx.xx.112`

   `route add -net 192.168.1.0/24 101.xx.xx.111`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
route add -net 192.168.2.0/24 101.xx.xx.110
```

3. 使用 `netstat -rn` 验证配置

```
bash-3.2# netstat -rn
Routing tables

Internet:
Destination        Gateway            Flags    Refs      Use  Netif Expire
default            10.[redacted].1    UGS         0 20224745    1/1
10.[redacted].0/24 link#3             U           0  7002455    1/1
10.[redacted].115  link#3             UHS         0        0    lo0
127.0.0.1          link#1             UH          0  7421390    lo0
192.168.0.0/24     10.[redacted]12    UGS         0        0    1/1
192.168.1.0/24     10.[redacted]11    UGS         0   319315    1/1
192.168.2.0/24     10.[redacted]0     UGS         0    41712    1/1
```

4. 将这些路由命令附加到 `/mpsconfig/svm.conf` 文件中。

   a. 在 NetScaler Console 中，使用以下命令访问 **svm.conf** 文件：

   ```
   vim /mpsconfig/svm.conf
   ```

   b. 在 **svm.conf** 文件中添加静态路由。

   例如，`route add -net 192.168.0.0/24 101.xx.xx.112`。

配置所需参数

在 Kubernetes 主节点中：

1. 在部署了 CPX 作为入口网关/Sidecar 的每个命名空间中，使用代理凭据创建 Secret。

   ```
   kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n <namespace>
   ```

2. `helm repo add citrix https://citrix.github.io/citrix-helm-charts/`

3. 部署 NetScaler CPX 作为入口网关

   ```
   helm install citrix-adc-istio-ingress-gateway citrix/citrix-adc-istio-ingress-gateway --version 1.2.1 --namespace <namespace> --set ingressGateway.EULA=YES,citrixCPX=true,ADMSettings.ADMFingerPrint=XX:00:X1:00:XX:0X:X0,A
   ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30
   ```

   下表列出了 Helm 图表中的可配置参数及其默认值：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述	默认值	可选/必选（HELM）
citrixCPX	NetScaler CPX	FALSE	NetScaler CPX 必需
xDSAdaptor.image	Citrix xDS 适配器容器的映像	quay.io/citrix/citrix-istio-adaptor:1.2.1	必填
ADMSettings.ADMIP	NetScaler Console IP 地址	空	NetScaler CPX 必填
ADMSettings.ADMFingerPrint	NetScaler Console 指纹。导航到 **设置 > 管理**，并在 **系统配置** 下单击 **查看指纹**	空	可选
ingressGateway.EULA	最终用户许可协议 (EULA) 条款和条件。如果为是，则表示用户同意 EULA 条款和条件。	否	NetScaler CPX 必填
ingressGateway.image	指定为入口网关运行的 NetScaler CPX 镜像	quay.io/citrix/citrix-k8s-cpx-ingress:13.0–58.30	NetScaler CPX 必需

4. 部署 Citrix SideCar 注入器。

```
helm install cpx-sidecar-injector citrix/citrix-cpx-istio-sidecar-injector --version 1.2.1 --namespace <namespace> set cpxProxy.EULA=YES,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSettings.ADMIP=<xx.xx.xx.xx> citrix/citrix-k8s-cpx-ingress,cpxProxy.tag=13.0-58.30
```

下表列出了 Helm chart 中的可配置参数及其默认值：

参数	描述	默认值
ADMSettings.ADMIP	NetScaler Console IP 地址	无
cpxProxy.image	用作 Sidecar 代理的 NetScaler CPX 镜像	quay.io/citrix/citrix-k8s-cpx-ingress:13.0–58.30

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述	默认值
cpxProxy.imagePullPolicy	NetScaler 的镜像拉取策略	IfNotPresent
cpxProxy.EULA	最终用户许可协议 (EULA) 条款和条件。如果为“是”，则表示用户同意 EULA 条款和条件。	否
cpxProxy.cpxSidecarMode	NetScaler CPX 的环境变量。它指示 NetScaler CPX 是否以 Sidecar 模式运行。	是

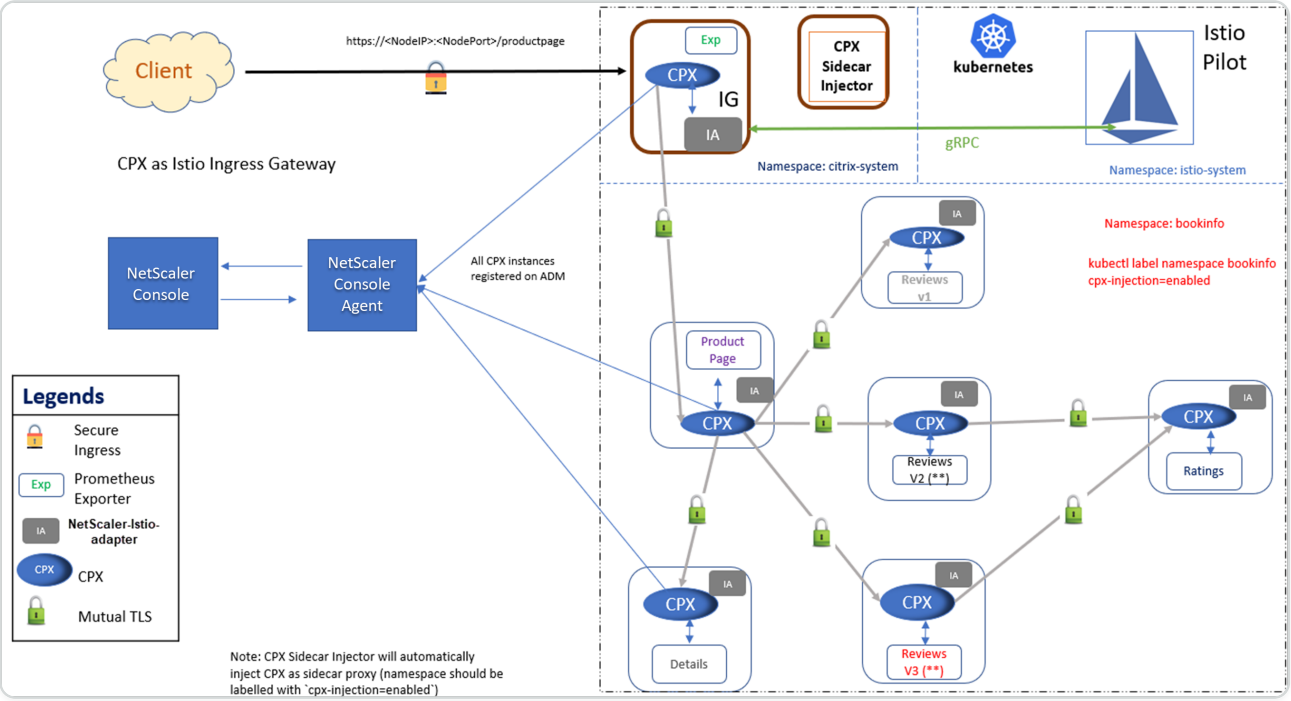
5. 在任何需要 CPX Sidecar 注入的命名空间上设置标签。

   `kubectl label namespace <app-namespace> cpx-injection=enabled`

   执行步骤 3 和 5 后，您可以看到 NetScaler CPX 已在 NetScaler Console 中注册。

部署示例应用程序

假设您要部署以下应用程序：



执行以下步骤以部署示例应用程序：

1. `kubectl create namespace citrix-system`
2. `kubectl create namespace bookinfo`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. `kubectl label namespace bookinfo cpx-injection=enabled`
4. `kubectl create secret generic admlogin --from-literal=username=<uername> --from-literal=password=<password> -n citrix-system`

   注意

   > 您可以选择自己的用户名和密码。

5. `kubectl create secret generic admlogin --from-literal=username=<username> --from-literal=password=<password> -n bookinfo`

   注意

   > 您可以选择自己的用户名和密码。

6. `helm install citrix-adc-istio-ingress-gateway citrix/citrix-adc-istio-ingress-gateway --version 1.2.1 --namespace citrix-system --set ingressGateway.EULA=YES,citrixCPX=true,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSetting IP address>,ingressGateway.image=quay.io/citrix/citrix-k8s-cpx-ingress,ingressGateway.tag=13.0-58.30`

   注意

   > 您必须提供控制台指纹以及代理或控制台 IP 地址

7. `helm install cpx-sidecar-injector citrix/citrix-cpx-istio-sidecar-injector --namespace citrix-system --set cpxProxy.EULA=YES,ADMSettings.ADMFingerPrint=xx:xx:xx:xx,ADMSettings.ADMIP=<ADM agent IP address>,cpxProxy.image=quay.io/citrix/citrix-k8s-cpx-ingress,cpxProxy.tag=13.0-58.30`

   注意

   > 您必须提供控制台指纹以及代理或控制台 IP 地址

8. `helm install bookinfo bookinfo/ --namespace bookinfo --set citrixIngressGateway.namespace=citrix-system`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在 NetScaler Console 中添加 Kubernetes 集群

要添加 Kubernetes 集群：

1. 使用管理员凭据登录到 NetScaler Console。
2. 导航到 **编排** > **Kubernetes** > **集群**。 将显示“集群”页面。
3. 单击 **添加**。
4. 在“**添加集群**”页面中，指定以下参数：

   a. **名称** - 指定一个您选择的名称。

   b. **API 服务器 URL** - 您可以从 Kubernetes 主节点获取 API 服务器 URL 详细信息。

      i. 在 Kubernetes 主节点上，运行命令 `kubectl cluster-info`。

      ```
      root@kmaster:[redacted]# kubectl cluster-info
      Kubernetes master is running at https://10.[redacted]:6443
      KubeDNS is running at https://10.[redacted]:6443/api/v1/namespaces/kube-system/
      services/kube-dns:dns/proxy

      To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
      ```

      ii. 输入为“**Kubernetes master is running at.**”显示的 URL。

   c. **身份验证令牌** - 指定身份验证令牌。身份验证令牌用于验证 Kubernetes 集群与 NetScaler Console 之间通信的访问权限。要生成身份验证令牌：

      在 Kubernetes 主节点上：

      i. 使用以下 YAML 创建服务帐户：

      ```
      apiVersion: v1

      kind: ServiceAccount

      metadata:

        name: <name>

        namespace: <namespace>
      ```

      ii. 运行 `kubectl create -f <yaml file>`。

      服务帐户已创建。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

iii. 运行 `kubectl create clusterrolebinding <name> --clusterrole=cluster-admin --serviceaccount=<namespace>:<name>` 将集群角色绑定到服务帐户。

服务帐户现在具有集群范围的访问权限。

创建服务帐户时会自动生成一个令牌。

iv. 运行 `kubectl describe sa <name>` 查看令牌。

v. 要获取密钥字符串，请运行 `kubectl describe secret <token-name>`。

```
root@kmaster:~# kubectl describe secret citrixadm-sa-token-79knw
Name:         citrixadm-sa-token-79knw
Namespace:    default
Labels:       <none>
Annotations:  kubernetes.io/service-account.name: citrixadm-sa
              kubernetes.io/service-account.uid: 136270eb-1fe1-11ea-b603-72328a2
af136

Type:  kubernetes.io/service-account-token

Data
====
ca.crt:     1025 bytes
namespace:  7 bytes
token:      eyJhbGciOiJSUzI1NiIsImtpZCI6IiJ9.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2V
hY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJkZWZhdWx0Iiw
ia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6ImNpdHJpeGFkbS1zYS10b2t
lbi03OWtudyIsImt1YmVybmV0ZXMuaW8vc2VydmljZWFjY291bnQvc2VydmljZS1hY2NvdW50Lm5hbWU
iOiJjaXRyaXhhZG0tc2EiLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3V
udC51aWQiOiIxMzYyNzBlYi0xZmUxLTExZWEtYjYwMy03MjMyOGEyYWYxMzYiLCJzdWIiOiJzeXN0ZW0
6c2VydmljZWFjY291bnQ6ZGVmYXVsdDpjaXRyaXhhZG0tc2EifQ.JsU4JPcyFoXA6Vn5Dxa137ca_hI0
wzY1Ajv0ctHN7NeU4YC_I6H5xgNAKnqj2rJPlQEmSZQygPOrxduLDYsNBCT9fH4sv1aBdOzzpkCIDW6y
6BmX4IaC6HTFPGO54zSDzjPmuKkPzyIRa4twUSvxfhwXE6JRy99iJjgPBraL65ct99bcVXF5nMDdexro
Iw23M8lcknV5fPuD33WhieS17WbXlq_ZYEA4WaulGXi9veHczN1S9oFPUlnM3d13R7A63bZjCKvWYlnN
7W5etxd2dfLgEJysixj8lKRxUifL2f04lfWM8ucwKVb8TumsMqG7eturRF5SxSYNodmBKNNkIA
```

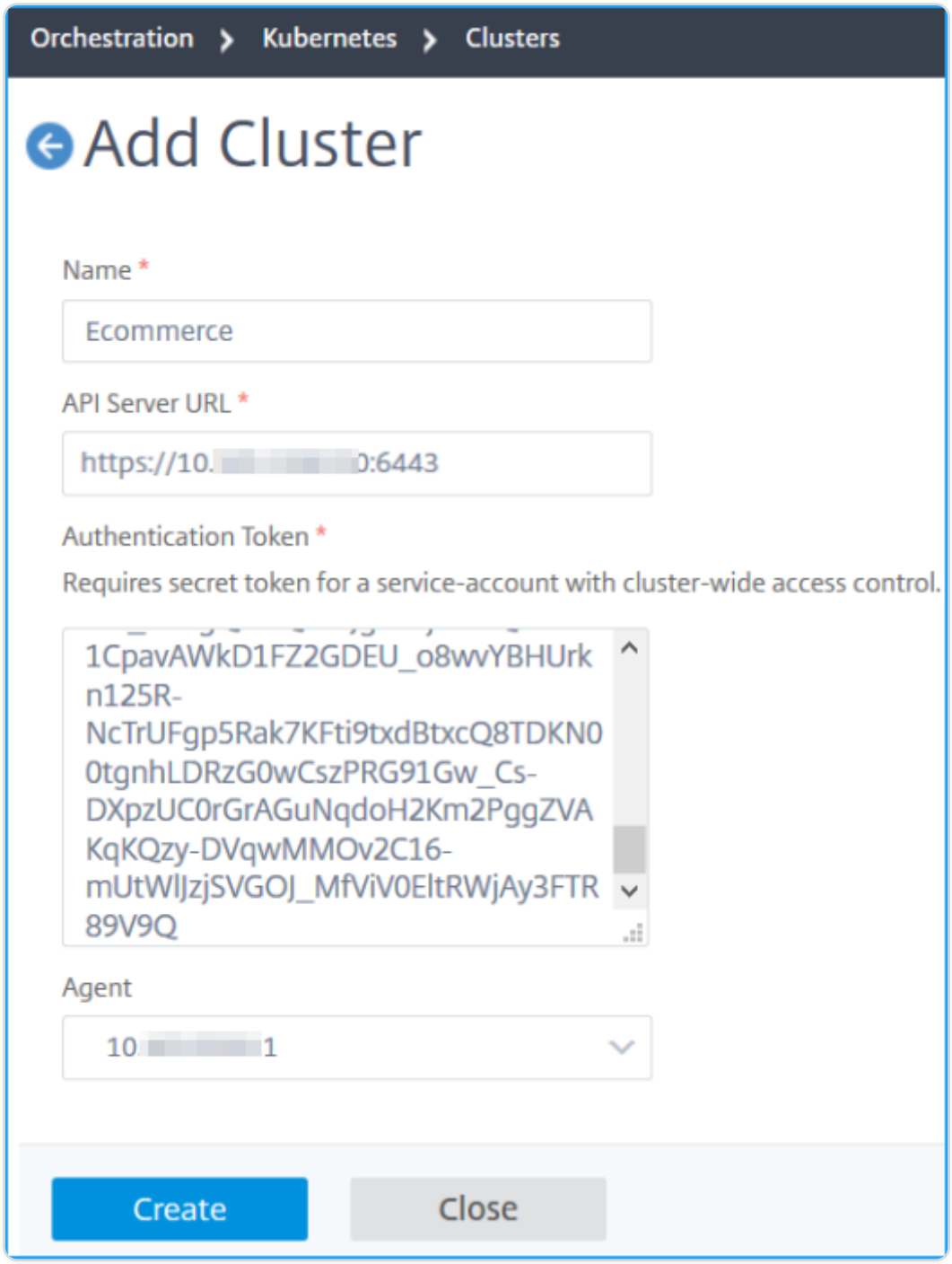
d. 从列表中选择代理。

注意

> 如果您正在使用代理，请确保选择您在 CPX YAML 中添加的同一代理。

e. 单击 **创建**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



启用自动选择虚拟服务器进行许可

注意

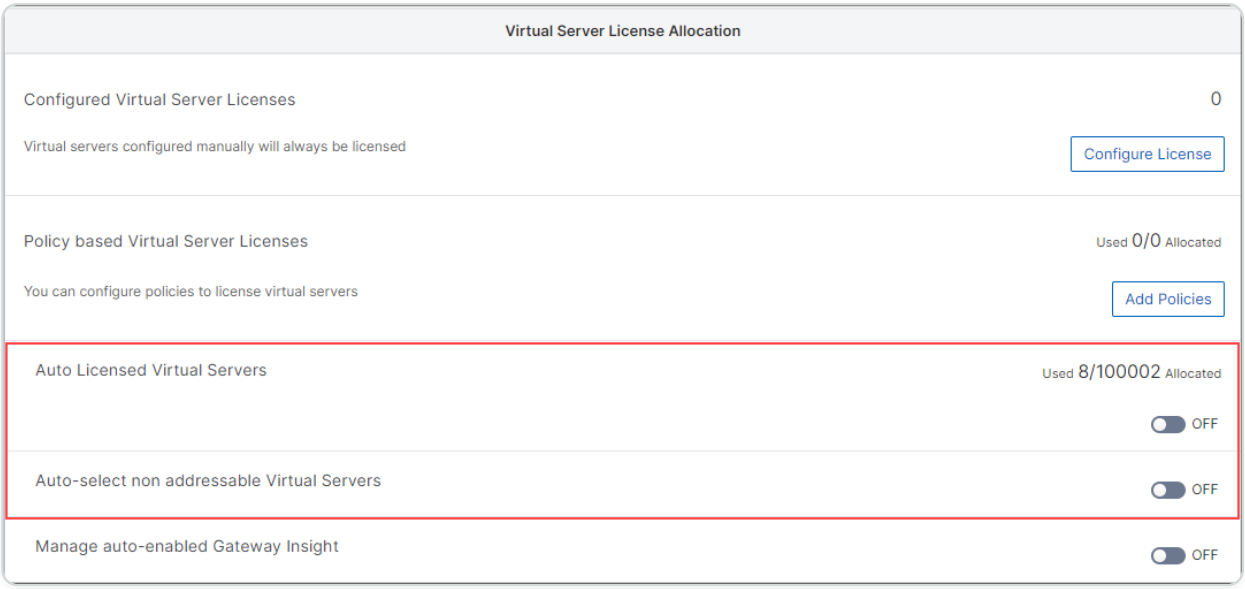
> 确保您有足够的虚拟服务器许可证。有关更多信息，请参阅许可

在NetScaler Console中添加Kubernetes集群后，您必须确保自动选择虚拟服务器进行许可。虚拟服务器必须获得许可才能在服务图表中显示数据。要自动选择虚拟服务器：

1. 导航到 **设置 > 许可与分析配置**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 在 **虚拟服务器许可证摘要** 下，启用 **自动选择虚拟服务器** 和 **自动选择不可寻址虚拟服务器**。



启用Web事务和TCP事务设置

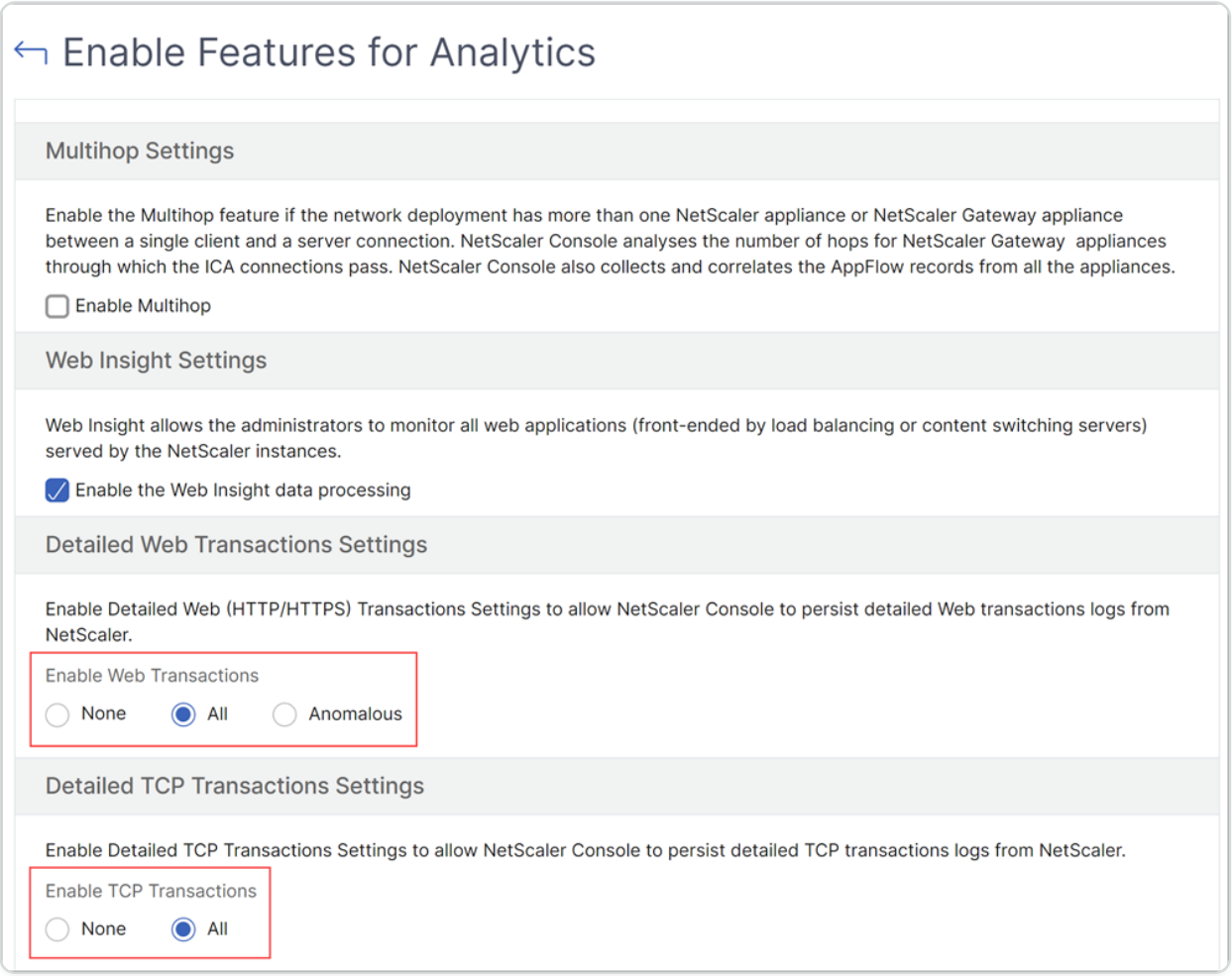
添加Kubernetes集群并启用自动选择虚拟服务器后，将 **Web事务设置** 和 **TCP事务设置** 更改为 **所有**。

1. 导航到 **设置 > 分析设置**。

   显示 **分析设置** 页面。

2. 单击 **启用分析功能**。
3. 在 **Web事务设置** 下，选择 **所有**。
4. 在 **TCP事务设置** 下，选择 **所有**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 单击 **确定**。

将流量发送到微服务

接下来，您必须将流量发送到微服务，以便在 NetScaler Console 中填充服务图。

1. 确定入口 IP 和端口

   `export INGRESS_HOST=$(kubectl get pods -l app=citrix-ingressgateway -n citrix-system -o 'jsonpath={.items[0].status.hostIP}')`

   `export INGRESS_PORT=$(kubectl -n citrix-system get service citrix-ingressgateway -o jsonpath='{.spec.ports[?(@.name=="http2")].nodePort}')`

   `export SECURE_INGRESS_PORT=$(kubectl -n citrix-system get service citrix-ingressgateway -o jsonpath='{.spec.ports[?(@.name=="https")].nodePort}')`

2. 使用 cURL 访问 Bookinfo 前端应用程序。`productpage` 服务必须返回 200 OK 响应。

   `curl -kv https://$INGRESS_HOST:$SECURE_INGRESS_PORT/productpage`

   `curl -v http://$INGRESS_HOST:$INGRESS_PORT/productpage`

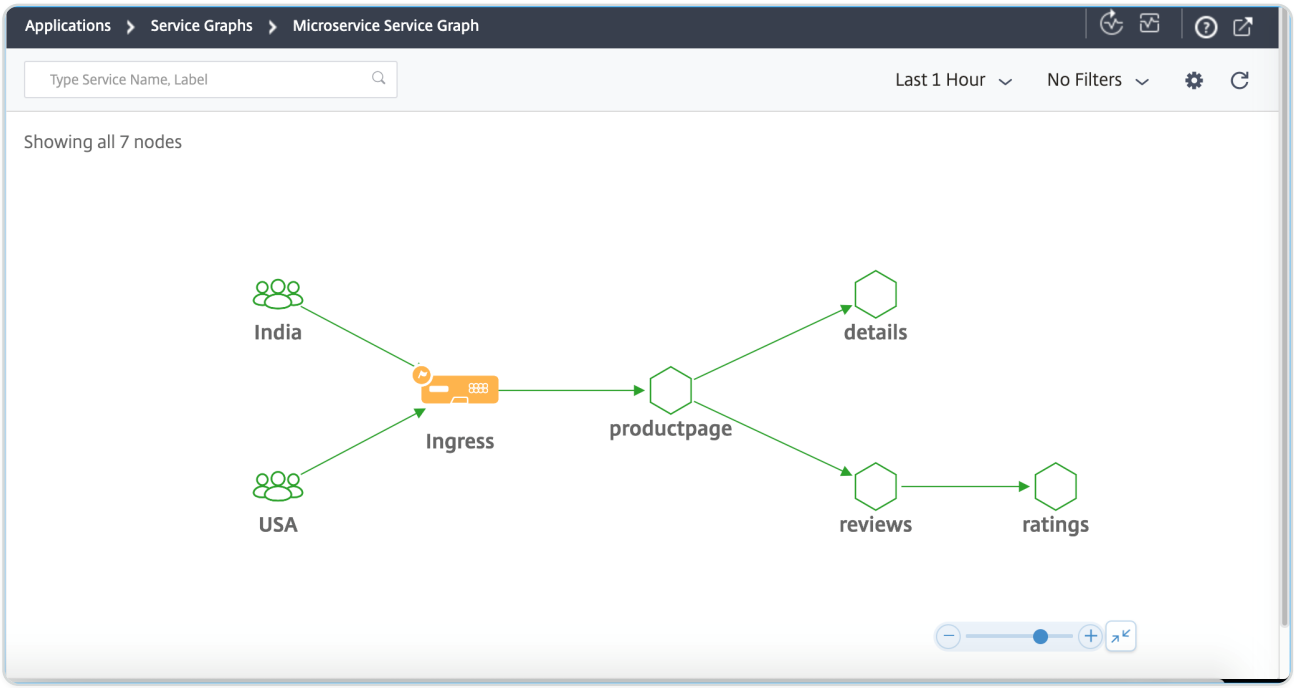
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 从浏览器访问 `https://$INGRESS_HOST:$SECURE_INGRESS_PORT/productpage`。

   显示 **Bookinfo** 页面。

4. 确保 $INGRESS_HOST 和 $SECURE_INGRESS_PORT 被 IP 地址和端口值替换。

将流量发送到微服务后，服务图将在大约 10 分钟内填充。



使用服务图，您可以分析各种服务详细信息，例如指标、错误等。有关更多信息，请参阅服务图。

数据治理（适用于 14.1-8.x 到 14.1-21.x 版本之间的 NetScaler Console）

Cloud Connect 使 Citrix Cloud 能够收集许可证、配置和使用数据，以实现许可证合规性，并管理、衡量和改进服务。从 14.1-8.x 或更高版本开始，您可以配置 Cloud Connect 以在 NetScaler Console 服务和本地 NetScaler Console 之间建立连接。通过启用 Cloud Connect，您可以：

- 将收集用于 弹性许可合规性 的强制性许可证和使用数据。
- 您可以在本地 NetScaler Console 中获取 **安全建议** 功能。有关更多信息，请参阅 Cloud Connect。

数据类别

下表提供了启用 Cloud Connect 后收集的参数详细信息：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

类别	描述	我们用它做什么？	必需/可选
许可证遥测数据	有关许可证权利、使用情况、高级 NetScaler 部署数据以及 NetScaler 功能使用数据的信息。	许可证合规性以及管理、衡量和改进服务。	必需
功能使用数据	有关 Console 部署和 Console 功能使用数据的信息。	用于管理、衡量和改进服务。	可选

数据治理（适用于 NetScaler ADM 14.1-4.42 或更早版本）

如果您的 NetScaler ADM 版本为 14.1-4.x 或更低，您可以在 Citrix Cloud 上创建客户身份，以将有关 ADM 运行状况、状态和其他指标的重要统计数据从本地部署发送到 Citrix Cloud 帐户。Citrix 收集统计数据以了解 NetScaler ADM 的使用情况。

- **在 Citrix Cloud™ 上创建客户身份** - 用于将有关 ADM 运行状况、状态和其他指标的重要统计数据从 ADM 本地部署发送到 Citrix Cloud 帐户。

  创建客户身份后，“Cloud Connect”通过创建 Citrix Cloud 帐户来建立 ADM 本地部署与 NetScaler® Console 服务之间的连接。请参阅，配置客户身份。
- **配置维护脚本** - 用于优化数据库。数据库优化可能会创建表、更改列等。相同的“Cloud Connect”功能用于配置维护脚本。请参阅使用维护脚本优化数据库。
- **客户用户体验改进计划 (CUXIP)** - 此程序默认启用。它从 NetScaler ADM 收集使用数据。此数据允许通过引导式工作流、搜索文章、产品通知、反馈、调查等方式优化 ADM 体验。请参阅，客户用户体验改进计划。

配置客户身份

NetScaler Console 要求您在开始访问信息之前在 ADM GUI 上进行身份验证。您必须先在 Citrix Cloud 服务上注册，然后才能在 ADM 上进行身份验证。在 ADM GUI 上提供 Citrix Cloud 用户凭据。有关详细信息，请参阅注册 Citrix Cloud。

在 NetScaler ADM 上进行身份验证有多种方式。以下部分描述了如果您是 ADM 的新用户或现有用户的工作流。

工作流 1 - 如果您是新用户

1. 在选定的虚拟机管理程序上完成 NetScaler ADM 的安装。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 配置各种所需的 IP 地址。
3. 在 Web 浏览器中，键入 NetScaler ADM 的 IP 地址。
4. 在“**用户名**”和“**密码**”字段中，输入管理员凭据。

   此时将打开“**配置客户身份**”页面，您必须使用 Citrix Cloud 凭据进行身份验证。

   如果您尚未在 Citrix Cloud 上创建帐户，请单击 Citrix Cloud 进行注册。
5. 单击 **Authenticate** 并提供您在 Citrix Cloud 上注册时使用的电子邮件地址。
6. 选中 **I agree to share data** 旁边的复选框以进行遥测，然后单击 **Submit**。

工作流 2 - 如果您是升级到最新 ADM 版本的现有用户

1. 将 NetScaler ADM 升级到最新版本后，在 Web 浏览器中键入 NetScaler ADM 的 IP 地址。
2. 在 **User Name** 和 **Password** 字段中，输入管理员凭据。
3. 将打开 **Configure Customer Identity** 页面，您必须使用您的 Citrix Cloud 凭据进行身份验证。

   如果您尚未在 Citrix Cloud 上创建帐户，请单击 Citrix Cloud 进行注册。
4. 单击 **Authenticate** 并提供您在 Citrix Cloud 上注册时使用的电子邮件地址。
5. 选中“I agree to share data for telemetry”旁边的复选框，然后单击 Submit。

作为现有用户，您还可以通过以下两种方式之一在 ADM 上配置您的身份：

- 导航到 **设置 > 系统管理**，然后单击 **身份验证**。
- 单击 ADM GUI 右上角的云符号。 成功身份验证后，`X` 将变为绿色复选标记。

注意

确保以下域已列入白名单：

- `*.citrixnetworkapi.net`
- `*.blob.core.windows.net`

通过将您的数据上传到 NetScaler ADM 并使用 NetScaler ADM 功能，您同意并允许 Citrix 收集、存储、传输、维护、处理和使用有关您的 NetScaler 产品和服务的技术、用户或相关信息。

Citrix 收到的信息始终根据 Citrix.com 隐私政策 进行处理。

诊断和数据收集

NetScaler ADM 使用客户身份收集以下遥测数据：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **在 ADM 中执行的操作：**
  - 使用 NetScaler ADM UI/API 界面执行的操作。
  - 使用 NetScaler ADM SDK 界面执行的操作。
  - 单日操作计数。此计数包括来自 API 或 UI 的任何非 GET 请求。
  - ADM 完成的 NetScaler 升级计数。
- **NetScaler ADM 许可证信息**：授权虚拟服务器计数。
- **关键统计数据：**
  - 事件规则总数。
  - 用户定义的 StyleBook 总数。
  - 托管和自定义应用程序的数量。
  - 注册代理的数量。
  - NetScaler 的总吞吐量 (Rx+Tx)。
  - 托管实例的数量。此数量还包括管理员分区。
  - 使用 NetScaler ADM SaaS 的管理员数量。
- **NetScaler ADM 的地理位置**
- **部署信息**：此信息包括部署类型，例如高可用性、灾难恢复和 ADM 代理。

为什么要收集数据?

收集到的遥测数据有助于：

- 推荐正确的 NetScaler ADM 大小调整和部署。
- 主动排查 ADM 本地部署中的问题。

谁可以使用这些数据?

Citrix 是所收集信息的唯一所有者。Citrix 有权访问/收集您自愿提供给我们的信息。我们不会将此信息出售或出租给任何人。除了为满足您的请求所必需的情况外，我们不会与组织外部的任何第三方共享您的信息。示例：发货或主动解决问题。

我们会保留您的数据多长时间?

通常，我们会存储个人/使用数据，直到用户正在使用我们的服务。或者，我们有其他目的这样做。此后，数据存储时间不会超过法律要求或允许的时间，也不会超过内部报告和对账所需的时间。

所有遥测数据存储期限不超过 13 个月或 396 天。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

使用维护脚本进行数据库优化

维护脚本用于解决 ADM 本地部署中的数据库相关问题。ADM 软件会自动从 ADM 服务下载数据库维护脚本，从而更快地解决数据库相关问题。以前，这些问题是通过手动运行脚本来解决的。

借助此功能，ADM 本地部署会定期从 ADM 服务下载数据库维护脚本。为此，请务必配置客户身份。

维护脚本每天和每周运行。此外，这些脚本可能会创建表或添加/删除列以提高数据库性能。

客户用户体验改进计划

在 Citrix Systems，我们的目标是为用户提供引人入胜的产品体验。**客户用户体验改进计划 (CUXIP)** 使用 Pendo 通过提供搜索文章、应用内指南等方式，引导用户完成一些常见但详细的任务。我们还帮助用户及时了解所有最新公告。

CUXIP 收集哪些使用数据?

使用数据全部与用户行为有关。使用数据也称为事件级数据，它包括从用户在网站上访问的页面到某个功能的点击次数的所有内容。使用数据是关于用户如何在我们的应用程序中移动的宝贵信息。此数据有助于优化用户的体验。

以下是我们收集的一些使用数据：

- 页面浏览量、在每个页面上花费的时间的详细信息。
- 访客 ID 是一个唯一的匿名标识符，用于帮助识别页面上的唯一访客数量。
- 调查统计数据 – 分数、视图、提交数量等。

CUXIP 如何帮助您?

我们使用使用数据来改善您使用 ADM 的体验。以下是我们旨在增强客户用户体验的一些方式：

- 应用内引导式工作流程和搜索相关文章的功能。
- 在应用内参与调查，以帮助改进产品。
- 及时了解最新公告和其他通知。
- 向产品团队发布问题或反馈。

CUXIP 如何工作?

NetScaler ADM 设备可以位于内部网络中。浏览器必须具有互联网连接才能获得 CUXIP 上的引导式协助的优势。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

如何在我的 ADM 上禁用 CUXIP?

要禁用 CUXIP，请在 ADM GUI 中执行以下操作：

1. 导航到 **设置 > 系统管理**。
2. 在 **CUXIP 设置**中，禁用 CUXIP。

我们的隐私政策变更

我们可能会不时更新我们的隐私政策。我们将通过在此页面上发布新的隐私政策来通知您这些更改。在更改生效之前，我们将通过电子邮件和/或在我们的服务上发布醒目通知告知您，并更新本隐私政策顶部的“生效日期”。

建议您定期查看本隐私政策以了解任何更改。本隐私政策的更改在发布到 Citrix 隐私政策 页面时生效。

参考

Citrix 隐私政策：`<https://www.citrix.com/about/legal/privacy/>`

用于 Cloud Connect 的可选遥测数据

下表显示了在您启用 Cloud Connect 后收集的可选数据列表：

参数	描述
t_ten	已连接到 NetScaler Console 的租户总数
部署	检查 NetScaler Console 部署类型是独立部署还是高可用性对
is_dr	检查灾难恢复节点是否已配置
is_agt	检查代理是否已配置
is_cloud	检查 NetScaler Console 部署是 NetScaler Console 服务还是本地 NetScaler Console
is_cntr	检查 NetScaler Console 部署是否在 Kubernetes 集群中
平台	托管 NetScaler Console 的平台。例如，Citrix Hypervisor

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
security_advisory_enabled	检查 NetScaler Console 本地部署中是否启用了安全建议
total_users	NetScaler Console 本地用户的总数
total_gui_requests	过去 24 小时内登录到 NetScaler Console GUI 的用户总数
total_api_requests	过去 24 小时内通过 API 发送到 NetScaler Console 的请求总数。这还包括远程代理用户（来自代理的请求）。
total_api_external_requests	通过 API 发送到 NetScaler Console 的请求总数，不包括来自代理的请求
total_success_preauth_requests	生成预授权令牌的成功请求总数
total_custom_apps	NetScaler Console 中的自定义应用程序总数
total_managed_apps	NetScaler Console 中的托管应用程序总数
total_apps	NetScaler Console 中的应用程序总数
total_custom_sites	NetScaler Console 中配置的自定义站点总数
total_agents	已配置的代理总数
total_active_agents	处于 UP 状态的代理总数
total_custom_event_rules	NetScaler Console 中创建的自定义事件规则总数
total_event_rules	在 NetScaler Console 中创建的事件规则总数
total_stylebook_config_store_count	在 NetScaler Console 中创建的配置包总数
total_user_sb_stylebook_count	在 NetScaler Console 中创建的自定义配置包总数
total_config_audit	在 NetScaler Console 中配置的配置审计模板总数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
total_config_job	在 NetScaler Console 中创建的配置作业总数
total_ssl_certs	从 NetScaler Console 创建/修改/删除的 SSL 证书总数
total_network_report	在 NetScaler Console 中创建的网络报告总数
total_k8s	托管在 Kubernetes 集群上的 NetScaler Console。Kubernetes 集群总数。
total_ipam	NetScaler Console 中添加的 IPAM 提供商总数
total_rbac_groups	NetScaler Console 中配置的 RBAC 组总数
total_ingress_deployed	Kubernetes 中的入口控制器总数。
total_ipam_configured	NetScaler Console 中添加的 IPAM 网络总数
total_web_transaction_analytics	启用 Web 事务分析的 NetScaler 实例总数
total_pager_duty_profile	NetScaler Console 中添加的 PagerDuty 配置文件总数
total_slack_profile	NetScaler Console 中添加的 Slack 配置文件总数
total_api_discovery	接收 API 请求的 NetScaler 实例总数
t_radius_svr	在 NetScaler Console 中配置的 RADIUS 身份验证服务器总数
t_ldap_svr	在 NetScaler Console 中配置的 LDAP 身份验证服务器总数
t_tacacs_svr	在 NetScaler Console 中配置的 TACACS 身份验证服务器总数
t_att	已启用 Security Insight 的设备发出的请求总数
计数	已启用 HDX Insight 的设备发出的请求总数
计数	通过 VPN 连接的用户总数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
计数	通过虚拟桌面连接的用户总数
agent_id	部署的代理的唯一ID
平台	代理所在的平台。例如，Citrix Hypervisor
版本	代理版本
城市	代理部署所在的城市
国家	代理部署所在的国家
区域	代理部署所在的区域
根	NetScaler Console 在 /var、/root、/flash、/var/mps 目录中的磁盘利用率详细信息
总计	NetScaler Console 的总磁盘空间（单位：字节）
已用	NetScaler Console 的总已用磁盘空间
可用	NetScaler Console 的总可用磁盘空间
Adm_analt_dx - 功能	识别出问题的分析类型（Bot、WAF、Web Insight、Service Graph 等）
Adm_analt_dx - 问题类型	已识别问题所属的问题类别。例如，许可、配置
Adm_analt_dx - 子问题类型	已识别问题的子问题类别。子问题可以是 NO_VIPS_LICENSED、BOT_INSIGHT_IN_ACTION_DISABLED、NS_FEATURE_DISABLED、VSERVER_WITHOUT_BOT_POLICY_BINDING、NO_COLLECTORS_PRESENT、APPFLOWPARAM_DISABLED、ICA_APPFLOW_POLICY_BINDING、VSERVER_WITHOUT_APPFIREWALL_POLICY_BINDING、SECURITY_INSIGHT_IN_ACTION_DISABLED、NO_CPX_VIPS_PRESENT、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
	COLLECTOR_UNBOUND_IN_VSERVER、VSERVER_WITHOUT_APPFLOW_POLICY_BINDING
产品	产品名称
isCloud	是本地部署还是云部署
isContainer	是否为容器部署
mas_platform	NetScaler Console 平台
功能	在负载均衡/内容切换虚拟服务器上启用的分析功能
total_lbvserver_ft_enabled	至少启用一个分析功能的负载均衡虚拟服务器总数
total_csvserver_ft_enabled	至少启用一个分析功能的内容切换虚拟服务器总数
feature_enabled_on_vpn	在 VPN 虚拟服务器上启用的分析功能
total_vpnvserver_ft_enabled	至少启用一个分析功能的 VPN 虚拟服务器总数

NetScaler® 遥测程序的可选遥测数据

NetScaler Console 功能使用情况

下表显示了作为 NetScaler 遥测程序一部分收集的可选数据列表：

参数	描述
平台	托管 NetScaler Console 的平台。例如，Citrix Hypervisor
部署	检查 NetScaler Console 部署类型是独立部署还是 HA 对
is_agt	检查代理是否已配置

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
is_cloud	检查 NetScaler Console 部署是 NetScaler Console 服务还是本地 NetScaler Console
is_cntr	检查 NetScaler Console 部署是否在 Kubernetes 集群中
is_dr	检查是否配置了灾难恢复节点
t_ten	连接到 NetScaler Console 的租户总数
num_of_ns_upgrade_jobs	已使用的升级作业总数
security_advisory_enabled	NetScaler Console 本地部署中是否启用了安全建议
网络洞察	lb 或 cs 虚拟服务器中是否启用了 Web Insight
webinisight_usage	是否有任何活动的 HDX 会话（是或否）
adm_analyt_hdx_apps	已启用 HDX Insight 的设备发出的请求总数
adm_analyt_hdx_users	通过虚拟桌面连接的用户数量
adm_analyt_sec_insight	已启用安全洞察的设备发出的请求总数
adm_analyt_vpn_users	通过 VPN 连接的用户总数
adm_analyt_webinsight	已启用 Web 洞察的设备发出的请求总数
异常洞察	指示请求功能是否在 lb 或 cs 虚拟服务器中启用
计数	与分析相关的总问题计数
功能	已识别问题的功能类别。功能可以是 BOT_INSIGHT、DEVICE、GATEWAY_INSIGHT、HDX_INSIGHT、SECURITY_INSIGHT、SERVICE_GRAPH、SWG_INSIGHT、WEB_INSIGHT、WEB_SECURITY_BOT_INSIGHT
功能	在负载平衡虚拟服务器上启用的分析功能

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
功能	在内容切换虚拟服务器上启用的分析功能
功能	在 VPN 虚拟服务器上启用的分析功能
网关洞察	指示 VPN 虚拟服务器上是否启用了 ICA_REQUEST 功能
gwinsight_usage	指示过去一天是否有任何 HDX 用户（是或否）
gw_hdx_insights	HDX Insight 和 Gateway Insight 导出已启用
HDX洞察	指示 VPN 服务器中是否启用了 ICA_Request 功能
hdxinsight_usage	指示过去一天是否有任何 HDX 用户
issue_type	已识别问题所属的问题类别。例如，许可、配置
安全洞察	指示安全洞察是否在 lb 或 cs 虚拟服务器中启用
secinsight_usage	过去一天是否发现任何安全攻击（是或否）
sub_issue_type	已识别问题的子问题类别。子问题可以是 NO_VIPS_LICENSED, BOT_INSIGHT_IN_ACTION_DISABLED, NS_FEATURE_DISABLED, VSERVER_WITHOUT_BOT_POLICY_BINDING, NO_COLLECTORS_PRESENT, APPFLOWPARAM_DISABLED, ICA_APPFLOW_POLICY_BINDING, VSERVER_WITHOUT_APPFIREWALL_POLICY_BINDING, SECURITY_INSIGHT_IN_ACTION_DISABLED, NO_CPX_VIPS_PRESENT, COLLECTOR_UNBOUND_IN_VSERVER, VSERVER_WITHOUT_APPFLOW_POLICY_BINDING
total_api_discovery	接收 API 请求的 NetScaler 实例总数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
total_csvserver_ft_enabled	至少启用一个分析功能的总内容交换虚拟服务器数量
total_lbvserver_ft_enabled	至少启用一个分析功能的总负载平衡虚拟服务器数量
total_vpnserver_ft_enabled	至少启用一个分析服务器的总 VPN 虚拟服务器数量
total_web_transaction_analytics	启用 Web 事务分析的 NetScaler 实例总数
t_radius_svr	在 NetScaler Console 中配置的 RADIUS 身份验证服务器总数
t_ldap_svr	在 NetScaler Console 中配置的 LDAP 身份验证服务器总数
t_tacacs_svr	在 NetScaler Console 中配置的 TACACS 身份验证服务器总数
agt_pl_azure	代理平台类型
agt_pl_citrix_hypervisor	代理平台类型
agt_pl_docker	代理平台类型
agt_pl_esx	代理平台类型
agt_pl_hyper_v	代理平台类型
agt_pl_gcp	代理平台类型
agt_pl_kvm	代理平台类型
agt_pl_kubernetes	代理平台类型
agt_pl_unknown	代理平台类型
agt_pl_aws	代理平台类型
agent_id	已部署代理的唯一 ID

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
城市	部署代理的城市
国家	部署代理的国家
平台	托管 NetScaler Console 的平台。例如，Citrix Hypervisor
区域	部署代理的区域
total_active_agents	处于 UP 状态的代理总数
total_agents	配置的代理总数
版本	代理版本
城市	数据中心城市
isCloud	是本地部署还是云部署
mas_platform	NetScaler Console 平台
生产	产品名称
prodVer	Console 构建版本
total_k8s	托管在 Kubernetes 集群上的 NetScaler Console。Kubernetes 集群总数
total_apps	NetScaler Console 中的应用程序总数
total_custom_sites	在 NetScaler Console 中配置的自定义站点总数
total_managed_apps	NetScaler Console 中管理的总应用程序数
total_custom_apps	NetScaler Console 中的自定义应用程序总数
根	NetScaler Console 在 /var、/root、/flash、/var/mps 目录中的磁盘利用率详细信息
总计	NetScaler Console 磁盘总空间（单位：字节）
已用	NetScaler Console 已用磁盘总空间

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
空闲	NetScaler Console 可用磁盘总空间
total_api_requests	过去 24 小时内通过 API 向 NetScaler Console 发出的总请求数。这还包括远程代理用户（来自代理的请求）。
total_api_external_requests	排除来自代理的请求后，通过 API 发送到 NetScaler Console 的总请求数
total_gui_requests	过去 24 小时内登录到 NetScaler Console GUI 的用户总数
total_users	NetScaler Console 本地用户的总数
total_config_audit	在 NetScaler Console 中配置的配置审计模板总数
total_config_job	在 NetScaler Console 中创建的配置作业总数
total_ssl_certs	从 NetScaler Console 创建/修改/删除的 SSL 证书总数
total_custom_event_rules	在 NetScaler Console 中创建的自定义事件规则总数
total_event_rules	在 NetScaler Console 中创建的事件规则总数
total_ingress_deployed	Kubernetes 中 Ingress 控制器的总数。
total_ipam	NetScaler Console 中添加的 IPAM 提供程序的总数
total_ipam_configured	NetScaler Console 中添加的 IPAM 网络的总数
total_network_report	NetScaler Console 中创建的网络报告总数
total_pager_duty_profile	NetScaler Console 中添加的 PagerDuty 配置文件的总数
gw_hdx_insights	是否启用了 HDX Insight 和 Gateway Insight 导出

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
total_rbac_groups	NetScaler Console 中配置的 RBAC 组的总数
total_slack_profile	NetScaler Console 中添加的 Slack 配置文件总数
total_ssl_certs	从 NetScaler Console 创建/修改/删除的 SSL 证书总数
total_stylebook_config_store_count	在 NetScaler Console 中创建的配置包总数
total_user_sb_stylebook_count	在 NetScaler Console 中创建的自定义配置包总数
配置包	从 StyleBooks 存储的配置包总数
isContainer	NetScaler Console 是否部署在容器平台中
百分比	用于 var_mps、root、flash、var 的磁盘空间总数

Cloud Connect 所需的遥测数据

下表显示了在您启用 Cloud Connect 后收集的所需数据列表：

参数	描述
onprem_ip	NetScaler Console 的 IP 地址
onprem_customer_id	Citrix Cloud 标识
onprem_time_stamp	数据上传时的数据和时间戳
on_prem_version	NetScaler Console 本地版本
total_blx_device	NetScaler Console 本地部署中托管的 BLX 实例总数
total_managed_devices	NetScaler Console 中托管的 NetScaler 实例总数
total_active_managed_devices	处于 UP 状态的 NetScaler 实例总数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
total_ns_device	NetScaler Console 中托管的 MPX 实例总数
total_ng_device	NetScaler Console 中托管的 Gateway 实例总数
total_ngvpx_device	NetScaler Console 中托管的 Gateway VPX 实例总数
total_nswg_device	NetScaler Console 中托管的 Web Gateway 实例总数
total_nswgvpx_device	NetScaler Console 中托管的 Web Gateway VPX 实例总数
total_nsvpx_device	NetScaler Console 中托管的 VPX 实例总数
total_cpx_device	NetScaler Console 中托管的 CPX 实例总数
total_nsap_device	NetScaler Console 中管理分区实例总数
total_nssdx_device	NetScaler Console 中托管的 SDX 实例总数
total_waf_devices	启用了 WAF 违规的 NetScaler 实例总数
total_gw_devices	启用了 SSL VPN 的 NetScaler 实例总数
total_icaproxy_devices	NetScaler Console 中启用了 HDX Insight 的 NetScaler 实例总数
total_bot_devices	启用了 Bot 违规的 NetScaler 实例总数
total_pooled_devices	具有池化许可证的 NetScaler 实例总数（包括托管和非托管）
total_lb_devices	配置了负载均衡虚拟服务器的 NetScaler 实例总数
total_lb_devices_http	配置了负载均衡 HTTP 虚拟服务器的 NetScaler 实例总数
total_lb_devices_ssl	配置了负载均衡 SSL 虚拟服务器的 NetScaler 实例总数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
total_cs_devices	配置了内容交换虚拟服务器的 NetScaler 实例总数
total_gslb_devices	配置了全局服务器负载均衡虚拟服务器的 NetScaler 实例总数
total_aaa_devices	配置了 AAA 虚拟服务器的 NetScaler 实例总数
device_id	VPX 实例唯一 ID
版本	VPX 实例的构建版本
状态	VPX 实例的当前状态（UP 或 Down）
设备平台	托管 VPX 实例的平台
st	正在拉取数据时的当前时间
授权池实例数	授权的池实例总数
已用池实例数	已使用的池实例总数
授权池 FIPS 实例数	授权的池 FIPS 实例总数
已用池 FIPS 实例数	总已用池 FIPS 实例
pool_entvcpu_entitled	总池企业版 vCPU 授权
pool_entvcpu_used	总已用池企业版 vCPU
pool_entbw_entitled	总池企业版带宽授权 [MBps]
pool_entbw_used	总池企业版带宽已用 [MBps]
pool_pltbw_entitled	总池白金版带宽授权 [MBps]
pool_pltbw_used	总池白金版带宽已用 [MBps]
pool_pltvcpu_entitled	总池白金版 vCPU 授权
pool_pltvcpu_used	总池白金vCPU已用量

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
pool_stdbw_entitled	总池标准带宽授权量
pool_stdbw_used	总池标准带宽已用量
pool_stdvcpu_entitled	总池标准vCPU授权量
pool_stdvcpu_used	总池标准vCPU已用量
pool_cpxvcpu_entitled	总池CPX vCPU授权量
pool_cpxvcpu_used	总池CPX vCPU已用量
pool_perc_instances_used	已用实例的百分比
pool_perc_vcpu_used	已用 vCPU 的百分比
pool_perc_bw_used	已用带宽的百分比
total_entitled_vservers	授权虚拟服务器总数
total_used_vservers	已用虚拟服务器总数
total_discovered_vservers	已发现虚拟服务器总数
perc_used_vservers	已用/授权虚拟服务器的百分比
perc_discovered_vservers	已发现/授权虚拟服务器的百分比
is_local_license	检查许可证是否托管在 NetScaler Console 中
license_edition	许可证类型（白金版/标准版/企业版）
is_pooled_license	检查许可证是否为池化许可证
model_id	实例的模型 ID
plt_license_allocation	白金版许可证分配
ent_license_allocation	企业版许可证分配
std_license_allocation	标准版许可证分配

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参数	描述
许可证结束日期	许可证到期前的总天数
平台	设备类型
instance_id	实例的唯一标识符
instance_mode	检查实例是独立实例还是高可用性对
instance_state	实例状态（启动/停止）
flex_vpx_inst_entitled	授权的 VPX 实例总数
flex_vpx_inst_allocated	已分配的 VPX 实例总数
flex_sdx_inst_entitled	授权的 SDX 实例总数
flex_sdx_inst_allocated	已分配的 SDX 实例总数
flex_mpx_inst_entitled	授权的 MPX 实例总数
flex_mpx_inst_allocated	已分配的 MPX 实例总数
flex_plt_bw_entitled	授权的白金带宽
flex_plt_bw_allocated	已分配的白金带宽
flex_ent_bw_entitled	授权的企业带宽
flex_ent_bw_allocated	已分配的企业带宽
flex_std_bw_entitled	授权的标准带宽
flex_std_bw_allocated	分配的标准带宽
flex_vpx_fips_inst_entitled	授权的 FIPS 实例总数
flex_vpx_fips_inst_allocated	分配的 FIPS 实例总数
NS许可类型	许可类型（弹性或固定）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler® 遥测程序所需的遥测数据

作为 NetScaler 遥测程序一部分收集的数据列在 遥测数据治理 文档中。

注意：

某些参数通过从 NetScaler Console 推送到 NetScaler 实例的脚本收集。

通过遥测收集的信息，例如电子邮件地址、用户名和 IP 地址，通过使用单向哈希算法在源头对信息进行哈希处理，从而安全地进行假名化。因此，Citrix 无法访问或读取这些值。此遥测数据仅用于逻辑资产匹配目的。

许可

当实例通过 `https` 协议发现时，NetScaler Console 需要经过验证的 NetScaler 许可证来管理和监控 NetScaler 实例。

NetScaler Console 支持以下许可证版本。请联系您的 NetScaler 销售代表或合作伙伴购买 NetScaler Console 许可证。

Express 版本 – 您可以使用 Express 版本许可证管理和监控任意数量的实例。默认情况下，将应用 Express 版本许可证。

Advanced 版本 - 它允许管理发现的应用程序，并查看已购买的虚拟服务器以及免费虚拟服务器的分析数据。

注意事项：

- 对于版本 **13.1-9.x 或更早版本**，您可以管理多达 30 个已发现的应用程序或虚拟服务器并查看分析数据。超出 30 个已发现的应用程序或 30 个虚拟服务器后，您必须购买并应用 Advanced 许可证。例如，如果您购买 100 个虚拟服务器许可证，则您有权使用多达 130 个虚拟服务器许可证。
- 对于版本 **13.1-12.x 或更高版本**，您可以管理多达两个已发现的应用程序或虚拟服务器并查看分析数据。超出两个已发现的应用程序或两个虚拟服务器后，您必须购买并应用 Advanced 许可证。例如，如果您购买 100 个虚拟服务器许可证，则您有权使用多达 102 个虚拟服务器许可证。

升级到 13.1-12.x 到 14.1-17.x 版本后：

- 所有 Express 默认免费虚拟服务器在 30 天内保持功能正常。您可以在 30 天内选择两个虚拟服务器并应用两个默认许可证。如果在升级后 30 天内未采取任何用户操作，NetScaler Console

© 1997–2026 Citrix Systems, Inc. All rights reserved.

将随机向两个虚拟服务器应用许可证，并取消其余虚拟服务器的许可证。您必须购买并应用新的 Advanced 许可证才能启用这些虚拟服务器。

- 升级后，NetScaler Console 行为发生以下变化：
  - NetScaler Console 提供额外的 30 天时间来执行所需操作。
  - 在 30 天内，将阻止为 30 个 Express 免费虚拟服务器分配新的虚拟服务器。
    - 例如，如果您在升级到 12.x 之前可用的虚拟服务器许可证数量为 30 个，并且只使用了 20 个已获得许可的虚拟服务器，则您只能使用这 20 个虚拟服务器，并且在 30 天内不允许为剩余的 10 个虚拟服务器授予许可证。
  - 但是，在 30 天内，作为管理员，您仍然可以应用 Advanced NetScaler Console 许可证并分配新的虚拟服务器。

下表提供了许可详细信息：

功能	选项	精简版	高级版	NETSCALER 许可证
应用程序	应用程序仪表板	最多两个虚拟服务器。	有权使用所有已购买的虚拟服务器许可证和额外的两个虚拟服务器。	应用程序仪表板上与 NetScaler Web App Firewall 相关的信息需要 Premium（或）Advanced with App Firewall 许可证。
	网络洞察	最多两个虚拟服务器。	有权使用所有已购买的虚拟服务器许可证和额外的两个虚拟服务器。	不适用
	服务图	最多两个虚拟服务器。	享有所有已购买的虚拟服务器许可证以及额外的两个虚拟服务器的权利。	不适用

© 1997–2026 Citrix Systems, Inc. All rights reserved.

功能	选项	精简版	高级版	NETSCALER 许可证
	配置 > StyleBooks	无限制	无限制	不适用
安全	安全仪表板	最多两个虚拟服务器。	享有所有已购买的虚拟服务器许可证以及额外的两个虚拟服务器的权利。	安全仪表板上与 NetScaler Web App Firewall 相关的信息需要 Premium（或）Advanced with App Firewall 许可证。
	安全违规	最多两个虚拟服务器。	享有所有已购买的虚拟服务器许可证以及额外的两个虚拟服务器。	Premium（或）Advanced，带应用程序防火墙许可证
	用户和端点	最多两个虚拟服务器。	享有所有已购买的虚拟服务器许可证以及额外的两个虚拟服务器。	不适用
网关	HDX 洞察	最多两个虚拟服务器。	享有所有已购买的虚拟服务器许可证以及额外的两个虚拟服务器。	Advanced（报告 < 1 小时）Premium（报告 = 无限制）
	网关洞察	最多两个虚拟服务器。	享有所有已购买的虚拟服务器许可证以及额外的两个虚拟服务器。	Advanced（报告 < 1 小时）Premium（报告 = 无限制）
基础架构	基础架构分析	无限制	无限制	不适用
	实例	无限制	无限制	不适用

© 1997–2026 Citrix Systems, Inc. All rights reserved.

功能	选项	精简版	高级版	NETSCALER 许可证
	SSL 控制板	无限制	无限制	不适用
	事件	无限制	无限制	不适用
	网络功能	无限制	无限制	不适用
	网络报告	无限制	无限制	不适用
	池化许可证	无限制	无限制	不适用
	配置 > 配置作业、配置模板和配置建议	无限制	无限制	不适用
	升级作业	无限制	无限制	不适用
	编排	无限制	无限制	不适用
设置	RBAC 和外部身份验证（实例级别）	无限制	无限制	不适用
	RBAC 和外部身份验证	无限制	无限制	不适用

*对于 Citrix Director 与 NetScaler Console 的集成支持 – Citrix Director 必须拥有高级许可证。

更多虚拟服务器的许可证以 10 个虚拟服务器包的形式提供。您可以通过 NetScaler Console GUI 获取有效许可证并将其添加到 NetScaler Console 服务器上。

高可用性

NetScaler Console 服务器可以包含 VIP、CICO 和池化容量许可证。当许可证颁发给 NetScaler Console 服务器时，许可证将绑定到服务器的主机 ID。限制将许可证分配给不同的 NetScaler Console 服务器。

如果将 NetScaler Console 高可用性对配置为许可证服务器，则主服务器和辅助服务器必须具有相同的许可证文件。因此，在 NetScaler Console 高可用性部署中，NetScaler Console 支持将相同的许可证文件分配给这两个服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意

- 如果您安装了 NetScaler Console 12.1-49.x 或更早版本，您有 30 天的时间来维护辅助节点上的许可。30 天后，您必须联系 Citrix 重新托管原始许可证。
- 在 12.1-50.x 及更高版本中，NetScaler Console 许可证会自动同步到辅助节点。
- 在 12.1-50.x 及更高版本中，池化许可证会自动同步到辅助节点。

NetScaler Console 高可用性节点之间如何同步许可证?

当发生故障转移时，辅助服务器将承担主服务器的角色。主服务器的真实主机 ID 被配置为新主服务器的虚拟主机 ID。许可证文件使用虚拟主机 ID 识别新的主服务器。

- **真实主机 ID** - 此 ID 是根据 NetScaler Console 服务器的 MAC 地址生成的。每个 NetScaler Console 独立部署都有一个唯一的主机 ID。
- **虚拟主机 ID** - 此 ID 在 HA 部署期间自动生成。NetScaler Console 主服务器的真实主机 ID 用作辅助服务器的虚拟主机 ID。此 ID 以加密格式存储在 NetScaler Console 数据库中，并且限制对该 ID 的任何修改。虚拟主机 ID 优先于真实主机 ID。

NetScaler Console 高可用性节点之间同步的许可证(/en-us/netscaler-application-delivery-management-software/media/license-ha-support-console.png)

假设 Node-1 是主服务器，Node-2 是辅助服务器。Node-1 的虚拟主机 ID 与 Node-2 同步。

1. Node-1 中可用的许可证文件将同步到 Node-2。
2. Node-1 上的任何新许可证文件都会定期同步到 Node-2。
3. NetScaler Console 确保许可证服务器仅在 Node-1 上运行，以避免许可证容量翻倍。
4. NetScaler 实例使用浮动 IP 地址从 Node-1 签出许可证。

许可证锁定到 NetScaler 实例。要从 NetScaler Console HA 签出许可证，实例需要特定的 NetScalerNetScaler IP 地址。当您在负责许可的主服务器上应用许可证时，它将应用于该实例上的所有未来许可证。您只能从安装了许可证的服务器中删除许可证。

编排

编排模块独立于许可，并且始终可用。

升级虚拟服务器许可证

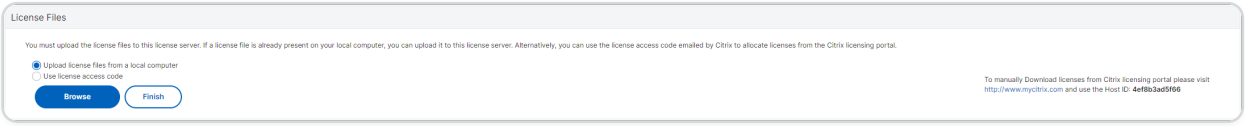
您可以升级 NetScaler Console 上的许可，以监控和管理 NetScaler 上托管的更多虚拟服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要升级您的 NetScaler 许可证：

1. 使用管理员凭据登录到 NetScaler Console。
2. 导航到 **基础架构 > 池化许可**。
3. 转到 **License Files**，然后选择以下选项之一：
   - **从本地计算机上传许可证文件**。如果许可证已存在于您的本地计算机上，请单击 **Browse** 并选择您要用于分配许可证的许可证文件 (.lic)。单击 **Finish**。
   - **使用许可证激活码**。Citrix 会通过电子邮件发送您购买的许可证的许可证访问码。在文本框中输入许可证访问码，然后单击 **Get Licenses**。

> **注意**
>
> 如果您选择此选项，NetScaler Console 必须连接到 Internet，或者必须有可用的代理服务器。



4. 您可以随时从“许可证设置”页面添加更多许可证。

验证

您可以通过导航到 **Settings > Licensing & Analytics Configuration** 来验证 NetScaler Console 上安装的许可证。

管理虚拟服务器

您可以选择要通过 NetScaler Console 管理和监控的虚拟服务器或第三方虚拟服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意事项

- 默认情况下，NetScaler Console 在每个虚拟服务器轮询周期后随机授权虚拟服务器。
- 如果您的 NetScaler Console 中发现的虚拟服务器总数低于已安装的虚拟服务器许可证数量，则 NetScaler Console 默认授权所有虚拟服务器。

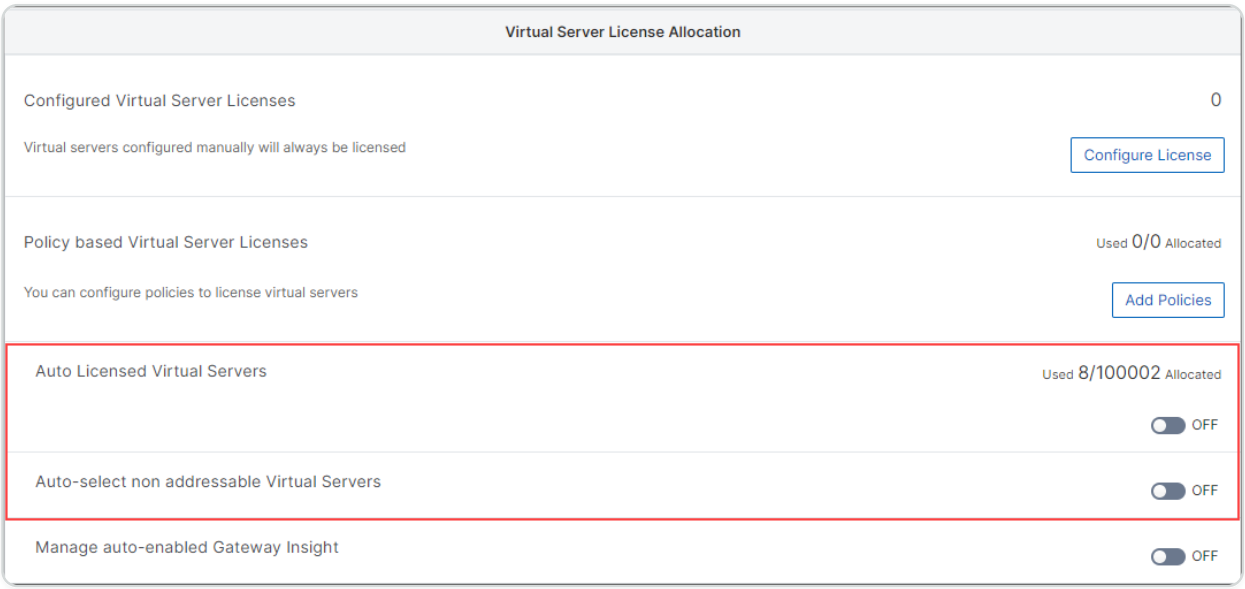
要手动选择虚拟服务器，或将授权限制为有限的虚拟服务器，您必须首先禁用虚拟服务器的自动授权，然后选择要管理的虚拟服务器。

禁用虚拟服务器的自动授权

1. 导航到 **设置 > 授权和分析配置**。

   仪表板显示可用的虚拟服务器许可证、托管的虚拟服务器及其类型以及许可证到期信息。

2. 在 **虚拟服务器许可证分配** 中，禁用 **自动授权虚拟服务器** 和 **自动选择不可寻址的虚拟服务器**。



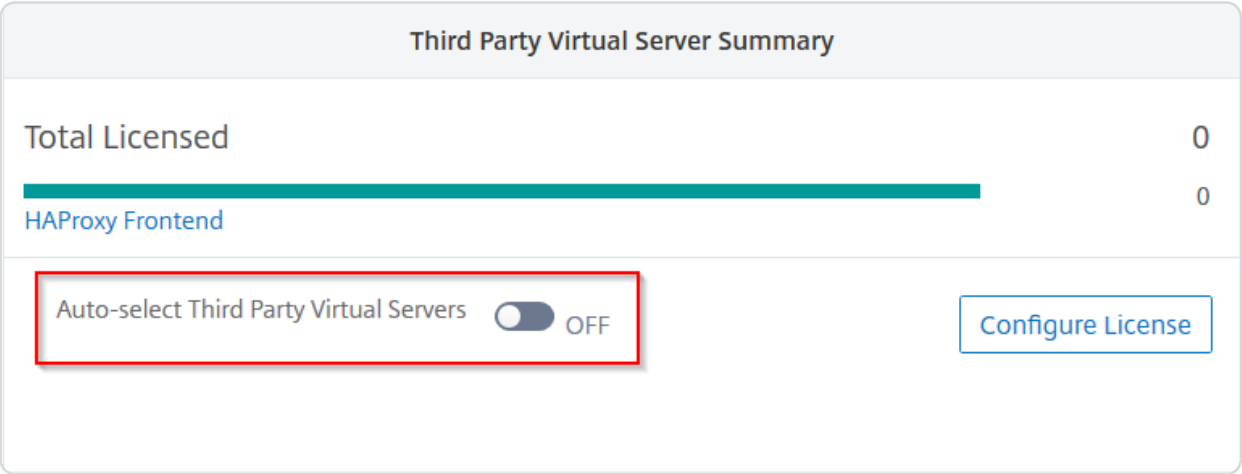
选择第三方虚拟服务器进行授权

1. 导航到 **设置 > 授权和分析配置**。

   仪表板显示可用的虚拟服务器许可证、托管的虚拟服务器及其类型以及许可证到期信息。

2. 在 **第三方虚拟服务器摘要** 中，禁用 **自动选择第三方虚拟服务器**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



手动应用虚拟服务器许可证

您可以手动将许可证应用于单个虚拟服务器。

1. 在“**虚拟服务器许可证分配**”中，选择“**配置许可证**”。

   将显示“**所有虚拟服务器**”页面。

2. 使用属性 `Licensed: No` 筛选未获得许可的虚拟服务器。
3. 选择要获得许可的虚拟服务器。
4. 单击“**许可证**”。

配置基于策略的虚拟服务器许可

您可以配置策略以将许可证应用于虚拟服务器。此策略控制您要自动许可的虚拟服务器数量。它还仅将许可证应用于所选实例的虚拟服务器。

单击“**编辑策略**”，您可以指定以下内容：

- 分别设置 CPX 实例上的虚拟服务器限制以应用许可证。NetScaler Console 会将许可证应用于 CPX 实例上的虚拟服务器，直至达到指定限制。

  重要

  此限制适用于 CPX 实例，但 sidecar 部署类型除外。

  要查看 sidecar 部署类型的 CPX 实例，请使用属性 `License Type: Freely Managed` 筛选虚拟服务器。

- 在选定的 NetScaler 实例 (MPX/VPX/BLX) 上设置虚拟服务器限制以应用许可证。NetScaler Console 会将许可证应用于 NetScaler 实例上的虚拟服务器，直至达到指定限制。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 选择优先的 NetScaler 实例以应用虚拟服务器许可证。因此，NetScaler Console 只能将许可证应用于所选实例的虚拟服务器。

编辑策略以将许可证应用于虚拟服务器(/en-us/netscaler-application-delivery-management-software/media/configure-license-policy.png)

查看已获得许可的虚拟服务器

将许可证应用于虚拟服务器后，您可以查看已获得许可的虚拟服务器或第三方虚拟服务器。

1. 导航到 **设置 > 许可和分析配置**。
2. 在 **虚拟服务器许可证摘要** 中的 **总许可** 部分中单击虚拟服务器类型。

为不可寻址的虚拟服务器配置自动许可证支持

NetScaler Console 默认情况下不会自动将许可证应用于不可寻址的虚拟服务器。要许可不可寻址的虚拟服务器，您必须禁用自动许可选项并手动选择不可寻址的虚拟服务器。这会增加您在最初应用许可证时手动选择不可寻址服务器的工作量。此外，每当新的不可寻址虚拟服务器添加到您的网络时，您还需要手动选择它们。

NetScaler Console 在 **虚拟服务器许可证分配** 下提供了一个选项。如果您启用 **自动选择不可寻址的虚拟服务器** 选项，许可证将自动应用于不可寻址的虚拟服务器。

注意

- NetScaler Console 默认情况下仍然不会自动选择不可寻址的虚拟服务器进行许可。
- 应用程序分析（App Dashboard）是目前唯一在已获得许可的不可寻址虚拟服务器上支持的分析功能。

备份和恢复 HA 对中的 NetScaler Console 配置

您可以备份 NetScaler Console 的当前配置。在 NetScaler Console 的 HA 部署中，您可以从任一服务器备份和恢复 NetScaler Console 配置。如果您使用负载平衡虚拟服务器 IP 地址进行备份，则备份文件可以存储在任一服务器上，并且必须手动检查。

如果仅当一个节点处于活动状态时进行恢复，或者在恢复过程中发生故障转移，则恢复过程将无法完成。

备份 NetScaler Console 配置：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

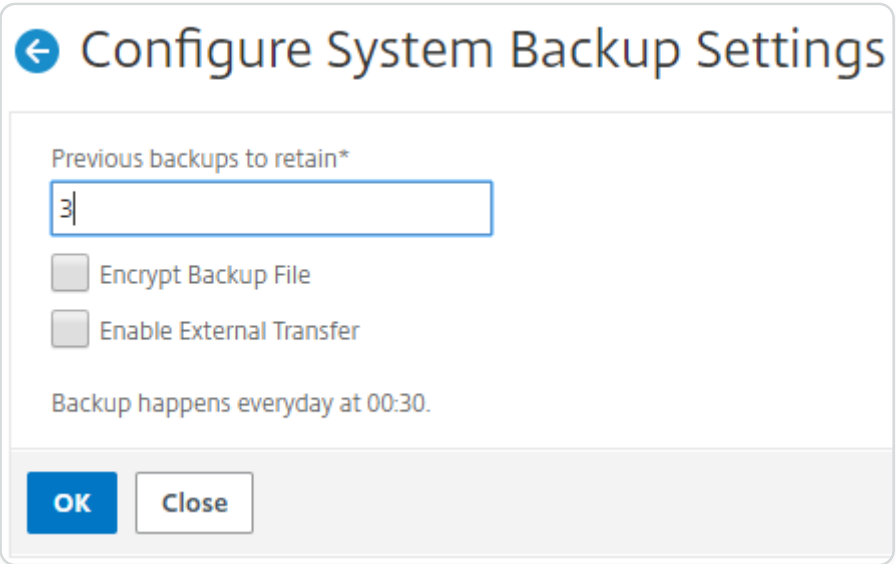
1. 导航到 **System** \> **Advanced Settings** \> **Backup Files**，然后单击 **Back Up**。
2. 要加密备份文件，请选中 **Password Protect file** 复选框。

从备份文件恢复 NetScaler Console 配置：

1. 导航到 **系统** \> **高级设置** \> **备份文件**。
2. 选择要恢复的备份文件，然后单击 **Restore**。

配置系统备份设置：

1. 导航到 **系统** \> **系统管理**。在 **备份设置** 下，单击 **系统备份设置**。
2. 在 **Configure System Backup Settings** 页面上，指定以下内容：
   - 要保留的备份数量。您最多只能保留 10 个备份。
   - 加密备份文件。
   - 启用外部传输。您可以将备份文件的副本传输到另一个系统作为预防措施。当您想要恢复配置时，必须首先将文件上传到 NetScaler Console 服务器，然后执行恢复操作。指定服务器、用户名和密码、端口、要使用的传输协议以及目录路径。要了解有关外部传输的更多信息，请参阅 将 NetScaler Console 备份文件传输到外部系统。
3. 点击 **确定**。



配置系统通知设置

您可以将通知发送给选定的用户组，以处理各种系统相关功能。这些系统功能被组织成事件类别，例如 SystemReboot、StatusPoll 和 SystemState。您可以将 NetScaler Console 配置为通过电子邮件或短信向您发送通知。您必须配置电子邮件服务器或短消息服务 (SMS) 网关服务器，或同时配置

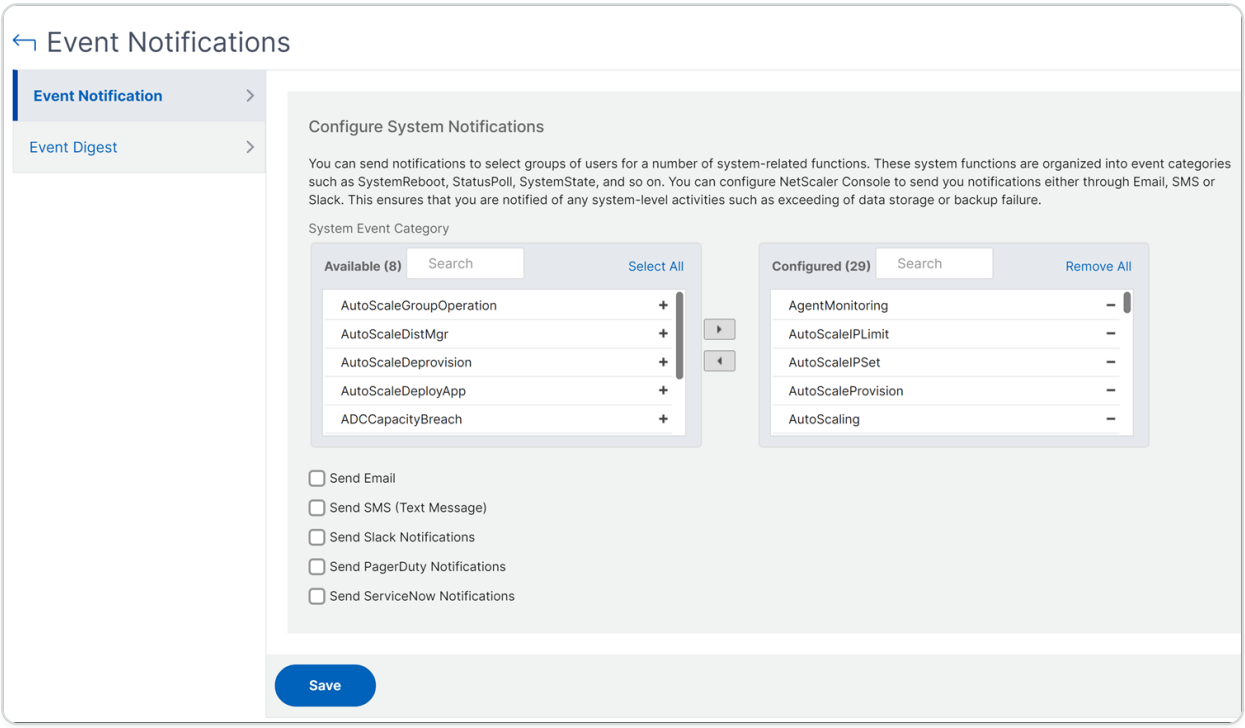
© 1997–2026 Citrix Systems, Inc. All rights reserved.

两者，才能向用户发送电子邮件和短信通知。这可确保您收到任何系统级活动（例如用户登录或系统重启）的通知。

例如，当有人尝试使用 CLI 登录 NetScaler Console 且登录尝试失败时，您可能希望向两名用户发送电子邮件通知。您必须通过选择 UserLogin 类别来配置系统通知，并创建电子邮件通知服务器或选择现有的电子邮件分发列表来发送通知。

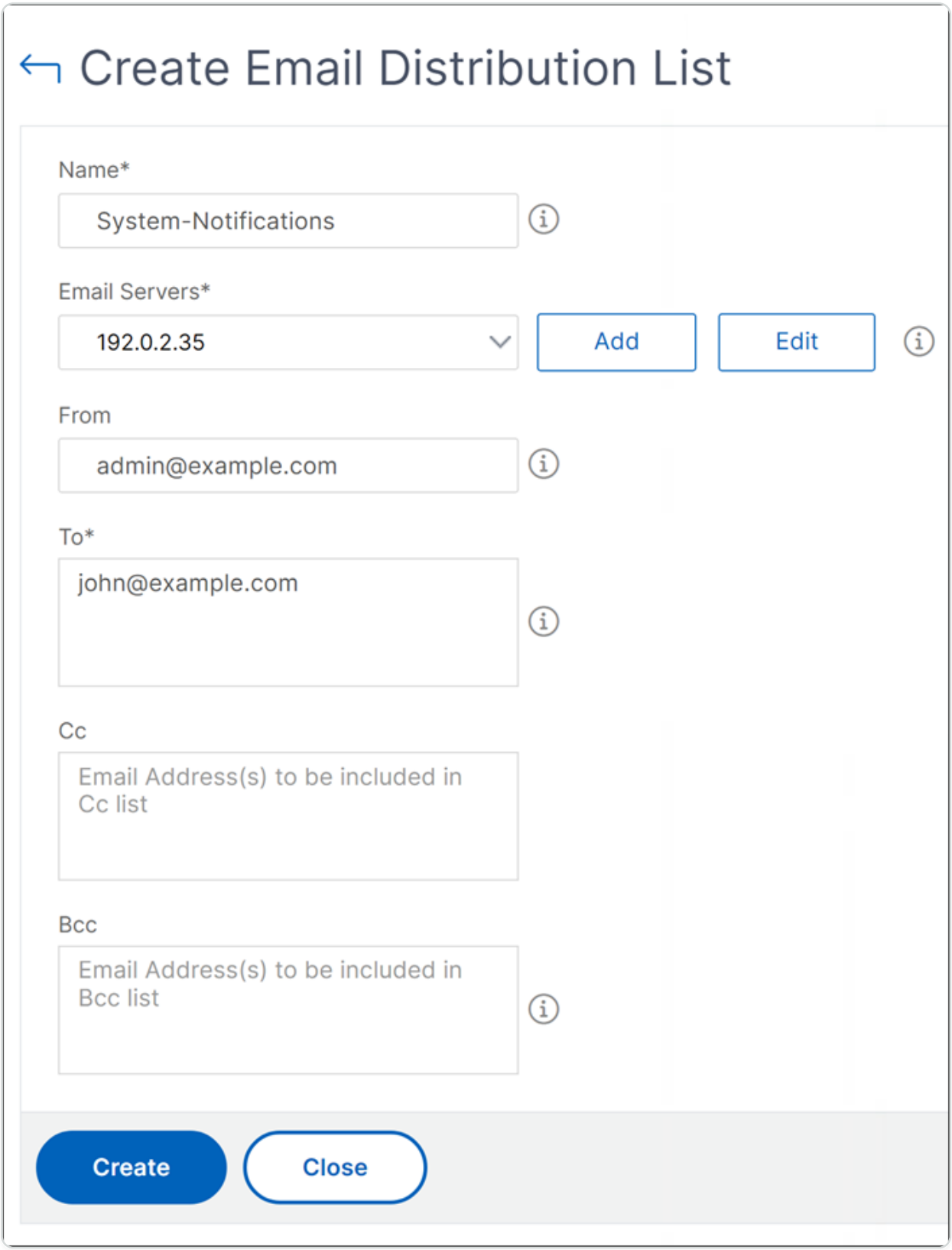
在 NetScaler Console 上配置系统通知设置：

1. 导航到 **系统** \> **通知**。在 **设置** 下，单击 **更改通知设置**。
2. 在 **Configure System Notification Settings** 页面上，在 **Category** 下，选择一个类别，例如 **UserLogin**。



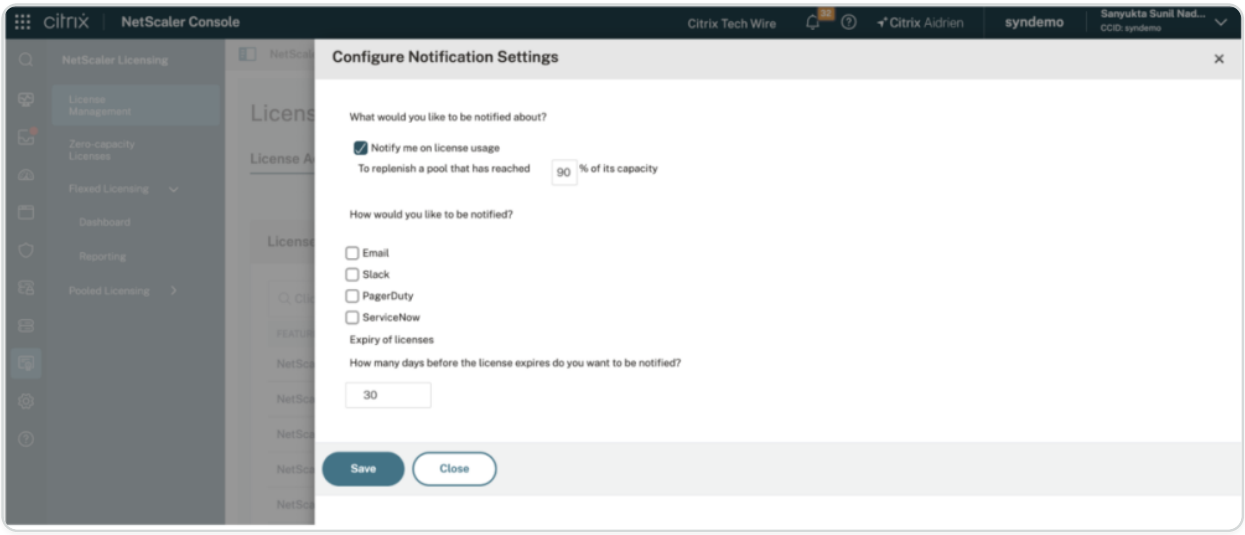
3. 选择 **Send Email**，然后从下拉列表中选择一个电子邮件分发，或者单击“**+**”图标以创建新的电子邮件分发列表，如以下图所示。如果要发送短信通知，请选择 **Send SMS (Text Message)**，然后单击“**+**”图标并指定短信服务器详细信息以创建短信分发列表。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



为某些事件类别设置通知后，每当发生与该类别相关的事件时，都会通过电子邮件或短信向收件人发送通知。在此示例中，当用户使用 CLI 登录 NetScaler Console 失败时，您可以看到电子邮件通知。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



系统通知针对以下事件发送：

类别	原因
BackupFailure	系统备份失败
DataStorageExceeded	数据库存储超出许可证中指定的限制
DeviceBackupFailure	实例备份失败
`HAMonitoring`	系统 HA 故障转移发生，对等节点无心跳，且数据库同步失败
HealthMontoring	CPU、RAM 或磁盘利用率超出阈值
LicensePool	许可证池超出阈值
许可证	应用许可证时失败
PasswordRecovery	密码恢复失败或成功
PerfCounterThresholdHigh	性能计数器值超出限制
PerfCounterThresholdNormal	性能计数器值正常
PolicyFailed	任何系统策略失败
RemoteDeviceBackupFailure	远程实例备份失败
RemoteSystemBackupFailure	远程系统备份失败

© 1997–2026 Citrix Systems, Inc. All rights reserved.

类别	原因
RemoteSystemBackupNormal	远程系统备份成功
SSLCertThreshold	证书阈值被突破
StatusPoll	实例状态的任何更改
子系统状态	子系统状态的任何更改
系统重启	系统已重启
系统状态	系统状态的任何更改
陷阱配置失败	在实例上添加 SNMP 陷阱时发生故障
用户登录	用户身份验证失败

为地理地图配置站点

NetScaler Console 站点是特定地理位置中 NetScaler 实例的逻辑分组。一个站点中可以有多个 NetScaler 实例，这些实例可以由 NetScaler Console 服务器进行监控和管理。您可以使用 NetScaler Console 服务器管理来自受管实例的数据，例如 syslog、AppFlow 和 SNMP 等。

创建站点：

1. 导航到 **Infrastructure > Instances > Sites**，然后单击 **Add**。
2. 在 **Create Site** 页面中，指定以下信息：

   a. **站点类型**：选择 **Data Center**。

   > **注意**
   >
   > 站点可以作为主数据中心或分支机构运行。请相应选择。

   b. **类型**：从列表中选择 AWS 作为云提供商。

   > **注意**
   >
   > 相应地勾选 **Use existing VPC as a site** 复选框。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. **站点名称**：键入站点的名称。

d. **城市**：键入城市。

e. **邮政编码**：键入邮政编码。

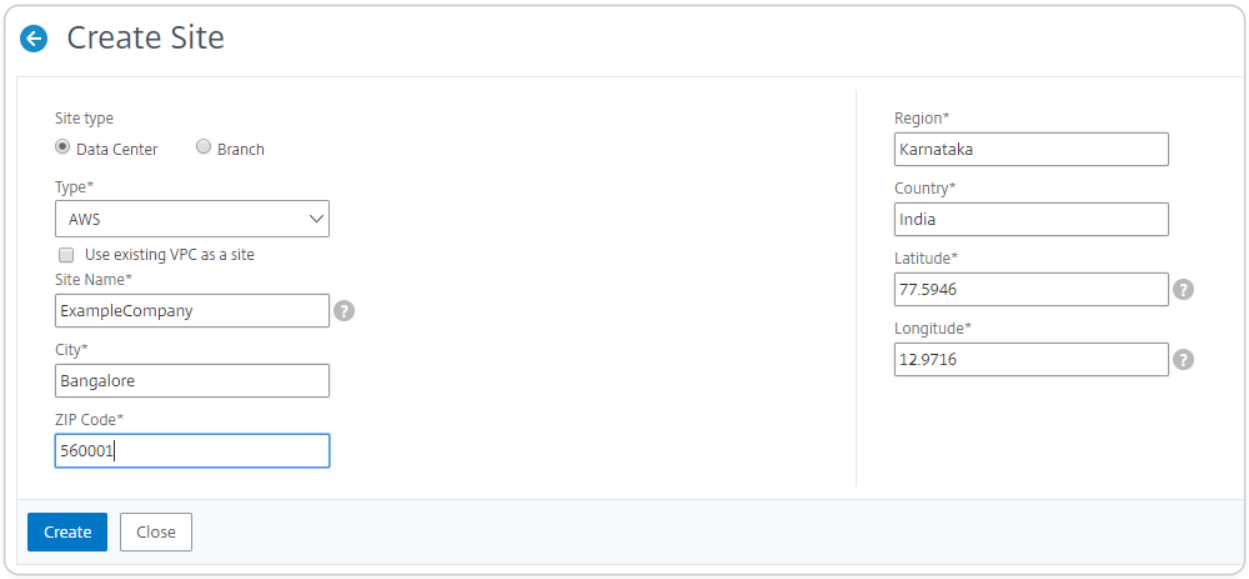
f. **区域**：键入区域。

g. **国家/地区**：输入国家/地区

h. **纬度**：输入该位置的纬度。

i. **经度**：输入该位置的经度。

3. 单击**创建**。



有关将 NetScaler 实例添加到 NetScaler Console 的更多信息，请参阅将实例添加到 NetScaler Console。

© 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.