

NetScaler SDX 13.1

Contents

简介	17
发行说明	18
开始使用管理服务用户界面	19
登录到管理服务用户界面	19
初始设置向导	20
在 SDX 设备上预配实例	21
控制台访问	21
管理服务统计信息	22
管理服务和 NetScaler 实例的单点登录	22
管理主页	22
端口	23
数据治理	25
什么是 NetScaler Console 服务连接？	25
什么是 NetScaler Console 服务？	25
如何启用 NetScaler Console 服务连接？	26
使用 NetScaler Console 服务连接捕获哪些数据？	26
数据是如何使用的？	26
收集的数据保留多长时间？	27
数据存储在哪里以及安全性如何？	27
如何禁用 NetScaler Console 服务连接？	27
NetScaler SDX 设备 Console Advisory Connect 简介	28
Console Advisory Connect 如何支持 NetScaler Console 服务？	28
哪些版本的 NetScaler 支持 Console Advisory Connect？	29
如何启用 Console Advisory Connect？	29
如何启用和禁用 Console Advisory Connect？	29
使用 CLI	29

使用 GUI	30
使用 NITRO API	30
NetScaler Console 内置代理行为	31
参考	31
单一捆绑包升级	32
注意事项	32
将整个设备升级到 13.1	33
支持的升级路径	33
相关信息	34
升级 NetScaler 实例	34
上传软件映像	35
通过下载构建文件创建备份	35
上传 XVA 文件	35
通过下载 XVA 文件创建备份	35
升级 NetScaler VPX 实例	35
升级 VPX 实例	36
相关信息	36
管理和监控 SDX 设备	37
修改 SDX 设备的网络配置	37
更改默认用户帐户的密码	37
修改设备的区域时区	37
修改设备的主机名	37
VLAN 过滤	38
配置时钟同步	38
启用 NTP 同步	38
修改身份验证选项	39
查看 SDX 设备属性	39
查看设备的实时吞吐量	40

查看实时 CPU 和内存使用情况	41
查看所有核心的 CPU 使用情况	41
在 SDX 设备上安装 SSL 证书	41
查看管理服务上的 SSL 证书	41
NetScaler 实例的 SSL 证书和密钥	42
修改系统设置	42
重新启动设备	42
关闭设备	42
SDX 管理域	43
将资源分配给子域的示例	43
将用户分配给域	44
在 SDX 22000 平台上管理 RAID 磁盘分配	44
查看驱动器属性和操作	45
逻辑驱动器	45
创建新的逻辑驱动器	45
物理驱动器	45
存储库	46
SDX 许可概述	48
许可证激活服务	48
在 SDX 设备上管理许可证	49
先决条件	49
使用管理服务分配许可证	49
分配许可证	50
许可证激活服务	52
LAS 的 NetScaler 版本兼容性	53
先决条件	53
通过使用 NetScaler GUI 过渡到 LAS	53
许可证激活文件的行为和到期	60

许可证合同到期	60
在 LAS 许可工作流程期间发送到 LAS 的信息	61
监控已转换为 LAS 的 NetScaler SDX (SVM) 的最佳实践	62
先决条件	62
监控 LAS 激活 blob 过期	63
监控许可证权利到期（合同到期）	65
SDX 资源可视化工具	67
管理接口	68
配置接口	68
重置接口参数为其默认值	69
显示 VPX 实例上的虚拟接口到物理接口的映射	69
将 MAC 地址分配到接口	70
禁用或启用 SDX 设备上的物理接口	71
SDX 设备上的巨型帧	71
用例：巨型到巨型设置	72
用例：非巨型帧到巨型帧设置	75
用例：巨型帧和非巨型帧流在同一组接口上的共存	80
在 SDX 设备上配置 SNMP	85
添加 SNMP 陷阱目标	86
下载 MIB 文件	87
下载 MIB 文件	87
添加 SNMP 管理器社区	87
配置 SNMP 管理器	87
为 SNMPv3 查询配置 SDX 设备	88
添加 SNMP 管理器	88
配置 SNMP 视图	88
配置视图	89
配置 SNMP 用户	89

配置用户	89
配置 SNMP 警报	90
配置 syslog 通知	90
配置 syslog 服务器	91
配置 syslog 参数	91
配置邮件通知	91
配置 SMTP 服务器	91
配置邮件配置文件	92
配置短信通知	92
配置 SMS 服务器	92
配置 SMS 配置文件	92
监视和管理在 SDX 设备上配置的实体的实时状态	93
查看虚拟服务器的状态	93
查看服务状态	94
查看服务组的状态	95
查看服务器状态	96
配置轮询间隔	97
监控和管理 NetScaler 实例上生成的事件	98
查看所有事件	98
SDX 设备上 NetScaler 实例的 Call Home 支持	103
系统运行状况监控	105
监控 SDX 设备上的存储资源	106
监控 SDX 设备上的硬件传感器	107
监视 SDX 设备上的接口	107
配置系统通知设置	108
配置系统通知设置	108
从管理服务启用和禁用功能	109
使用 GUI 启用或禁用功能	109

配置管理服务	110
管理客户端会话	110
配置策略	110
重新启动管理服务	111
删除管理服务文件	112
生成用于技术支持的 tar 存档	112
管理服务的 CLI 支持	112
配置身份验证和授权设置	113
添加用户组	113
添加用户组	114
配置用户帐户	115
配置用户帐户	115
删除用户帐户	116
设置身份验证类型	116
设置身份验证类型	116
启用或禁用基本身份验证	117
配置外部身份验证服务器	117
添加 RADIUS 服务器	117
添加 RADIUS 服务器	117
添加 LDAP 身份验证服务器	118
添加 LDAP 服务器	118
对 LDAP 用户的 SSH 公钥身份验证支持	120
为 FQDN 名称解析添加主 DNS	121
添加 TACACS 服务器	121
添加 TACACS 服务器	122
从管理服务配置链路聚合	122
从管理服务配置通道	123
从管理服务配置通道	123

访问控制列表	124
使用准则	125
如何配置 ACL	125
启用 ACL 功能	125
创建 ACL 规则	126
启用 ACL 规则	127
ACL 规则的其他操作	128
禁用 ACL 规则	128
编辑 ACL 规则	128
删除 ACL 规则	128
重新编号 ACL 规则的优先级	129
故障排除	129
设置 NetScaler 实例集群	130
注意事项	130
在 SDX 设备上设置集群	131
将存在于一个 SDX 设备上的 NetScaler 实例添加到配置在另一个 SDX 设备上的群集	133
配置集群链路聚合	134
配置 SSL 密码以安全地访问管理服务	138
限制	138
支持的 SSL 密码	138
预定义密码组	145
查看预定义的密码组	146
创建自定义密码组	146
查看现有 SSL 密码绑定	147
将密码绑定到 HTTPS 服务	147
备份和恢复 SDX 设备配置数据	148
备份当前配置	148
计划备份	148

编辑备份策略	148
手动将备份文件传输到外部备份服务器	149
将备份文件传输到外部备份服务器	149
还原设备	149
从备份文件还原设备	150
还原 NetScaler 实例	151
执行设备重置	152
重置设备的配置	152
重置设备的配置	153
将设备重置为出厂版本	153
将设备重置为出厂版本	153
将设备重置为单个捆绑包映像版本	154
先决条件	154
将设备重置为单个捆绑包映像版本	155
级联外部身份验证服务器	155
级联外部身份验证服务器	155
解锁用户	156
使用 GUI 解锁用户	156
使用 CLI 解锁用户	156
预配 NetScaler 实例	157
创建管理员配置文件	157
创建管理员配置文件	158
上传 NetScaler .xva 映像	159
上传 NetScaler .xva 文件	159
通过下载 NetScaler .xva 文件创建备份	159
添加 NetScaler 实例	159
许可证分配	161
加密分配	161

资源分配	161
在 SDX 上为 NetScaler VPX 启用额外管理 CPU 的推荐做法	165
概述	165
何时启用额外的管理 CPU	166
实例管理	167
网络设置	167
管理 VLAN 设置	170
修改 NetScaler 实例	170
将 VLAN 限制到特定的虚拟接口	171
指定允许的 VLAN ID	172
从管理服务为实例配置 VLAN	172
管理加密容量	173
查看 SDX 设备的加密容量	173
在预置 VPX 实例时分配加密容量	174
不同 SDX 设备可用的 ACU 计数器最小值	175
查看加密硬件运行状况	176
注意事项	176
ACU 到 PKE 资源转换表	176
如何解读 ACU 到 PKE 资源转换表	178
传统 SSL 芯片到 ACU 和 SCU 转换表	179
预置第三方虚拟机	180
SECUREMATRIX GSB	181
预配 SECUREMATRIX GSB 实例	181
预配 SECUREMATRIX 实例	181
监视 SECUREMATRIX GSB 实例	182
管理 SECUREMATRIX GSB 实例	182
升级 SECUREMATRIX GSB 实例的 SDX 工具文件	183
升级和降级 SECUREMATRIX GSB 实例	183

排查 SECUREMATRIX GSB 实例	184
趋势科技 InterScan Web 安全	185
卫士通 防护系统	186
预配 Websense Protector 实例	186
将 XVA 映像上传到 SDX 设备	186
预配 Websense protector 实例	187
监视 Websense Protector 实例	187
管理 Websense Protector 实例	187
启动、停止、重新启动、强制停止或强制重新启动 Websense Protector 实例	187
升级 Websense Protector 实例的 SDX 工具文件	188
上传 SDX 工具文件	188
升级 SDX 工具	188
将 Websense Protector 实例升级到更高版本	188
上传软件映像	188
升级实例	189
对 Websense Protector 实例进行故障排除	189
Ping 实例	189
跟踪实例的路由	189
重新发现实例	189
BlueCat DNS/DHCP	189
预配 BlueCat DNS/DHCP 实例	190
监视 BlueCat DNS/DHCP 实例	191
管理 BlueCat DNS/DHCP 实例	191
升级适用于 BlueCat DNS/DHCP 实例的 SDXTools 文件	192
重新发现 BlueCat DNS/DHCP 实例	192
CA 接入网关	193
预配 CA Access Gateway 实例	193
监视 CA Access Gateway 实例	194

管理 CA Access Gateway 实例	194
派拓网络 VM 系列	194
调配 PaloAlto VM 系列实例	195
监视 Palo Alto VM-Series 实例	195
管理 PaloAlto VM-Series 实例	195
排除 PaloAlto VM-Series 实例故障	196
在 NetScaler SDX 设备上部署 Citrix SD-WAN VPX 实例	197
先决条件	197
Citrix SD-WAN VPX 要求	197
MCN 和站点支持的吞吐量	197
支持吞吐量的硬件要求	198
数据中心拓扑	198
在 NetScaler SDX™ 上预置 Citrix SD-WAN VPX 实例	199
配置 Citrix SD-WAN VPX 实例	200
相关信息	200
SDX 中的带宽计量	202
具有固定吞吐量速率的专用带宽	202
具有最低保证吞吐量和带宽突发能力的专用带宽	202
选择带宽分配模式	202
确定 VPX 实例的最大突发带宽	204
检查吞吐量和数据消耗统计信息	204
配置和管理 NetScaler 实例	206
在 NetScaler 实例上创建 SNIP 地址	206
在 NetScaler 实例上添加 SNIP 地址	206
保存配置	206
保存 NetScaler 实例上的配置	206
管理 NetScaler 实例	207
启动、停止、删除或重新启动 NetScaler 实例	207

删除 NetScaler 实例文件	207
删除 NetScaler 实例文件	207
应用管理配置	207
在 NetScaler 实例上应用管理员配置	208
安装和管理 SSL 证书	208
将证书文件上传到 SDX 设备	208
将 SSL 证书文件上传到 SDX 设备	208
要通过下载 SSL 证书文件创建备份	209
将 SSL 密钥文件上传到 SDX 设备	209
要将 SSL 密钥文件上传到 SDX 设备	209
通过下载 SSL 密钥文件创建备份	209
在 NetScaler 实例上安装 SSL 证书	209
在 NetScaler 实例上安装 SSL 证书	210
在 NetScaler 实例上更新 SSL 证书	210
在 NetScaler 实例上更新 SSL 证书	210
轮询 NetScaler 实例上的 SSL 证书	211
配置轮询间隔	211
执行立即轮询	211
在 NetScaler 实例上启用 L2 模式	211
允许实例上的 L2 模式	212
在接口上配置虚拟 MAC	212
在 SDX 管理服务上配置 VMAC	213
将 IPv4 或 IPv6 VRID 添加到接口或 LA 通道	214
生成分区 MAC 地址以在 SDX 设备上的 NetScaler 实例中配置管理分区	215
适用于 VPX 实例的变更管理	216
查看适用于 VPX 实例的变更管理	216
轮询任何 NetScaler 实例配置的更新	217
配置 NetScaler 实例的审计模板	217

监控 NetScaler 实例	218
查看 VPX 实例的属性	218
查看 VPX 实例的属性	218
查看 NetScaler 实例的运行配置和已保存配置	219
查看 NetScaler 实例的运行配置和已保存配置	220
Ping NetScaler 实例	220
Ping NetScaler 实例	220
跟踪 NetScaler 实例的路由	220
跟踪 NetScaler 实例的路由	220
重新发现 NetScaler 实例	220
重新发现 NetScaler 实例	220
使用日志监控操作和事件	221
查看审计日志	221
查看任务日志	221
查看任务设备日志	222
查看任务命令日志	222
查看事件	222
NetScaler SDX 设备的用例	224
当管理服务 and NetScaler 实例位于同一网络时进行整合	224
按此示例所示置备 NetScaler 实例 1	226
当管理服务 and NetScaler 实例位于不同网络时进行整合	226
预配 NetScaler 实例 1，如本例所示	228
跨安全区域整合	228
为每个实例使用专用接口进行整合	228
配置 NetScaler 实例 5 和 3，如本示例所示	230
多个实例共享物理端口的整合	230
在此示例中预配 NetScaler 实例 7 和 4	232
NITRO API	233

获取 NITRO 包	233
.NET SDK	234
系统 API	234
配置 API	235
创建资源	235
检索资源详细信息	237
检索资源统计信息	237
更新资源	238
删除资源	239
批量操作	239
异常处理	240
REST Web 服务	241
系统 API	241
配置 API	244
创建资源	244
获取资源详细信息和统计信息	246
更新资源	247
删除资源	248
批量操作	248
异常处理	251
NITRO 的工作原理	251
Java 开发工具包	252
系统 API	252
配置 API	253
创建资源	253
检索资源详细信息	255
检索资源统计信息	255
更新资源	256

删除资源	257
批量操作	257
异常处理	258
fix	260

简介

NetScaler SDX 设备是一个多租户平台，您可以在其上预配和管理多个 NetScaler 虚拟机（实例）。SDX 设备通过允许单个管理员配置和管理设备并将每个托管实例的管理权限委派给租户来满足云计算和多租户要求。SDX 设备使设备管理员能够为每个租户提供以下优势：

- 一个完整的实例。每个实例都具有以下权限：
 - 专用 CPU 和内存资源
 - 独立的实体空间
 - 独立运行其选择的版本和内部版本
 - 生命周期独立性
- 完全隔离的网络。针对特定实例的流量仅发送到该实例。

SDX 设备提供在设备上预配的管理服务。管理服务提供用户界面（HTTP 和 HTTPS 模式）和 API，用于配置、管理和监视设备、管理服务和实例。Citrix® 自签名证书已预打包以支持 HTTPS。Citrix 建议您使用 HTTPS 模式访问管理服务用户界面。

发行说明

发行说明描述了特定版本或内部版本 NetScaler 软件的增强功能、更改、错误修复和已知问题。NetScaler SDX 发行说明作为 ADC 发行说明的一部分进行介绍。

有关 SDX 13.1 增强功能、已知问题和错误修复的详细信息，请参阅 [ADC 发行说明](#)。

开始使用管理服务用户界面

要开始配置、管理和监控设备、管理服务和虚拟实例，请使用浏览器连接到管理服务用户界面。然后，在设备上预配虚拟实例。

您可以使用以下受支持的浏览器之一连接到管理服务用户界面：

- IE 浏览器
- 谷歌浏览器
- 苹果 Safari 浏览器
- 火狐浏览器

登录到管理服务用户界面

1. 在您的 Web 浏览器地址字段中，键入以下内容之一：

`http://Management Service IP Address`

或

`https://Management Service IP Address`

2. 在登录页面中，在“**用户名**”和“**密码**”字段中，键入管理服务的用户名和密码。默认用户名为 `nsroot`。如果默认密码不起作用，请尝试键入设备的序列号。序列号条形码位于设备的背面。首次使用默认凭据登录后，您必须更改默认的 `nsroot` 密码。有关更改管理员密码的信息，请参阅[更改默认用户帐户的密码](#)。
3. 单击“显示选项”，然后执行以下操作：
 - a. 在“**启动位置**”列表中，选择登录用户界面后必须立即显示的页面。可用选项包括“主页”、“监控”、“配置”、“文档”和“下载”。例如，如果您希望管理服务在登录时显示“配置”页面，请在“**启动位置**”列表中选择“配置”。
 - b. 在“**超时**”中，键入会话过期的时间长度（分钟、小时或天）。最小超时值为 15 分钟。

“**启动于**”和“**超时**”设置在会话之间保持不变。仅在清除缓存后，其默认值才会恢复。
4. 单击“**登录**”以登录到管理服务用户界面。

初始设置向导

您可以使用设置向导在一个流程中完成所有首次配置。

您可以使用该向导配置网络配置详细信息和系统设置、更改默认管理密码以及管理和更新许可证。

您还可以使用此向导修改在初始配置期间为 SDX 设备指定的网络配置详细信息。

要访问向导，请导航到“**配置 > 系统**”，然后在“**设置设备**”下，单击“**设置向导**”。输入以下参数的值。

- **接口**：将设备连接到管理工作站或网络的管理接口。可能的值：0/1、0/2。默认值：0/1。
- **网关**：将流量转发到设备子网之外的路由器的 IP 地址。
- 如果要将 IPv4 地址用于管理服务，请选中 IPv4 复选框，然后输入以下参数的详细信息：
 - **设备管理 IP**：用于通过 Web 浏览器访问管理服务的 IPv4 地址。
 - **子网掩码**：SDX 设备所在的子网掩码。
- **DNS**：主 DNS 服务器的 IPv4 地址。主 DNS 服务器不支持 IPv6 地址。
- 如果要将 IPv6 地址用于管理服务，请选中 IPv6 复选框，然后输入以下参数的详细信息：
 - **管理服务 IP 地址**：用于通过 Web 浏览器访问管理服务的 IPv6 地址。
 - **网关 IPv6 地址**：将流量转发到设备子网之外的路由器的 IPv4 地址。
- 选择**附加 DNS**以添加除主 DNS 服务器之外的额外 DNS 服务器 IP 地址。IP 地址可以是 IPv4 或 IPv6。

Network Configuration

Management Service

Interface*
0/1

Gateway*
10 . 102 . 103 . 1

☒ IPv4

Appliance Management IP*
10 . 102 . 103 . 239

Netmask*
255 . 255 . 255 . 0

DNS
10 . 140 . 50 . 5

☐ IPv6

☐ Additional DNS

Appliance Supportability

☐ Configure Appliance supportability

OK Close

重要！

Citrix® 建议您禁用设备可支持性以提高安全性。要禁用设备可支持性，请导航到**系统 > 网络配置**并清除**配置设备可支持性**复选框。

在**系统设置**下，您可以指定管理服务和 NetScaler 实例之间只能通过安全通道进行通信。您还可以限制对管理服务用户界面的访问。客户端只能通过 HTTPS 登录管理服务用户界面。

您可以修改管理服务和 Citrix Hypervisor 的时区。默认时区为 UTC。您可以通过选择**更改密码**复选框并键入新密码来更改管理员密码。

在“管理许可证”下，您可以管理和分配许可证。您可以使用硬件序列号 (HSN) 或许可证访问代码来分配许可证。或者，如果许可证已存在于您的本地计算机上，您可以将其上传到设备。

选择设备上的许可证，然后单击**完成**以完成初始配置。

在 SDX 设备上预配实例

您可以使用管理服务在 SDX 设备上预配一个或多个 NetScaler 或第三方实例。您可以安装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，则管理服务不允许预配更多实例。

有关预配第三方实例的信息，请参阅[第三方虚拟机](#)。

控制台访问

您可以从管理服务界面访问 NetScaler 实例、管理服务、Citrix Hypervisor 和第三方虚拟机的控制台。此访问有助于调试和排查 SDX 设备上托管的实例。

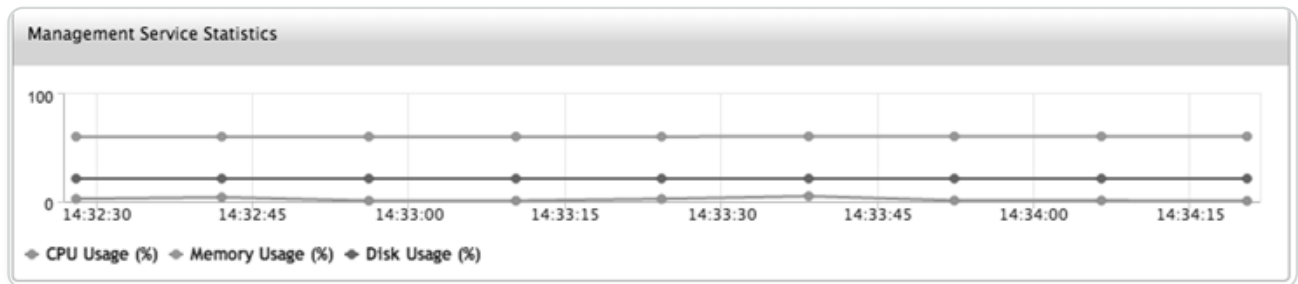
要访问虚拟机的控制台，请导航到实例列表，从列表中选择虚拟机，然后在**操作**列表中单击**控制台访问**。

要访问管理服务或 Citrix Hypervisor 的控制台，请导航到**配置 > 系统**，然后在**控制台访问**下，单击**管理服务**或 **Citrix Hypervisor** 链接。

注意：Internet Explorer 浏览器不支持控制台访问。Citrix 建议仅通过管理服务 HTTPS 会话使用控制台访问功能。

管理服务统计信息

仪表板现在包含管理服务统计信息，用于监控 SDX 设备上管理服务对内存、CPU 和磁盘资源的使用情况。



管理服务和 NetScaler 实例的单点登录

使用用户凭据登录管理服务后，无需再次提供用户凭据即可登录实例。默认情况下，**超时值**设置为 30 分钟，并且配置选项卡在新浏览器窗口中打开。

管理主页

管理服务主页为您提供 SDX 设备及其上预配的实例的性能概览。有关 SDX 设备和实例的信息显示在小工具中，您可以根据需要添加和删除这些小工具。

主页上默认提供以下小工具。

- **系统资源**：显示设备上的 CPU 核心总数、SSL 芯片总数、可用 SSL 芯片数、总内存和可用内存。
- **系统 CPU | 内存使用率 (%)**：以图形格式显示设备的 CPU 和内存利用率百分比。
- **系统 WAN/LAN 吞吐量 (Mbps)**：以实时绘制并定期更新的图表形式显示 SDX 设备传入和传出流量的总吞吐量。
- **NetScaler 实例**：显示 NetScaler 实例的属性。显示的属性包括名称、VM 状态、实例状态、IP 地址、Rx (Mbps)、Tx (Mbps)、HTTP 请求/秒以及 CPU 使用率 (%) 和内存使用率 (%)。注意：首次登录时，主页不显示与 NetScaler 实例相关的任何数据，因为您尚未在设备上预配任何实例。
- ****健康监控事件****：显示最近 25 个事件，包括其严重性、消息以及事件发生的日期和时间。

您可以在主页上执行以下操作：

- 查看和隐藏 NetScaler 实例详细信息

您可以通过单击“名称”列中的实例名称来查看和隐藏特定 NetScaler 实例的详细信息。您还可以单击“全部展开”以展开所有实例节点，并单击“全部折叠”以折叠所有实例节点。

- 添加和删除小工具

您还可以添加小工具来查看其他系统信息。

要添加这些小工具，请单击主页右上角的箭头 (<<) 按钮，在搜索框中输入关键字，然后单击 Go。允许的字符为：a-z、A-Z、0-9、\、\$、* 和 _。在搜索框中不输入任何字符而单击 Go 可显示所有可用小工具。显示小工具后，单击“添加到仪表板”。

目前，您可以将以下小工具添加到主页：

- **管理程序详细信息：**“管理程序详细信息”小工具显示有关 Citrix Hypervisor 正常运行时间、版本、iSCSI 限定名称 (IQN)、产品代码、序列号、构建日期和构建号的详细信息。
- **许可证：**“许可证”小工具显示以下详细信息：SDX 硬件平台、该平台支持的最大实例数、最大支持吞吐量 (Mbps) 和可用吞吐量 (Mbps)。

如果您删除了主页上默认可用的小工具，可以通过搜索该小工具将其重新添加回主页。

端口

SDX 设备上必须打开以下端口才能正常运行。

类型	端口	详细信息
TCP	80	用于传入的 HTTP (GUI 和 NITRO) 请求。是访问 SDX 管理服务界面的主要接口之一。
TCP	443	用于传入的安全 HTTP (GUI 和 NITRO) 请求。是访问 SDX 管理服务界面的主要接口之一。
TCP	22	用于 SSH 和 SCP 访问 SDX 管理服务界面。
UDP	162	SDX 管理服务界面侦听来自托管在 SDX 设备上的 NetScaler 实例的 SNMP 陷阱。

类型	端口	详细信息
UDP	161	SDX 管理服务接口监听 SNMP 遍历/获取请求。

数据治理

什么是 NetScaler Console 服务连接？

NetScaler Application Delivery Management (ADM) 服务连接是一项功能，可实现 NetScaler SDX 设备无缝载入 NetScaler Console 服务。此功能使 NetScaler SDX 设备能够自动安全地连接到 NetScaler Console 服务，并向其发送系统、使用情况和遥测数据。根据这些数据，您可以在 NetScaler Console 服务上获得有关 NetScaler 基础设施的洞察和建议。

通过使用 NetScaler Console 服务连接功能并将您的 NetScaler SDX 设备载入 NetScaler Console 服务，您可以管理所有本地或云端的 NetScaler 和 NetScaler Gateway 资产。此外，您还可以受益于访问丰富的可见性功能集，这些功能有助于快速识别性能问题、高资源使用率、关键错误等。NetScaler Console 服务为您的 NetScaler 实例和应用程序提供了广泛的功能。有关 NetScaler Console 服务的更多信息，请参阅 [NetScaler Application Delivery Management Service](#)。

重要

- 本文档适用于 NetScaler SDX 设备。有关 NetScaler 设备的更多信息，请参阅 [NetScaler 设备 NetScaler Console 服务连接简介](#)。
- NetScaler Gateway 也支持 NetScaler Console 服务连接功能。为方便起见，在后续章节中未明确提及 NetScaler Gateway 设备。

注意： NetScaler Console 服务连接功能已针对 NetScaler 实例和 NetScaler Gateway 实例发布。但是，NetScaler Console 服务上的相应功能将在即将发布的版本中提供。此功能的价值将很快随着 NetScaler Console 服务版本的发布而释放。Citrix 将在发布时更新此说明。一旦在 NetScaler Console 服务上发布，即可使用此新功能的好处。

什么是 NetScaler Console 服务？

NetScaler Console 服务是一种基于云的解决方案，通过提供有关 NetScaler SDX 实例以及应用程序健康状况、性能和安全性的分析洞察和精选的基于机器学习的建议，帮助您管理、监控、编排、自动化和故障排除 NetScaler SDX 实例。有关更多信息，请参阅 [NetScaler Console 服务概述](#)。

如何启用 NetScaler Console 服务连接？

在您安装或升级 NetScaler SDX 到 13.1 版本后，NetScaler Console 服务连接默认启用。

使用 NetScaler Console 服务连接捕获哪些数据？

使用 NetScaler Console 服务连接捕获以下详细信息：

- **NetScaler SDX 详细信息**

- 管理 IP 地址
- 平台描述
- 平台类型
- 主机名
- 系统 ID
- 编码序列 ID
- 版本
- 序列 ID
- 主机 ID
- 类型
- 构建类型

- **关键使用指标**

- 管理 CPU 百分比
- 内存使用百分比
- CPU 使用百分比
- 系统正常运行时间
- 系统日期时间

数据是如何使用的？

通过收集数据，NetScaler 可以提供有关您的 NetScaler SDX 安装的及时且深入的见解，其中包括：

- **关键指标。**有关 CPU、内存、吞吐量、SSL 吞吐量的关键指标的详细信息，并突出显示 NetScaler SDX 实例上的异常行为。

- **严重错误。** 您的 NetScaler 实例上可能发生的任何严重错误。
- **部署建议。** 识别以独立模式部署但吞吐量高且容易出现单点故障的 NetScaler 实例。

收集的数据保留多长时间？

收集的任何数据保留时间不超过 13 个月。

如果您决定通过在 NetScaler 中禁用 NetScaler Console 服务连接功能来终止使用该服务，则任何先前收集的数据将在 30 天后删除。

数据存储在哪里以及安全性如何？

NetScaler Console 服务连接收集的所有数据都存储在以下三个区域之一：美国、欧盟以及澳大利亚和新西兰 (ANZ)。有关更多信息，请参阅 [地理注意事项](#)。

数据在数据库层以严格的租户隔离方式安全存储。

如何禁用 NetScaler Console 服务连接？

如果您想通过 NetScaler Console 服务连接禁用数据收集，请参阅 [如何启用和禁用 NetScaler Console 服务连接](#)。

NetScaler SDX 设备 Console Advisory Connect 简介

NetScaler Console 服务是一种基于云的解决方案，可帮助您管理、监控、编排、自动化 NetScaler SDX 设备并对其进行故障排除。它还为您的应用程序的运行状况、性能和安全性提供分析见解和精选的基于机器学习的建议。有关详细信息，请参阅 [NetScaler Console 服务](#)。

Console Advisory Connect 是一项功能，可实现将 NetScaler SDX 设备无缝载入 NetScaler Console 服务。此功能有助于 NetScaler SDX 设备和 NetScaler Console 服务作为整体解决方案运行，为客户提供多重优势。

Console Advisory Connect 功能使 NetScaler SDX 实例能够自动连接到 NetScaler Console 服务，并向其发送系统、使用情况和遥测数据。利用这些数据，NetScaler Console 服务会就您的 NetScaler SDX 基础架构提供一些见解和建议，例如快速识别性能问题和高资源使用率。

为了利用 NetScaler Console 服务的强大功能，您可以选择将 NetScaler SDX 设备载入 NetScaler Console 服务。载入过程使用 Console Advisory Connect，使您的体验无缝且更快。

注意要点

- Console Advisory Connect 现已在 NetScaler MPX、SDX 和 VPX 实例以及 NetScaler Gateway 设备上可用。

有关详细信息，请参阅 [数据治理](#)。

Console Advisory Connect 如何支持 NetScaler Console 服务？

以下是 NetScaler 上的 Console Advisory Connect 功能如何与 NetScaler Console 服务交互的高级工作流程。

1. NetScaler SDX 设备上的 Console Advisory Connect 功能使用周期性探测请求自动连接到 NetScaler Console 服务。
2. 此请求包含系统、使用情况和遥测数据，NetScaler Console 服务会利用这些数据就您的 NetScaler 基础架构提供一些见解和建议，例如快速识别性能问题和高资源使用率。

3. 您可以查看这些见解和建议，并决定将 NetScaler SDX 设备载入 NetScaler Console 服务，以开始管理您的 NetScaler SDX 设备。
4. 当您决定载入时，Console Advisory Connect 功能有助于无缝完成载入。

哪些版本的 NetScaler 支持 Console Advisory Connect?

Console Advisory Connect 在所有 NetScaler 平台和所有设备型号（MPX、VPX 和 SDX）上均受支持。从 NetScaler 13.0 版本 build 64.xx 开始，Console Advisory Connect 默认在 NetScaler SDX 设备上启用。

如何启用 Console Advisory Connect?

如果您是现有的 NetScaler 客户，并升级到 NetScaler 13.0 版本 build 64.xx，Console Advisory Connect 将作为升级过程的一部分默认启用。

如果您是新的 NetScaler 客户，安装 NetScaler 13.0 版本 build 64.xx，Console Advisory Connect 将作为安装过程的一部分默认启用。

注意

与新的 NetScaler 设备不同，现有的 NetScaler SDX 设备通过 Citrix Insight Service (CIS) 或 Call Home 查找路由。

如何启用和禁用 Console Advisory Connect?

您可以通过 CLI、GUI 或 NITRO API 方法启用和禁用 Console Advisory Connect。

使用 CLI

使用 CLI 启用 Console Advisory Connect

在命令提示符下，键入：

```
set autoreg_setting autoreg=true
```

使用 CLI 禁用 Console Advisory Connect

在命令提示符下，键入：

```
set autoreg_setting autoreg=false
```

使用 CLI 显示 Console Advisory Connect 设置

```
show autoreg_setting
```

```
autoreg: true
```

```
is_banner_displayed: true
```

Done

使用 GUI

使用 NetScaler GUI 禁用 Console Advisory Connect

1. 导航到 **System**。在 **System** 页面上，单击 **System Settings** 部分下的 **Configure Console Advisory Connect**。
2. 在 **Configure NetScaler Console Parameters** 页面上，清除 **Enable Console Advisory Connect**，然后单击 **OK**。

← Configure Console Advisory Connect

☐ Enable Console Advisory Connect

This feature helps you discover your NetScaler SDX effortlessly on NetScaler Console service and get insights and curated machine learning based recommendations for applications and NetScaler SDX infrastructure. This feature lets the NetScaler SDX instance automatically send system, usage and telemetry data to NetScaler Console service.

Click [here](#) to learn more about this feature.

You can also configure this feature anytime on the NetScaler SDX appliance using the SDX command line interface or GUI. For NetScaler VPX instances running on SDX, you can configure this feature anytime using the NetScaler VPX command line interface, API or GUI Settings.

Use of this feature is subject to the Citrix End User Service Agreement [here](#)

Save

Close

使用 NITRO API

您可以使用 NITRO 命令禁用 Console Advisory Connect。

```
curl -X PUT -H "Content-Type:application/json" http://192.0.2.10/nitro/v1/config/sdx_autoreg -d '{"sdx_autoreg":{"autoreg":"false"}}' -u nsroot:Test@1
```

NetScaler Console 内置代理行为

从 NetScaler 13.0 build 61.xx 及更高版本开始，NetScaler SDX 实例具有内置代理，并带有 Console Advisory Connect 功能。NetScaler SDX 实例上可用的 NetScaler Console 内置代理作为活动守护程序启动，并与 NetScaler Console 服务通信。与 NetScaler Console 服务建立通信后，内置代理会定期自动升级到最新的软件版本。

参考

有关 Console Advisory Connect 的更多信息，请参阅以下主题：

- 数据治理：[数据治理](#)。
- NetScaler Console 服务：[NetScaler Console 服务](#)。

单一捆绑包升级

注意： 在您将 NetScaler SDX 设备安装或升级到 13.1 版本后，NetScaler Console 服务连接默认启用。有关更多详细信息，请参阅数据治理和 NetScaler Console 服务连接。

单一捆绑包升级将除 NetScaler VPX 实例映像之外的所有组件组合到一个映像文件中。此文件称为单一捆绑包映像 (SBI)。

注意：

Lights Out Management (LOM) 固件已添加到 SBI 中，Citrix® 客户无需单独升级 LOM。更新 LOM 可能会使升级过程增加长达 30 分钟。有关 LOM 的更多信息，请参阅 [NetScaler SDX 设备上的 Lights Out Management 端口](#)。

对于 SDX 9100 和 16000 平台，升级到包含较新 LOM 固件的 SBI 后，您必须手动触发 LOM 更新。

使用此映像，您可以一步升级所有组件，从而消除各种组件之间不兼容的可能性。单一捆绑包升级还可确保您的设备始终运行 Citrix® 经过测试和支持的版本。由于所有 SDX 组件都组合在一个文件中，因此 SDX 映像文件大于 Management Service 映像文件。

映像的文件名格式为 `build-sdx-13.1-<build_number>.tgz`。在 Management Service 升级到 SDX 13.1 后，新的 GUI 不会显示上传 Citrix Hypervisor 映像文件、补充包或热修复程序的选项。这些选项缺失是因为 SDX 13.1 不支持升级单个组件。

注意事项

- 单一捆绑包升级是一个多步骤过程，可能需要长达 90 分钟。
- 首先，Management Service 将升级到较新的提供版本。在升级过程中，与 Management Service 的连接可能会丢失。重新连接到 Management Service 以监视升级状态。
- 接下来，新的 Management Service 会升级 Citrix Hypervisor 并完成设备的其余升级。11.0 及更高版本的 Management Service 可以执行完整的 Citrix Hypervisor 升级。
- 在 Citrix Hypervisor™ 升级期间，请勿重新启动设备。
- Citrix recommends that you use a Citrix Hypervisor serial console (or LOM console) to monitor the Citrix Hypervisor upgrade.

将整个设备升级到 13.1

注意：升级过程会多次重启整个 SDX 设备，包括所有 VPX 实例。在执行此过程之前，如果 VPX 实例处于 HA 设置中，请将所有主 HA 节点故障转移到辅助节点。如果您没有 HA 部署，请相应地规划停机时间。

升级设备：

1. 上传单个捆绑包映像文件，导航到 **Configuration > Management Service > Software Images**，然后单击 **Upload**。
2. 导航到 **配置 > 系统 > 系统管理**。
3. 在“System Administration”组中，单击 **Upgrade Appliance**。升级过程需要几分钟。

升级前，管理服务会显示以下信息：

- 单个捆绑包映像文件名。
- 设备上运行的 SDX 当前版本。
- 设备将升级到的选定版本。
- 升级设备的大致时间。
- 其他信息。

在单击 **Upgrade Appliance** 之前，请确保您已查看屏幕上显示的所有信息。升级过程一旦开始，就无法中止。

支持的升级路径

出厂映像	升级到 12.1	升级到 13.1	升级到 14.1
10.5 (EoL)	不支持；用更新的镜像替换 FRU 启动盘	不支持；用更新的镜像替换 FRU 启动盘	不支持；用更新的镜像替换 FRU 启动盘
11.0 (EoL)	不支持；用更新的镜像替换 FRU 启动盘	不支持；用更新的镜像替换 FRU 启动盘	不支持；用更新的镜像替换 FRU 启动盘
11.1 (EoL)	支持（到 12.1-56.x 及更高版本）	仅支持到 12.1 版本	仅支持到 13.1 版本
12.1	不推荐	支持	仅支持到版本 13.1

出厂映像	升级到 12.1	升级到 13.1	升级到 14.1
13.0 (生命周期结束)	不支持；避免从 13.0 升级	不支持；避免从 13.0 升级	不支持；避免从 13.0 升级
13.1	不适用	支持	支持
14.1	不适用	不适用	支持

相关信息

[NetScaler SDX 硬件-软件兼容性矩阵](#)

升级 NetScaler 实例

注意

- 在将 NetScaler SDX 设备安装或升级到 13.1 版本后，NetScaler Console 服务连接默认启用。有关更多详细信息，请参阅[数据治理](#)和[NetScaler Console 服务连接](#)。
- 从 13.1 版本 build 37.x 及更高版本开始，NetScaler SDX 设备升级过程只需要一次重新启动，而不是两次。

升级 NetScaler 实例的过程包括上传构建文件，然后升级 NetScaler 实例。

重要

不支持使用管理服务降级 ADC 实例。请使用实例 CLI 进行降级。

在升级 NetScaler 实例之前，请将 NetScaler 软件映像上传到 NetScaler SDX 设备。要安装新实例，您需要 NetScaler XVA 文件。

在“软件映像”窗格中，您可以查看以下详细信息。

- 名称：** NetScaler 实例软件映像文件的名称。文件名包含版本号和内部版本号。例如，文件名 build-10-53.5_nc.tgz 指的是版本 10 build 53.5。
- 上次修改时间：** 文件上次修改的日期。
- 大小：** 文件大小（以 MB 为单位）。

上传软件映像

1. 在导航窗格中，展开 NetScaler，然后单击“软件映像”。
2. 在“软件映像”窗格中，单击“上传”。
3. 在“上传 NetScaler 软件映像”对话框中，单击“浏览”并选择要上传的 NetScaler 映像文件。
4. 单击“上传”。映像文件将显示在 NetScaler 软件映像窗格中。

通过下载构建文件创建备份

1. 在“软件映像”窗格中，选择要下载的文件，然后单击“下载”。
2. 在消息框中，从“保存”列表中选择“另存为”。
3. 在“另存为”消息框中，浏览到要保存文件的位置，然后单击“保存”。

上传 XVA 文件

1. 在导航窗格中，展开 NetScaler，然后单击“软件映像”。
2. 在“软件映像”窗格中，在“XVA 文件”选项卡上，单击“上传”。
3. 在“上传 NetScaler XVA 文件”对话框中，单击“浏览”并选择要上传的 NetScaler XVA 文件。
4. 单击“上传”。XVA 文件将显示在“XVA 文件”窗格中。

通过下载 XVA 文件创建备份

1. 在“XVA 文件”窗格中，选择要下载的文件，然后单击“下载”。
2. 在消息框中，从“保存”列表中选择“另存为”。
3. 在“另存为”消息框中，浏览到要保存文件的位置，然后单击“保存”。

升级 NetScaler VPX 实例

您可以使用管理服务升级设备上运行的一个或多个 VPX 实例。在升级实例之前，请确保您已将正确的版本上传到 SDX 设备。

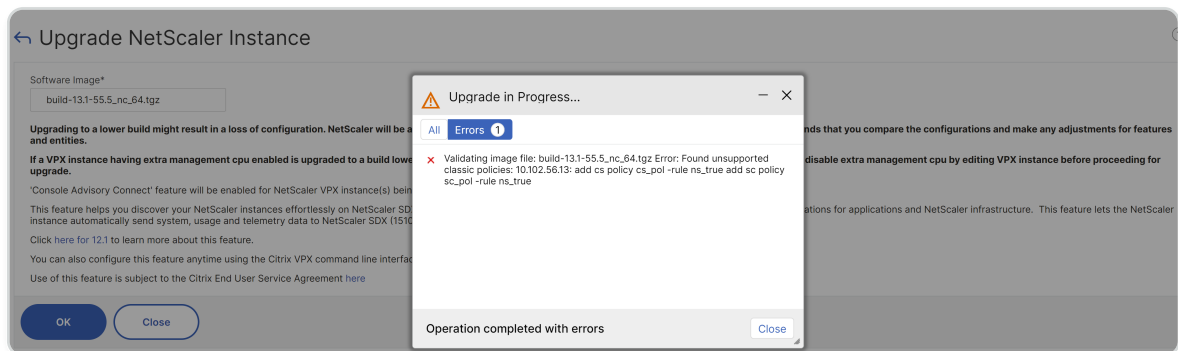
在开始升级任何实例之前，请确保您了解许可框架和许可证类型。软件版本升级（例如从标准版到企业版，或从企业版到白金版）可能需要新的许可证。另请注意以下事项：

- 为防止任何配置丢失，请在升级任何实例之前保存每个实例上的配置。
- 您还可以从“实例”节点升级单个实例。为此，请从“实例”节点中选择该实例。在详细信息窗格中，选择该实例，然后在“操作”下拉菜单中单击“升级”。

重要

- 如果您使用 SDX 管理服务而不是 VPX GUI 升级 VPX 实例，升级映像是备份文件的一部分，可让您顺利恢复实例。
- 如果您的配置包含经典策略，则在升级实例时可能会收到错误“发现不支持的经典策略”。在这种情况下，您必须手动将经典策略转换为高级策略。有关详细信息，请参阅 [NetScaler 经典策略功能和特性状态变更公告](#)。

以下是错误消息示例：



升级 VPX 实例

1. 在“配置”选项卡上，在导航窗格中，单击“NetScaler”。
2. 在详细信息窗格中，在“NetScaler 配置”下，单击“升级”。
3. 在“升级 NetScaler”对话框中，在“软件映像”中，选择要升级到的 NetScaler 升级版本构建文件。
4. 从“实例 IP 地址”下拉列表中，选择要升级的实例的 IP 地址。
5. 单击“确定”，然后单击“关闭”。

相关信息

[NetScaler SDX 硬件-软件兼容性矩阵](#)

管理和监控 SDX 设备

NetScaler SDX 设备启动并运行后，您可以从管理服务用户界面执行各种任务来管理和监控设备。

修改 SDX 设备的网络配置

您可以修改在初始配置期间为 SDX 设备提供的网络配置详细信息。

要修改 SDX 设备的网络配置，请单击“**系统**”。在“**系统**”窗格的“**设置设备**”组下，单击“**网络配置**”，然后在向导中输入详细信息。

注意：在“**网络配置**”中，当您启用对 Citrix Hypervisor™ 的访问时，将显示警告消息“访问将在六小时后自动禁用”。

更改默认用户帐户的密码

默认用户帐户提供对 NetScaler SDX 设备所有功能的完全访问权限。为确保安全，仅在必要时使用默认管理员帐户。只有职责需要完全访问权限的个人才必须知道默认管理员帐户的密码。Citrix 建议经常更改默认管理员密码。如果忘记密码，可以通过将设备设置恢复为出厂默认设置来将密码重置为默认值，然后可以更改密码。

要更改默认用户帐户的密码，请单击“**系统**”>“**用户管理**”>“**用户**”。选择一个用户，然后单击“**编辑**”以更改密码。

修改设备的区域时区

您可以修改管理服务和 Citrix Hypervisor 的时区。默认时区为 UTC。

要修改时区，请单击“**系统**”，然后在“**系统设置**”组中单击“**更改时区**”。

修改设备的主机名

您可以通过导航到“**系统 > 系统设置 > 更改主机名**”来更改管理服务的主机名。Citrix Hypervisor 主机名将在备份/恢复操作期间进行备份和恢复。在配置重置期间，Citrix Hypervisor 主机名将重置为默认值“netscaler-sdx”。

VLAN 过滤

VLAN 过滤提供共享物理端口的 VPX 实例之间的数据隔离。例如，如果您在两个不同的 VLAN 上配置了两个 VPX 实例并启用了 VLAN 过滤，则一个实例无法查看另一个实例的流量。如果禁用 VLAN 过滤，所有实例都可以看到标记或未标记的广播数据包，但数据包会在软件级别被丢弃。如果启用 VLAN 过滤，每个标记的广播数据包只到达属于相应标记 VLAN 的实例。如果没有实例属于相应的标记 VLAN，则数据包会在硬件级别 (NIC) 被丢弃。

如果在接口上启用了 VLAN 过滤，则该接口上可以使用有限数量的标记 VLAN。10G 接口上为 63 个标记 VLAN，1G 接口上为 32 个标记 VLAN。VPX 实例只接收具有已配置 VLAN ID 的数据包。如果您在该接口上将 VLAN 过滤器的状态从 DISABLED 更改为 ENABLED，请重新启动与该接口关联的 VPX 实例。

SDX 设备上默认启用 VLAN 过滤。如果您在接口上禁用 VLAN 过滤，则可以在该接口上配置多达 4096 个 VLAN。

注意：VLAN 过滤只能在运行 Citrix Hypervisor 6.0 版本的 SDX 设备上禁用。

要在接口上启用 VLAN 过滤，请单击 **System > Interfaces**。选择一个接口，然后单击 **VLAN Filter** 并输入详细信息以启用 VLAN 过滤。

配置时钟同步

启用网络时间协议 (NTP) 同步时，管理服务将重新启动。您可以将 SDX 设备配置为与 NTP 服务器同步其本地时钟。因此，SDX 设备上的时钟将与网络上的其他服务器具有相同的日期和时间设置。如果设备重新启动、升级或降级，时钟同步配置不会改变。但是，该配置不会传播到高可用性设置中的辅助 NetScaler 实例。

如果您添加 NTP 服务器或更改任何身份验证参数，时钟会立即同步。您还可以显式启用和禁用 NTP 同步。

注意：如果您没有本地 NTP 服务器，您可以在官方 NTP 站点找到公共、开放访问的 NTP 服务器列表，<http://www.ntp.org>。在将 NetScaler 配置为使用公共 NTP 服务器之前，请务必阅读“参与规则”页面（链接包含在所有公共时间服务器页面上）。

要配置 NTP 服务器，请单击 **System > NTP Servers**。

启用 NTP 同步

1. 在导航窗格中，展开 **System**，然后单击 **NTP Servers**。
2. 在详细信息窗格中，单击 **NTP Synchronization**。
3. 在 **NTP Synchronization** 对话框中，选择 **Enable NTP Sync**。

4. 单击 **OK**，然后单击 **Close**。

修改身份验证选项

1. 在导航窗格中，展开“**系统**”，然后单击“**NTP 服务器**”。
2. 在详细信息窗格中，单击“**身份验证参数**”。
3. 在“**修改身份验证选项**”对话框中，设置以下参数：
 - **身份验证**—启用 NTP 身份验证。可能的值：YES、NO。默认值：YES。
 - **受信任密钥 ID**—受信任的密钥 ID。添加 NTP 服务器时，从此列表中选择一个密钥标识符。
最小值：1。最大值：65534。
 - **吊销间隔**—Autokey 方案使用的某些加密值重新随机化的间隔，以 2 的幂表示，单位为秒。
默认值：17 ($2^{17}=36$ 小时)。
 - **自动最大间隔**—Autokey 协议使用的会话密钥列表重新生成的间隔，以 2 的幂表示，单位为秒。默认值：12 ($2^{12}=1.1$ 小时)。
4. 单击“**确定**”，然后单击“**关闭**”。

查看 SDX 设备属性

在“**配置**”选项卡上，查看系统属性，例如 CPU 核心数和 SSL 芯片数、总可用内存和空闲内存以及各种产品详细信息。

要查看 SDX 设备的属性，请单击“**配置**”选项卡。

您可以查看有关系统资源、管理程序、许可证和系统的以下信息：

系统资源：

- **CPU 总核心数**：SDX 设备上的 CPU 核心数。
- **SSL 芯片总数**：SDX 设备上的 SSL 芯片总数。
- **空闲 SSL 芯片**：尚未分配给实例的 SSL 芯片总数。
- **总内存 (GB)**：设备总内存（以 GB 为单位）。
- **空闲内存 (GB)**：空闲设备内存（以 GB 为单位）。

管理程序信息：

- **运行时间**：自设备上上次重新启动以来的时间，以天、小时和分钟为单位。
- **版本**：安装在 SDX 设备上的 Citrix Hypervisor 版本。
- **版本**：安装在 SDX 设备上的 Citrix Hypervisor 版本。

- **iSCSI IQN**：iSCSI 限定名称。
- **产品代码**：Citrix Hypervisor 的产品代码。
- **序列号**：Citrix Hypervisor 的序列号。
- **内部版本日期**：Citrix Hypervisor 的内部版本日期。
- **内部版本号**：Citrix Hypervisor 的内部版本号。
- **补充包**：安装在 SDX 设备上的补充包版本。

许可证信息：

- **平台**：硬件平台的型号，基于已安装的许可证。
- **最大实例数**：您可以在 SDX 设备上设置的最大实例数，基于已安装的许可证。
- **可用实例数（共享）**：可配置的实例数，取决于仍然可用的 CPU 核心数。
- **最大吞吐量 (Mbps)**：设备上可达到的最大吞吐量，基于已安装的许可证。
- **可用吞吐量 (Mbps)**：基于已安装的许可证的可用吞吐量。

系统信息：

- **平台**：硬件平台的型号。
- **产品**：NetScaler® 产品的类型。
- **版本**：在 SDX 设备上运行的 NetScaler 版本和内部版本。
- **IP 地址**：管理服务的 IP 地址。
- **主机 ID**：Citrix Hypervisor 主机 ID。
- **系统 ID**：Citrix Hypervisor 系统 ID。
- **序列号**：Citrix Hypervisor 序列号。
- **系统时间**：以“日 月 日期 时:分:秒 时区 年”格式显示的系统时间。
- **运行时间**：自管理服务上次重新启动以来的时间，以天、小时和分钟为单位。
- **BIOS 版本**：BIOS 版本。

查看设备的实时吞吐量

SDX 设备传入和传出流量的总吞吐量以实时图表形式绘制，并定期更新。默认情况下，传入和传出流量的吞吐量会一起绘制在图表上。

要查看 SDX 设备的吞吐量，请在 GUI 上单击 **Dashboard**，然后选中 **System Throughput (Mbps)**

。

查看实时 CPU 和内存使用情况

您可以查看设备的 CPU 和内存使用情况图表。该图表实时绘制并定期更新。

要查看 SDX 设备的 CPU 和内存使用情况，请在 GUI 上单击 **Dashboard**，然后选中 **Management Service Statistics**。

查看所有核心的 CPU 使用情况

您可以查看 SDX 设备上每个 CPU 核心的使用情况。

CPU 核心使用情况窗格显示以下详细信息：

- **核心编号**：设备上的 CPU 核心编号。
- **物理 CPU**：该核心的物理 CPU 编号。
- **超线程**：与该 CPU 核心关联的超线程。
- **实例**：正在使用该 CPU 核心的实例。
- **平均核心使用率**：平均核心使用率，以百分比表示。

要查看 SDX 设备上所有核心的 CPU 使用率，请在 GUI 上单击 **Dashboard** 并选中 **System CPU Usage (%)**。

在 SDX 设备上安装 SSL 证书

SDX 设备随附默认 SSL 证书。出于安全原因，您可能希望用自己的 SSL 证书替换此证书。为此，您必须首先将 SSL 证书上传到管理服务，然后安装该证书。安装 SSL 证书会终止与管理服务的所有当前客户端会话。登录管理服务以执行任何其他配置任务。

要安装 SSL 证书，请单击 **System**。在 **Set Up Appliance** 组中，单击 **Install SSL Certificate** 并在向导中输入详细信息。

查看管理服务上的 SSL 证书

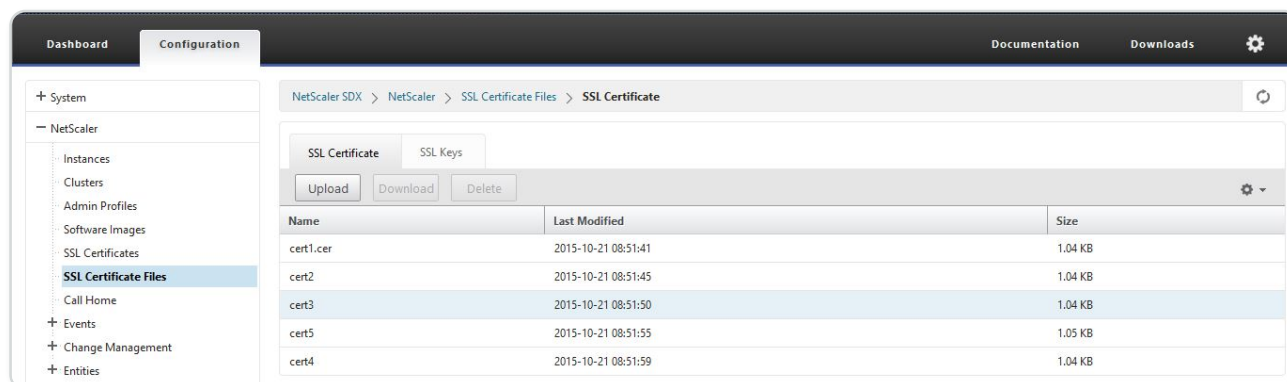
管理服务使用 SSL 证书进行安全的客户端连接。查看此证书的详细信息，例如有效期状态、颁发者、主题、到期天数、有效期起止日期、版本和序列号。

要查看 SSL 证书，请单击 **System**，然后在 **Set Up Appliance** 组中，单击 **View SSL Certificate**。

NetScaler 实例的 SSL 证书和密钥

NetScaler 实例的 SSL 证书和密钥的单独视图提供了增强的可用性。使用新的管理服务节点“SSL Certificate Files”来上传和管理可安装在 NetScaler 实例上的 SSL 证书以及相应的公钥和私钥对。

要访问 NetScaler 实例的 SSL 证书和密钥，请导航到 **Configuration > NetScaler > SSL Certificate Files**。



修改系统设置

出于安全原因，您可以指定管理服务和 VPX 实例之间只能通过安全通道进行通信。您还可以限制对管理服务用户界面的访问。客户端只能通过 HTTPS 登录管理服务用户界面。

要修改系统设置，请单击 **Configuration > System**，然后在“System Settings”组中，单击 **Change System Settings**。

重新启动设备

管理服务提供重启 SDX 设备选项。重启期间，设备会关闭所有托管实例，然后重启 Citrix Hypervisor。Citrix Hypervisor 重启后，它会启动所有托管实例以及管理服务。

要重启设备，请单击 **Configuration > System**，然后在“系统管理”组中单击 **Reboot Appliance**。

关闭设备

您可以从管理服务关闭 SDX 设备。

要关闭设备，请单击 **Configuration > System**，然后在“系统管理”组中单击 **Shut Down Appliance**

。

SDX 管理域

SDX 管理域功能可帮助您创建多个管理域。您可以使用管理域来隔离不同部门的资源。因此，管理域可以提高对资源的控制，并且资源可以在各个域之间分配以实现最佳利用。

SDX 设备附带固定资源，例如 CPU 核心、数据吞吐量、内存、磁盘空间、SSL 芯片以及可预置的特定实例数量。您可以创建的实例数量取决于许可证。

SDX 设备最多支持三级管理域。设备出厂时，所有资源都分配给所有者。

您创建的任何管理域都是所有者域的子域。在每种情况下，子域的资源都从父域的资源池中分配。管理域中的用户可以访问该域的资源。他们无权访问同一层级中其他域的资源，也无权访问尚未分配给其域的父域资源。但是，父域中的用户可以访问该域子域的资源。

将资源分配给子域的示例

表 1 列出了默认根域的资源。SDX 管理员可以将这些资源分配给子域。在此示例中，管理员最多可以分配 10 个 CPU 核心和 840 GB 磁盘空间。

表 1. 所有者资源

CPU 核心	10
吞吐量 (Mbps)	18500
内存 (MB)	87300
磁盘空间 (GB)	840
SSL 芯片	36
实例	36

表 2 列出了分配给名为 *Test* 的子域的资源。此子域已分配其父域 10 个 CPU 核心中的 5 个，剩余 5 个核心可分配给所有者的其他子域。

表 2. Test 域的资源

CPU 核心	5
吞吐量 (Mbps)	1024

内存 (MB)	2048
磁盘空间 (GB)	40
SSL 芯片	8
实例	4

创建子域时，*Test* 域管理员只能分配表 2 中列出的资源。*Test* 域只能有一个级别的子域，因为只能创建三个级别的域。

下图显示了子域之间资源分配的另一个示例，其中使用的值与表 1 和表 2 中所列的值不同。

要创建管理域，请导航到 **Configuration > System > Administrative Domain** 并选择所需的选项。按照屏幕上的说明进行操作。创建新域后，使用管理服务的登录页面登录此域，并提供域名和用户名。例如，如果您创建了一个名为 *NewDomain* 的域，其中包含用户 *NewUser*，则以 *NewDomain\NewUser* 身份登录。

将用户分配给域

创建子域时，会自动创建两个用户组：一个管理员组和一个只读组。默认情况下，每个用户都属于管理员组。用户可以添加到多个组。

在 SDX 22000 平台上管理 RAID 磁盘分配

NetScaler SDX 22040/22060/22080/22100/22120 设备现在包含一个独立磁盘冗余阵列 (RAID) 控制器，该控制器最多可支持八个物理磁盘。多个磁盘不仅可以提高性能，还可以增强可靠性。可靠性对于 SDX 设备尤为重要，因为该设备托管许多虚拟机，并且磁盘故障会影响多个虚拟机。管理服务上的 RAID 控制器支持 RAID 1 配置，该配置实现了磁盘镜像。也就是说，两个磁盘维护相同的数据。如果 RAID 1 阵列中的一个磁盘发生故障，其镜像会立即提供所有所需数据。

RAID 1 磁盘镜像将两个物理驱动器组合成一个逻辑驱动器。逻辑驱动器的可用容量相当于其一个物理驱动器的容量。例如，组合两个 1 TB 驱动器会创建一个总可用容量为 1 TB 的单个逻辑驱动器。这种驱动器组合在设备看来是一个单一的逻辑驱动器。

SDX 设备出厂时带有一个配置，其中包括逻辑驱动器 0 和逻辑驱动器 1。逻辑驱动器 0 分配给管理服务和 Citrix Hypervisor，逻辑驱动器 1 分配给您预置的 NetScaler 实例。要使用更多物理驱动器，您必须创建新的逻辑驱动器。

查看驱动器属性和操作

SDX 设备最多支持八个物理驱动器插槽，即设备两侧各有一对四个插槽。您可以将物理驱动器插入插槽中。在使用物理驱动器之前，必须将其作为逻辑驱动器的一部分。

在管理服务中，**Configuration > System > RAID** 屏幕包含逻辑驱动器、物理驱动器和存储库的选项卡。

逻辑驱动器

在 **Configuration > System > RAID > Logical Drives** 选项卡上，您可以查看每个逻辑驱动器的名称、状态、大小以及有关其组成物理驱动器的信息。下表描述了虚拟驱动器的状态。

状态	描述
最佳	虚拟驱动器运行状况良好。所有已配置的驱动器均在线。
降级	虚拟驱动器运行状况不佳。其中一个已配置的驱动器已发生故障或处于离线状态。
失败	虚拟驱动器已失败。
脱机	虚拟驱动器对 RAID 控制器不可用。

您还可以通过选择逻辑驱动器并单击 **Show Physical Drive** 来查看与逻辑驱动器关联的物理驱动器的详细信息。

创建新的逻辑驱动器

1. 导航到 **Configuration > System > RAID**，然后选择 **Logical Drives** 选项卡。
2. 单击 **Add**。
3. 在 **Create Logical Disk** 对话框中，选择两个包含运行正常的物理驱动器的插槽，然后单击 **Create**。

物理驱动器

SDX 设备最多支持八个物理插槽，即设备两侧各有一对四个插槽。在 **Configuration > System > RAID > Physical Drives** 选项卡上，您可以查看以下信息：

- **插槽**：—与物理驱动器关联的物理插槽。
- **大小**：—物理驱动器的大小。

- **固件状态：**—固件的状态。可能的值：
 - **联机，已启动：**—物理驱动器已启动并由 RAID 控制。
 - **未配置（良好）：**—物理驱动器状况良好，可以作为逻辑驱动器对的一部分添加。
 - **未配置（不良）：**—物理驱动器状况不佳，不能作为逻辑驱动器的一部分添加。
- **外部状态：**—指示磁盘是否为空。
- **逻辑驱动器：**—关联的逻辑驱动器。

在**物理驱动器**窗格中，您可以对物理驱动器执行以下操作：

- **初始化：**—初始化磁盘。如果物理驱动器状态不佳，并且必须作为逻辑驱动器对的一部分添加，则可以对其进行初始化。
- **重建：**—启动驱动器重建。当驱动器组中的某个驱动器发生故障时，您可以通过重新创建故障前存储在该驱动器上的数据来重建该驱动器。RAID 控制器会重新创建存储在驱动器组中其他驱动器上的数据。
- **定位：**—在设备上定位驱动器，通过使与该驱动器关联的驱动器活动 LED 闪烁来指示。
- **停止定位：**—停止在设备上定位驱动器。
- **准备移除：**—停用选定的物理驱动器，以便可以将其移除。

存储库

在**配置 > 系统 > RAID > 存储库**选项卡上，您可以查看 SDX 设备上存储库的状态。您还可以查看未连接的存储库驱动器的信息，并且可以通过选择该驱动器然后单击**移除**来移除此类驱动器。**存储库**选项卡显示每个存储库的以下信息：

- **名称：**—存储库驱动器的名称。
- **驱动器是否已连接：**—存储库是否已连接。如果驱动器未连接，您可以单击**移除**进行删除。
- **大小：**—存储库的大小。
- **已用空间：**—正在使用的存储库空间量。

向 SDX 22000 设备添加逻辑驱动器

要向 SDX 22000 平台添加额外的逻辑驱动器，请执行以下操作：

1. 登录到管理服务。
2. 导航到 **配置 > 系统 > RAID**。
3. 在 SDX 22000 设备背面，将两个空白 SSD 插入插槽号 4 和 5。您可以在运行中的系统中添加 SSD。注意：确保 SSD 经过 NetScaler® 认证。

4. 在管理服务中，导航到 **Configuration > System > RAID** 和 **Physical Drives** 选项卡。您将看到已添加的 SSD。
5. 导航到 **Logical Drive** 选项卡，然后单击 **Add**。
6. 在 **Create Logical Disk** 页面中：
 - a. 在 **First Slot** 下拉列表中，选择 4。
 - b. 在 **Second Slot** 下拉列表中，选择 5。
 - c. 单击 **Create**。

注意： 在管理服务中，插槽编号从零开始。因此，管理服务中的插槽编号与物理设备上的插槽编号不同。

逻辑驱动器已创建并列在 **逻辑驱动器选项卡** 下。单击刷新图标以更新逻辑驱动器的顺序。

在 SDX 22000 设备上添加第二个逻辑驱动器

要添加另一个逻辑驱动器，请将 SSD 插入插槽号 6 和 7。在 **创建逻辑磁盘** 页面中，从“**第一个插槽**”列表中选择 6，然后从“**第二个插槽**”列表中选择 7。

用空白 SSD 驱动器替换有故障的 SSD 驱动器

要用空白 SSD 驱动器替换有故障的 SSD 驱动器，请执行以下操作：

1. 导航到“**配置 > 系统 > RAID**”。
2. 在“**物理驱动器**”选项卡上，选择要替换的有故障驱动器。
3. 单击“**准备移除**”以移除驱动器。
4. 单击刷新图标以刷新物理驱动器列表。
5. 从插槽中物理移除有故障的驱动器。
6. 将新的 Citrix® 验证 SSD 插入您移除有故障 SSD 的插槽中。
7. 在管理服务中，导航到“**配置 > 系统 > RAID**”。新 SSD 将列在“**物理驱动器**”部分。驱动器重建过程将自动开始。

单击刷新图标以检查重建过程的状态。重建过程完成后，您可以在 **固件状态** 列中看到“联机”、“已启动”状态。

SDX 许可概述

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 Flexed 许可证 (CPL/UHMC)、传统 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 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。

所有其他形式的传统 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。

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。

许可证激活服务

许可证激活服务 (LAS) 是一种新的基于云的许可解决方案，可替代传统的基于文件的许可。LAS 引入了新的模块，用于激活 Citrix 和 NetScaler 产品，确保了许可证管理的无缝和现代化方法。

注意：

LAS 是一种许可机制，而不是许可类型。

有关详细信息，请参阅 [许可证激活服务](#)。

在 SDX 设备上管理许可证

注意：

有关许可详细信息，请参阅 NetScaler SDX 管理服务用户界面。

在 NetScaler SDX 管理服务中，您可以使用硬件序列号 (HSN) 或许可证访问代码来分配许可证。管理服务软件会在内部获取设备的序列号，而 Citrix 会在您购买许可证时通过电子邮件发送许可证访问代码。

另外，如果许可证已存在于本地计算机上，则可以将其上传到设备。

对于所有其他功能，例如退回或重新分配许可证，您必须使用许可门户。或者，您仍然可以使用许可门户进行许可证分配。有关详细信息，请参阅 [在 citrix.com 上管理许可证](#)。

有关 SDX 许可选项的信息，请参阅：

- [选择正确的平台和版本选项](#)。
- [许可模型](#)

注意： 安装永久许可证或池许可证不需要重新启动 SDX 设备。

先决条件

要使用硬件序列号或许可证访问代码分配许可证：

1. 您必须能够通过设备访问公共域。例如，设备必须能够访问 www.citrix.com。许可证分配软件会在内部访问 Citrix 许可门户以获取您的许可证。要访问公共域，您必须配置管理服务 IP 地址并设置 DNS 服务器。
2. 您的许可证必须与您的硬件关联，或者您必须拥有有效的许可证访问代码。

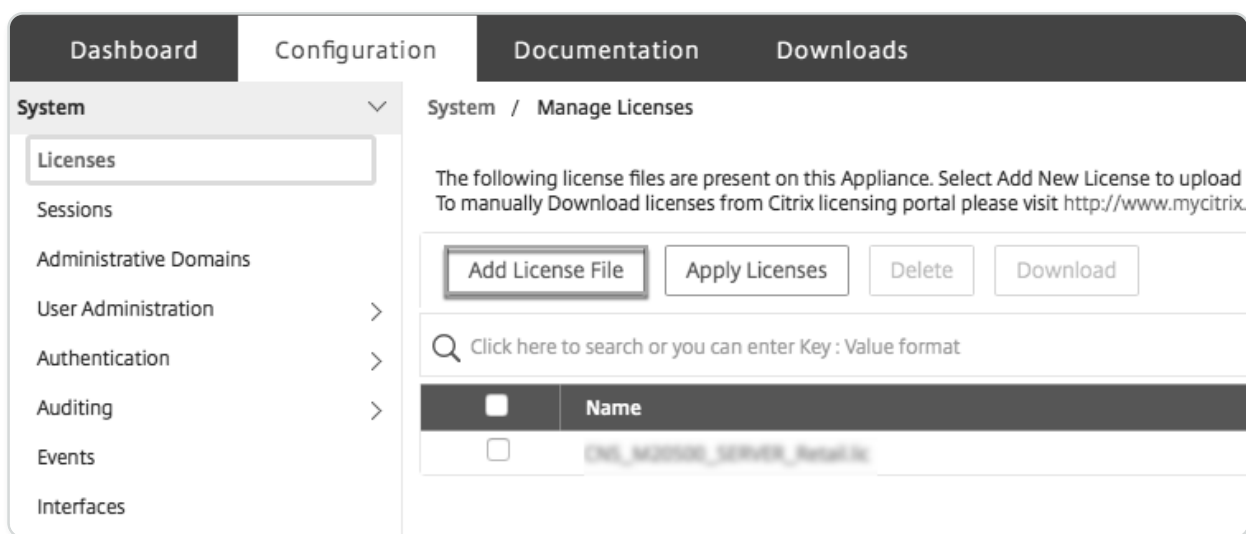
使用管理服务分配许可证

如果您的许可证已与您的硬件关联，则许可证分配过程可以使用硬件序列号。否则，您必须键入许可证访问代码。

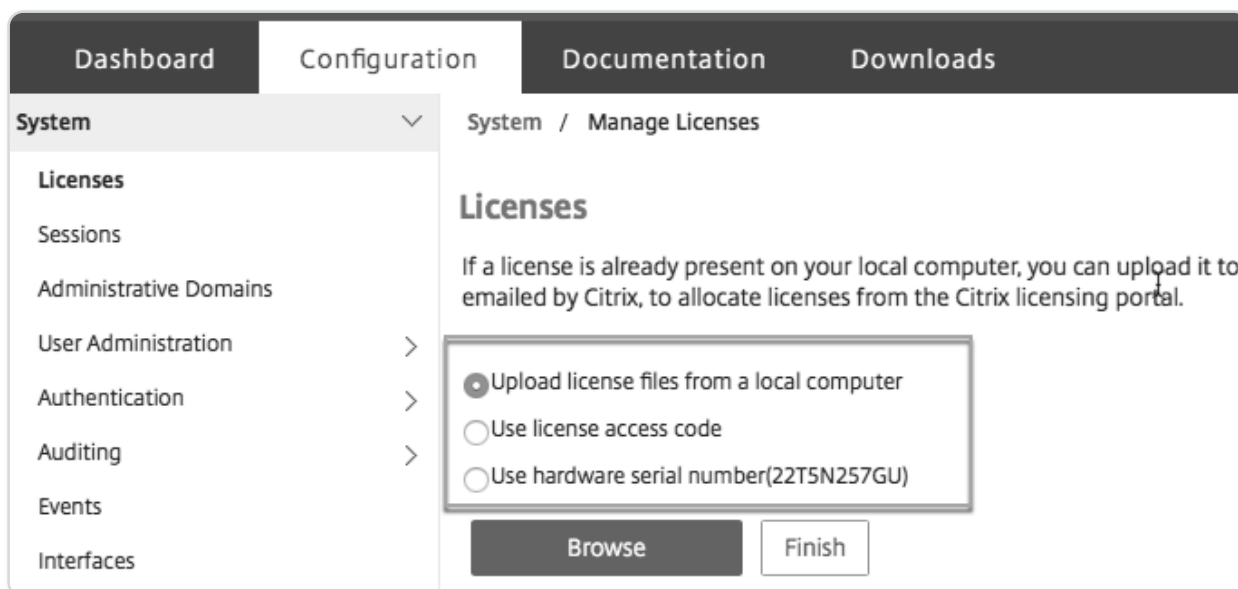
您可以根据部署需要部分分配许可证。例如，如果您的许可证文件包含 10 个许可证，但您当前只需要六个许可证，则可以立即分配六个许可证，稍后分配更多许可证。您不能分配超过许可证文件中存在的许可证总数。

分配许可证

1. 在 Web 浏览器中，键入 SDX 设备管理服务的 IP 地址（例如， `<http://10.102.126.251>` ）。
2. 在“用户名”和“密码”中，键入管理员凭据。
3. 在“配置”选项卡上，导航到“系统 > 许可证”。
4. 在详细信息窗格中，单击“添加许可证文件”。



5. 接下来，选择以下选项之一：
 - 从本地计算机上传许可证文件（此选项默认选中）
 - 使用许可证访问代码
 - 使用硬件序列号



- **从本地计算机上传许可证文件：**如果选择此选项，请单击“浏览”从本地计算机中选择零容量许可证。然后，单击“完成”。
 - a. 零容量许可证成功应用后，**许可证模式**部分将显示在**许可证**页面上。
 - b. 您可以选择**池许可证**或**自管理池许可证**。
 - c. 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。
 - d. 在**端口号**字段中，输入许可服务器端口。默认值：27000。
 - e. 单击**获取许可证**。
 - f. 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**。
 - g. 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。

注意：

从 NetScaler 13.1 build 30.x 版本开始，NetScaler SDX 设备支持自管理池许可证。通过此许可证，您可以简化许可证文件上传到许可服务器的过程并实现自动化。您可以使用 NetScaler Console 创建一个包含通用带宽或 vCPU 和实例池的许可框架。

- **使用许可证访问代码：**如果选择此选项，请在**许可证访问代码**字段中提供 **LAC**，或选中复选框以通过代理服务器连接。然后，单击**获取许可证**。
 - a. 选择要用于分配许可证的许可证文件。
 - b. 在**分配列**中，输入要分配的许可证数量。然后，单击**下载**。

如果许可证已下载，它将显示在**许可证文件**下。选择许可证文件，然后单击**应用许可证**。

- **使用硬件序列号**：如果选择此选项，软件将内部获取设备的序列号，并使用此号码显示您的许可证。
 - a. 单击**获取许可证**，或选中**通过代理服务器连接**复选框，然后单击**获取许可证**。

下载许可证文件后，选择许可证文件，然后点击“**应用许可证**”。

有关池化许可的信息，请参阅[将 NetScaler SDX 中的永久许可证升级到 NetScaler 池化容量](#)。

许可证激活服务

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 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。

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，确保了许可证管理的无缝和现代化方法。

注意：

LAS 是一种许可机制，而非许可证类型。LAS 支持 NetScaler 部署的定期带宽许可。LAS 不支持所有其他形式的传统 NetScaler 许可证，例如永久许可证。

LAS 的 NetScaler 版本兼容性

要使用 LAS，您的 NetScaler 必须运行以下最低版本之一或更高版本：

- **NetScaler ADC**：14.1 内部版本 51.80、13.1 内部版本 60.29、13.1 内部版本 37.247 (FIPS)
- **管理服务 (NetScaler SVM)**：14.1 内部版本 51.83、13.1 内部版本 60.30

注意：

对于 SDX 设备，请将管理服务 (SVM) 升级到支持 LAS 的内部版本，并过渡到基于 LAS 的许可。VPX 内部版本不影响 LAS 兼容性。

先决条件

要使用 LAS，请确保您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，请参阅[权利](#)。
- 确保您的 NetScaler 运行在与 LAS 兼容的版本上。

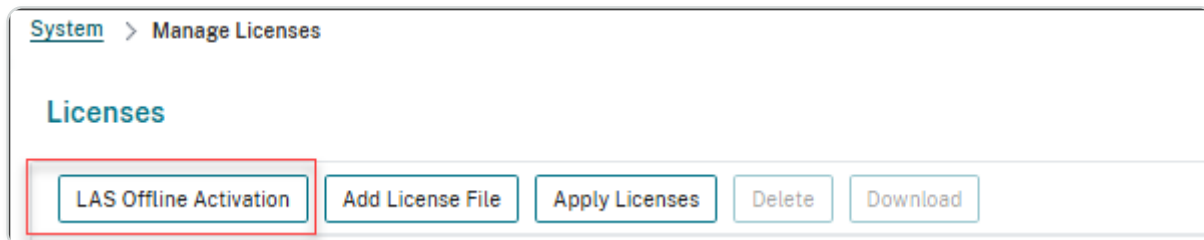
通过使用 NetScaler GUI 过渡到 LAS

如果您是以下情况，请按照本节中描述的步骤操作：

- 使用基于文件的许可并正在转向基于定期带宽 LAS 的许可的定期带宽客户。
- 拥有未授权的 NetScaler 并希望使用基于 LAS 的定期带宽许可。

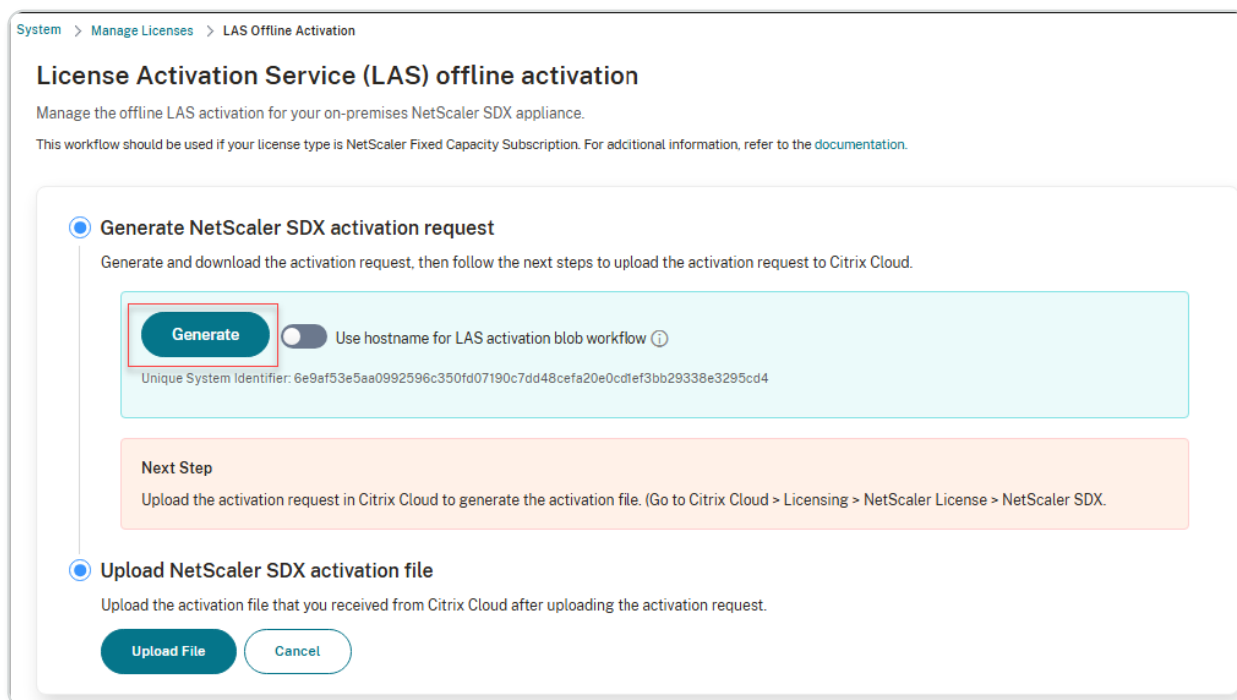
- 使用基于文件的永久许可客户，并正在转向基于 LAS 的定期带宽许可。

步骤 1： 在 NetScaler GUI 中，导航到 **System > Licenses** 并选择 **LAS Offline Activation** 选项。



步骤 2： LAS 激活通过生成一个激活请求文件开始，该文件包含特定 NetScaler SDX 实例的唯一身份信息。

1. 要生成 LAS 激活请求文件，请在 **Generate NetScaler SDX activation request** 部分下，单击 **Generate**。



2. 生成激活请求文件后，单击 **Download** 将其保存到本地系统。

注意：

激活请求文件在 7 天后过期。请在此时间范围内完成 **步骤 3** 中描述的激活过程，以确保文件仍然有效。

System > Manage Licenses > LAS Offline Activation

License Activation Service (LAS) offline activation

Manage the offline LAS activation for your on-premises NetScaler SDX appliance.

This workflow should be used if your license type is NetScaler Fixed Capacity Subscription. For additional information, refer to the [documentation](#).

☒ **Generate NetScaler SDX activation request**

Generate and download the activation request, then follow the next steps to upload the activation request to Citrix Cloud.

6e9af53e5aa0992596c350fd07190c7dd48cefa20e0cd1ef3bb29338e3295cd4_activation_request.tgz
File

Feb 03 2026 18:40:40 IST
Expires on

Download

Next Step

Upload the activation request in Citrix Cloud to generate the activation file. (Go to Citrix Cloud > Licensing > NetScaler License > NetScaler SDX.)

☒ **Upload NetScaler SDX activation file**

Upload the activation file that you received from Citrix Cloud after uploading the activation request.

Upload File Cancel

步骤 3： 将 **步骤 2** 中生成的激活请求文件上传到 Citrix Cloud™ (LAS UI)，为您的 NetScaler 生成许可证激活文件或 blob。

1. 登录 Citrix Cloud 并导航到 **Citrix Cloud > 许可 > NetScaler 许可证 > NetScaler SDX**。
2. 上传在 **步骤 2** 中生成的激活请求文件。
3. 文件成功上传后，为您的 NetScaler 选择所需的许可证类型。

注意：

如果您有多个固定期限带宽权益，下拉菜单会显示所有可用权益。请为该 NetScaler 实例选择合适的权益。

4. 选择许可证类型后，生成并下载许可证激活文件或 blob。

注意：

许可证激活文件或 blob 自生成之日起一年内有效。

NetScaler (ADC, SVM) offline activation

A profile for your NetScaler instance will be created automatically before generating an offline license activation file. [Learn more](#)

1. Upload offline activation request

Create an offline activation request on your NetScaler instance. Retrieve the resulting TGZ file and upload it here in Citrix Cloud. For more information, refer to the [product documentation](#).



6e9af53e5aa0992596c350fd07190c7dd48cefa20e0cd1ef3bb29338e3295cd4_activation_request.tgz
Size: 0.56 KB

[Remove file](#)

2. Select license type

Instance	Type
SDX	SDX 9120 Premium

Continue

3. Generate NetScaler activation file

Generate and download the activation file here in Citrix Cloud. Then, follow the [product documentation](#) to upload this file to the NetScaler instance.

Generate activation file

Close

步骤 4： 返回 NetScaler GUI，导航到 **System > Licenses** 并选择 **LAS Offline Activation** 选项。

1. 在“**上传 NetScaler SDX 激活文件**”部分，单击“**上传文件**”以上传在“**步骤 3**”中生成的许可证激活文件或 blob。

System > Manage Licenses > LAS Offline Activation

License Activation Service (LAS) offline activation

Manage the offline LAS activation for your on-premises NetScaler SDX appliance.

This workflow should be used if your license type is NetScaler Fixed Capacity Subscription. For additional information, refer to the [documentation](#).

- Generate NetScaler SDX activation request**
Generate and download the activation request, then follow the next steps to upload the activation request to Citrix Cloud.

6e9af53e5aa0992596c350fd07190c7dd48cefa20e0cd1ef3bb29338e3295cd4_activation_request.tgz
File

Feb 03 2026 18:40:40 IST
Expires on

Download

Next Step
Upload the activation request in Citrix Cloud to generate the activation file. (Go to Citrix Cloud > Licensing > NetScaler License > NetScaler SDX.)

- Upload NetScaler SDX activation file**
Upload the activation file that you received from Citrix Cloud after uploading the activation request.

Upload File

Cancel

2. 上传激活文件后，单击“是”确认激活。

License Activation Service (LAS) offline activation

Manage the offline LAS activation for your on-premises NetScaler ADC appliance.

Confirm

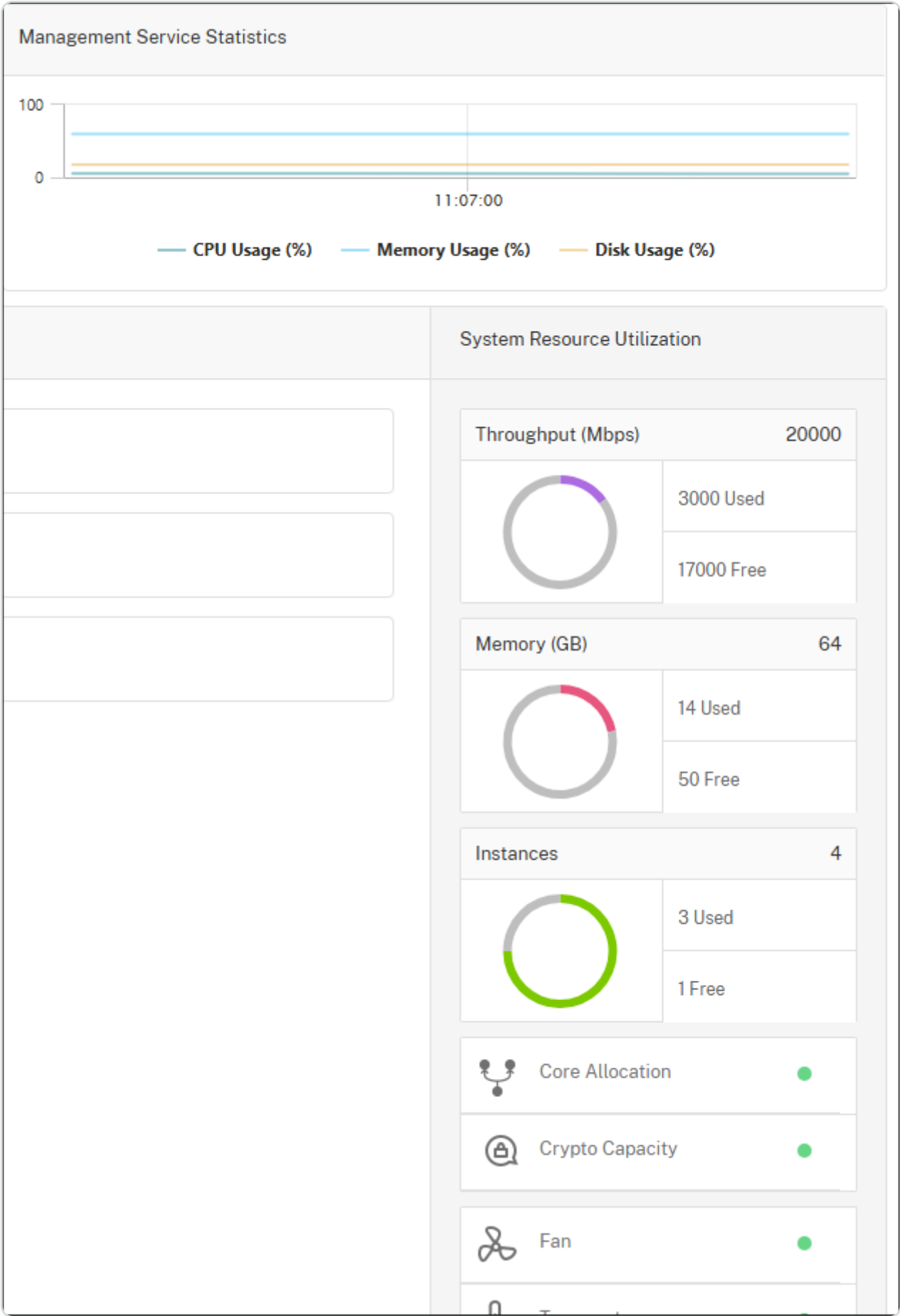
The file has been uploaded successfully. Do you want to Activate now?

Yes

No

Next Step

步骤 5：您的 NetScaler SDX 现已通过 LAS 获得许可。



步骤 6：监控和管理许可证激活文件或 blob，以确保持续运行。

许可证激活文件或 blob 的有效期为一年。您可以在界面中查看上次续订或激活日期以及即将到来的续订或激活日期。

为了保持 NetScaler 功能的连续性，请在即将到来的续订日期到期之前，点击“立即续订”并重复“步骤 2”到“步骤 5”。

System > Manage Licenses > LAS Offline Activation

License Activation Service (LAS) offline activation

Manage the offline LAS activation for your on-premises NetScaler SDX appliance.

This workflow should be used if your license type is NetScaler Fixed Capacity Subscription. For additional information, refer to the [documentation](#).

● Active LAS Activation Status	Sep 20 2026 05:29:59 IST Upcoming Renewal	Nov 21 2025 15:53:21 IST Last Renewal/Activation	6e9af53e5aa0992596c350fd0 7190c7dd48cefa20e0cd1ef3bb 29338e3295cd4 Unique System Identifier	Renew now
--	---	--	---	------------------

220 Days
License Entitlement Expiry

重要提示：

如果您未能及时续订并应用许可证激活文件或 blob，NetScaler 将变为未授权状态。

步骤 7： 登录 **Citrix Cloud** 并导航到 **Licensing > NetScaler licenses > NetScaler SDX** 以查看 LAS 激活 blob。

注意：

默认情况下，LAS 使用系统标识符 (`lsguid`) 来识别用于激活 blob 列表的 NetScaler 部署。

如果选择了主机名而不是系统标识符 (`lsguid`)，则主机名将显示在 **NetScaler GUI** 字段中。

Licensing > Licensed deployments > NetScaler > NetScaler (ADC, SVM)

NetScaler (ADC, SVM)

Manage the offline licensing for your NetScaler instances. Upload a license request generated from your disconnected NetScaler instance and then download the corresponding activation file to complete the licensing process. [Learn more](#)

Note: This UI workflow is for NetScaler Fixed Capacity Subscription Licenses only. Please ensure that you are following this [document](#).

Create profile

Search NetScaler

Sort by Expiration date

Offline activated nssdx-mgmt Device IP	Expires May 11, 2026	...
---	-----------------------------	------------

注意：

一旦迁移到 LAS 完成，请删除 SVM 上的本地基于文件的许可证。基于文件的许可证位于 SVM 文件夹 `/mpsconfig/license` 中，必须使用 shell 提示符从该文件夹中删除。

许可证激活文件的行为和到期

许可证激活文件或 blob 自生成之日起一年内有效。客户有责任跟踪即将到来的续订日期，并在文件到期前续订。

重要提示：

未能在许可证激活文件到期日之前续订，将导致 NetScaler 变为未授权状态。

许可证合同到期

通过导航到 **System > Licenses > LAS offline activation**，可以在 **License Entitlement Expiry** 下查看许可证合同到期前的剩余天数。

System > Manage Licenses > LAS Offline Activation

License Activation Service (LAS) offline activation

Manage the offline LAS activation for your on-premises NetScaler SDX appliance.

This workflow should be used if your license type is NetScaler Fixed Capacity Subscription. For additional information, refer to the [documentation](#).

● Active LAS Activation Status	Sep 20 2026 05:29:59 IST Upcoming Renewal	Nov 21 2025 15:53:21 IST Last Renewal/Activation	6e9af53e5aa0992596c350fd0 7190c7dd48cefa20e0cd1ef3bb 29338e3295cd4 Unique System Identifier	Renew now
-----------------------------------	--	---	--	---------------------------

220 Days
License Entitlement Expiry

为确保 NetScaler 正常运行，您必须在许可证合同到期前续订许可证合同并完成 [使用 NetScaler GUI 转换为 LAS](#) 部分中概述的步骤：

重要提示

- 如果许可证合同未及时续订，您的 NetScaler 将变为未授权状态。
- NetScaler 实例在许可证到期后将停止正常运行，包括配置丢失和流量处理完全关闭。

在 LAS 许可工作流期间发送到 LAS 的信息

本节详细介绍了在每次初始请求和每次 LAS 激活 blob 刷新请求期间，作为激活 blob 请求的一部分发送到 LAS 的所有信息。

下表总结了在许可工作流期间发送到 LAS 的参数。

参数	描述	在 LAS 工作流中的必要性
类型	硬编码，用于识别离线 NetScaler 的 LAS 部署类型	用于 LAS 侧跟踪
lsguid/lxid	NetScaler 的唯一 ID	LAS 绑定参数
NSIP 和主机名	NetScaler 当前的主机名，格式为 IP_hostname	用于 LAS 侧跟踪
构建版本	NetScaler 版本和内部版本	用于 LAS 侧跟踪
请求时间	请求包 (tgz) 创建时的时间戳	LAS 绑定参数
组织ID	客户的组织 ID	LAS 绑定参数
客户端ID	客户的 CC ID	LAS 绑定参数
平台	NetScaler 外形和型号	LAS 绑定参数
老化日期	NetScaler 版本和内部版本的软件发布日期	用于 LAS 侧跟踪
最后激活ID	续订期间发送的先前 LAS 激活 ID	LAS 绑定参数
UI版本	确保文件完整性验证	文件完整性验证

配置 LAS 激活标识符

从 NetScaler ADC 或管理服务 (SVM) 14.1-60.57、NetScaler ADC 或管理服务 13.1-61.26 以及 NetScaler FIPS 13.1-37.259 开始，NetScaler (ADC 或管理服务) 部署的基于 LAS 的许可工作流不再使用 IP 地址和主机名。而是，LAS 使用系统标识符 (lsguid) 来唯一标识 NetScaler (ADC 或管理服务) 部署。

要使用主机名而不是系统标识符 (`lsguid`)，请从 NetScaler GUI 中手动选择将主机名用于 LAS 激活 blob 工作流程选项。

激活用于 LAS 激活的主机名

1. 导航到 **系统 > 许可证 > LAS 激活**。
2. 打开将主机名用于 LAS 激活 blob 工作流程切换开关。

System > Manage Licenses > LAS Offline Activation

License Activation Service (LAS) offline activation

Manage the offline LAS activation for your on-premises NetScaler SDX appliance.

This workflow should be used if your license type is NetScaler Fixed Capacity Subscription. For additional information, refer to the [documentation](#).

Generate NetScaler SDX activation request

Generate and download the activation request, then follow the next steps to upload the activation request to Citrix Cloud.

Generate

Use hostname for LAS activation blob workflow ⓘ

Unique System Identifier: a2bc4b2a98b6ad1712dafaefeb3ee18cc83d0ef46cda1e2b01ee418c333c874

Next Step

Upload the activation request in Citrix Cloud to generate the activation file. (Go to Citrix Cloud > Licensing > NetScaler License > NetScaler SDX.

Upload NetScaler SDX activation file

Upload the activation file that you received from Citrix Cloud after uploading the activation request.

Upload File

监控已转换为 LAS 的 NetScaler SDX (SVM) 的最佳实践

本节详细介绍了在使用 LAS 和 NetScaler SDX (SVM) 且拥有固定容量订阅许可证类型时，可用于监控 NetScaler SDX 的最佳实践。

先决条件

- 阅读 [适用于 NetScaler 的 LAS](#) 页面，包括适用于 NetScaler SDX (SVM) 的 LAS 常见问题解答。
- 阅读 [许可证激活服务](#) 并完成您的 LAS 迁移。
- 确保您设置了相关通知，并定期监控 NetScaler SDX (SVM) GUI 和 CLI。

注意：

我们计划持续改进通知功能，并相应地更新此文档。

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

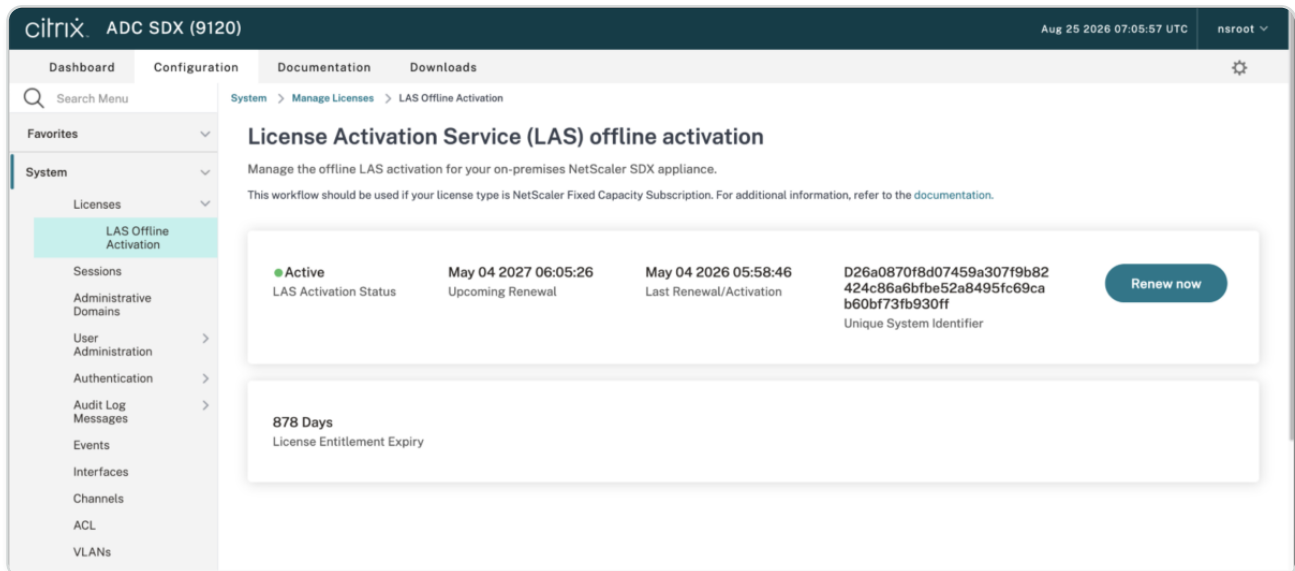
62

监控 LAS 激活 blob 过期

您可以使用 SVM GUI 和 CLI 跟踪 LAS 激活 blob 的过期情况，避免意外的许可证中断。

SVM GUI：

导航到 **SVM GUI > 配置 > 系统 > 许可证 > LAS 离线激活 > ADC 许可证**，并监控您的 **即将续订**。



SVM CLI：

您可以使用 `show license` 命令并参考 `Expiry Days` 参数的值。

示例：

```
show license
```

```
Platform: 9120
```

```
Cluster: false
```

```
Maximum Instances: 4
```

```
Available Instances: 4
```

```
Maximum Throughput (Mbps): 20000
```

```
Available Throughput (Mbps): 20000
```

```
isPooledLicense: false
```

Expiry Days: 208

isLASLicense: false

isLASFixedLicense: true

Done

```
> show license

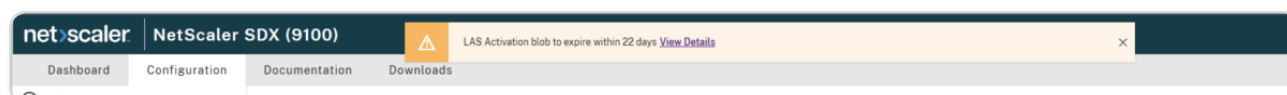
Platform: 9120
Cluster: false
Maximum Instances: 4
Available Instances: 4
Maximum Throughput (Mbps): 20000
Available Throughput (Mbps): 20000
isPooledLicense: false
Expiry Days: 208
isLASLicense: false
isLASFixedLicense: true

Done
```

通知

SVM GUI 上的横幅：

此 GUI 横幅由 NetScaler SDX 实例默认触发，当 LAS 激活 blob 在不到 30 天内即将过期时。每次用户登录时，它都会显示在 GUI 上。



基于 SNMP 的通知

SNMP 陷阱或警报对于即将过期的情况命名为 `LicenseExpiry`，对于已过期的情况命名为 `LicenseExpired`。

当 LAS 激活 blob 在不到 30 天内即将过期时，SNMP 陷阱 `LicenseExpiry` 由 NetScaler SDX 实例默认触发。此陷阱每 24 小时生成一次，从 LAS 激活 blob 过期前 30 天开始，并持续到 blob 过期为止。

您必须为 SDX/SVM 设置 SNMP 陷阱目标。设置完成后，您将收到这些 SNMP 陷阱。

示例：

```
[EventNotification[#1]] Inside: send_ns_snmp_trap_LicenseExpiry
```

NAME	STATUS	SEVERITY	THRESHOLD	TIME (MIN)
backupFailed	Enabled	Major	-NA-	-NA-
bmcFirmwareVersionError	Enabled	Major	-NA-	-NA-
bmcFirmwareVersionNormal	Enabled	Informational	-NA-	-NA-
cpuTempError	Enabled	Critical	60	-NA-
cpuTempNormal	Enabled	Informational	-NA-	-NA-
cpuUsageHigh	Enabled	Critical	80	-NA-
cpuUsageNormal	Enabled	Major	-NA-	-NA-
deviceAdded	Enabled	Informational	-NA-	-NA-
deviceBooted	Enabled	Informational	-NA-	-NA-
deviceBootFailed	Enabled	Critical	-NA-	-NA-
deviceModified	Enabled	Informational	-NA-	-NA-
devicePowerStateChanged	Enabled	Informational	-NA-	-NA-
deviceRebooted	Enabled	Informational	-NA-	-NA-
deviceRebootFailed	Enabled	Critical	-NA-	-NA-
deviceRemoved	Enabled	Informational	-NA-	-NA-
deviceStateChanged	Enabled	Major	-NA-	-NA-
deviceStateCleared	Enabled	Informational	-NA-	-NA-
ExtraMgmtCPUNotSupported	Enabled	Critical	-NA-	-NA-
ExtraMgmtCPUSupported	Enabled	Informational	-NA-	-NA-
HypervisorDiskUtilizationHigh	Enabled	Critical	98	-NA-
HypervisorDiskUtilizationNormal	Enabled	Informational	-NA-	-NA-
LicenseExpired	Enabled	Critical	-NA-	-NA-
LicenseExpiry	Enabled	Critical	-NA-	-NA-
VPXInterfacesAreNotInSync	Enabled	Critical	-NA-	-NA-
VPXInterfacesInSync	Enabled	Informational	-NA-	-NA-

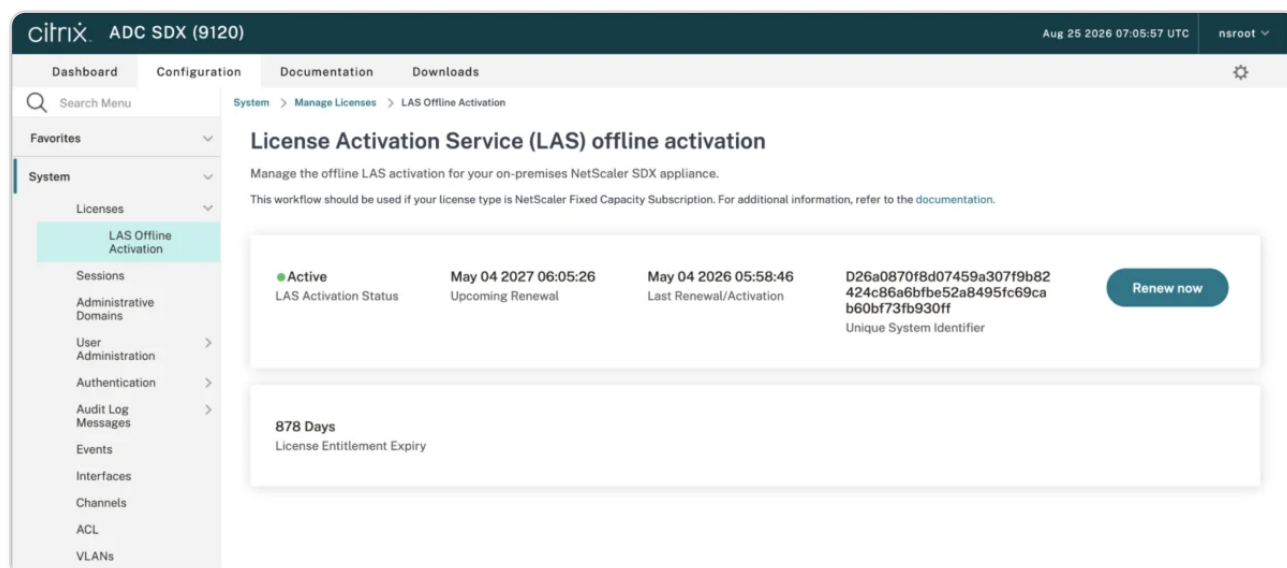
您可以通过导航到 **System > Events** 查看生成的事件。显示的消息是：“LAS 激活 blob 将在 **5** 天内过期”。

SEVERITY	SOURCE	DATE	CATEGORY	MESSAGE
Critical	10.214.28.109	Aug 30 2026 11:39:27 IST	LicenseExpiry	Licenses expire in 5 days.
Critical	10.214.28.109	Aug 30 2026 11:39:27 IST	Licenses	LAS Activation blob to expire within 20 days

监控许可证权利到期（合同到期）

SVM GUI：

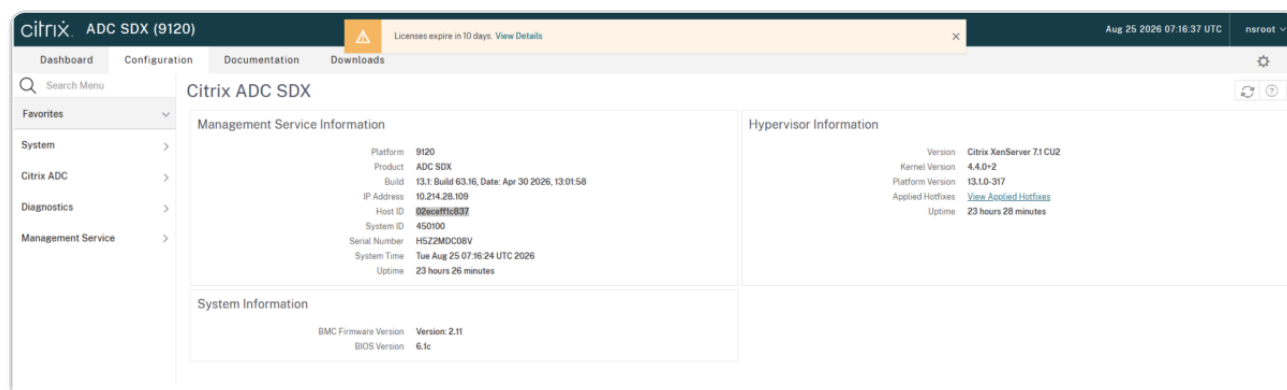
导航到 **SVM GUI > Configuration > System > Licenses > LAS Offline Activation > ADC Licenses** 并监控您的 许可证授权到期。



通知

SVM GUI 上的横幅：

当许可证授权在不到 30 天内即将到期时，NetScaler SDX 实例会触发 SVM GUI 上的此横幅。它会在每次用户登录时显示在 GUI 上。



基于 SNMP 的通知：

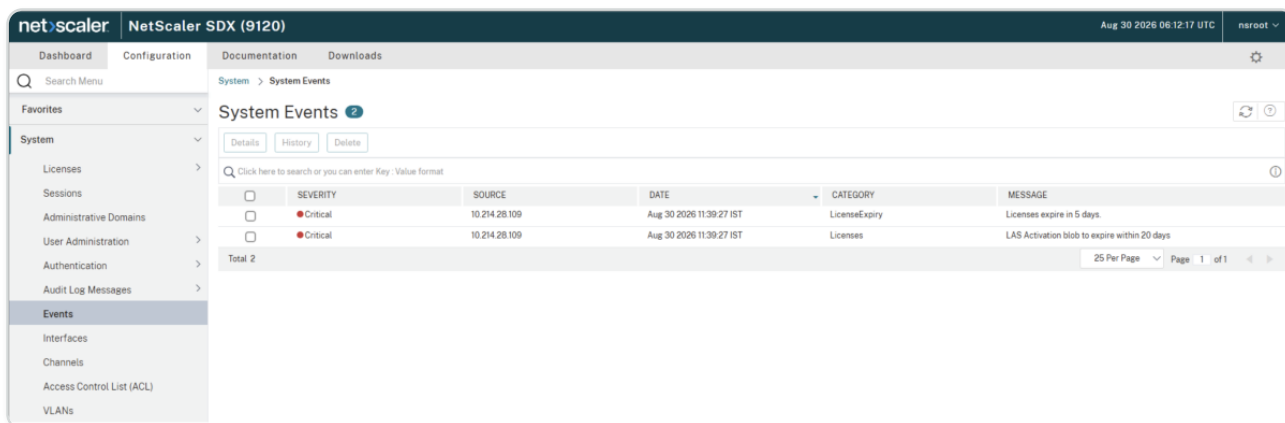
NetScaler SDX 会生成许可证授权到期事件。

SNMP trap 或警报对于即将到期的情况命名为 `LicenseExpiry`，对于已到期的情况命名为 `LicenseExpired`。

当许可证授权在不到 30 天内即将到期时，NetScaler SDX 实例会默认触发 SNMP trap `LicenseExpiry`。此 trap 从许可证授权到期前 30 天开始，每 24 小时生成一次，直到其到期。

您必须为 SDX/SVM 设置一个 SNMP trap 目标。设置完成后，您将收到这些 SNMP trap。

导航到 **SDX GUI > System > Events** 以查看这些事件。显示的消息是：“许可证授权将在 `x` 天内到期”（最新版本）或“许可证将在 `x` 天内到期”（某些旧版本）。



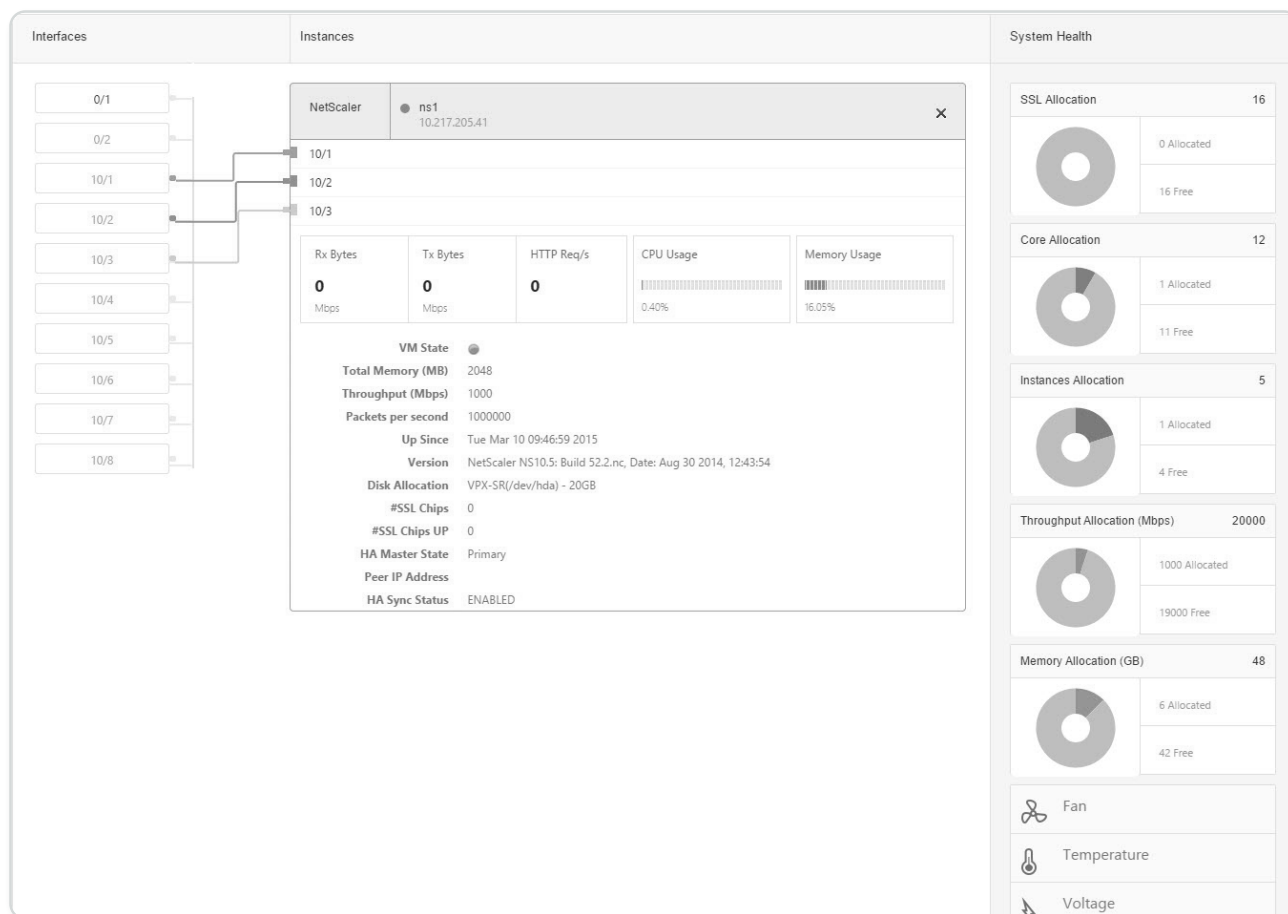
SDX 资源可视化工具

当在 NetScaler SDX 设备上预置 NetScaler 实例时，需要为实例分配各种资源，例如 CPU、吞吐量、内存。在当前的 SDX 中，不显示有关各种可用资源的信息。

使用资源可视化工具，可以在单个仪表板中显示可用于预置实例的所有可用资源。所有可用和已用资源都以图形格式显示。除了可分配的资源外，资源可视化工具还显示其他参数，例如电源状态和温度。

资源可视化工具还显示实例正在使用的各种资源。要查看与实例关联的各种资源，请在可视化工具中单击实例名称。可视化工具的右侧以图形格式显示所有可用和已用资源。

下图显示了资源可视化工具中捕获的详细信息：



管理接口

在**接口**窗格中，您可以显示 VPX 实例上虚拟接口到 SDX 设备之间的映射，并为接口分配 MAC 地址。

注意： 连接了直连电缆 (DAC) 的接口不支持自动协商。

在**接口**窗格的接口列表中，**状态**列中的 UP 表示接口正在正常接收流量。DOWN 表示存在网络问题，导致接口无法发送或接收流量。

重要： 不建议对超过 1 GB 的连接进行流量控制。

配置接口

- 在**配置**选项卡上的导航窗格中，展开**系统**，然后单击**接口**。
- 在**接口**窗格中，单击要配置的接口，然后单击**编辑**。
- 在**配置接口**窗口中，为以下参数指定值：
 - 自动协商**— 启用自动协商。可能的值：ON、OFF。默认值：ON。
 - 速度**— 接口的以太网速度，单位为 Mb/s。可能的值：10、100、1000 和 10000。

- **双工**— 接口的双工操作类型。可能的值：Full、Half、NONE。默认值：NONE。
- **流量控制自动协商**— 自动协商流量控制参数。可能的值：ON、OFF。默认值：ON
- **Rx 流量控制**— 启用 Rx 流量控制。可能的值：ON、OFF。默认值：ON
- **Tx 流量控制**— 启用 Tx 流量控制。可能的值：ON、OFF。默认值：ON

4. 单击 **确定**，然后单击 **关闭**。

重置接口参数为其默认值

1. 在 **配置** 选项卡上的导航窗格中，展开 **系统**，然后单击 **接口**。
2. 在 **接口** 窗格中，单击要重置的接口，然后单击 **重置**。

显示 VPX 实例上的虚拟接口到物理接口的映射

在 NetScaler VPX 实例中，GUI 和 CLI 显示实例上的虚拟接口到设备上的物理接口的映射。

登录到 VPX 实例后，在配置实用程序中，导航到 **网络**，然后单击 **接口**。实例上的虚拟接口编号以及设备上相应的物理接口编号显示在 **描述** 字段中，如下图所示：

在 CLI 中，键入 `show interface` 命令。例如：

```
> show interface

1) Interface 10/3 (10G VF Interface, PF 10/4) #2

flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>

MTU=1500, native vlan=1, MAC=6e:b6:f5:21:5d:db, uptime 43h03m35s

Actual: media FIBER, speed 10000, duplex FULL, fctl NONE, throughput 10000

RX: Pkts(2547925) Bytes(287996153) Errs(0) Drops(527183) Stalls(0)

TX: Pkts(196) Bytes(8532) Errs(0) Drops(0) Stalls(0)

NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)

Bandwidth thresholds are not set.

...
```

将 MAC 地址分配到接口

While you are provisioning an ADC instance on an SDX appliance, the Citrix Hypervisor™ internally assigns a MAC address to a virtual interface associated with that instance. The same MAC address might be assigned to a virtual interface associated with another instance on the same appliance or on another appliance. To prevent the assignment of duplicate MAC addresses, you can enforce unique MAC addresses.

有两种方法可以将 MAC 地址分配给接口：

1. 为接口分配基本 MAC 地址和范围：管理服务通过使用基本地址和范围分配唯一的 MAC 地址。
2. 分配全局基本 MAC 地址：全局基本 MAC 地址适用于所有接口。然后，管理服务会为所有接口生成 MAC 地址。如果设置了全局基本 MAC 地址，则 1G 接口的范围设置为 8。10G 接口的范围设置为 64。如果全局基本 MAC 地址设置为 00:00:00:00:00:00，请参阅下表中的示例基本 MAC 地址。

物理接口	基本 MAC 地址
0/1	00:00:00:00:00:00
0/2	00:00:00:00:00:08
1/1	00:00:00:00:00:10
1/2	00:00:00:00:00:18
1/3	00:00:00:00:00:20
1/4	00:00:00:00:00:28
1/5	00:00:00:00:00:30
1/6	00:00:00:00:00:38
1/7	00:00:00:00:00:40
1/8	00:00:00:00:00:48
10/1	00:00:00:00:00:50
10/2	00:00:00:00:00:90

表 1. 从全局基本 MAC 地址生成的示例基本 MAC 地址

管理端口的基本 MAC 地址仅供参考。管理服务仅为 1/x 和 10/x 端口生成基于基本 MAC 地址的 MAC 地址。

注意：您无法将基本 MAC 地址分配给通道。

要执行各种 MAC 地址操作，请单击“**系统 > 接口**”。选择一个接口，然后单击“**编辑**”。在“**配置接口**”窗口中执行 MAC 地址操作。

禁用或启用 SDX 设备上的物理接口

如果您未使用 SDX 设备上的任何物理接口，可以使用管理服务禁用该物理接口。此操作有助于提高安全性。

注意：默认情况下，SDX 设备上的所有物理接口均已启用。此外，如果接口被 VPX 或通道使用，则无法禁用该接口。

要禁用物理接口：

1. 在“**Configuration**”（配置）选项卡上的导航窗格中，展开“**System**”（系统），然后单击“**Interfaces**”（接口）。
2. 在“**Interfaces**”（接口）窗格中，选择要禁用的接口。
3. 在“**Action**”（操作）下拉列表中，单击“**Disable**”（禁用）。

如果要使用已禁用的物理接口，可以使用管理服务启用该接口。

要启用已禁用的物理接口：

1. 在“**Configuration**”（配置）选项卡上的导航窗格中，展开“**System**”（系统），然后单击“**Interfaces**”（接口）。
2. 在“**Interfaces**”（接口）窗格中，选择要启用的已禁用接口。
3. 在“**Action**”（操作）下拉列表中，单击“**Enable**”（启用）。

SDX 设备上的巨型帧

NetScaler SDX 设备支持接收和传输包含高达 9216 字节 IP 数据的巨型帧。与标准 IP MTU 大小 1500 字节相比，巨型帧可以更高效地传输大型文件。

NetScaler SDX 设备可在以下部署场景中使用巨型帧：

- **巨型到巨型**：设备以巨型帧形式接收数据，并以巨型帧形式发送数据。
- **非巨型到巨型**：设备以非巨型帧形式接收数据，并以巨型帧形式发送数据。

- **巨型到非巨型**：设备以巨型帧形式接收数据，并以非巨型帧形式发送数据。

在 SDX 设备上预置的 NetScaler 实例在负载平衡配置中支持以下协议的巨型帧：

- TCP
- 任何其他基于 TCP 的协议
- SIP

有关巨型帧的更多信息，请参阅用例。

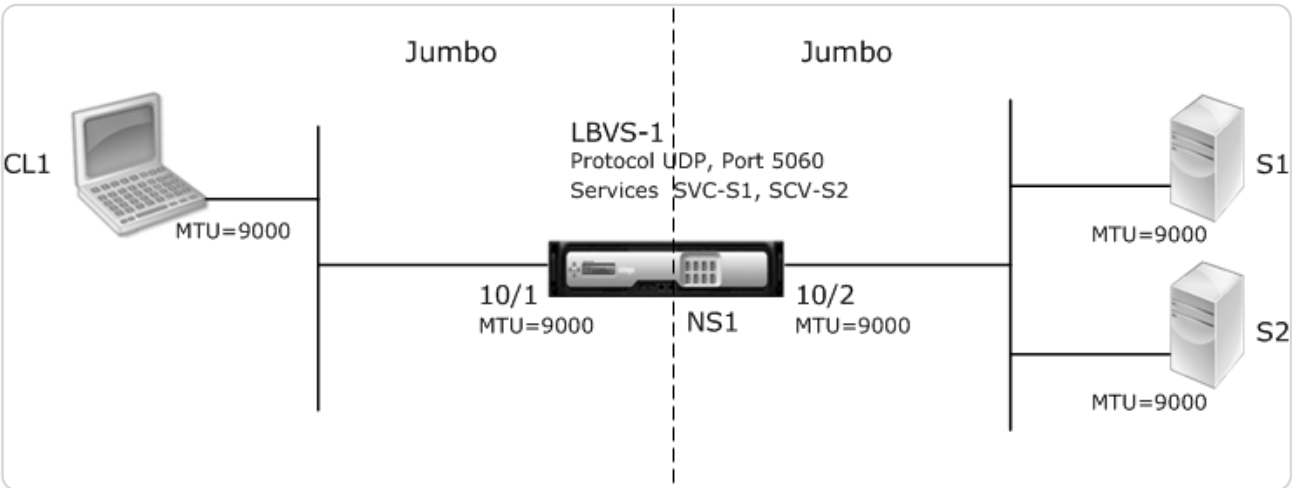
用例：巨型到巨型设置

考虑一个巨型到巨型设置的示例，其中在 NetScaler 实例 NS1 上配置的 SIP 负载平衡虚拟服务器 LBVS-1 用于在服务器 S1 和 S2 之间负载平衡 SIP 流量。客户端 CL1 与 NS1 之间的连接以及 NS1 与服务器之间的连接都支持巨型帧。

NS1 的接口 10/1 接收或发送来自或发往客户端 CL1 的流量。NS1 的接口 10/2 接收或发送来自或发往服务器 S1 或 S2 的流量。NS1 的接口 10/1 和 10/2 分别属于 VLAN 10 和 VLAN 20。

为了支持巨型帧，接口 10/1、10/2 以及 VLAN 10、VLAN 20 的 MTU 设置为 9216。

此设置示例中的所有其他网络设备，包括 CL1、S1、S2，也都配置为支持巨型帧。



下表列出了示例中使用的设置。

实体	名称	详细信息
客户端 CL1 的 IP 地址	CL1	192.0.2.10
服务器的 IP 地址	S1	198.51.100.19
	S2	198.51.100.20

实体	名称	详细信息
为接口（通过使用管理服务接口）和 NS1 上的 VLAN（通过使用 CLI）指定的 MTU。	10/1	9000
	10/2	9000
	VLAN 10	9000
	VLAN 20	9000
NS1 上代表服务器的服务	SVC-S1	IP 地址: 198.51.100.19; 协议: SIP; 端口: 5060
NS1 上代表服务器的服务	SVC-S2	IP 地址: 198.51.100.20; 协议: SIP; 端口: 5060
VLAN 10 上的负载均衡虚拟服务器	LBVS-1	IP 地址: 203.0.113.15; 协议: SIP; 端口: 5060; SVC-S1, SVC-S2

以下是 CL1 对 NS1 的请求的流量流：

- CL1 创建一个 20000 字节的 SIP 请求，发送给 LBVS1。
- CL1 将请求数据以 IP 分段的形式发送到 NS1 的 LBVS1。每个 IP 分段的大小等于或小于 CL1 将这些分段发送到 NS1 的接口上设置的 MTU (9000)。
 - 第一个 IP 分段的大小 === 9000
 - 第二个 IP 分段的大小 === 9000
 - 最后一个 IP 分段的大小 === 2068
- NS1 在接口 10/1 接收请求 IP 分段。NS1 接受这些分段，因为每个分段的大小都等于或小于接口 10/1 的 MTU (9000)。
- NS1 重新组装这些 IP 分段，形成 27000 字节的 SIP 请求。NS1 处理此请求。
- LBVS-1 的负载均衡算法选择服务器 S1。
- NS1 将请求数据以 IP 分段的形式发送到 S1。每个 IP 分段的大小等于或小于 NS1 将这些分段发送到 S1 的接口 10/2 的 MTU (9000)。IP 数据包的源地址是 NS1 的 SNIP 地址。
 - 第一个 IP 分段的大小 === 9000

- 第二个 IP 分段的大小 === 9000
- 最后一个 IP 分段的大小 === 2068

以下是本例中 S1 对 CL1 的响应流量流向：

1. 服务器 S1 创建一个 30000 字节的 SIP 响应，发送到 NS1 的 SNIP 地址。
2. S1 将响应数据以 IP 分片的形式发送到 NS1。每个 IP 分片的大小等于或小于 S1 将这些分片发送到 NS1 的接口上设置的 MTU (9000)。
 - 第一个 IP 分片的大小 === 9000
 - 第二个和第三个 IP 分片的大小 === 9000
 - 最后一个 IP 分片的大小 === 3088
3. NS1 在接口 10/2 接收响应 IP 分片。NS1 接受这些分片，因为每个分片的大小等于或小于接口 10/2 的 MTU (9000)。
4. NS1 重新组装这些 IP 分片以形成 27000 字节的 SIP 响应。NS1 处理此响应。
5. NS1 将响应数据以 IP 分片的形式发送到 CL1。每个 IP 分片的大小等于或小于接口 10/1 的 MTU (9000)，NS1 从该接口将这些分片发送到 CL1。IP 分片的源地址是 LBVS-1 的 IP 地址。这些 IP 数据包的源地址是 LBVS-1 的 IP 地址，目标地址是 CL1 的 IP 地址。
 - 第一个 IP 分片的大小 === 9000
 - 第二个和第三个 IP 分片的大小 === 9000

最后一个 IP 分片的大小 === 3088

配置任务：

在 SDX 管理服务上，导航到“**Configuration > System > Interfaces**”页面。选择所需的接口，然后单击“**Edit**”。设置 MTU 值，然后单击“**OK**”。

示例：

将接口 10/1 的 MTU 值设置为 9000，将接口 10/2 的 MTU 值设置为 9000。

登录到 NetScaler 实例，并使用 ADC 命令行界面完成剩余的配置步骤。

下表列出了在 NetScaler 实例上创建所需配置的任务、命令和示例。

任务	ADC 命令语法	示例
创建 VLAN 并设置所需 VLAN 的 MTU 以支持巨型帧。	<pre>add vlan <id> -mtu <positive_integer>; show vlan <id></pre>	<pre>add vlan 10 -mtu 9000; add vlan 20 -mtu 9000</pre>
将接口绑定到 VLAN。	<pre>bind vlan <id> -ifnum <interface_name>; show vlan <id></pre>	<pre>bind vlan 10 -ifnum 10/1; bind vlan 20 -ifnum 10/2</pre>
添加 SNIP 地址。	<pre>add ns ip <IPAddress> <netmask> -type SNIP; show ns ip</pre>	<pre>add ns ip 198.51.100.18 255.255.255.0 -type SNIP</pre>
创建表示 SIP 服务器的服务。	<pre>add service <serviceName> <ip> SIP_UDP <port>; show service <name></pre>	添加服务 SVC-S1 198.51.100.19 SIP_UDP 5060; dd 服务 SVC-S2 198.51.100.20 SIP_UDP 5060
创建 SIP 负载平衡虚拟服务器 并将其绑定到服务	<pre>add lb vserver <name> SIP_UDP <ip> <port>; bind lb vserver <vserverName> <serviceName>; show lb vserver <name></pre>	<pre>add lb vserver LBVS-1 SIP_UDP 203.0.113.15 5060; bind lb vserver LBVS-1 SVC-S1; bind lb vserver LBVS-1 SVC-S2</pre>
<pre>bind lb vserver LBVS-1 SVC-S2</pre>	<pre>save ns config; show ns config</pre>	

用例：非巨型帧到巨型帧设置

考虑一个非巨型帧到巨型帧设置的示例，其中在 NetScaler 实例 NS1 上配置的负载平衡虚拟服务器 LBVS1 用于在服务器 S1 和 S2 之间平衡流量。客户端 CL1 和 NS1 之间的连接支持非巨型帧，而 NS1 和服务器之间的连接支持巨型帧。

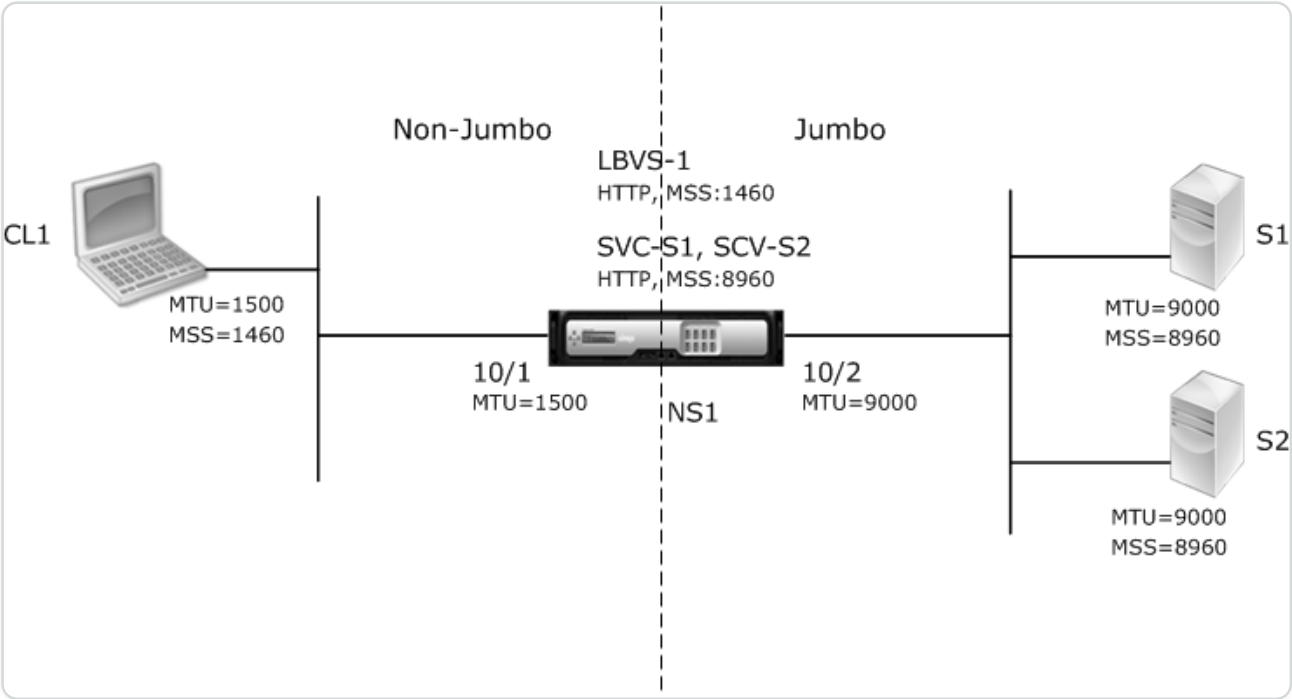
NS1 的接口 10/1 接收或发送来自或发往客户端 CL1 的流量。NS1 的接口 10/2 接收或发送来自或发往服务器 S1 或 S2 的流量。

NS1 的接口 10/1 和 10/2 分别属于 VLAN 10 和 VLAN 20。为了仅支持 CL1 和 NS1 之间的非巨型帧，接口 10/1 和 VLAN 10 的 MTU 都设置为默认值 1500。

为了支持 NS1 和服务端之间的巨型帧，接口 10/2 和 VLAN 20 的 MTU 都设置为 9000。

NS1 和服务端之间的服务端以及所有其他网络设备也配置为支持巨型帧。由于 HTTP 流量基于 TCP，因此在每个端点都相应地设置了 MSS 以支持巨型帧：

- 对于 CL1 和 NS1 的虚拟服务端 LBVS1 之间的连接，NS1 上的 MSS 在 TCP 配置文件中设置，然后绑定到 LBVS1。
- 对于 NS1 的 SNIP 地址与 S1 之间的连接，NS1 上的 MSS 在 TCP 配置文件中设置，然后该配置文件绑定到 NS1 上代表 S1 的服务 (SVC-S1)。



下表列出了此示例中使用的设置：

实体	名称	详细信息
客户端 CL1 的 IP 地址	CL1	192.0.2.10
服务器的 IP 地址	S1	198.51.100.19
	S2	198.51.100.20
接口 10/1 的 MTU（通过使用管理服务接口）。	1500	
为接口 10/2 设置的 MTU（通过使用管理服务接口）。	9000	

实体	名称	详细信息
NS1 上 VLAN 10 的 MTU（通过使用 ADC 命令行界面）。	1500	
为 NS1 上 VLAN 20 设置的 MTU（通过使用 ADC 命令行界面）。	9000	
NS1 上代表服务器的服务	SVC-S1	IP 地址: 198.51.100.19; 协议: HTTP; 端口: 80; MSS: 8960
	SVC-S2	IP 地址: 198.51.100.20; 协议: HTTP; 端口: 80; MSS: 8960
VLAN 10 上的负载均衡虚拟服务器	LBVS-1	IP 地址: 203.0.113.15; 协议: HTTP; 端口: 80。绑定的服务: SVC-S1, SVC-S2; MSS: 1460

以下是本示例中 CL1 向 S1 发送请求的流量流向：

1. 客户端 CL1 创建一个 200 字节的 HTTP 请求，发送到 NS1 的虚拟服务器 LBVS-1。
2. CL1 打开与 NS1 的 LBVS-1 的连接。CL1 和 NS1 在建立连接时交换各自的 TCP MSS 值。
3. 由于 NS1 的 MSS 大于 HTTP 请求，CL1 将请求数据以单个 IP 数据包的形式发送到 NS1。 1.

</div>

Size of the request packet = [IP Header + TCP Header + TCP Request] =
[20 + 20 + 200] = 240

</div>

4. NS1 在接口 10/1 接收请求数据包，然后处理数据包中的 HTTP 请求数据。
5. LBVS-1 的负载均衡算法选择服务器 S1，NS1 在其一个 SNIP 地址和 S1 之间打开连接。NS1 和 CL1 在建立连接时交换各自的 TCP MSS 值。

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

77

6. 由于 S1 的 MSS 大于 HTTP 请求，NS1 将请求数据以单个 IP 数据包的形式发送到 S1。

a. 请求数据包大小 = [IP 报头 + TCP 报头 +] = 240

以下是本示例中 S1 对 CL1 响应的流量流向：

1. 服务器 S1 创建一个 18000 字节的 HTTP 响应，发送到 NS1 的 SNIP 地址。
2. S1 将响应数据分段为 NS1 的 MSS 的倍数，并将这些分段以 IP 数据包的形式发送到 NS1。这些 IP 数据包源自 S1 的 IP 地址，目标是 NS1 的 SNIP 地址。
 - 前两个数据包的大小 = = = 9000
 - 最后一个数据包的大小 = = = 2120
3. NS1 在接口 10/2 接收响应数据包。
4. NS1 从这些 IP 数据包中组装所有 TCP 段，形成 18000 字节的 HTTP 响应数据。NS1 处理此响应。
5. NS1 将响应数据分段为 CL1 的 MSS 的倍数，并通过接口 10/1 将这些分段以 IP 数据包的形式发送到 CL1。这些 IP 数据包源自 LBVS-1 的 IP 地址，目标是 CL1 的 IP 地址。
 - 除最后一个数据包外，所有数据包的大小 = = = 1500
 - 最后一个数据包的大小 = = = 520

配置任务：

在 SDX 管理服务上，导航到“**配置 > 系统 > 接口**”页面。选择所需的接口，然后单击“**编辑**”。设置 MTU 值，然后单击“**确定**”。

示例：

设置以下 MTU 值：

- 对于 10/1 接口，设置为 1500
- 对于 10/2 接口，设置为 9000

登录到 NetScaler 实例，并使用 ADC 命令行界面完成剩余的配置步骤。

下表列出了在 NetScaler 实例上创建所需配置的任务、命令和示例。

任务	ADC 命令行语法	示例
创建 VLAN 并设置所需 VLAN 的 MTU 以支持巨型帧。	<pre>add vlan <id> -mtu <positive_integer>; show vlan <id></pre>	<pre>add vlan 10 -mtu 1500; add vlan 20 -mtu 9000</pre>
绑定接口到 VLAN。	<pre>bind vlan <id> -ifnum <interface_name>; show vlan <id></pre>	<pre>bind vlan 10 -ifnum 10/1; bind vlan 20 -ifnum 10/2</pre>
添加 SNIP 地址。	<pre>add ns ip <IPAddress> <netmask> -type SNIP; show ns ip</pre>	<pre>add ns ip 198.51.100.18 255.255.255.0 -type SNIP</pre>
创建代表 HTTP 服务器的服务	<pre>add service <serviceName> <ip> HTTP <port>; show service <name></pre>	<pre>add service SVC-S1 198.51.100.19 http 80; add service SVC-S2 198.51.100.20 http 80</pre>
创建 HTTP 负载均衡虚拟服务器并将服务绑定到它	<pre>add lb vserver <name> HTTP <ip> <port>; bind lb vserver <vserverName> <serviceName>; show lb vserver <name></pre>	<pre>add lb vserver LBVS-1 http 203.0.113.15 80; bind lb vserver LBVS-1 SVC-S1</pre>
创建自定义 TCP 配置文件并设置其 MSS 以支持巨型帧。	<pre>add tcpProfile <name> -mss <positive_integer>; show tcpProfile <name></pre>	<pre>add tcpprofile NS1- SERVERS-JUMBO -mss 8960</pre>
将自定义 TCP 配置文件绑定到所需服务。	<pre>set service <Name> -tcpProfileName <string>; show service <name></pre>	<pre>set service SVC-S1 -tcpProfileName NS1- SERVERS-JUMBO; set service SVC-S2 -tcpProfileName NS1- SERVERS-JUMBO</pre>
保存配置	<pre>save ns config; show ns config</pre>	

用例：巨型帧和非巨型帧流在同一组接口上的共存

考虑一个示例，其中负载均衡虚拟服务器 LBVS1 和 LBVS2 在 NetScaler 实例 NS1 上配置。LBVS1 用于在服务器 S1 和 S2 之间负载均衡 HTTP 流量，全局用于在服务器 S3 和 S4 之间负载均衡流量。

CL1 位于 VLAN 10 上，S1 和 S2 位于 VLAN20 上，CL2 位于 VLAN 30 上，S3 和 S4 位于 VLAN 40 上。VLAN 10 和 VLAN 20 支持巨型帧，而 VLAN 30 和 VLAN 40 仅支持非巨型帧。

换句话说，CL1 和 NS1 之间的连接以及 NS1 和服务器 S1 或 S2 之间的连接支持巨型帧。CL2 和 NS1 之间的连接以及 NS1 和服务器 S3 或 S4 之间的连接仅支持非巨型帧。

NS1 的接口 10/1 接收或发送来自或发往客户端的流量。NS1 的接口 10/2 接收或发送来自或发往服务器的流量。

接口 10/1 作为标记接口绑定到 VLAN 10 和 VLAN 20。接口 10/2 作为标记接口绑定到 VLAN 30 和 VLAN 40。

为了支持巨型帧，接口 10/1 和 10/2 的 MTU 设置为 9216。

在 NS1 上，VLAN 10 和 VLAN 30 的 MTU 设置为 9000 以支持巨型帧。VLAN 20 和 VLAN 40 的 MTU 设置为默认值 1500 以仅支持非巨型帧。

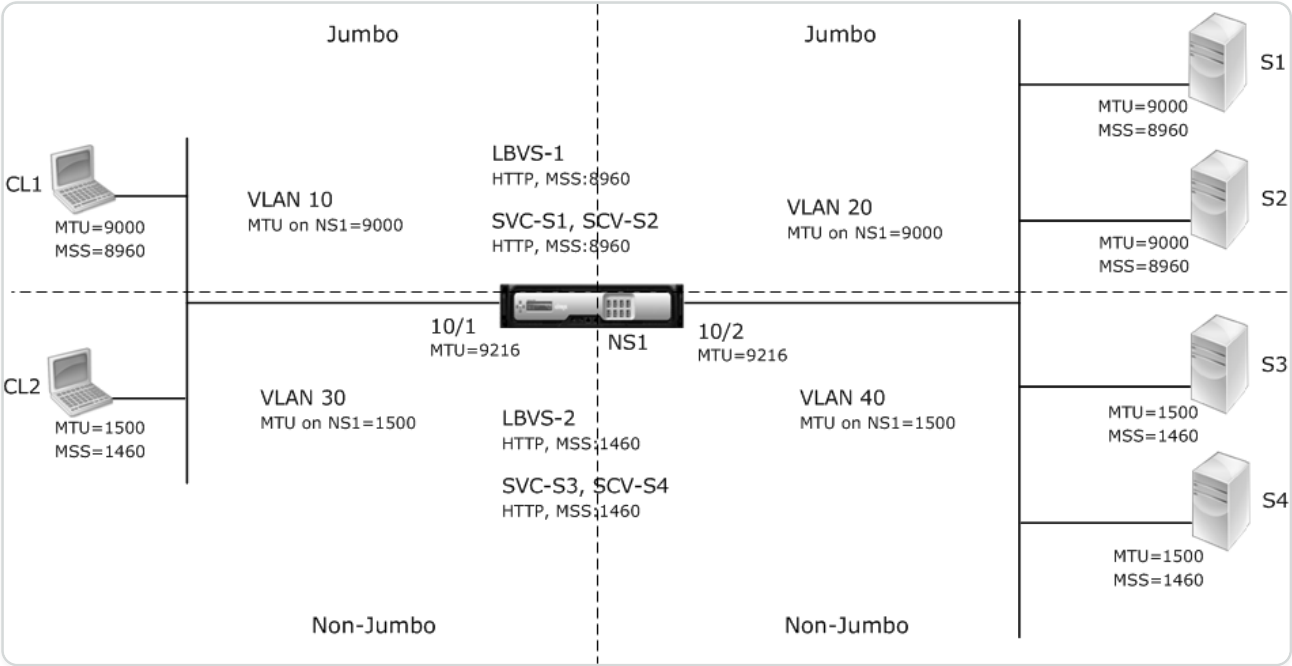
ADC 接口上 VLAN 标记数据包的有效 MTU 是接口 MTU 或 VLAN MTU 中的较低者。例如：

- 接口 10/1 的 MTU 为 9216。VLAN 10 的 MTU 为 9000。在接口 10/1 上，VLAN 10 标记数据包的有效 MTU 为 9000。
- 接口 10/2 的 MTU 为 9216。VLAN 20 的 MTU 为 9000。在接口 10/2 上，VLAN 20 标记数据包的有效 MTU 为 9000。
- 接口 10/1 的 MTU 为 9216。VLAN 30 的 MTU 为 1500。在接口 10/1 上，VLAN 30 标记数据包的有效 MTU 为 1500。
- 接口 10/2 的 MTU 为 9216。VLAN 40 的 MTU 为 1500。在接口 10/2 上，VLAN 40 标记数据包的有效 MTU 为 1500。

CL1、S1、S2 以及 CL1 与 S1 或 S2 之间的所有网络设备都配置为巨型帧。

由于 HTTP 流量基于 TCP，因此在每个端点相应地设置了 MSS 以支持巨型帧。

- 对于 CL1 和 NS1 的虚拟服务器 LBVS-1 之间的连接，NS1 上的 MSS 在 TCP 配置文件中设置，然后绑定到 LBVS1。
- 对于 NS1 的 SNIP 地址和 S1 之间的连接，NS1 上的 MSS 在 TCP 配置文件中设置，然后绑定到代表 NS1 上 S1 的服务 (SVC-S1)。



下表列出了此示例中使用的设置。

实体	名称	详细信息
客户端 IP 地址	CL1	192.0.2.10
	CL2	192.0.2.20
服务器 IP 地址	S1	198.51.100.19
	S2	198.51.100.20
	S3	198.51.101.19
	S4	198.51.101.20
NS1 上的 SNIP 地址	198.51.100.18; 198.51.101.18	
NS1 上为接口和 VLAN 指定的 MTU	10/1	9216
	10/2	9216
VLAN 10	9000	
VLAN 20	9000	
VLAN 30	9000	

实体	名称	详细信息
VLAN 40	1500	
默认 TCP 配置文件	nstcp_default_profile	MSS: 1460
自定义 TCP 配置文件	ALL-JUMBO	MSS: 8960
NS1 上表示服务器的服务	SVC-S1	IP 地址: 198.51.100.19; 协议: HTTP; 端口: 80; TCP 配置文件: ALL-JUMBO (MSS: 8960)
	SVC-S2	IP 地址: 198.51.100.20; 协议: HTTP; 端口: 80; TCP 配置文件: ALL-JUMBO (MSS: 8960)
	SVC-S3	IP 地址: 198.51.101.19; 协议: HTTP; 端口: 80; TCP 配置文件: nstcp_default_profile (MSS: 1460)
	SVC-S4	IP 地址: 198.51.101.20; 协议: HTTP; 端口: 80; TCP 配置文件: nstcp_default_profile (MSS: 1460)
NS1 上的负载均衡虚拟服务器	LBVS-1	IP 地址 = 203.0.113.15 ; 协议 : HTTP ; 端口 : 80。绑定服务 : SVC-S1, SVC-S2 ; TCP 配置文件 : ALL-JUMBO (MSS: 8960)
	LBVS-2	IP 地址 = 203.0.114.15 ; 协议 : HTTP ; 端口 : 80。绑定服务 : SVC-S3, SVC-S4 ; TCP 配置文件 : nstcp_default_profile (MSS: 1460)

以下是 CL1 对 S1 请求的流量流：

1. 客户端 CL1 创建一个 20000 字节的 HTTP 请求，发送到 NS1 的虚拟服务器 LBVS-1。
2. CL1 打开与 NS1 的 LBVS-1 的连接。CL1 和 NS1 在建立连接时交换其 TCP MSS 值。

3. 由于 NS1 的 MSS 值小于 HTTP 请求，CL1 将请求数据分段为 NS1 的 MSS 的倍数，并将这些分段以标记为 VLAN 10 的 IP 数据包发送到 NS1。
 - 前两个数据包的大小 = = = 9000
 - 最后一个数据包的大小 = = = 2120
4. NS1 在接口 10/1 接收这些数据包。NS1 接受这些数据包，因为这些数据包的大小等于或小于接口 10/1 对于 VLAN 10 标记数据包的有效 MTU (9000)。
5. NS1 从 IP 数据包中组装所有 TCP 段，形成 20000 字节的 HTTP 请求。NS1 处理此请求。
6. LBVS-1 的负载均衡算法选择服务器 S1，NS1 在其一个 SNIP 地址和 S1 之间建立连接。NS1 和 CL1 在建立连接时交换各自的 TCP MSS 值。
7. NS1 将请求数据分段为 S1 的 MSS 的倍数，并将这些分段以标记为 VLAN 20 的 IP 数据包发送到 S1。
 - 前两个数据包的大小 = = = 9000
 - 最后一个数据包的大小 = = = 2120

以下是 S1 对 CL1 响应的流量：

1. 服务器 S1 创建一个 30000 字节的 HTTP 响应，发送到 NS1 的 SNIP 地址。
2. S1 将响应数据分段为 NS1 的 MSS 的倍数，并将这些分段以标记为 VLAN 20 的 IP 数据包形式发送到 NS1。这些 IP 数据包源自 S1 的 IP 地址，目标是 NS1 的 SNIP 地址。
 - 前三个数据包的大小 = = = 9000
 - 最后一个数据包的大小 = = = 3160
3. NS1 在接口 10/2 接收响应数据包。NS1 接受这些数据包，因为它们的大小等于或小于接口 10/2 对于 VLAN 20 标记数据包的有效 MTU 值 (9000)。
4. NS1 从这些 IP 数据包中组装所有 TCP 段，形成 30000 字节的 HTTP 响应。NS1 处理此响应。
5. NS1 将响应数据分段为 CL1 的 MSS 的倍数，并将这些分段以标记为 VLAN 10 的 IP 数据包形式，从接口 10/1 发送到 CL1。这些 IP 数据包源自 LBVS 的 IP 地址，目标是 CL1 的 IP 地址。
 - 前三个数据包的大小 = [IP 标头 + TCP 标头 + = = 9000
 - 最后一个数据包的大小 = = = 3160

配置任务：

在 SDX 管理服务上，导航到 **Configuration > System > Interfaces** 页面。选择所需的接口，然后单击 **Edit**。设置 MTU 值，然后单击 **OK**。

示例：

设置以下 MTU 值：

- 对于 10/1 接口，设置为 9216
- 对于 10/2 接口，MTU 为 9216

登录到 NetScaler 实例，并使用 ADC 命令行界面完成剩余的配置步骤。

下表列出了在 NetScaler 实例上创建所需配置的任务、命令和示例。

任务	语法	示例
创建 VLAN 并设置所需 VLAN 的 MTU，以支持巨型帧。	<pre>add vlan <id> -mtu <positive_integer>; show vlan <id></pre>	<pre>add vlan 10 -mtu 9000; add vlan 20 -mtu 9000; add vlan 30 -mtu 1500; add vlan 40 -mtu 1500</pre>
将接口绑定到 VLAN。	<pre>bind vlan <id> -ifnum <interface_name>; show vlan <id></pre>	<pre>bind vlan 10 -ifnum 10/1 -tagged; bind vlan 20 -ifnum 10/2 -tagged; bind vlan 30 -ifnum 10/1 -tagged; bind vlan 40 -ifnum 10/2 -tagged</pre>
添加 SNIP 地址。	<pre>add ns ip <IPAddress> <netmask> -type SNIP; show ns ip</pre>	<pre>add ns ip 198.51.100.18 255.255.255.0 -type SNIP; a dd ns ip 198.51.101.18 255.255.255.0 -type SNIP</pre>
创建代表 HTTP 服务器的服务。	<pre>add service <serviceName> <ip> HTTP <port>; show service <name></pre>	<pre>add service SVC-S1 198.51.100.19 http 80; add service SVC-S2 198.51.100.20 http 80; add service SVC-S3 198.51.101.19 http 80; add service SVC-S4 198.51.101.20 http 80</pre>

任务	语法	示例
创建 HTTP 负载均衡虚拟服务器并将服务绑定到它	<pre>add lb vserver <name> HTTP <ip> <port> ; bind lb vserver <vserverName> <serviceName> ; show lb vserver <name></pre>	<pre>add lb vserver LBVS-1 http 203.0.113.15 80 ; bind lb vserver LBVS-1 SVC-S1 ; bind lb vserver LBVS-1 SVC-S2</pre>
	<pre>add lb vserver LBVS-2 http 203.0.114.15 80 ; bind lb vserver LBVS-2 SVC-S3 ; bind lb vserver LBVS-2 SVC-S4</pre>	
创建自定义 TCP 配置文件并设置其 MSS 以支持巨型帧。	<pre>add tcpProfile <name> -mss <positive_integer> ; show tcpProfile <name></pre>	<pre>add tcpprofile ALL- JUMBO -mss 8960</pre>
将自定义 TCP 配置文件绑定到所需的负载均衡虚拟服务器和服务。	<pre>set service <Name> -tcpProfileName <string> ; s how service <name></pre>	<pre>set lb vserver LBVS-1 - tcpProfileName ALL-JUMBO ; s et service SVC-S1 - tcpProfileName ALL-JUMBO ; s et service SVC-S2 - tcpProfileName ALL-JUMBO</pre>
保存配置	<pre>save ns config ; show ns config</pre>	

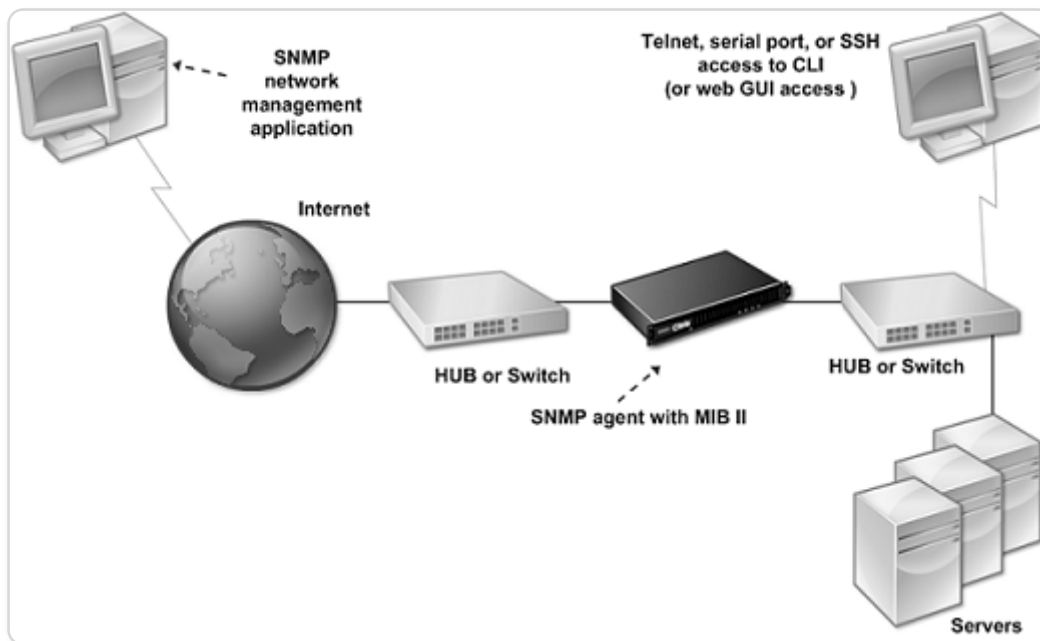
在 SDX 设备上配置 SNMP

您可以在 NetScaler SDX 设备上配置 SNMP 代理，以生成称为陷阱的异步事件。每当 SDX 设备出现异常情况时，就会生成陷阱。然后，这些陷阱会发送到一个名为 *陷阱侦听器* 的远程设备，该设备会发出 SDX 设备上的异常情况信号。

除了配置 SNMP 陷阱目标、下载 MIB 文件以及配置一个或多个 SNMP 管理器之外，您还可以为 SNMPv3 查询配置 NetScaler SDX 设备。

下图显示了一个已启用并配置 SNMP 的 SDX 设备的网络。图中，每个 SNMP 网络管理应用程序都使用 SNMP 与 SDX 设备上的 SNMP 代理进行通信。

图 1. 支持 SNMP 的 SDX 设备



SDX 设备上的 SNMP 代理仅生成符合 SNMPv2 的陷阱。支持的陷阱可在 SDX MIB 文件中查看。您可以从 SDX 用户界面中的“下载”页面下载此文件。

添加 SNMP 陷阱目标

1. 在配置选项卡中，在导航窗格中，展开 **系统 > SNMP**，然后单击“SNMP 陷阱目标”。
2. 在“SNMP 陷阱目标”窗格中，单击“添加”。
3. 在“配置 SNMP 陷阱目标”页面中，为以下参数指定值：
 - 目标服务器 — 陷阱侦听器的 IPv4 地址，用于向其发送 SNMP 陷阱消息。
 - 端口 — 陷阱侦听器侦听陷阱消息的 UDP 端口。必须与陷阱侦听器上的设置匹配，否则侦听器将丢弃消息。最小值：1。默认值：162。
 - 社区 — 随陷阱消息发送的密码（字符串），以便陷阱侦听器可以对其进行身份验证。可包含字母、数字、连字符 (-)、句点 (.)、井号 (#)、空格 ()、at (@)、等号 (=)、冒号 (:) 和下划线 (_) 字符。注意：在陷阱侦听器设备上指定相同的社区字符串，否则侦听器将丢弃消息。默认值：public。
4. 单击“添加”，然后单击“关闭”。您添加的 SNMP 陷阱目标将显示在“SNMP 陷阱”窗格中。

要修改 SNMP 陷阱目标的参数值，请在“SNMP 陷阱目标”窗格中，选择要修改的陷阱目标，然后单击“修改”。在“修改 SNMP 陷阱目标”对话框中，修改参数。

要删除 SNMP 陷阱，请在“SNMP 陷阱目标”窗格中，选择要删除的陷阱目标，然后单击“删除”。在“确认”消息框中，单击以删除 SNMP 陷阱目标。

下载 MIB 文件

在开始监控 SDX 设备之前，必须下载以下文件。

****SDX-MIB-smiv2.mib。** **此文件由 SNMPv2 管理器和 SNMPv2 陷阱侦听器使用。

该文件包含一个 NetScaler 企业 MIB，它提供 SDX 特定的事件。

下载 MIB 文件

1. 登录到 SDX 设备用户界面的“下载”页面。
2. 在“SNMP 文件”下，单击“SNMP v2 - MIB 对象定义”。您可以使用 MIB 浏览器打开该文件。

添加 SNMP 管理器社区

在 SDX 设备上配置 SNMP 管理器，以查询和监控设备以及设备上托管的受管设备。此外，您必须向 SNMP 管理器提供所需的设备特定信息。对于 IPv4 SNMP 管理器，您可以指定主机名而不是管理器的 IP 地址。如果这样做，则必须添加一个 DNS 命名服务器，将 SNMP 管理器的主机名解析为其 IP 地址。

至少配置一个 SNMP 管理器。如果您不配置 SNMP 管理器，设备将不接受或响应来自网络上任何 IP 地址的 SNMP 查询。如果您配置了一个或多个 SNMP 管理器，设备将仅接受并响应来自这些特定 IP 地址的 SNMP 查询。

配置 SNMP 管理器

1. 在“配置”选项卡上的导航窗格中，展开“系统”，然后展开“SNMP”。
2. 单击“管理器”。
3. 在详细信息窗格中，单击“添加”。
4. 在“创建 SNMP 管理器社区”页面中，设置以下参数：
 - SNMP 管理器 — SNMP 管理器的 IPv4 地址。或者，您可以指定已分配给 SNMP 管理器的主机名，而不是 IPv4 地址。如果这样做，您必须添加一个 DNS 域名服务器，将 SNMP 管理器的主机名解析为其 IP 地址。
 - 社区 — SNMP 社区字符串。可包含 1 到 31 个字符，包括大写和小写字母、数字以及连字符 (-)、句点 (.)、井号 (#)、at (@)、等号 (=)、冒号 (:) 和下划线 (_) 字符。
 - 选中“启用管理网络”复选框，以使用网络掩码指定 SNMP 管理器。
 - 在“网络掩码”字段中，输入 SNMP 社区的网络掩码。
5. 单击“添加”，然后单击“关闭”。

为 SNMPv3 查询配置 SDX 设备

SNMPv3 基于 SNMPv1 和 SNMPv2 的基本结构和体系结构。但是，SNMPv3 增强了基本体系结构，以整合管理和安全功能，例如身份验证、访问控制、数据完整性检查、数据源验证、消息及时性检查和数据机密性。

NetScaler SDX 设备支持以下实体，使您能够实施 SNMPv3 的安全功能：

- SNMP 视图
- SNMP 用户

这些实体协同工作以实施 SNMPv3 安全功能。创建视图以允许访问 MIB 的子树。

添加 SNMP 管理器

配置 SDX 设备以允许相应的 SNMP 管理器查询它。同时向 SNMP 管理器提供所需的设备特定信息。对于 IPv4 SNMP 管理器，您可以指定主机名而不是管理器的 IP 地址。如果这样做，您必须添加一个 DNS 域名服务器，将 SNMP 管理器的主机名解析为其 IP 地址。

配置至少一个 SNMP 管理器。如果您不配置 SNMP 管理器，设备将不接受或响应来自网络上任何 IP 地址的 SNMP 查询。如果您配置了一个或多个 SNMP 管理器，设备将仅接受并响应来自这些特定 IP 地址的 SNMP 查询。

配置 SNMP 管理器：

1. 导航到“系统 > 配置”页面。
2. 在“配置”选项卡上的导航窗格中，展开“系统”，然后展开“SNMP”。
3. 单击“管理器”。
4. 在详细信息窗格中，单击“添加”。
5. 在“添加 SNMP 管理器社区”对话框中，设置以下参数：
 - **SNMP 管理器**—SNMP 管理器的 IPv4 地址。或者，您可以指定已分配给 SNMP 管理器的主机名，而不是 IPv4 地址。如果这样做，您必须添加一个 DNS 名称服务器，将 SNMP 管理器的主机名解析为其 IP 地址。
 - **社区**—SNMP 社区字符串。可包含 1 到 31 个字符，包括大写和小写字母、数字以及连字符 (-)、句点 (.)、井号 (#)、at 符号 (@)、等号 (=)、冒号 (:) 和下划线 (_) 字符。
6. 单击“添加”，然后单击“关闭”。

配置 SNMP 视图

SNMP 视图限制用户访问 MIB 的特定部分。SNMP 视图用于实施访问控制。

配置视图

1. 在“配置”选项卡上的导航窗格中，展开“系统”，然后展开“SNMP”。
2. 单击“视图”。
3. 在详细信息窗格中，单击添加。
4. 在“添加 SNMP 视图”对话框中，设置以下参数：
 - 名称—SNMPv3 视图的名称。可包含 1-31 个字符，包括大写和小写字母、数字以及连字符 (-)、句点 (.)、井号 (#)、at 符号 (@)、等号 (=)、冒号 (:) 和下划线 (_) 字符。选择一个有助于识别 SNMPv3 视图的名称。
 - 子树—MIB 树的特定分支（子树），您希望将其与此 SNMPv3 视图关联。将子树指定为 SNMP OID。
 - 类型—在此视图中包含或排除由子树参数指定的子树。当您在 SNMPv3 视图中包含了一个子树（例如 A），并且希望从 SNMPv3 视图中排除 A 的特定子树（例如 B）时，此设置会很有用。

配置 SNMP 用户

创建 SNMP 视图后，添加 SNMP 用户。SNMP 用户可以访问查询 SNMP 管理器所需的 MIB。

配置用户

1. 在“配置”选项卡上，在导航窗格中，展开“系统”，然后展开“SNMP”。
2. 单击“用户”。
3. 在详细信息窗格中，单击添加。
4. 在“创建 SNMP 用户”页面中，设置以下参数：
 - 名称—SNMPv3 用户的名称。可包含 1-31 个字符，包括大写和小写字母、数字以及连字符 (-)、句点 (.)、井号 (#)、at 符号 (@)、等号 (=)、冒号 (:) 和下划线 (_) 字符。
 - 安全级别—设备与 SNMPv3 用户之间通信所需的安全级别。从以下选项中选择：
 - 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。
 - 身份验证协议—设备和 SNMPv3 用户用于验证它们之间通信的身份验证算法。在 SNMP 管理器中配置 SNMPv3 用户时，请指定相同的身份验证算法。

- 身份验证密码—身份验证算法使用的密码短语。可包含 1-31 个字符，包括大写和小写字母、数字以及连字符 (-)、句点 (.)、井号 (#)、空格 ()、at (@)、等号 (=)、冒号 (:) 和下划线 (_) 字符。
- 隐私协议—设备和 SNMPv3 用户用于加密它们之间通信的加密算法。在 SNMP 管理器中配置 SNMPv3 用户时，请指定相同的加密算法。
- 视图名称—要绑定到此 SNMPv3 用户的已配置 SNMPv3 视图的名称。SNMPv3 用户可以访问绑定到此 SNMPv3 视图的类型为 INCLUDED 的子树，但不能访问类型为 EXCLUDED 的子树。

配置 SNMP 警报

设备提供了一组预定义的条件实体，称为 SNMP 警报。当满足 SNMP 警报的条件集时，设备会生成 SNMP trap 消息并将其发送到已配置的 trap 侦听器。例如，当启用 deviceAdded 警报时，每当在设备上配置设备（实例）时，就会生成 trap 消息并将其发送到 trap 侦听器。您可以为 SNMP 警报分配严重级别。当您这样做时，相应的 trap 消息将分配该严重级别。

以下是设备上定义的严重级别，按严重性降序排列：

- 严重
- 主要
- 次要
- 警告
- 信息性（默认）

例如，如果您为名为 deviceAdded 的 SNMP 警报设置了警告严重级别，则在添加设备时生成的 trap 消息将分配警告严重级别。

您还可以配置 SNMP 警报，以便在满足该警报的条件时记录生成的相应陷阱消息。

要修改预定义的 SNMP 警报，请单击 **System > SNMP > Alarms**。

配置 syslog 通知

SYSLOG 是一种标准日志记录协议。它包含两个组件：在 NetScaler SDX 设备上运行的 SYSLOG 审计模块，以及可在远程系统上运行的 SYSLOG 服务器。SYSLOG 使用 UDP 进行数据传输。

运行 SYSLOG 服务器时，它会连接到 SDX 设备。然后，设备开始将所有日志信息发送到 SYSLOG 服务器，服务器可以在将日志条目存储到日志文件之前对其进行筛选。一个 SYSLOG 服务器可以接

收来自多个 SDX 设备上的日志信息，一个 SDX 设备也可以将日志信息发送到多个 SYSLOG 服务器。

SYSLOG 服务器从 SDX 设备收集的日志信息以消息形式存储在日志文件中。 这些消息通常包含以下信息：

- 生成日志消息的 SDX 设备的 IP 地址
- 时间戳
- 消息类型
- 日志级别（严重、错误、通知、警告、信息、调试、警报或紧急）
- 消息信息

您可以使用此信息分析警报源，并在必要时采取纠正措施。首先配置设备发送日志信息的 syslog 服务器，然后指定记录日志消息的数据和时间格式。

配置 syslog 服务器

1. 导航到 **系统 > 通知 > Syslog 服务器**。
2. 在详细信息窗格中，单击 **添加**。
3. 在 **创建 Syslog 服务器** 页面中，为 syslog 服务器参数指定值。有关参数的说明，请将鼠标悬停在相应字段上。
4. 单击 **添加**，然后单击 **关闭**。

配置 syslog 参数

1. 导航到 **系统 > 通知 > Syslog 服务器**。
2. 在详细信息窗格中，单击 **Syslog Parameters**。
3. 在 **Configure Syslog Parameters** 页面上，指定日期和时间格式。
4. 单击 **OK**，然后单击 **Close**。

配置邮件通知

配置 SMTP 服务器，以便在每次发出警报时接收电子邮件。首先配置 SMTP 服务器，然后配置邮件配置文件。在邮件配置文件中，使用逗号分隔收件人的地址。

配置 SMTP 服务器

1. 导航到 **System（系统） > Notifications（通知） > Email（电子邮件）**。

2. 在详细信息窗格中，单击 **Email Server（电子邮件服务器）** 选项卡，然后单击 **Add（添加）**。
3. 在 **Create Email Server（创建电子邮件服务器）** 页面中，为服务器参数指定值。
 - **Server name / IP address（服务器名称/IP 地址）**：输入 SMTP 邮件服务器的服务器名称或 IP 地址。
 - **Port（端口）**：输入端口号。默认值为 25。
 - **Authentication（身份验证）**：选择此选项以验证对电子邮件服务器的访问。
 - **Secure（安全）**：选择此选项以创建安全的电子邮件连接。默认情况下，TLS 1.2 用于加密电子邮件通信。
4. 单击 **Create（创建）**。

配置邮件配置文件

1. 导航到 **System（系统） > Notifications（通知） > Email（电子邮件）**。
2. 在详细信息窗格中，单击 **Email（电子邮件）** 选项卡，然后单击 **Add（添加）**。
3. 在 **Create Email Distribution List（创建电子邮件分发列表）** 页面中，为参数指定值。有关参数的说明，请将鼠标悬停在相应的字段上。
4. 单击 **创建**。

配置短信通知

配置短消息服务 (SMS) 服务器，以便在每次触发警报时接收 SMS 消息。首先配置 SMS 服务器，然后配置 SMS 配置文件。在 SMS 配置文件中，使用逗号分隔收件人地址。

配置 SMS 服务器

1. 导航到 **系统 > 通知 > 短信**。
2. 在详细信息窗格中，单击 **SMS 服务器**，然后单击 **添加**。
3. 在 **创建 SMS 服务器** 页面中，指定 SMS 服务器参数的值。这些参数的值由供应商提供。
4. 单击 **创建**，然后单击 **关闭**。

配置 SMS 配置文件

1. 导航到 **系统 > 通知 > 短信**。
2. 在详细信息窗格中，单击 **SMS 分发列表**，然后单击 **添加**。
3. 在 **创建 SMS 分发列表** 页面中，指定邮件配置文件参数的值。要查看参数的说明，请将鼠标悬停在相应的字段上。

4. 单击 **创建**，然后单击 **关闭**。

监视和管理在 SDX 设备上配置的实体的实时状态

NetScaler SDX 设备可以监视和管理 SDX 设备上托管的虚拟设备中的虚拟服务器、服务、服务组和服务器的状态。您可以监视虚拟服务器的运行状况以及服务或服务组上次状态更改以来的时间等值。此监视使您能够了解实体的实时状态，并在 NetScaler 实例上配置了许多实体时，可以轻松管理这些实体。

仪表板(/en-us/sdx/media/entity-1-citrix.png)

查看虚拟服务器的状态

您可以监视虚拟服务器状态和运行状况的实时值。您还可以查看虚拟服务器的属性，例如名称、IP 地址和虚拟服务器类型。

查看虚拟服务器的状态

1. 在“配置”选项卡上的导航窗格中，单击 ****NetScaler > 实体 > 虚拟服务器****。
2. 在右侧窗格的“虚拟服务器”下，查看以下统计信息：
 - 设备名称 — 配置虚拟服务器的 VPX 的名称。
 - 名称 — 虚拟服务器的名称。
 - 协议 — 虚拟服务器的服务类型。例如，HTTP、TCP 和 SSL。
 - 有效状态 — 基于备份虚拟服务器状态的虚拟服务器的有效状态。例如，UP、DOWN 或 OUT OF SERVICE。
 - 状态 — 虚拟服务器的当前状态。例如，UP、DOWN 或 OUT OF SERVICE。
 - 运行状况 — 处于 UP 状态并绑定到虚拟服务器的服务百分比。以下公式用于计算运行状况百分比： $(\text{绑定 UP 服务的数量} \times 100) / \text{绑定服务的总数}$
 - IP 地址 — 虚拟服务器的 IP 地址。客户端将连接请求发送到此 IP 地址。
 - 端口 — 虚拟服务器侦听客户端连接的端口。
 - 上次状态更改 — 自虚拟服务器状态上次更改以来的经过时间（以天、小时、分钟和秒为单位）。即虚拟服务器处于当前状态的持续时间。此信息仅适用于在 NetScaler 9.0 及更高版本上配置的虚拟服务器。

! [仪表板1](https://docs.netScaler.com/content/dam/netScaler/us/en/sdx/media/entity-2-citrix.png)

查看绑定到虚拟服务器的服务和组

您可以监视绑定到虚拟服务器的服务和组的服务的实时状态。此监视功能可让您检查可能导致虚拟服务器运行状况百分比降低的服务状态，以便您可以采取适当措施。

要查看绑定到虚拟服务器的服务和组

1. 在“配置”选项卡上的左侧窗格中，单击 **NetScaler > 实体 > 虚拟服务器**。
2. 在详细信息窗格中的“虚拟服务器”下，单击要显示绑定服务和组的虚拟服务器的名称，然后在“操作”下，单击“绑定服务”或“绑定服务组”。或者，右键单击虚拟服务器的名称，然后单击“绑定服务”或“绑定服务组”。

NetScaler SDX > NetScaler > Entities > Virtual Servers							
Select Action	Protocol	Effective State	State	Health	IP Address	Port	Last State Change
ns2(10.102.163.5) v2	HTTP	Up	Up	100	10.102.161.13	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5) v3	SSL	Up	Up	100	10.102.161.14	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5) spotted_vip_1	HTTP	Up	Up	100	10.102.161.15	443	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5) spotted_vip_2	SSL	Up	Up	100	10.102.161.16	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5) spotted_vip_3	HTTP	Up	Up	100	10.102.161.71	443	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4) v1	HTTP	Up	Up	100	10.102.161.18	80	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4) v2	HTTP	Up	Up	100	10.102.161.13	80	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4) v3	SSL	Up	Up	100	10.102.161.14	80	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4) spotted_vip_1	HTTP	Up	Up	100	10.102.161.15	443	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4) spotted_vip_2	HTTP	Up	Up	100	10.102.161.16	80	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4) spotted_vip_3	SSL	Up	Up	100	10.102.161.71	443	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4) spotted_vip_3	HTTP	Up	Up	100	10.102.161.18	80	Mon, 10 Mar 2014 17:14:36 GMT

查看服务状态

您可以监视服务的实时状态值以及服务处于当前状态的持续时间。

要查看虚拟服务器的状态

1. 在“配置”选项卡上的导航窗格中，单击 **NetScaler > 实体 > 服务**。
2. 在详细信息窗格中的“服务”下，查看以下统计信息：
 - 设备名称 — 配置服务的设备的名称。
 - 名称 — 服务的名称。
 - 协议 — 服务类型，它决定了服务的行为。例如，HTTP、TCP、UDP 或 SSL。
 - 状态 — 服务的当前状态。例如，正常、关闭或停止服务。
 - IP 地址 — 服务的 IP 地址。
 - 端口 — 服务侦听的端口。
 - 上次状态更改 — 自服务状态上次更改以来的经过时间（以天、小时、分钟和秒为单位）。即服务处于当前状态的时长。

查看服务绑定的虚拟服务器

您可以查看服务绑定的虚拟服务器并监控虚拟服务器的实时状态。

要查看服务绑定的虚拟服务器

1. 在“配置”选项卡上，在导航窗格中，单击 **NetScaler > 实体 > 服务**。
2. 在详细信息窗格中，在“服务”下，单击要查看其绑定虚拟服务器的服务的名称。然后从“操作”菜单中选择“绑定虚拟服务器”。或者，右键单击该服务，然后单击“绑定虚拟服务器”。

! [仪表板3] (<https://docs.netScaler.com/content/dam/netScaler/us/en/sdx/media/entity-4-citrix.png>)

查看服务组的状态

您可以从 SDX 界面监控服务组成员的实时状态。

要查看服务组的状态

1. 在“配置”选项卡上，在导航窗格中，单击 **NetScaler > 实体 > 服务组**。
2. 在详细信息窗格中，在“服务组”下，查看以下统计信息：
 - 设备名称 — 配置服务组的设备的名称。
 - 名称 — 服务组的名称。
 - IP 地址 — 作为服务组成员的每个服务的 IP 地址。
 - 端口 — 服务组成员侦听的端口。
 - 协议 — 服务类型，它决定了服务组的行为。例如，HTTP、TCP、UDP 或 SSL。
 - 有效状态 — 虚拟服务器组的有效状态，基于备份虚拟服务器的状态。例如，UP、DOWN 或 OUT OF SERVICE
 - 状态 — 服务组的有效状态，基于服务组成员的状态。例如，UP、DOWN 或 OUT OF SERVICE。
 - 上次状态更改 — 自服务组成员上次状态更改以来的经过时间（以天、小时、分钟和秒为单位）。也就是说，服务组成员处于当前状态的时长。此信息仅适用于在 NetScaler 9.0 及更高版本上配置的服务组成员。

查看服务绑定的虚拟服务器

您可以查看服务绑定的虚拟服务器并监控虚拟服务器的实时状态。

要查看服务绑定的虚拟服务器

1. 在“配置”选项卡上，在左侧窗格中，单击 ****NetScaler > 实体 > 服务器****。
2. 在右侧窗格中，在“服务器”下，从列表中选择服务器，然后在“操作”菜单下，单击“绑定虚拟服务”。或者，右键单击服务并单击“绑定虚拟服务器”。

查看服务器状态

您可以监控和管理所有 NetScaler 实例中服务器的状态。此监控功能可让您了解服务器的实时状态，并在您拥有大量服务器时轻松管理这些服务器。

查看服务器状态

1. 在“配置”选项卡上的导航窗格中，单击 **NetScaler > 实体 > 服务器**。

2. 在详细信息窗格的“服务器”下，查看以下统计信息：

- 设备名称：指定配置服务器的设备的名称。
- 名称：指定服务器的名称。
- IP 地址：指定服务器的 IP 地址。客户端将连接请求发送到此 IP 地址。
- 状态：指定服务器的当前状态。例如，UP（正常）、DOWN（关闭）和 OUT OF SERVICE（停止服务）。
- 上次状态更改：指定自服务器上次状态更改以来经过的时间（以天、小时、分钟和秒为单位）。即服务器处于当前状态的持续时间。

Dashboard

Configuration

Documentation

Downloads

System

Service Formations

NetScaler

- Instances
- Clusters
- Admin Profiles
- Software Images
- SSL Certificates
- SSL Certificate Files
- Call Home
- Events
- Change Management
- Entities
 - Virtual Servers
 - Services
 - Service Groups
 - Servers

SECUREMATRIX CSB

NetScaler SDX > NetScaler > Entities > Servers

✓ Select Action
Enable
Disable

	Name	IP Address	State	Last State Change
ns2(10.102.163.5)	172.16.200.100	172.16.200.100	Ⓜ Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.101	172.16.200.101	Ⓜ Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.102	172.16.200.102	Ⓜ Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.103	172.16.200.103	Ⓜ Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.104	172.16.200.104	Ⓜ Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.105	172.16.200.105	Ⓜ Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.106	172.16.200.106	Ⓜ Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.107	172.16.200.107	Ⓜ Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.108	172.16.200.108	Ⓜ Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.109	172.16.200.109	Ⓜ Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.110	172.16.200.110	Ⓜ Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4)	172.16.200.100	172.16.200.100	Ⓜ Enabled	Mon, 10 Mar 2014 17:14:36 GMT

配置轮询间隔

您可以设置 SDX 设备轮询虚拟服务器、服务、服务组和服务器的实时值的时间间隔。默认情况下，设备每 30 分钟轮询一次值。

配置虚拟服务器、服务、服务组和服务器的轮询间隔。

1. 在“配置”选项卡上，单击 **NetScaler > 实体**，然后在右侧窗格中，单击“配置轮询间隔”。
2. 在“配置轮询间隔”对话框中，键入您希望设置为 SDX 轮询实体值的时间间隔的分钟数。轮询间隔的最小值为 30 分钟。单击“确定”。

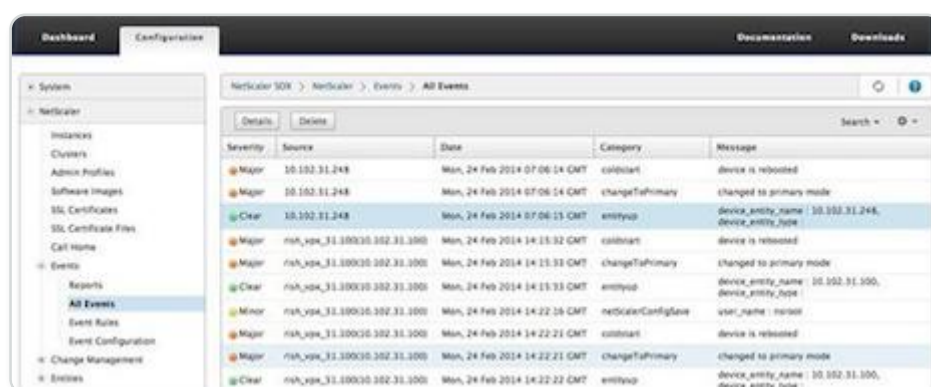
监控和管理 NetScaler 实例上生成的事件

使用事件功能监控和管理 NetScaler 实例上生成的事件。管理服务实时识别事件，帮助您立即解决问题并保持 NetScaler 实例高效运行。您还可以配置事件规则来筛选生成的事件，并接收通知以对筛选后的事件列表采取操作。

查看所有事件

您可以查看在 NetScaler SDX 设备上预置的 NetScaler 实例上生成的所有事件。您可以查看每个事件的详细信息，例如严重性、类别、日期、源和消息。

要查看事件，请导航到 **Configuration > NetScaler > Events > All Events**。



通过选择事件并单击 **Details** 按钮，您可以查看事件历史记录和实体详细信息。您还可以从此页面搜索特定事件或将其删除。

注意：删除事件后，将无法恢复。

- 查看报告

“报告”页面以图形格式显示事件摘要。您可以根据不同的时间范围查看报告。默认情况下，时间范围为“天”。

要显示报告，请导航到 **Configuration > NetScaler > Events > Reports**。以下是管理服务支持的图形报告

- 事件

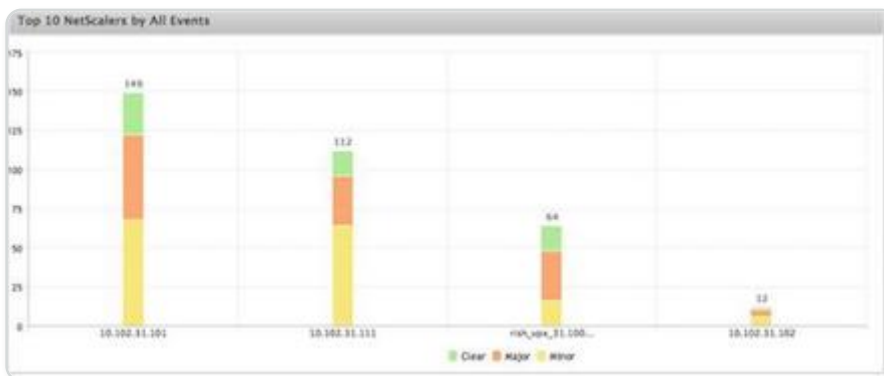
“事件”报告是一个饼图，显示事件数量，并根据其严重性进行分段和颜色编码。



要查看特定严重性事件的详细信息，请单击饼图的相应部分，您可以查看以下详细信息：

- 。来源：生成事件的系统名称、主机名或 IP 地址。
 - 。日期：生成警报的日期和时间。
 - 。类别：事件类别（例如，`entityup`）。
 - 。消息：事件描述。
- 。按所有事件排名的前 10 个 NetScaler 实例

此报告是一个条形图，显示在选定时间范围内根据事件数量排名的前 10 个 NetScaler 实例。



- 。按实体状态更改事件排名的前 10 个 NetScaler 实例

此报告是一个条形图，显示在选定时间范围内根据实体状态更改数量排名的前 10 个 NetScaler 实例。实体状态更改反映了实体启动、实体关闭或服务中断事件。



- **按阈值违规事件排名的前 10 个 NetScaler 实例**

此报告是一个条形图，显示在选定时间范围内根据阈值违规事件数量排名的前 10 个 NetScaler 实例。阈值违规事件反映了以下事件：

- CPU 利用率
- 内存利用率
- 磁盘使用率高
- 温度过高
- 电压过低
- 电压过高
- 风扇转速过低
- CPU 温度过高
- 接口吞吐量过低
- 接口带宽使用率过高
- 聚合带宽使用率过高

- **按硬件故障事件排名的前 10 个 NetScaler 实例** 此报告是一个条形图，根据所选时间范围内的硬件故障事件数量显示排名前 10 的 NetScaler 实例。硬件故障事件反映以下事件：

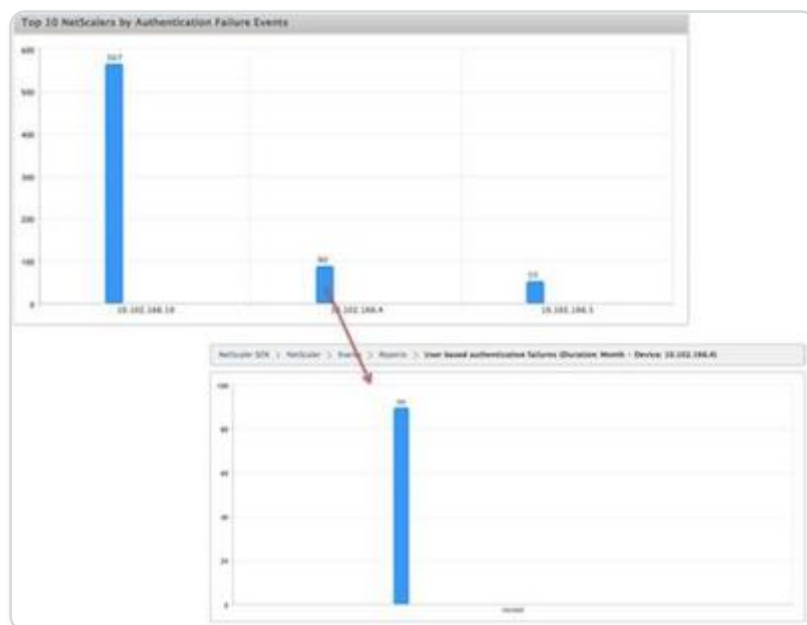
- 硬盘驱动器错误
- CompactFlash 错误
- 电源故障
- “SSL 卡故障”

- **按配置更改事件排名的前 10 个 NetScaler 实例**

此报告是一个条形图，根据所选时间范围内的配置更改事件数量显示排名前 10 的 NetScaler 实例。您可以单击图表以深入查看实例的用户配置更改。您可以通过单击此图表进一步查看授权和执行状态详细信息。

- **按身份验证失败事件排名的前 10 个 NetScaler 实例**

此报告是一个条形图，显示在选定时间范围内按身份验证失败事件数量排名的前 10 个 NetScaler 实例。您可以单击图表以深入查看某个实例的基于用户的身份验证失败。



- 配置事件规则

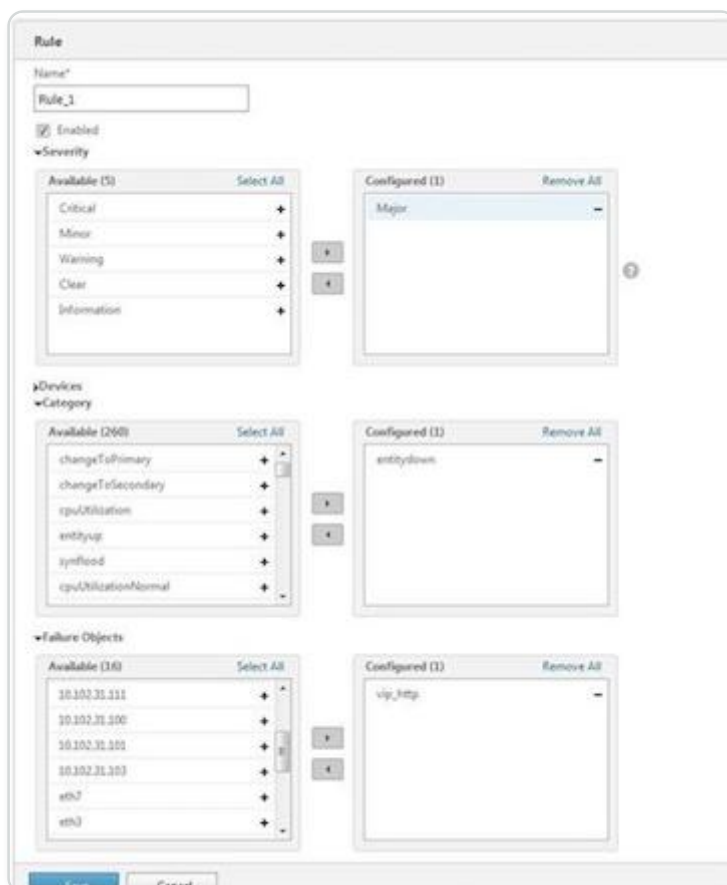
您可以通过配置具有特定条件并为规则分配操作的规则来筛选一组事件。当生成的事件符合规则中的筛选条件时，将执行与该规则关联的操作。您可以创建筛选器的条件包括：严重性、设备、失败对象和类别。

您可以为事件分配以下操作：

- **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。
- **发送短信操作** 针对符合筛选条件的事件发送短消息服务 (SMS)。

添加事件规则

- 导航到 **配置 > NetScaler > 事件 > 事件规则**，然后单击 **添加**。
- 在“规则”页面上设置以下参数：
 - **名称**—事件规则的名称。
 - **已启用**—启用事件规则。
 - **严重性**—要添加事件规则的事件的严重性。
 - **设备**—要为其定义事件规则的 NetScaler 实例的 IP 地址。
 - **类别**—由 NetScaler 实例生成的事件类别。
 - **故障对象**—已为其生成事件的实体实例或计数器。



注意：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以及所有证书相关事件的证书名称。

- c. 单击保存。
- d. 在“规则操作”下，您可以分配事件的通知操作。
 - a. 邮件配置文件—邮件服务器和邮件配置文件详细信息。当事件满足定义的筛选条件时，将触发一封电子邮件。
 - b. 短信配置文件—短信服务器和短信配置文件详细信息。当事件满足定义的筛选条件时，将触发一条短信。



- e. 单击完成。

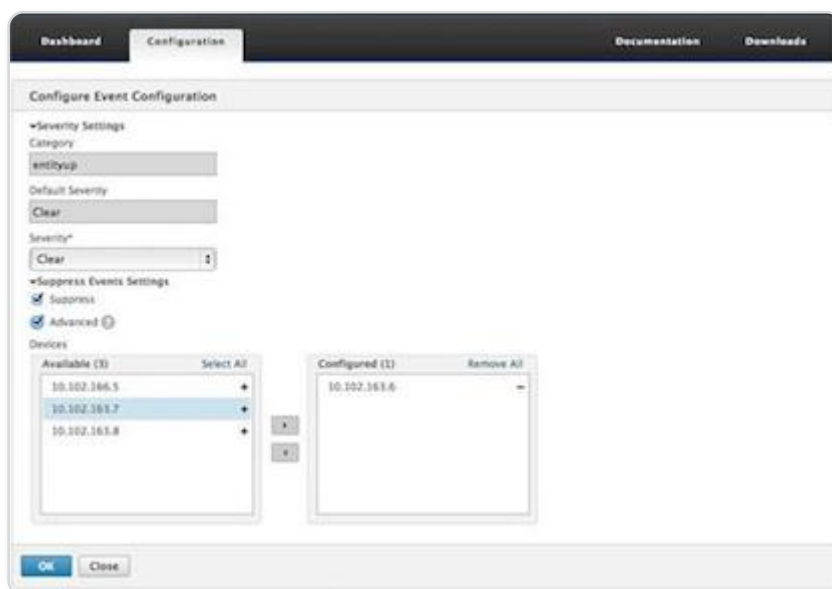
配置事件

您可以为 SDX 设备上的 NetScaler 实例生成的事件分配严重级别。您可以定义以下严重级别类型：严重、主要、次要、警告、清除和信息。您还可以抑制事件一段时间。要配置严重级别：

- a. 导航到 **Configuration > NetScaler > Events > Event Configuration**，从列表中选择事件，然后单击“配置严重级别”。



- b. 在“配置事件配置”页面上，从下拉列表中选择所需的严重级别。
- c. 此外，您可以通过选中“抑制”复选框来抑制事件。您还可以使用“高级”选项指定要抑制此事件的 NetScaler 实例。



- d. 单击“确定”。

SDX 设备上 NetScaler 实例的 Call Home 支持

Call Home 功能监控您的 NetScaler 实例是否存在常见错误情况。您现在可以从 Management Service 用户界面配置、启用或禁用 NetScaler 实例上的 Call Home 功能。

注意： NetScaler 实例必须先在 Citrix 技术支持服务器注册，然后 Call Home 才能在设备上出现预定义错误情况时将系统数据上传到服务器。在 NetScaler 实例上启用 Call Home 功能会启动注册过程。

在 NetScaler 实例上启用和禁用 Call Home

您可以从 Management Service 在 NetScaler 实例上启用 Call Home 功能。启用 Call Home 功能后，Call Home 进程会将 NetScaler 实例注册到 Citrix 技术支持服务器。注册需要一些时间才能完成。在此期间，Management Service 会显示注册进度。

要启用 Call Home 功能，请导航到 ****Configuration > NetScaler > Call Home****，选择 NetScaler 实例，然后单击“启用”按钮。在确认页面上，单击“是”。

要禁用 Call Home 功能，请导航到 ****Configuration > NetScaler > Call Home****，选择 NetScaler 实例，然后单击“禁用”按钮。在确认页面上，单击“是”。

如果您启用 Call Home，您可以配置以下选项：

1. （可选）指定管理员的电子邮件地址。Call Home 进程会将电子邮件地址发送到支持服务器，该服务器会存储该地址以供将来与 Call Home 相关的通信。
2. （可选）启用 Call Home 代理模式。Call Home 可以通过代理服务器将您的 NetScaler 实例数据上传到 Citrix TaaS 服务器。要使用此功能，请在您的 NetScaler 实例上启用它，并指定 HTTP 代理服务器的 IP 地址和端口号。从代理服务器到 TaaS 服务器（通过 Internet）的所有流量都通过 SSL 加密，因此数据安全和隐私不会受到损害。

从 Management Service 在 NetScaler 实例上配置 Call Home

您可以在单个实例上或同时在多个实例上配置 Call Home 功能。

要在单个 NetScaler 实例上配置 Call Home 功能，请导航到 ****Configuration > NetScaler > Call Home****，选择 NetScaler 实例，然后单击“配置”按钮。在“配置 Call Home”页面上，单击“确定”。

![Call Home 配置图 1](https://docs.netscaler.com/content/dam/netscaler/us/en/sdx/media/call-home-1-citrix.png)

要在多个 NetScaler 实例上配置 Call Home 功能，请导航到 **Configuration > NetScaler**。在右侧窗格中，单击“Call Home”。在“配置 Call Home”页面上，从“可用实例”部分选择 NetScaler 实例，指定其他详细信息，然后单击“确定”。

! [Call Home 配置图 2](https://docs.netscaler.com/content/dam/netscaler/us/en/sdx/media/call-home-2-citrix.png)

-

轮询 NetScaler 实例

要从所有 NetScaler 实例轮询 Call Home 功能并查看当前状态，请导航到 **配置 > NetScaler > Call Home**，然后点击 **立即轮询**。在确认页面上，点击 **是**。

系统运行状况监控

系统运行状况监控可检测受监控组件中的错误，以便您可以采取纠正措施以避免故障。NetScaler SDX 设备上监控以下组件：

- 硬件和软件资源
- 物理磁盘和虚拟磁盘
- 硬件传感器，例如风扇、温度、电压和电源传感器
- 接口

在 **Monitoring**（监控）选项卡中，单击 **System Health**（系统运行状况）。将显示所有组件的摘要。要查看受监控组件的详细信息，请展开 **System Health**（系统运行状况），然后单击要监控的组件。

- 监控 SDX 设备上的资源

您可以监控 SDX 设备上的硬件和软件组件，并在必要时采取纠正措施。要查看受监控的组件，请在“监控”选项卡中展开“系统运行状况”，然后单击“资源”。将显示硬件和软件资源的详细信息。

对于所有硬件组件，将显示当前值和预期值。对于软件组件（BMC 固件版本除外），当前值和预期值显示为不适用 (NA)。

- **名称：** 组件的名称，例如 CPU、内存或 BMC 固件版本。
- **状态：** 组件的状态（条件）。对于硬件和 BMC 固件版本，ERROR 表示与预期值存在偏差。对于对 Citrix Hypervisor™ 的调用，ERROR 表示管理服务无法使用 API、HTTP、PING 或 SSH 调用与 Citrix Hypervisor 通信。对于运行状况监控器插件，ERROR 表示该插件未安装在 Citrix Hypervisor 上。
- **当前值：** 组件的当前值。在正常情况下，当前值与预期值相同。
- **预期值：** 组件的预期值。不适用于对 Citrix Hypervisor 的软件调用。

监控 SDX 设备上的存储资源

您可以监控 SDX 设备上的磁盘，并在必要时采取纠正措施。要查看受监控的组件，请在 **Monitoring**（监控）选项卡中，展开 **System Health**（系统运行状况），然后单击 **Storage**（存储）。将显示物理磁盘以及从物理磁盘创建的虚拟磁盘或分区的详细信息。

对于磁盘 (Disk)，将显示以下详细信息：

- **名称** 物理磁盘的名称。
- **大小：** 磁盘大小，以 GB 为单位。
- **已用：** 磁盘上的数据量，以 GB 为单位。
- **事务/秒：** 每秒读取或写入的块数。此数字从 `iostat` 输出中读取。
- **读取块/秒：** 每秒读取的块数。您可以使用此值来衡量磁盘的输出速率。
- **写入块/秒：** 每秒写入的块数。您可以使用此值来衡量磁盘的输入速率。
- **总读取块数：** 自上次启动设备以来读取的块数。
- **总写入块数：** 自上次启动设备以来写入的块数。

对于虚拟磁盘或分区 (Storage Repository)，将显示以下详细信息：

- **驱动器托架：** 驱动器托架中驱动器的编号。您可以根据此参数对数据进行排序。
- **状态：** 驱动器托架中驱动器的状态（条件）。可能的值：
 - 良好：驱动器状态良好，可供使用。
 - 故障：驱动器已发生故障，必须更换。
 - 缺失：在驱动器托架中未检测到驱动器。
 - UNKNOWN: 驱动器托架中存在一个未格式化的新驱动器。

- **名称：** 存储库的系统定义名称。
- **大小：** 存储库的大小，单位为 GB。
- **已用：** 存储库中数据的量，单位为 GB。

监控 SDX 设备上的硬件传感器

您可以监控 SDX 设备上的硬件组件，并在必要时采取纠正措施。在**监控**选项卡中，展开**系统运行状况**，然后单击**硬件传感器**。监控功能会显示不同风扇的速度、不同组件的温度和电压以及电源状态的详细信息。

对于风扇速度，将显示以下详细信息：

- **名称：** 风扇的名称。
- **状态：** 风扇的状态（条件）。ERROR 表示偏离预期值。NA 表示风扇不存在。
- **当前值 (RPM)：** 当前每分钟转数。

温度信息包括以下详细信息：

- **名称：** 组件的名称，例如 CPU 或内存模块（例如，P1-DIMM1A）。
- **状态：** 组件的状态（条件）。ERROR 表示当前值超出范围。
- **当前值（摄氏度）：** 组件的当前温度，单位为摄氏度。

电压信息包括以下详细信息：

- **名称：** 组件名称，例如 CPU 核心。
- **状态：** 组件的状态（条件）。ERROR 表示当前值超出范围。
- **当前值（伏特）：** 组件上存在的当前电压。

有关电源的信息包括以下详细信息：

- **名称：** 组件名称。
- **状态：** 组件的状态（条件）。可能的值：
 - **错误：** 只有一个电源连接或正在工作。
 - **正常：** 两个电源都已连接并按预期工作。

监视 SDX 设备上的接口

您可以监视 SDX 设备上的接口，并在必要时采取纠正措施。在**监视**选项卡中，展开**系统运行状况**，然后单击**接口**。监视功能详细说明了每个接口的以下信息：

- **接口**：SDX 设备上的接口编号。
- **状态**：接口状态。可能的值：UP、DOWN。
- **已分配/总计的 VF**：分配给接口的虚拟功能 (VF) 数量，以及该接口上可用的虚拟功能数量。不同的平台支持不同数量的 VF。
- **发送数据包**：自设备上上次启动以来发送的数据包数量。
- **接收数据包**：自设备上上次启动以来接收的数据包数量。
- **发送字节**：自设备上上次启动以来传输的字节数。
- **接收字节**：自设备上上次启动以来接收的字节数。
- **发送错误**：自设备上上次启动以来数据传输中的错误数。
- **接收错误**：自设备上上次启动以来数据接收中的错误数。

配置系统通知设置

您可以发送通知，以便与选定的用户组就多项系统相关功能进行通信。您可以在 SDX Management Service 中设置通知服务器，以配置电子邮件和短消息服务 (SMS) 网关服务器，从而向用户发送电子邮件和文本 (SMS) 通知。

注意

升级到 SDX Management Service 11.1 版本后，将为所有事件类别启用系统通知，并且通知将发送到现有的电子邮件或 SMS 配置文件。

配置系统通知设置

1. 导航到 **系统 \> 通知 \> 设置**，然后单击 **更改通知设置**。
2. 在 **配置系统通知设置** 页面中，输入以下详细信息：
 - **类别** – SDX 管理服务生成的事件类别。
 - **电子邮件** – 从下拉菜单中选择一个电子邮件分发列表。您也可以通过单击 **+** 图标并在相应字段中输入新的电子邮件服务器详细信息来创建新的电子邮件分发列表。
 - **短信（文本消息）** – 从下拉菜单中选择一个短信分发列表。您也可以创建一个新的短信分发列表，方法是单击 **+** 图标并在相应字段中输入新的短信服务器详细信息。
3. 单击 **确定**。

从管理服务启用和禁用功能

注意

此功能在版本 13.1 build 12.x 及更高版本中可用。

在 NetScaler SDX 设备上，管理服务在后台轮询 NetScaler 实例以执行操作，例如 SSL 证书、网络功能和配置审计。可以根据您的要求选择启用或禁用此轮询。禁用此轮询可提高管理服务和 ADC 实例的性能。

使用 GUI 启用或禁用功能

1. 导航到 **系统 > 系统设置**。
2. 单击 **配置功能**。
3. 选择一个功能，然后单击 **Enable** 或 **Disable**。

配置管理服务

管理服务允许您管理客户端会话并执行配置任务，例如根据您的要求创建和管理用户帐户以及调整备份和清理策略。您还可以重新启动管理服务并升级管理服务的版本。您还可以创建管理服务和 Citrix Hypervisor™ 的 tar 文件并将其发送给技术支持。

管理客户端会话

当用户登录到管理服务时，会创建一个客户端会话。您可以在设备的“**会话**”窗格中查看所有客户端会话。

在“**会话**”窗格中，您可以查看以下详细信息：

- **用户名**：用于会话的用户帐户。
- **IP 地址**：创建会话的客户端的 IP 地址。
- **端口**：用于会话的端口。
- **登录时间**：在 SDX 设备上创建当前会话的时间。
- **上次活动时间**：在会话中上次检测到用户活动的时间。
- **会话过期时间**：会话过期剩余时间。

要查看客户端会话，请在“**配置**”选项卡上，导航到“**系统 > 会话**”。

要结束客户端会话，请在“**会话**”窗格中，单击要删除的会话，然后单击“**结束会话**”。

您无法从启动该会话的客户端结束会话。

配置策略

为了将日志数据的大小保持在可管理的范围内，SDX 设备会在指定时间自动运行备份和数据清除策略。

清除策略每天凌晨 00:00 运行，并指定设备上要保留的数据天数。默认情况下，设备会清除超过 3 天的数据，但您可以指定要保留的数据天数。只有事件日志、审计日志和任务日志会被清除。

备份策略每天凌晨 00:30 运行，并创建日志和配置文件备份。默认情况下，该策略保留三个备份，但您可以指定要保留的备份数量。此外，使用备份策略，您可以：

- 加密备份文件。
- 配置 SDX 设备，使用 FTP、SFTP 和 SCP 将备份文件传输到外部备份服务器。

要指定清除日志数据的天数：

1. 在“**Configuration**”选项卡上的导航窗格中，单击“**System**”。
2. 在“**System**”窗格中，在“**Policy Administration**”下，单击“**Prune Policy**”。
3. 在“**Modify Prune Policy**”对话框中，在“**Data to keep (days)**”中，指定设备在任何给定时间必须保留的数据天数。
4. 单击“**OK**”。

要配置备份策略：

1. 在“**Configuration**”选项卡上的导航窗格中，单击“**System**”。
2. 在“**System**”窗格中，在“**Policy Administration**”下，单击“**Backup Policy**”。
3. 在“**Modify Backup Policy**”对话框中，在“**Previous Backups**”中，指定设备在任何给定时间必须保留的备份数量。
4. 选择“**Encrypt Backup File**”以加密备份文件。
5. 选择 **外部传输** 并执行以下操作将备份文件传输到外部备份服务器：
 - a. 在 **服务器** 字段中，输入外部备份服务器的主机名或 IP 地址。
 - b. 在 **用户名** 和 **密码** 字段中，输入访问外部备份服务器的用户名和密码。
 - c. 在 **端口** 字段中，输入端口号。
 - d. 在 **传输协议** 字段中，选择要用于将备份文件传输到外部备份服务器的协议。
 - e. 在 **目录路径** 字段中，输入外部备份服务器中要存储备份文件的目录路径。
6. **传输后从管理服务中删除文件**：如果您希望在将备份文件传输到外部备份服务器后从 SDX 设备中删除备份文件，请选择此选项。
7. 单击 **确定**。

重新启动管理服务

您可以从 **系统** 窗格重新启动管理服务。重新启动管理服务不会影响实例的运行。在管理服务重新启动过程中，实例将继续运行。

重新启动管理服务：

1. 在 **配置** 选项卡上，在导航窗格中，单击 **系统**。

2. 在 **系统** 窗格中，在 **系统管理** 下，单击 **重新启动管理服务**。

删除管理服务文件

您可以从 SDX 设备中删除任何不需要的管理服务构建和文档文件。

删除管理服务文件：

1. 在“**配置**”选项卡上的导航窗格中，展开“**管理服务**”，然后单击要删除的文件。
2. 在“**详细信息**”窗格中，选择文件名，然后单击“**删除**”。

生成用于技术支持的 tar 存档

您可以使用“技术支持”选项生成数据和统计信息的 tar 存档，以提交给 Citrix® 技术支持。此 tar 存档可以为管理服务或 Citrix Hypervisor 生成，也可以同时为两者生成。然后，您可以将文件下载到本地系统并将其发送给 Citrix 技术支持。

在“**技术支持**”窗格中，您可以查看以下详细信息。

- **名称：** tar 存档文件的名称。文件名指示 tar 是用于管理服务还是 Citrix Hypervisor 服务器。
- **上次修改时间：** 此文件上次修改的日期。
- **大小：** tar 文件的大小。

生成用于技术支持的 tar 存档：

1. 在“**配置**”选项卡上，导航到“**诊断 > 技术支持**”。
2. 在“**详细信息**”窗格中，从“**操作**”列表中选择“**生成技术支持文件**”。
3. 在“**生成技术支持文件**”对话框中，从“**模式**”列表中选择相应的选项。
4. 单击“**确定**”。

下载用于技术支持的 tar 存档：

1. 在“**技术支持**”窗格中，选择要下载的技术支持文件。
2. 从“**操作**”列表中，选择“**下载**”。文件将保存到您的本地计算机。

管理服务的 CLI 支持

您现在可以使用 CLI 对管理服务执行操作。支持以下操作：

- 添加、设置、删除 — 用于配置资源。

- 执行 — 用于执行系统级操作。例如，管理服务升级或关机，或重新启动。
- 保存 — 用于添加接口，这些接口用于预配。

要访问 CLI，请从连接到管理服务 IP 地址的任何工作站启动安全外壳 (SSH) 客户端。使用管理员凭据登录。

您可以从手册页访问有关命令用法和语法的详细信息。

注意： 不支持通过控制台访问 CLI。

配置身份验证和授权设置

NetScaler SDX 管理服务的身份验证可以是本地的，也可以是外部的。通过外部身份验证，管理服务根据外部服务器的响应授予用户访问权限。管理服务支持以下外部身份验证协议：

- 远程身份验证拨入用户服务 (RADIUS)
- 终端访问控制器访问控制系统 (TACACS)
- 轻量级目录访问协议 (LDAP)

管理服务还支持来自 SSH 的身份验证请求。SSH 身份验证仅支持键盘交互式身份验证请求。SSH 用户的授权仅限于管理员权限。具有只读权限的用户无法通过 SSH 登录。

要配置身份验证，请指定身份验证类型并配置身份验证服务器。

通过管理服务的授权是本地的。管理服务支持两个级别的授权。具有管理员权限的用户可以对管理服务执行任何操作。具有只读权限的用户只能执行读取操作。SSH 用户的授权仅限于管理员权限。具有只读权限的用户无法通过 SSH 登录。

RADIUS 和 LDAP 的授权通过组提取支持。您可以在管理服务上配置 RADIUS 或 LDAP 服务器时设置组提取属性。提取的组名与管理服务上的组名匹配，以确定授予用户的权限。一个用户可以属于多个组。在这种情况下，如果用户所属的任何组具有管理员权限，则该用户具有管理员权限。可以在配置期间设置默认身份验证组属性。此组与提取的组一起用于授权。

在 TACACS 授权中，TACACS 服务器管理员必须允许具有管理员权限的用户使用特殊命令“admin”，并拒绝具有只读权限的用户使用此命令。当用户登录到 SDX 设备时，管理服务会检查用户是否具有运行此命令的权限。如果用户具有权限，则为用户分配管理员权限；否则，为用户分配只读权限。

添加用户组

组是需要访问公共信息或执行类似任务的用户的逻辑集合。您可以根据一组共同操作将用户组织到组中。通过向组而不是单个用户提供特定权限，您可以在创建用户时节省时间。

如果您使用外部身份验证服务器进行身份验证，则可以将 SDX 中的组配置为与身份验证服务器上配置的组匹配。当属于某个组（其名称与身份验证服务器上的组匹配）的用户登录并进行身份验证时，该用户将继承该组的设置。

添加用户组

1. 在“**Configuration**”选项卡上，在“**System**”下，展开“**User Administration**”，然后单击“**Groups**”。
2. 在详细信息窗格中，单击**添加**。

Create System Group

Group Name*
 ⓘ × Please enter value

Group Description

☐ System Access

Permission*
 read-write ⌵ ⓘ

☐ Configure User Session Timeout

Users

Available (2) Select All

nsroot	+
config-user	+

▶
◀

Configured (0) Remove All

No items

☒ All Instances

Create **Close**

3. 在**创建系统组**页面上，设置以下参数：

- 组名称
- 组描述

- 系统访问：选中此框可授予对整个 SDX 设备及其上运行的实例的访问权限。或者，对于实例级访问，请在**实例**下指定实例。
- 权限
- 配置用户会话超时
- 用户：属于该组的数据库用户。选择要添加到组的用户。

4. 单击**创建**和**关闭**。

****注意：****要在从版本 10.5 升级到版本 11.1 的 SDX 设备上创建具有管理员角色的组，请选择“读写”权限和“系统访问”复选框。在 SDX 10.5 中，此复选框不可用，并且权限值为“admin”和“read-only”。

配置用户帐户

用户登录 SDX 设备以执行设备管理任务。要允许用户访问设备，您必须在该 SDX 设备上为该用户创建用户帐户。用户在设备上执行本地身份验证。

****重要提示：****密码适用于 SDX 设备、管理服务和 Citrix Hypervisor。请勿直接在 Citrix Hypervisor 上更改密码。

配置用户帐户

1. 在“**Configuration**”选项卡上，在“**System**”下，展开“**Administration**”，然后单击“**Users**”。“Users”窗格显示现有用户帐户及其权限的列表。
2. 在“**Users**”窗格中，执行以下操作之一：
 - 要创建用户帐户，请单击“**Add**”。
 - 要修改用户帐户，请选择用户，然后单击“**Modify**”。
3. 在“**Create System User**”或“**Modify System User**”对话框中，设置以下参数：
 - 名称*—帐户的用户名。名称中允许使用以下字符：字母 a 到 z 和 A 到 Z、数字 0 到 9、句点 (.)、空格和下划线 (_)。最大长度：128。您无法更改名称。
 - 密码*—用于登录设备的密码。最大长度：128
 - 确认密码*—密码。
 - 权限*—用户在设备上的权限。可能的值：
 - admin—用户可以执行与管理服务相关的所有管理任务。
 - read-only—用户只能监视系统并更改帐户密码。默认值：admin。

- 启用外部身份验证—为此用户启用外部身份验证。管理服务在数据库用户身份验证之前尝试外部身份验证。如果此参数被禁用，则用户不会通过外部身份验证服务器进行身份验证。 **注意： **如果远程身份验证服务器不可访问，用户可能会失去对设备的访问权限。在这种情况下，身份验证将回退到默认的 admin 用户 (`nsroot`)。
- 配置会话超时—使您能够配置用户可以保持活动状态的时间段。指定以下详细信息：
 - 会话超时—用户会话可以保持活动状态的时间段。
 - 会话超时单位—超时单位，以分钟或小时为单位。
- 组—将组分配给用户。

***必填参数**

4. 单击“创建”或“确定”，然后单击“关闭”。您创建的用户将列在“用户”窗格中。

删除用户帐户

1. 在“配置”选项卡上的导航窗格中，展开“系统”，展开“管理”，然后单击“用户”。
2. 在“用户”窗格中，选择用户帐户，然后单击“删除”。
3. 在“确认”消息框中，单击“确定”。

设置身份验证类型

在管理服务界面中，您可以指定本地或外部身份验证。默认情况下，外部身份验证对本地用户禁用。可以通过勾选 启用外部身份验证选项来启用它，该选项在添加本地用户或修改用户设置时可用。

重要提示： 仅在设置 RADIUS、LDAP 或 TACACS 身份验证服务器后才支持外部身份验证。

设置身份验证类型

1. 在“配置”选项卡上的“系统”下，单击“身份验证”。
2. 在详细信息窗格中，单击“身份验证配置”。
3. 设置以下参数：
 - 服务器类型—为用户身份验证配置的身份验证服务器类型。可能的值：LDAP、RADIUS、TACACS 和本地。
 - 服务器名称 — 在管理服务中配置的身份验证服务器的名称。菜单中列出了为所选身份验证类型配置的所有服务器。
 - 启用回退本地身份验证 — 此外，当外部身份验证失败时，您可以选择使用本地身份验证对用户进行身份验证。此选项默认启用。

4. 单击“确定”。

启用或禁用基本身份验证

您可以使用基本身份验证对管理服务 NITRO 接口进行身份验证。从版本 13.1 build 59.x 开始，**允许基本身份验证**选项默认禁用。

执行以下操作以使用管理服务界面启用或禁用基本身份验证。

1. 在“**配置**”选项卡上，单击“**系统**”。
2. 在“**系统设置**”组中，单击“**更改系统设置**”。
3. 在“配置系统设置”对话框中，选中“**允许基本身份验证**”以启用，或清除“**允许基本身份验证**”以禁用。
4. 单击“**确定**”。

配置外部身份验证服务器

NetScaler SDX 管理服务可以使用本地用户帐户或通过外部身份验证服务器对用户进行身份验证。设备支持以下身份验证类型：

- **本地** — 使用密码对管理服务进行身份验证，无需引用外部身份验证服务器。用户数据存储在管理服务本地。
- **RADIUS** — 对外部 RADIUS 身份验证服务器进行身份验证。
- **LDAP** — 对外部 LDAP 身份验证服务器进行身份验证。
- **TACACS** — 对外部终端访问控制器访问控制系统 (TACACS) 身份验证服务器进行身份验证。

要配置外部身份验证，请指定身份验证类型并配置身份验证服务器。

添加 RADIUS 服务器

要配置 RADIUS 身份验证，请将身份验证类型指定为 RADIUS，并配置 RADIUS 身份验证服务器。

管理服务支持根据 RADIUS 规范进行 RADIUS 质询响应身份验证。可以在 RADIUS 服务器上为 RADIUS 用户配置一次性密码。当用户登录到 SDX 设备时，系统会提示用户指定此一次性密码。

添加 RADIUS 服务器

1. 在 **Configuration**（配置）选项卡上，在 **System**（系统）下，展开 **Authentication**（身份验证），然后单击 **Radius**（RADIUS）。
2. 在详细信息窗格中，单击 **Add**（添加）。

3. 在 **Create Radius Server**（创建 RADIUS 服务器）对话框中，键入或选择参数的值：

- **名称*** — 服务器名称。
- **服务器名称/IP 地址***—完全限定域名 (FQDN) 或服务器 IP 地址。 **注意：** DNS 必须能够将指定的 FQDN 解析为 IP 地址，并且只有主 DNS 用于解析 FQDN。要手动设置主 DNS，请参阅“添加用于 FQDN 名称解析的主 DNS”部分。
- **端口***—RADIUS 服务器运行的端口。默认值：1812。
- **超时***—系统等待 RADIUS 服务器响应的秒数。默认值：3。
- **密钥***—客户端和服务端之间共享的密钥。系统与 RADIUS 服务器之间通信需要此信息。
- **启用 NAS IP 地址提取**—如果启用，管理服务 IP 地址将根据 RADIUS 协议作为 `nasip` 发送到服务器。
- **NASID**—如果配置，此字符串将根据 RADIUS 协议作为 `nasid` 发送到 RADIUS 服务器。
- **组前缀**—用于 RADIUS 组提取的 RADIUS 属性中组名前缀的前缀字符串。
- **组供应商 ID**—用于 RADIUS 组提取的供应商 ID。
- **组属性类型**—用于 RADIUS 组提取的属性类型。
- **组分隔符**—用于 RADIUS 组提取的 RADIUS 属性中分隔组名称的组分隔符字符串。
- **IP 地址供应商标识符**—RADIUS 中表示内网 IP 的属性的供应商 ID。值为 0 表示该属性未进行供应商编码。
- **IP 地址属性类型**—RADIUS 响应中远程 IP 地址属性的属性类型。
- **密码供应商标识符**—RADIUS 响应中密码的供应商 ID。用于提取用户密码。
- **密码属性类型**—RADIUS 响应中密码属性的属性类型。
- **密码编码**—密码在从系统传输到 RADIUS 服务器的 RADIUS 数据包中必须如何编码。可能的值：pap、chap、mschapv1 和 mschapv2。
- **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。
- **记账**—使管理服务能够使用 RADIUS 服务器记录审计信息。

4. 单击“创建”，然后单击“关闭”。

添加 LDAP 身份验证服务器

要配置 LDAP 身份验证，请将身份验证类型指定为 LDAP，并配置 LDAP 身份验证服务器。

添加 LDAP 服务器

1. 在“**配置**”选项卡上，在“**系统**”下，展开“**身份验证**”，然后单击“**LDAP**”。

2. 在详细信息窗格中，单击“添加”。

3. 在“创建 LDAP 服务器”对话框中，键入或选择参数的值：

- 名称*—服务器的名称。
- 服务器名称/IP 地址*—FQDN 或服务器 IP 地址。**注意：**DNS 必须能够将指定的 FQDN 解析为 IP 地址，并且只有主 DNS 用于解析 FQDN。要手动设置主 DNS，请参阅“添加用于 FQDN 名称解析的主 DNS”部分。
- 端口*—LDAP 服务器运行的端口。默认值：389。
- 超时*—系统等待 LDAP 服务器响应的秒数。
- 基本 DN—LDAP 搜索必须开始的基本或节点。
- 类型—LDAP 服务器的类型。可能的值：Active Directory (AD) 和 Novell Directory Service (NDS)。
- 管理绑定 DN — 用于绑定到 LDAP 服务器的完整可分辨名称。
- 管理密码 — 用于绑定到 LDAP 服务器的密码。
- 验证 LDAP 证书 — 选中此选项以验证从 LDAP 服务器收到的证书。
- LDAP 主机名 — LDAP 服务器的主机名。如果启用了 validateServerCert 参数，此参数指定 LDAP 服务器证书上的主机名。主机名不匹配会导致连接失败。
- 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。
- 搜索筛选器 — 与默认 LDAP 用户搜索字符串结合以形成值的字符串。例如，`vpnallowed=true` 与 `ldaploginname` `samaccount` 和用户提供的用户名 `bob` 结合，将生成以下 LDAP 搜索字符串：`(&(vpnallowed=true)(samaccount=bob))`。
- 组属性 — 用于从 LDAP 服务器提取组的属性名称。
- 子属性名称 — 用于从 LDAP 服务器提取组的子属性名称。
- 安全类型 — 设备与身份验证服务器之间通信的加密类型。可能的值：

PLAINTEXT：无需加密。

TLS：使用 TLS 协议进行通信。

SSL：使用 SSL 协议进行通信
- 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。
- 引用 — 启用跟踪从 LDAP 服务器收到的 LDAP 引用。
- 最大 LDAP 引用数 — 要跟踪的最大 LDAP 引用数。

- 启用更改密码 — 允许用户在密码过期时修改密码。只有当配置的安全类型为 TLS 或 SSL 时，才能更改密码。
- 启用嵌套组提取 — 启用嵌套组提取功能。
- 最大嵌套级别 — 允许进行组提取的级别数。
- 组名称标识符 — 在 LDAP 服务器中唯一标识组的名称。
- 组搜索属性 — LDAP 组搜索属性。用于确定组所属的组。
- 组搜索子属性 — LDAP 组搜索子属性。用于确定组所属的组。
- 组搜索过滤器 — 与默认 LDAP 组搜索字符串组合以形成搜索值的字符串。

4. 单击“创建”，然后单击“关闭”。

对 LDAP 用户的 SSH 公钥身份验证支持

SDX 设备现在可以通过 SSH 公钥身份验证对 LDAP 用户进行登录身份验证。公钥列表存储在 LDAP 服务器中的用户对象上。在身份验证期间，SSH 从 LDAP 服务器提取 SSH 公钥。如果任何检索到的公钥支持 SSH，则登录成功。

提取的公钥的相同属性名称必须同时存在于 LDAP 服务器和 NetScaler SDX 设备中。

重要

对于基于密钥的身份验证，您必须通过在 `/etc/sshd_config` 文件中按以下方面设置 `Authorizedkeysfile` 的值来指定公钥的位置：

```
AuthorizedKeysFile .ssh/authorized_keys
```

系统用户。 您可以通过在 `/etc/sshd_config` * 文件中设置 `Authorizedkeysfile`` 的值来指定任何系统用户的公钥位置。

LDAP 用户。 检索到的公钥存储在 `/var/pubkey/<user_name>/tmp_authorized_keys-<pid>` 目录中。`pid` 是用于区分同一用户并发 SSH 请求的唯一编号。此位置是身份验证过程中用于保存公钥的临时位置。身份验证完成后，公钥将从系统中删除。

要使用该用户登录，请从 shell 提示符处运行以下命令：

```
$ ssh -i <private key> <username>@<IPAddress>
```

使用 GUI 配置 LDAP 服务器：

1. 导航到 **系统 > 认证 > LDAP**。

2. 在 LDAP 页面上，单击“**服务器**”选项卡。
3. 单击任何可用的 LDAP 服务器。
4. 在“**配置身份验证 LDAP 服务器**”页面上，选择“**身份验证**”。

The screenshot shows the 'Configure LDAP Server' page in NetScaler. The 'Name' field is 'ldap-ssh'. The 'Server Name / IP Address*' field contains '10.102.166.70'. The 'Security Type*' dropdown is set to 'TLS'. The 'Port*' field is '389'. The 'Server Type*' dropdown is set to 'AD'. The 'Time-out (seconds)*' field is '3'. There are checkboxes for 'Validate LDAP Certificate' and 'Authentication'. The 'SSH Public key*' field contains 'sshPublicKeys'.

注意：

清除“身份验证”复选框，以使用“sshPublicKeys”对 LDAP 用户进行身份验证。

为 FQDN 名称解析添加主 DNS

如果使用服务器的 FQDN 而不是其 IP 地址定义 RADIUS 或 LDAP 服务器，请手动设置主 DNS 以解析服务器名称。您可以使用 GUI 或 CLI。

要使用 GUI 设置主 DNS，请转到 **System > Network Configuration > DNS**。

要使用 CLI 设置主 DNS，请按照以下步骤操作。

1. 打开安全外壳 (SSH) 控制台。
2. 使用管理员凭据登录到 NetScaler SDX 设备。
3. 运行 `networkconfig` 命令。
4. 选择相应的菜单并更新 DNS IPv4 地址，然后保存更改。

如果再次运行 `networkconfig` 命令，您将看到更新后的 DNS 地址。

添加 TACACS 服务器

要配置 TACACS 身份验证，请将身份验证类型指定为 TACACS，并配置 TACACS 身份验证服务器。

添加 TACACS 服务器

1. 在**配置**选项卡上，在**系统**下，展开**身份验证**，然后单击**TACACS**。
2. 在详细信息窗格中，单击**添加**。
3. 在“创建 TACACS 服务器”对话框中，键入或选择以下参数的值：
 - 名称 — TACACS 服务器的名称
 - IP 地址 — TACACS 服务器的 IP 地址
 - 端口 — TACACS 服务器运行的端口。默认值：49
 - 超时 — 系统等待 TACACS 服务器响应的最长时间（秒）
 - TACACS 密钥 — 客户端和服务器之间共享的密钥。系统与 TACACS 服务器通信需要此信息
 - 记账 — 使管理服务能够使用 TACACS 服务器记录审计信息
 - 组属性名称 — 在 TACACS+ 服务器中配置的组属性的名称

创建 TACACS 服务器(/en-us/sdx/media/create-tacacs-server-citrix.png)

4. 单击 **创建**，然后单击 **关闭**。

从管理服务配置链路聚合

链路聚合将多个以太网链路组合成一个高速链路。配置链路聚合可提高 NetScaler SDX 设备与其他连接设备之间通信通道的容量和可用性。聚合链路也称为“通道”。

当网络接口绑定到通道时，通道参数优先于网络接口参数。（即，网络接口参数将被忽略。）一个网络接口只能绑定到一个通道。

当网络接口绑定到通道时，它会丢弃其 VLAN 配置。该接口将从其最初所属的 VLAN 中移除，并添加到默认 VLAN。但是，您可以将通道重新绑定到旧 VLAN 或新 VLAN。例如，如果您将网络接口 1/2 和 1/3 绑定到 ID 为 2 的 VLAN (VLAN 2)，然后将它们绑定到通道 LA/1，则网络接口将移至默认 VLAN，但您可以将通道绑定到 VLAN 2。

注意：

- 一个接口必须只属于一个通道。
- 配置通道至少需要两个接口。
- 当您添加或修改 NetScaler 实例时，构成通道的接口不会显示在“网络设置”视图中。而是列出通道。

如果您使用分配给一个实例的三个接口配置通道，并且第二个实例使用其中一些接口，则管理服务将关闭第二个实例，修改网络设置，然后重新启动该实例。例如，假设有两个实例，Instance1 和 Instance2。配置这些实例时，接口 10/1、10/2 和 10/3 分配给 Instance1，接口 10/1 和 10/2 分配给 Instance2。如果使用接口 10/1、10/2 和 10/3 创建 LA 通道，则 Instance1 不会重新启动。但是，管理服务会关闭 Instance2，将接口 10/3 分配给 Instance2，然后重新启动 Instance2。

如果您从 LA 通道中移除接口，更改将存储在数据库中，并且当您添加或修改实例时，该接口会显示在“网络设置”视图中。在删除接口之前，仅列出该接口所属的通道。

从管理服务配置通道

您可以手动配置通道，也可以使用链路聚合控制协议 (LACP)。您不能将 LACP 应用于手动配置的通道，也不能手动配置由 LACP 创建的通道。从管理服务配置通道。然后在预配或修改 NetScaler 实例时选择该通道。

LA 通道是一个逻辑实体，用于提供链路冗余和带宽聚合。属于通道的接口不能分配单独的 IP 地址。

注意： NetScaler SDX 设备支持链路聚合，但不支持链路冗余。从 NetScaler 13.1 版本 27.x 及更高版本开始，明确不支持在 NetScaler SDX 设备上托管的 NetScaler VPX 实例上进行链路冗余配置。

从管理服务配置通道

1. 导航到 **System > Channels**。
2. 在详细信息窗格中，单击 **Add**。
3. 在 **Add Channel** 对话框中，设置以下参数：
 - 通道 ID — 要创建的 LA 通道的 ID。以 LA/x 格式指定 LA 通道，其中 x 的范围是 1 到接口数量的一半。LA 通道创建后无法更改。
 - 类型 — 通道类型。可能的值：
 - 静态 — 仅在数据接口上配置。
 - 主动-主动 — 仅在管理接口 0/x 上配置。
 - 主动-被动 — 仅在管理接口 0/x 上配置。
 - LACP — 在数据接口和管理接口 0/x 上配置。
 - 吞吐量（仅适用于静态通道和 LACP）— LA 通道吞吐量的低阈值，单位为 Mbps。在 HA 配置中，如果 LA 通道启用了 HA MON 且吞吐量低于指定阈值，则会触发故障转移。

- 带宽高（仅适用于静态通道和 LACP）—LA 通道的带宽使用率高阈值，单位为 Mbps。当 LA 通道的带宽使用率等于或大于指定的高阈值时，设备会生成 SNMP trap 消息。
 - 带宽正常（仅适用于静态通道和 LACP）—LA 通道的带宽使用率正常阈值，单位为 Mbps。当 LA 通道的带宽使用率在超过高阈值后，等于或低于指定的正常阈值时，NetScaler SDX 设备会生成 SNMP trap 消息，指示带宽使用率已恢复正常。
4. 在“**接口**”选项卡上，添加要包含在此通道中的接口。
 5. 在“**设置**”选项卡上，设置以下参数：
 - 通道状态（仅适用于静态通道）—启用或禁用 LA 通道。
 - LACP 时间（仅适用于 LACP）—如果链路未收到 LACPDU，则在此时间后链路将不再聚合。该值必须与 SDX 设备和伙伴节点上参与链路聚合的所有端口匹配。
 - HA 监控—在高可用性 (HA) 配置中，监控通道的故障事件。任何启用了 HA MON 的 LA 通道发生故障都会触发 HA 故障转移。
 - 标记所有—为此通道上发送的每个数据包添加一个四字节的 802.1q 标记。“ON”设置将标记应用于绑定到此通道的所有 VLAN。“OFF”将标记应用于除本机 VLAN 之外的所有 VLAN。
 - 别名—LA 通道的别名。仅用于提高可读性。要执行任何操作，必须指定 LA 通道 ID。
 6. 单击“**创建**”，然后单击“**关闭**”。

备注

- 如果 0/1 和 0/2 接口都属于 VPX 实例，并且该实例是群集的一部分，则无法创建管理 LA。
- 如果管理 LA 属于 VPX 实例，并且该实例是群集的一部分，则无法删除管理 LA。

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筛选 IP 流量并保护您的设备免受未经授权的访问。

您可以在 NetScaler SDX Management Service GUI 上配置 ACL，以限制和控制对设备的访问。

注意：

SDX 设备上的 ACL 从版本 12.0 57.19 开始受支持。

本主题包括以下部分：

- 使用准则
- 如何配置 ACL
- ACL 规则的其他操作
- 故障排除

使用准则

在设备上创建 ACL 时，请记住以下几点：

- 当您将 SDX 设备升级到版本 11.0 57.19 时，ACL 功能默认处于禁用状态。
- SDX 管理员只能通过 SDX 设备上的 ACL 控制入站数据包。
- 如果您使用 NetScaler® Application Delivery Management 来管理您的 SDX 设备，则必须创建适当的 ACL 规则以允许 MAS 和 SDX Management Service 之间的通信。
- SDX 设备上的任何其他配置，例如预配或删除 VPX、添加/删除外部服务器、SNMP 管理，都不需要更改现有的 ACL 配置。与这些实体的通信由管理服务负责。

如何配置 ACL

配置 ACL 涉及以下步骤：

- 启用 ACL 功能
- 创建 ACL 规则
- 启用 ACL 规则

注意：

您可以在不启用 ACL 功能的情况下创建 ACL 规则。但是，如果未启用该功能，则在创建 ACL 规则后无法启用它。

启用 ACL 功能

1. 要启用 ACL 功能，请登录 SDX 管理服务 GUI 并导航到 **Configuration > System > ACL**。
2. 使用切换按钮，打开 ACL 功能。



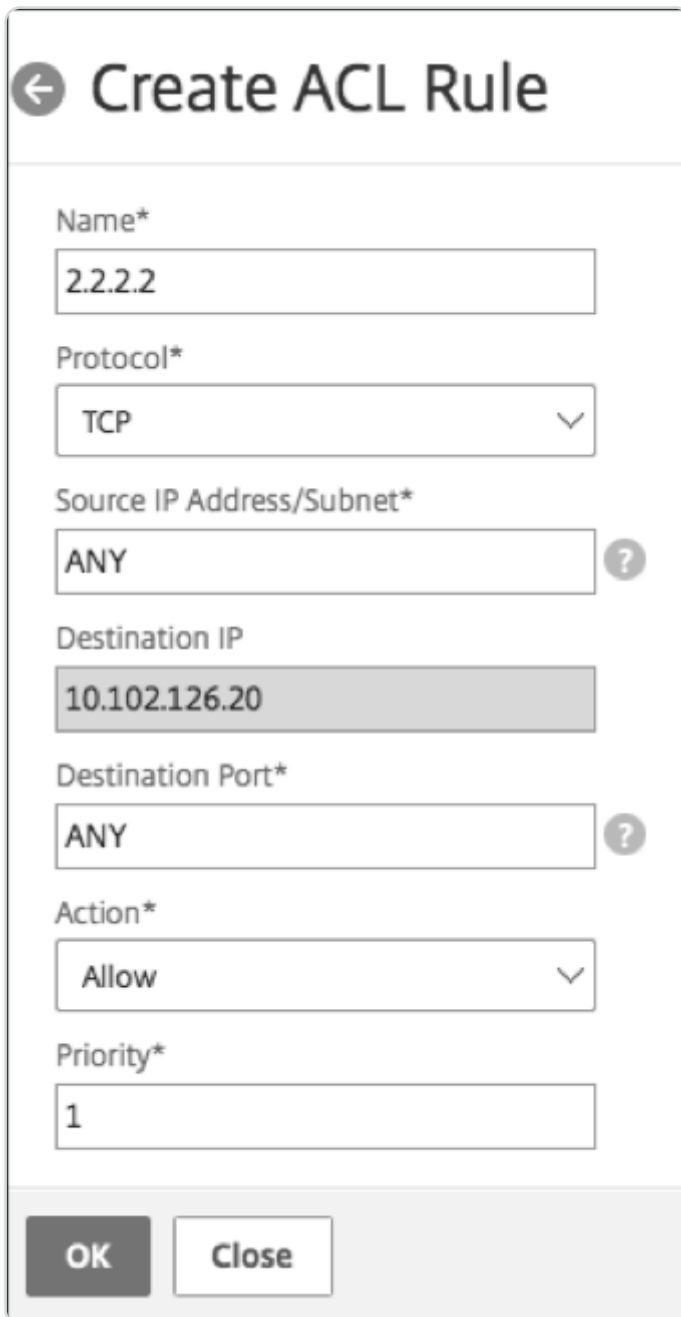
创建 ACL 规则

1. 在 ACL 页面上，单击 **Create Rule**。
2. **Create Rule** 窗口打开。添加下表中列出的详细信息。

|属性|描述| |--|--| |名称|添加名称。| |协议|从菜单中选择协议。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|SDX 管理服务 IP 地址将自动填充为目标 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 **ANY**。| |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。较低的优先级数字具有较高的优先级。例如，优先级数字 1 比优先级数字 1 具有更高的优先级。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** 以创建规则。

图：ACL 规则示例



The image shows a 'Create ACL Rule' dialog box. It has a back arrow icon and the title 'Create ACL Rule'. The form contains the following fields: 'Name*' with the value '2.2.2.2'; 'Protocol*' with a dropdown menu showing 'TCP'; 'Source IP Address/Subnet*' with the value 'ANY' and a help icon; 'Destination IP' with the value '10.102.126.20'; 'Destination Port*' with the value 'ANY' and a help icon; 'Action*' with a dropdown menu showing 'Allow'; and 'Priority*' with the value '1'. At the bottom are 'OK' and 'Close' buttons.

← Create ACL Rule

Name*
2.2.2.2

Protocol*
TCP

Source IP Address/Subnet*
ANY

Destination IP
10.102.126.20

Destination Port*
ANY

Action*
Allow

Priority*
1

OK Close

规则创建后，处于禁用状态。要使规则生效，必须启用该规则。

注意：

要启用规则，必须启用 ACL 功能。如果该功能已禁用，并且您尝试启用 ACL 规则，则会显示消息“ACL 未运行”。

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. 在提示符下，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：

1. 禁用 ACL 规则
2. 编辑 ACL 规则
3. 删除 ACL 规则
4. 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”选项卡。
4. 单击“是”以确认。

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. 从列表中单击“编辑规则”。“修改规则”窗口将打开。
3. 或者，选择该规则的单选按钮，然后单击“编辑规则”选项卡。“修改规则”窗口将打开。
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，则更改会立即生效。对于处于禁用状态的规则，更改会在您启用规则时生效。

删除 ACL 规则

1. 确保规则处于禁用状态。
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。从列表中单击“删除规则”。

3. 或者，选择该规则的单选按钮，然后单击“删除规则”选项卡。
4. 单击“是”进行确认。

注意：

您不能删除处于启用状态的规则。

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。从列表中单击“重新编号优先级”。
2. 或者，选择该规则的单选按钮，然后单击“选择操作”选项卡。
3. 选择“重新编号优先级”。
4. SDX 管理服务会自动为所有现有规则分配新的优先级编号，这些编号是 10 的倍数。
5. 编辑规则以根据您的要求分配优先级编号。有关如何编辑规则的更多信息，请参阅“编辑 ACL 规则”部分。

图. 现有优先级编号示例

☐	Priority ↑	Name	Source IP Address/Subnet
☐	1	2.2.2.2	ANY
☐	2	test1	1.1.1.1
☐	3	test2	ANY

图. 重新编号后，优先级编号为 10 的倍数的示例

☐	Priority ↑	Name	Source IP Address/Subnet
☐	10	2.2.2.2	ANY
☐	20	test1	1.1.1.1
☐	30	test2	ANY

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 设置不当而意外丢失对 SDX Management Service 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 和您的“root”帐户登录到 Citrix Hypervisor™ 管理 IP 地址。

2. 使用管理员权限登录到 Management Service VM 的控制台。
3. 运行命令 `pfctl -d`。
4. 通过 GUI 登录到 Management Service 并相应地重新配置 ACL。

设置 NetScaler 实例集群

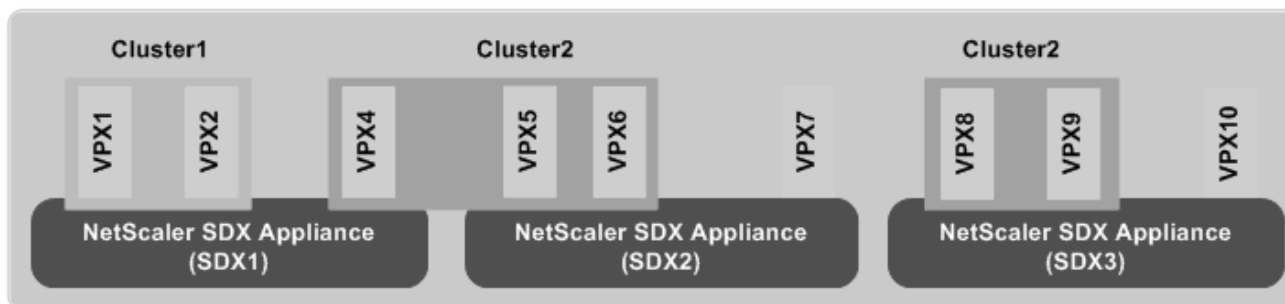
在一台或多台 SDX 设备上预配 NetScaler 实例后，您可以创建 NetScaler 实例集群。

Citrix® 建议您从 Management Service 执行集群配置。当您从 VPX 实例执行集群配置时，Management Service 会在每 30 分钟的自动发现过程中了解配置。在最坏的情况下，集群信息可能在 30 分钟内未被发现。虽然集群可能正常工作，但会遗漏一些针对集群依赖项的基本验证检查。Management Service 在 ADC 实例上配置集群之前会执行这些检查。因此，您必须从 Management Service 执行任何集群配置。

注意：

- 要设置集群，您必须了解 NetScaler 集群。有关更多信息，请参阅[集群](#)。
- 对于跨 SDX 设备拥有 NetScaler 实例的集群，Citrix 建议您使用来自三台 SDX 设备的 NetScaler 实例。此过程可确保始终满足至少 $(n/2 + 1)$ 个节点的集群标准。

图 1. SDX NetScaler 实例集群



上图显示了同一子网上的三台 SDX 设备：SDX1、SDX2 和 SDX3。这些设备上的 NetScaler 实例用于形成两个集群：Cluster1 和 Cluster2。

- Cluster1 包含 SDX1 上的两个实例。
- Cluster2 包含 SDX1 上的一个实例、SDX2 上的两个实例以及 SDX3 上的另外两个实例。

注意事项

- 建议为集群的每个节点使用 6 GB RAM。
- 托管在 NetScaler SDX™ 设备上的 NetScaler VPX 实例必须配置专用核心。
- SDX 平台不支持使用 Mellanox 接口（50G 和 100G）形成 CLAG。

- 集群中的所有节点必须是相同类型。您不能使用以下组合来形成集群：
 - 硬件设备和虚拟设备。
 - NetScaler VPX 实例和 NetScaler SDX 实例。
 - 不同 SDX 硬件平台上的 ADC 实例。
- NetScaler 实例必须是相同版本，且必须是 10.1 或更高版本。
- 所有 NetScaler 实例必须具有相同的功能许可证。
- 将配置添加到集群后，无法在单个 NetScaler 实例上更新配置。所有更改都必须通过集群 IP 地址执行。
- 所有 NetScaler 实例必须具有相同的资源（内存、CPU、接口等）。
- 背板 MTU 必须比数据接口 MTU 大 78 字节。
- 确保任何数据接口 MTU 在 9138 字节以内。
- 从版本 13.0 build 82.x 开始，在向集群添加节点时，系统会提示您添加 SNIP 地址。您还可以在添加节点时动态创建 SNIP 地址。此功能有助于解决严格源 IP 地址检查上的安全问题。
- **重要提示！** 请谨慎使用 **删除集群** 选项。当您单击 **删除集群** 时，集群将在没有任何警告的情况下被删除。

在 SDX 设备上设置集群

1. 登录到 SDX 设备。
2. 在 **Configuration** 选项卡上，导航到 **NetScaler > Clusters > Cluster Instances**。
3. 创建群集：
 - a. 单击“**创建群集**”。
 - b. 在“**创建群集**”对话框中，设置群集所需的参数。要查看参数说明，请将鼠标光标悬停在相应字段上。
 - c. 单击“**下一步**”以查看配置摘要。
 - d. 单击“**完成**”以创建群集。注意：当配置了 L2 VLAN 的 NetScaler 实例添加到群集时，`add VLAN` 命令将与 `sdxvlan` 参数设置为“是”一起保存。此参数是一个内部参数，用于避免在 SDX 群集形成期间丢失连接。
4. 向群集添加节点：
 - a. 单击“**添加节点**”。

- b. 在“**添加节点**”对话框中，配置添加群集节点所需的参数。要查看参数说明，请将鼠标光标悬停在相应字段上。
- c. 单击“**下一步**”以查看配置摘要。
- d. 单击“**完成**”以将节点添加到群集。
- e. 重复步骤 1 到 4 以向群集添加另一个节点。

创建群集后，必须通过群集 IP 地址访问它来对其进行配置。

如果群集实例中的节点属于同一 Citrix NetScaler SDX 设备，则当 NetScaler SDX 设备发生故障时，我们可能会失去仲裁。

您可以使用以下方法部署群集节点：

1. 从每个 NetScaler SDX 设备创建一个 VPX 实例，创建多个群集实例。

示例：

SDX1	SDX2	实例ID
VPX1	VPX1	1
VPX2	VPX2	2

1. 如果存在两个以上的 NetScaler SDX 设备，则使用来自所有设备的 VPX 实例创建单个集群实例，并使用 `quorumType Majority`。在这种情况下，请确保 VPX 实例在所有 NetScaler SDX 设备上均匀分布。

示例1：

SDX1	SDX2	SDX3	实例ID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	NA
VPX3	VPX3	VPX3	NA

示例2：

SDX1	SDX2	SDX3	INSTANCEID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	NA
VPX3	VPX3	VPX3	NA
VPX4	不适用	不适用	不适用

1. 使用所有 NetScaler SDX 设备中的所有 VPX 实例创建一个单独的群集实例。但使用 `quorum type NONE`。这有一些限制。

示例：

SDX1	SDX2	INSTANCEID
VPX1	VPX1	1
VPX2	VPX2	2
VPX3	不适用	不适用

当 `-quorumType` 参数设置为 `NONE` 时的限制：

- 拓扑必须在群集节点之间具有冗余链接，以避免因单点故障导致网络分区。
- 在任何群集操作（例如节点添加或移除）期间，群集可能会变得不稳定。

注意：

要获取 NetScaler 群集的更新列表（其中每个群集都至少有一个 SDX 设备上的 NetScaler 实例），请使用“重新发现”选项。

将存在于一个 SDX 设备上的 NetScaler 实例添加到配置在另一个 SDX 设备上的群集

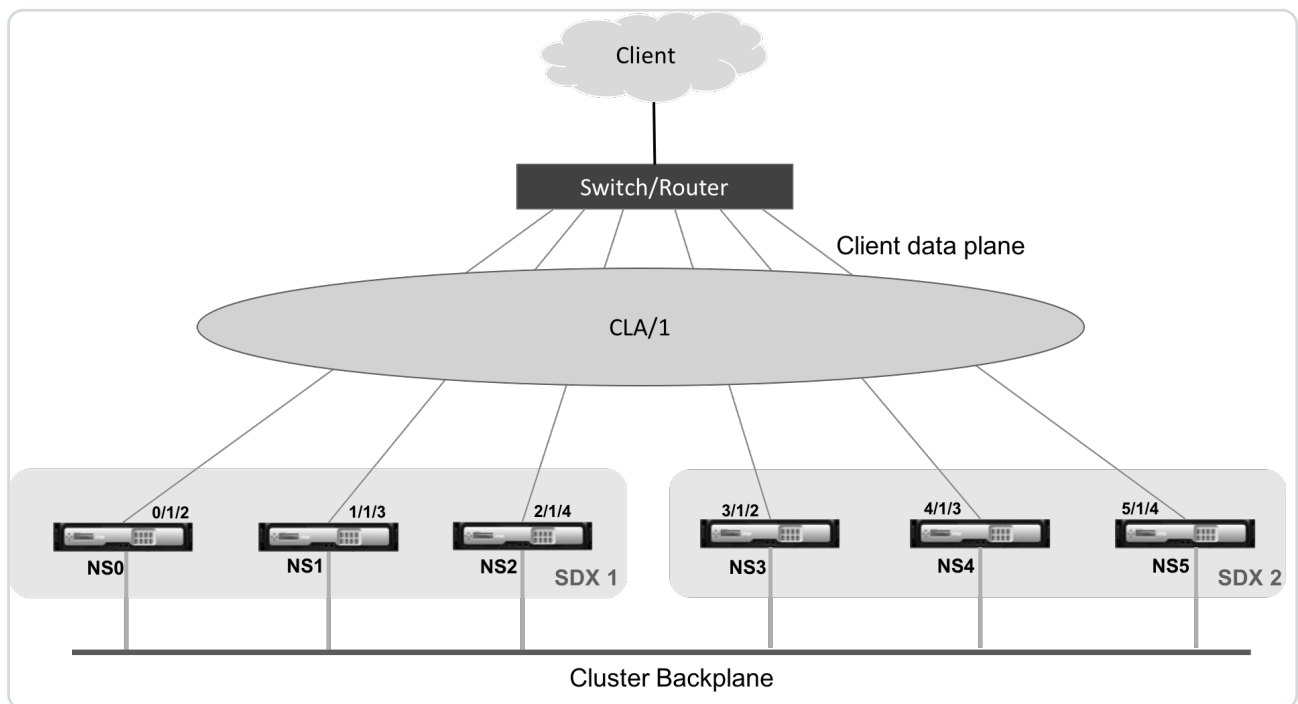
1. 登录到您要从中添加 NetScaler 实例的 SDX 设备。
2. 在“配置”选项卡上，导航到“NetScaler”，然后单击“群集”。
3. 单击“添加节点”。

4. 在“添加节点”对话框中，配置添加群集节点所需的参数。有关参数的说明，请将鼠标光标悬停在相应字段上。注意：请确保 群集 IP 地址和 群集 IP 密码参数的值是您要添加节点的群集的值。
5. 单击“下一步”以查看配置摘要。
6. 单击“完成”以将节点添加到群集。

配置集群链路聚合

集群链路聚合，顾名思义，将一组集群节点接口组合成一个通道。它是 NetScaler 链路聚合 (LA) 的扩展。唯一的区别是，链路聚合要求接口位于同一设备上，而集群链路聚合中的接口位于集群的不同节点上。有关链路聚合的更多信息，请参阅[配置链路聚合](#)。

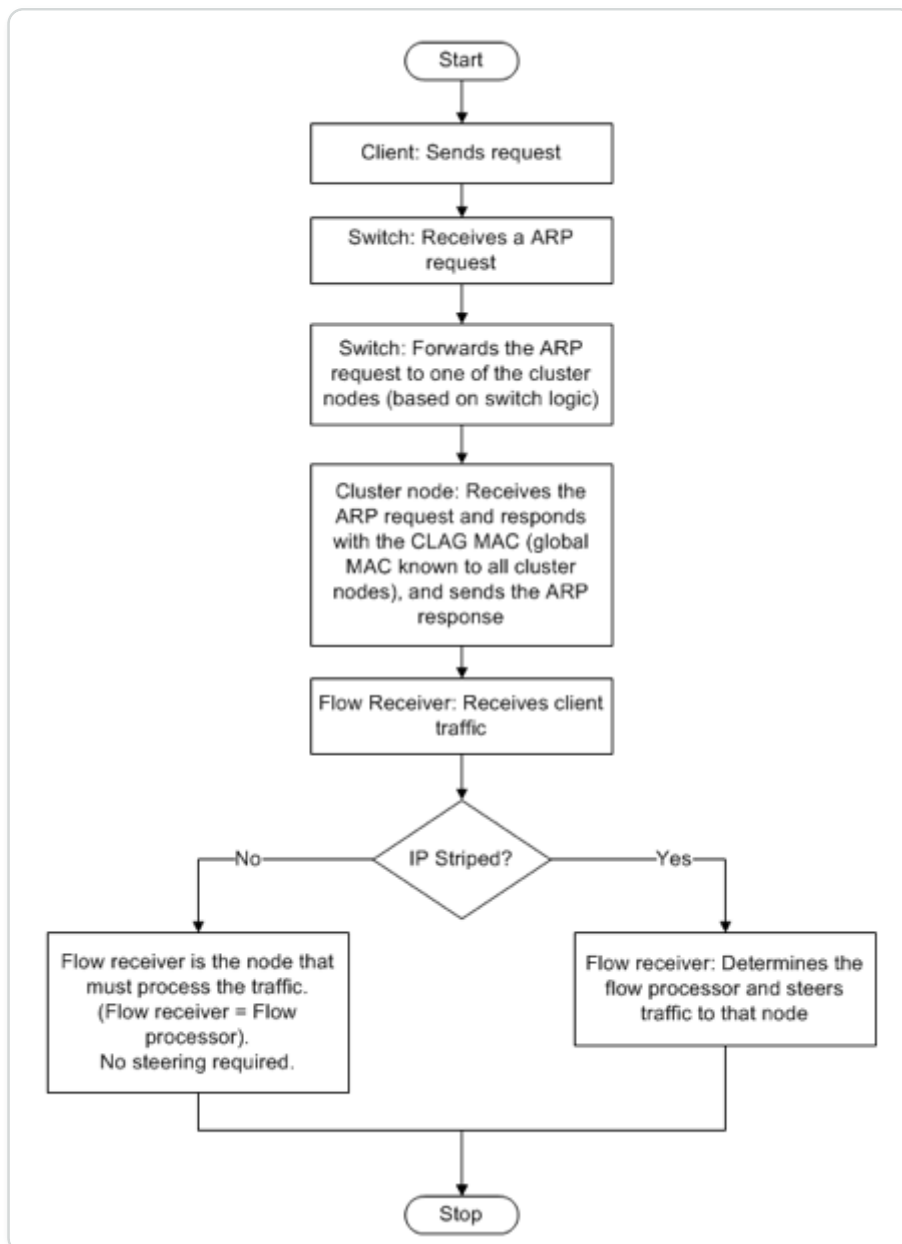
例如，考虑一个由两个 SDX 设备组成的六节点集群，其中所有六个节点都连接到上游交换机。通过绑定接口 0/1/2、1/1/3、2/1/4、3/1/2、4/1/3 和 5/1/4 形成一个集群 LA 通道 (CLA/1)。



集群 LA 通道具有以下属性：

- 每个通道都具有由集群节点协商确定的唯一 MAC 地址。
- 该通道可以绑定本地和远程 SDX 节点的接口。
- 一个集群中最多支持四个集群 LA 通道。
- 每个集群 LA 通道最多可绑定 16 个接口。
- 背板接口不能是集群 LA 通道的一部分。
- 当接口绑定到集群 LA 通道时，通道参数优先于网络接口参数。
- 一个网络接口只能绑定到一个通道。

- 请勿在集群 LA 通道（例如 CLA/1）或其成员接口上配置对集群节点的管理访问。当节点处于 INACTIVE 状态时，相应的集群 LA 接口将被标记为 POWER OFF，这将导致其失去管理访问权限。



在集群 IP 地址和外部连接设备上实施类似的配置。如果可能，请将上游交换机配置为根据 IP 地址或端口而不是 MAC 地址分发流量。

要点：

- 启用 LACP（通过将 LACP 模式指定为 ACTIVE 或 PASSIVE）。

注意： 确保 NetScaler 群集和外部连接设备上的 LACP 模式均未设置为 PASSIVE。

- 对于创建群集 LA 通道，LACP 密钥的值可以为 5 到 8。这些 LACP 密钥映射到 CLA/1、CLA/2、CLA/3 和 CLA/4。

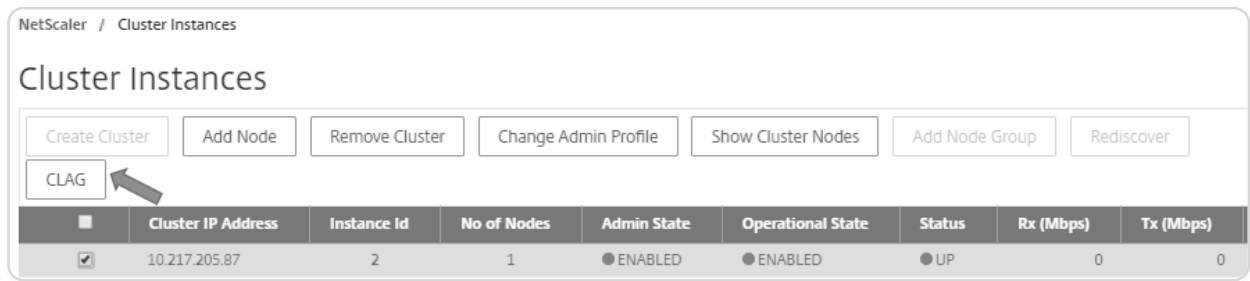
- 在 SDX 设备上，群集链路聚合组 (CLAG) 成员接口无法与其他虚拟机共享。
- 在上游交换机上，将 LACP 超时设置为“短”，以避免群集节点上出现长时间的流量黑洞。当上游交换机在 LACP 超时后才收到 CLAG 及其成员接口断电的通知时，此设置非常有用。

先决条件：

创建 NetScaler 实例群集。群集节点可以是同一 SDX 设备上的 NetScaler 实例，也可以是同一子网上可用的其他 SDX 设备上的 NetScaler 实例。

要使用 **Management Service** 配置群集 LA 通道，请执行以下操作：

1. 登录到 SDX 设备。
2. 在“配置”选项卡上，导航到“Citrix® ADC”，然后单击“群集”。
3. 在“群集实例”页面上，选择群集并单击“CLAG”。



4. 在“创建 CLAG”对话框中，执行以下操作：
 - a. 在“通道 ID”下拉列表中，选择群集 LA 通道 ID。
 - b. 在“接口”部分中，从“可用”选择框中，选择接口并单击“+”。
 - c. 选定的接口显示在已配置选择框下方。
5. 在设置部分中，执行以下操作：
 - a. 在别名字段中，输入集群 LA 通道的备用名称。
 - b. 在 LACP 超时字段中，选择以下值之一，以定义如果链接未收到 LACPDU，则链接不再聚合的时间间隔。
该值必须在 SDX 设备和伙伴节点上所有参与链路聚合的端口上匹配：
 - 长 – 30 秒
 - 短 – 1 秒
 - c. 对于高可用性 (HA) 配置，选中 HA 监控复选框以监控通道的故障事件。任何启用了 HA MON 的 LA 通道发生故障都会触发 HA 故障转移。

- d. 选择**标记所有**以向此通道上发送的每个数据包添加一个四字节的 802.1q 标记。**ON** 设置将标记应用于绑定到此通道的所有 VLAN。OFF 将标记应用于除本机 VLAN 之外的所有 VLAN。

6. 单击**创建**，为其中一个 SDX 设备配置 CLAG。

7. 在**确认**对话框中，单击**是**以刷新其他 SDX 设备中的 CLAG 设置。

注意：

- 如果选择**否**，则不配置 CLAG。
- 手动刷新其他 SDX 设备中的 CLAG 设置。
- MTU 设置在两台 SDX 设备上必须相同。MTU 设置必须在任一台 SDX 设备上手动更改。

8. 要在 **CLAGs** 对话框中更改 MTU 设置，请执行以下操作：

- a. 选择 **CLA/1** 并单击 **编辑**。
 - b. 在 **配置 CLAG** 对话框中，在 **MTU** 字段中手动设置 MTU，然后单击 **确定**。
9. 在 **确认** 对话框中，单击 **是**。

配置 SSL 密码以安全地访问管理服务

您可以从 NetScaler SDX 设备支持的 SSL 密码列表中选择 SSL 密码套件。绑定 SSL 密码的任意组合，以通过 HTTPS 安全地访问 SDX 管理服务。SDX 设备提供 37 个预定义的密码组，这些密码组是相似密码的组合，您可以从支持的 SSL 密码列表中创建自定义密码组。

限制

- 不支持绑定密钥交换为“DH”或“ECC-DHE”的密码。
- 不支持绑定身份验证为“DSS”的密码。
- 不支持绑定不属于支持的 SSL 密码列表的密码，或将这些密码包含在自定义密码组中。

支持的 SSL 密码

下表列出了支持的 SSL 密码。协议列中的值是支持的最低协议。例如，如果列出 SSLv3，则表示 SSLv3/TLSv1/TLSv1.1/TLSv1.2 都受支持。

CITRIX 密码名称	OPENSSL 密码名称	十六进制代码	协议	密钥交换算法	身份验证算法	消息身份验证码 (MAC) 算法
TLS1-AES-256-CBC-SHA	AES256-SHA	0x0035	SSLv3 协议	RSA	RSA	AES(256)
TLS1-AES-128-CBC-SHA	AES128-SHA	0x002F	SSLv3 协议	RSA	RSA	AES(128)
TLS1.2-AES-256-SHA256	AES256-SHA256	0x003D	TLSv1.2	RSA	RSA	AES(256)
TLS1.2-AES-128-SHA256	AES128-SHA256	0x003C	TLSv1.2	RSA	RSA	AES(128)

CITRIX 密码名称	OPENSSL 密码名称	十六进制代码	协议	密钥交换算法	身份验证算法	消息身份验证代码 (MAC) 算法
TLS1.2-AES256-GCM-SHA384	AES256-GCM-SHA384	0x009D	TLSv1.2	RSA	RSA	AES-GCM(256)
TLS1.2-AES128-GCM-SHA256	AES128-GCM-SHA256	0x009C	TLSv1.2	RSA	RSA	AES-GCM(128)
TLS1-ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA	0xC014	安全套接字层版本 3	ECC-DHE	RSA	AES(256)
TLS1-ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA	0xC013	安全套接字层版本 3	ECC-DHE	RSA	AES(128)
TLS1.2-ECDHE-RSA-AES-256-SHA384	ECDHE-RSA-AES256-SHA384	0xC028	TLSv1.2	ECC-DHE	RSA	AES(256)
TLS1.2-ECDHE-RSA-AES-128-SHA256	ECDHE-RSA-AES128-SHA256	0xC027	TLSv1.2	ECC-DHE	RSA	AES(128)
TLS1.2-ECDHE-RSA-AES256-	ECDHE-RSA-AES256-	0xC030	TLSv1.2	ECC-DHE	RSA	AES-GCM(256)

CITRIX 密码名称	OPENSSL 密码名称	十六进制代码	协议	密钥交换算法	身份验证算法	消息身份验证代码 (MAC) 算法
GCM-SHA384	GCM-SHA384					
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA-AES128-GCM-SHA256	0xC02F	TLSv1.2	ECC-DHE	RSA	AES-GCM(128)
TLS1.2-DHE-RSA-AES-256-SHA256	DHE-RSA-AES256-SHA256	0x006B	TLSv1.2	DH	RSA	AES(256)
TLS1.2-DHE-RSA-AES-128-SHA256	DHE-RSA-AES128-SHA256	0x0067	TLSv1.2	DH	RSA	AES(128)
TLS1.2-DHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES256-GCM-SHA384	0x009F	TLSv1.2	DH	RSA	AES-GCM(256)
TLS1.2-DHE-RSA-AES128-GCM-SHA256	DHE-RSA-AES128-GCM-SHA256	0x009E	TLSv1.2	DH	RSA	AES-GCM(128)
TLS1-DHE-RSA-	DHE-RSA-	0x0039	SSLv3 协议	DH	RSA	AES(256)

CITRIX 密码名称	OPENSSL 密码名称	十六进制代码	协议	密钥交换算法	身份验证算法	消息身份验证代码 (MAC) 算法
AES-256-CBC-SHA	AES256-SHA					
TLS1-DHE-RSA-AES-128-CBC-SHA	DHE-RSA-AES128-SHA	0x0033	安全套接层版本3	DH	RSA	AES(128)
TLS1-DHE-DSS-AES-256-CBC-SHA	DHE-DSS-AES256-SHA	0x0038	安全套接层版本3	DH	DSS	AES(256)
TLS1-DHE-DSS-AES-128-CBC-SHA	DHE-DSS-AES128-SHA	0x0032	SSLv3 协议	DH	DSS	AES(128)
TLS1-ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA-DES-CBC3-SHA	0xC012	安全套接字层版本3	ECC-DHE	RSA	3DES(168)
SSL3-EDH-RSA-DES-CBC3-SHA	EDH-RSA-DES-CBC3-SHA	0x0016	安全套接字层版本3	DH	RSA	3DES(168)
SSL3-EDH-DSS-DES-	EDH-DSS-DES-	0x0013	SSLv3 协议	DH	DSS	3DES(168)

CITRIX 密码名称	OPENSSL 密码名称	十六进制代码	协议	密钥交换算法	身份验证算法	消息身份验证代码 (MAC) 算法
CBC3-SHA	CBC3-SHA					
TLS1-ECDHE-RSA-RC4-SHA	ECDHE-RSA-RC4-SHA	0xC011	SSLv3 协议	ECC-DHE	RSA	RC4(128)
SSL3-DES-CBC3-SHA	DES-CBC3-SHA	0x000A	SSLv3 协议	RSA	RSA	3DES(168)
SSL3-RC4-SHA	RC4-SHA	0x0005	SSLv3 协议	RSA	RSA	RC4(128)
SSL3-RC4-MD5	RC4-MD5	0x0004	SSL版本3	RSA	RSA	RC4(128)
SSL3-DES-CBC-SHA	DES-CBC-SHA	0x0009	SSL版本3	RSA	RSA	DES(56)
SSL3-EXP-RC4-MD5	EXP-RC4-MD5	0x0003	SSLv3	RSA(512)	RSA	RC4(40)
SSL3-EXP-DES-CBC-SHA	EXP-DES-CBC-SHA	0x0008	SSLv3	RSA(512)	RSA	DES(40)
SSL3-EXP-RC2-CBC-MD5	EXP-RC2-CBC-MD5	0x0006	SSLv3 协议	RSA(512)	RSA	RC2(40)

CITRIX 密码名称	OPENSSL 密码名称	十六进制代码	协议	密钥交换算法	身份验证算法	消息身份验证代码 (MAC) 算法
SSL2-DES-CBC-MD5	DHE-DSS-AES128-SHA256	0x0040	SSLv2 协议	RSA	RSA	DES(56)
SSL3-EDH-DSS-DES-CBC-SHA	EDH-DSS-DES-CBC-SHA	0x0012	安全套接字层版本 3	DH	DSS	DES(56)
SSL3-EXP-EDH-DSS-DES-CBC-SHA	EXP-EDH-DSS-DES-CBC-SHA	0x0011	安全套接字层版本 3	DH(512)	DSS	DES(40)
SSL3-EDH-RSA-DES-CBC-SHA	EDH-RSA-DES-CBC-SHA	0x0015	安全套接字层版本 3	DH	RSA	DES(56)
SSL3-EXP-EDH-RSA-DES-CBC-SHA	EXP-EDH-RSA-DES-CBC-SHA	0x0014	安全套接字层版本 3	DH(512)	RSA	DES(40)
SSL3-ADH-RC4-MD5	ADH-RC4-MD5	0x0018	安全套接字层版本 3	DH	无	RC4(128)
SSL3-ADH-DES-	ADH-DES-	0x001B	安全套接字层版本 3	DH	无	3DES(168)

CITRIX 密码名称	OPENSSL 密码名称	十六进制代码	协议	密钥交换算法	身份验证算法	消息身份验证代码 (MAC) 算法
CBC3-SHA	CBC3-SHA					
SSL3-ADH-DES-CBC-SHA	ADH-DES-CBC-SHA	0x001A	安全套接字层版本 3	DH	无	DES(56)
TLS1-ADH-AES-128-CBC-SHA	ADH-AES128-SHA	0x0034	SSLv3 协议	DH	无	AES(128)
TLS1-ADH-AES-256-CBC-SHA	ADH-AES256-SHA	0x003A	SSLv3 协议	DH	无	AES(256)
SSL3-EXP-ADH-RC4-MD5	EXP-ADH-RC4-MD5	0x0017	SSLv3 协议	DH(512)	无	RC4(40)
SSL3-EXP-ADH-DES-CBC-SHA	EXP-ADH-DES-CBC-SHA	0x0019	SSLv3 协议	DH(512)	无	DES(40)
SSL3-NULL-MD5	NULL-MD5	0x0001	安全套接字层版本 3	RSA	RSA	无
SSL3-NULL-SHA	NULL-SHA	0x0002	安全套接字层版本 3	RSA	RSA	无

预定义密码组

下表列出了 SDX 设备提供的预定义密码组。

密码组名称	描述
所有	SDX 设备支持的所有密码，不包括 NULL 密码
默认	默认密码列表，加密强度 ≥ 128 位
kRSA	密钥交换算法为 RSA 的密码
KEDH	密钥交换算法为 Ephemeral-DH 的密码
DH	密钥交换算法为 DH 的密码
EDH	密钥交换/认证算法为 DH 的密码
aRSA	认证算法为 RSA 的密码
aDSS	认证算法为 DSS 的密码
aNULL	认证算法为 NULL 的密码
DSS	认证算法为 DSS 的密码
DES	加密算法为 DES 的密码
3DES	加密算法为 3DES 的密码
RC4	加密算法为 RC4 的密码
RC2	加密算法为 RC2 的密码
NULL	加密算法为 NULL 的密码
MD5	MAC 算法为 MD5 的密码
SHA1	MAC 算法为 SHA-1 的密码
SHA	MAC 算法为 SHA 的密码
NULL	加密算法为 NULL 的密码
RSA	密钥交换/认证算法为 RSA 的密码

密码组名称	描述
ADH	密钥交换算法为DH且认证算法为NULL的密码
SSL 版本 2	SSLv2 协议密码
TLSv1 版本	SSLv3/TLSv1 协议密码
TLSv1_ONLY	TLSv1 协议密码
EXP	导出密码
EXPORT	导出密码
EXPORT40	40位加密的导出密码
EXPORT56	具有 56 位加密的导出密码
低	低强度密码（56 位加密）
中	中等强度密码（128 位加密）
高	高强度密码（168 位加密）
AES	AES 密码
FIPS	FIPS 批准的密码
ECDHE	椭圆曲线临时 DH 密码
AES-GCM	加密算法为 AES-GCM 的密码
SHA2	MAC 算法为 SHA-2 的密码

查看预定义的密码组

要查看预定义的密码组，请在配置选项卡上的导航窗格中，展开**管理服务**，然后单击**密码组**。

创建自定义密码组

您可以从支持的 SSL 密码列表中创建自定义密码组。

创建自定义密码组：

1. 在**配置**选项卡上的导航窗格中，展开**管理服务**，然后单击**密码组**。
2. 在**密码组**窗格中，单击**添加**。
3. 在**创建密码组**对话框中，执行以下操作：
 - a. 在**组名称**字段中，输入自定义密码组的名称。
 - b. 在**密码组描述**字段中，输入自定义密码组的简要描述。
 - c. 在**密码套件**部分中，单击**添加**并选择要包含在支持的 SSL 密码列表中的密码。
 - d. 单击**创建**。

查看现有 SSL 密码绑定

要查看现有密码绑定，请在“**配置**”选项卡上的导航窗格中展开“**系统**”，然后单击“**系统设置**”下的“**配置 SSL 设置**”。



注意：

升级到最新版本的 Management Service 后，现有密码套件列表将显示 OpenSSL 名称。从升级后的 Management Service 绑定密码后，显示将使用 Citrix® 命名约定。

将密码绑定到 HTTPS 服务

1. 在“**配置**”选项卡上的导航窗格中，单击“**系统**”。
2. 在“**系统**”窗格中，在“系统设置”下，单击“**配置 SSL 设置**”。
3. 在“**编辑设置**”窗格中，单击“**密码套件**”。
4. 在“**密码套件**”窗格中，执行以下任一操作：
 - 要从预定义密码组中选择一个密码组，请选择“**密码组**”，从“**密码组**”列表选择一个密码组，然后单击“**确定**”。

- 要从支持的密码列表中进行选择，请选中“**密码套件**”复选框，单击“**添加**”以选择密码，然后单击“**确定**”。

备份和恢复 SDX 设备配置数据

NetScaler SDX 设备备份过程是一个单步过程，它会创建一个包含以下内容的备份文件：

- 单一捆绑包映像：
 - 思杰 Hypervisor™ 映像
 - Citrix Hypervisor 的修补程序和补充包
 - 管理服务映像
- XVA 映像
- 升级映像
- SDX 配置
- 配置

备份文件夹是 `/var/mps/backup/`。

备份当前配置

1. 在“**配置**”选项卡上，在导航窗格中，展开“**管理服务**”，然后单击“**备份文件**”。
2. 在“**备份文件**”窗格中，单击“**备份**”。
3. 在“**新建备份文件**”对话框中，选中“**密码保护文件**”复选框以加密备份文件。
4. 在 **密码** 和 **确认密码** 字段中，键入并确认备份文件的密码。
5. 单击 **继续**。

备份过程会创建一个备份文件。备份文件的文件名包含管理服务的当前 IP 地址以及执行备份时的时间戳。要检查备份文件可能存在的任何差异，请从 SDX GUI 导航到 **Configuration > System > Events/Alarms**。

计划备份

默认情况下，SDX 每 24 小时使用备份策略创建一个备份。使用备份策略，您可以定义要在 SDX 设备中保留的备份文件数量。此外，您可以使用密码加密计划备份文件，以确保备份文件的安全。

编辑备份策略

1. 在 **Configuration** 选项卡上，单击 **System**。

2. 在 **策略管理** 窗格中，单击 **备份策略**。
3. 在 **配置备份策略** 窗格中，执行以下操作：
 - a. 在 **要保留的以前备份** 字段中，键入要保留的备份文件数量。
 - b. 要加密备份文件，请选中 **加密备份文件** 复选框。
 - c. 在 **密码** 和 **确认密码** 字段中，键入并确认用于加密备份文件的密码。

手动将备份文件传输到外部备份服务器

在手动传输备份文件之前，请确保您已拥有外部备份服务器的详细信息。

将备份文件传输到外部备份服务器

1. 在**配置**选项卡上的导航窗格中，展开**管理服务**，然后单击**备份文件**。
2. 在**备份文件**窗格中，选择备份文件，然后单击**传输**。
3. 在**服务器**字段中，键入外部备份服务器的主机名或 IP 地址。
4. 在**用户名**和**密码**字段中，键入用于访问外部备份服务器的用户名和密码。
5. 在**端口**字段中，键入端口号。
6. 在**传输协议**字段中，选择要用于将备份文件传输到外部备份服务器的协议。
7. 在**目录路径**字段中，键入外部备份服务器中要存储备份文件的目录路径。
8. 选择**从管理服务中删除文件**，以便在将备份文件传输到外部备份服务器后，从 SDX 设备中删除该备份文件。
9. 单击**确定**。

还原设备

您可以将 SDX 设备还原到备份文件中可用的配置。在设备还原期间，所有当前配置都将被删除。

注意事项：

- 在使用其他 SDX 设备的备份文件还原 SDX 设备之前，请根据备份文件中可用的设置添加管理服务网络设置。
- 确保进行备份的平台变体与您尝试还原的平台变体相同。不支持在两种不同的平台变体之间还原备份文件。
- Citrix® 建议仅在设置网络配置后才还原 SDX 备份。您可以为 SVM 指定以下网络设置：
 - SVM IP 地址
 - 管理程序 IP 地址

- 子网掩码
- 网关
- DNS 服务器

从备份文件还原设备

1. 在“配置”选项卡上的导航窗格中，展开“管理服务”，然后单击“备份文件”。
2. 在“备份文件”窗格中，单击备份文件，然后单击“确定”。
3. 在“还原”对话框中，选择“设备还原”，然后单击“继续”。

将显示应用程序还原的不同组件：

- 许可证
- SDX 映像
- XVA 文件
- NetScaler 配置
- 摘要

如果备份文件中缺少任何必需组件，系统会提示您上传缺失的元素，然后才能继续。

要了解备份文件是否可以在当前 SDX 单一捆绑包映像版本上还原，请参阅下表。作为单一捆绑包映像的经验法则，任何较低版本的备份都无法在更高版本上还原。

当前 SDX 单一捆绑包映像版本	备份文件版本
11.1	支持 11.1、12.0、12.1、13.0；不支持 11.0
12.0	支持 12.0、12.1、13.0；不支持 11.0 和 11.1
12.1	支持 12.1、13.0；不支持 11.0、11.1、12.0
13.0	支持 13.0；不支持 11.0、11.1、12.0、12.1
13.1	支持 13.1；不支持 11.0、11.1、12.0、12.1、13.0

4. 在“许可证”页面上，检查是否存在有效许可证，然后单击“下一步”。
5. “SDX 映像”页面出现。如果执行还原不需要 SDX 映像，请单击“下一步”。否则，在出现提示时上传有效的 SDX 映像，然后单击“下一步”。

6. **“XVA 文件”**页面打开。如果所有实例的 XVA 映像都存在，请单击**“下一步”**。如果备份文件中缺少任何实例的 XVA 文件，您可以上传它或跳过还原此实例。单击**“下一步”**转到下一页。
7. NetScaler 配置页面打开。NetScaler 配置文件不是强制性的。您可以不还原其配置而预配实例。如果备份文件中缺少 NetScaler 配置文件，您可以只继续进行实例预配，或者跳过还原该实例。单击**“下一步”**转到下一页。
8. 摘要页面显示备份文件中所有实例的以下详细信息：
 - IP 地址
 - 主机名
 - SDX 版本
 - XVA 版本
 - 版本位
 - 还原：如果设备或实例已准备好还原，则会出现一个复选标记。如果未准备好，则会出现一个叉号。
 - 错误消息：如果设备或实例未准备好还原，则会出现一条错误消息来解释原因。
9. 单击**“还原”**以完成应用程序还原过程。

还原 NetScaler 实例

您可以将 SDX 设备中的 NetScaler 实例还原到备份文件中可用的 NetScaler 实例。

注意： 在以下情况下，VPX 实例无法还原：

- 实例未分配管理 NIC，并且
- 实例仅通过 LACP 从 SDX 管理服务进行管理。还原失败，因为 SDX 管理服务无法自动还原通道配置。为避免此问题，请手动还原通道配置以完成 VPX 实例还原。

要还原备份文件中的 NetScaler 实例：

1. 在**“配置”**选项卡上的导航窗格中，展开**“管理服务”**，然后单击**“备份文件”**。
2. 在**“备份文件”**窗格中，选择备份文件，然后单击**“还原”**。
3. 在**“还原”**对话框中，选择**“实例还原”**。
4. 选择要还原的 NetScaler 实例，然后单击**“继续”**。
5. （可选）如果备份文件已加密，则在出现提示时，键入密码，然后单击**“确定”**。

注意：

确保在运行正在还原的实例的 SDX 设备上存在适当的 XVA、构建映像和通道配置。

执行设备重置

NetScaler SDX 设备允许您：

- 重置设备的配置。

注意：

重置配置后，您必须使用设备序列号作为密码登录。

- 将设备重置为出厂版本。
- 将设备重置为特定的单一捆绑包映像版本。

在执行设备重置之前，请备份设备上存储的所有数据，包括设备上预置的所有 NetScaler 实例的设置。

Citrix® 建议您将文件存储在设备外部。执行设备重置会终止所有与管理服务当前的客户端会话。请重新登录管理服务以执行任何其他配置任务。准备好恢复数据时，请使用管理服务导入备份文件。

管理服务提供以下设备重置选项：

- 配置重置
- 出厂重置
- 全新安装

重置设备的配置

管理服务提供“配置重置”选项来重置设备的配置。“配置重置”选项执行以下操作：

- 删除 VPX 实例。
- 删除 SSL 证书和密钥文件。
- 删除许可证和技术存档文件。
- 删除设备上的 NTP 配置。
- 将时区恢复为 UTC。

- 将修剪和备份策略恢复为其默认设置。
- 删除管理服务映像。
- 删除 NetScaler SDX 映像。
- 删除所有 XVA 映像，但设备上最后访问的映像文件除外。
- 恢复默认接口设置。
- 恢复设备的默认配置，包括默认配置文件、用户和系统设置。
- 恢复适用于 Citrix Hypervisor™ 和管理服务的默认密码。
- 重新启动管理服务。

重置设备的配置

1. 导航到 **配置 > 系统 > 系统管理组**。
2. 单击 **设备重置**。
3. 在 **设备重置** 对话框中，在 **重置类型** 列表中选择 **配置重置**。
4. 单击 **确定**。

将设备重置为出厂版本

管理服务提供“恢复出厂设置”选项，用于将设备重置为出厂版本。“恢复出厂设置”选项会将管理服务和 Citrix Hypervisor 的当前 IP 地址重置为管理服务和 Citrix Hypervisor 的默认 IP 地址。

请确保备份设备上存储的所有数据，包括设备上预配的所有 NetScaler 实例的设置。Citrix 建议您将文件存储在设备外部。执行恢复出厂设置会终止与管理服务的所有当前客户端会话。重新登录管理服务以执行任何其他配置任务。准备好恢复数据时，请使用管理服务导入备份文件。

重要提示

请确保在执行恢复出厂设置之前将串行控制台电缆连接到设备。

将设备重置为出厂版本

1. 导航到 **配置 > 系统 > 系统管理**。
2. 单击 **设备重置**。
3. 在 **设备重置** 对话框中，在 **重置类型** 列表中选择 **恢复出厂设置**。
4. 单击 **确定**。

将设备重置为单个捆绑包映像版本

管理服务提供“全新安装”选项，允许您在设备上安装任意版本的单个捆绑包映像。它使您能够将单个捆绑包映像全新安装为新的默认启动映像。全新安装会删除 SDX 设备中的现有配置，但网络设置除外。

注意：

如果您的 SDX 设备出厂时软件版本为 11.0 或更早，则干净安装到 13.1 或更高版本将失败。

干净安装选项支持以下版本：

单一捆绑包映像版本	SDX 平台
11.0.xx	SDX 14xxx, SDX 25xxx。 注意： 如果其他 SDX 平台具有 10G 出厂分区，则支持干净安装选项。
11.1.xx	SDX 14xxx, SDX 25xxx。 注意： 如果其他 SDX 平台具有 10G 出厂分区，则支持干净安装选项。
11.1.51.x	所有 SDX 平台。
12.1.xx	所有 SDX 平台。
13.0.xx	所有 SDX 平台。
13.1.xx	所有 SDX 平台。

先决条件

请确保：

- 将所有主高可用性节点故障转移到不同的 SDX 设备。如果您不具备高可用性功能，请确保相应地规划停机时间。
- 将单个捆绑包映像下载到本地计算机。

重要提示：

使用“清洁安装”选项时，请确保不要重启或断电设备。设备将多次重启。

将设备重置为单个捆绑包映像版本

1. 导航到 **配置 > 系统 > 系统管理** 组。
2. 单击 **设备重置**。
3. 在 **Appliance Reset** 对话框中，从 **Reset Type** 列表中选择 **Clean Install**。
4. 单击 **OK**。

级联外部身份验证服务器

级联多个外部身份验证服务器可为外部用户提供连续、可靠的身份验证和授权过程。如果第一个身份验证服务器上的身份验证失败，管理服务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。

要启用级联身份验证，请将外部身份验证服务器添加到管理服务。有关详细信息，请参阅[配置外部身份验证](#)。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，要为级联身份验证添加四个外部身份验证服务器，您可以添加 RADIUS、LDAP 和 TACACS 服务器的任意组合。您还可以添加所有四个相同类型的服务器。您可以在 NetScaler Application Delivery Management 中配置多达 32 个外部身份验证服务器。

注意：

不支持通过 CLI 级联外部身份验证服务器。

级联外部身份验证服务器

1. 在“配置”选项卡上，在“系统”下，展开“身份验证”。
2. 在“身份验证”页面中，单击“身份验证配置”。
3. 在“身份验证配置”页面中，从“服务器类型”下拉列表中选择“外部”（您只能级联外部服务器）。
4. 单击“插入”，在打开的“外部服务器”页面上，选择一个或多个要级联的身份验证服务器。
5. 单击“确定”。

所选服务器显示在“身份验证服务器”页面上，如下图所示。要更改身份验证顺序，请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。

Authentication Configuration

The appliance can authenticate users with local user accounts or by using an external authentication server.

Server Type*

EXTERNAL

External Servers

Insert

Delete

☒	Server Type	Server Name
☒	RADIUS	10.102.166.80
☒	LDAP	_LDAP2
	LDAP	_LDAP1

☒ Enable fallback local authentication

OK

Close

解锁用户

NetScaler SDX 管理员可以在锁定间隔到期之前解锁用户。如果用户通过控制台登录到管理服务，则锁定不适用。锁定间隔也从秒更改为分钟。最小值 = 1 分钟。最大值 = 30 分钟。

使用 GUI 解锁用户

1. 导航到 **配置 > 系统 > 用户管理 > 用户**。
2. 选择要解锁的用户。
3. 单击 **Unlock**。

使用 CLI 解锁用户

在命令提示符下，键入：

```
set systemuser id=<ID> unlock=true
```

预配 NetScaler 实例

注意

在将 NetScaler SDX 设备安装或升级到 13.1 版本后，NetScaler Console 服务连接默认启用。有关更多详细信息，请参阅数据治理和 NetScaler Console 服务连接。

您可以使用管理服务在 SDX 设备上预配一个或多个 NetScaler 实例。您可以安装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，则管理服务不允许预配更多 NetScaler 实例。

注意：

您可以在网络接口上配置最多 20 个 VPX 实例，独立于底层硬件平台。

在 SDX 设备上预配 NetScaler VPX 实例包含以下步骤。

1. 定义要附加到 NetScaler 实例的管理员配置文件。此配置文件指定管理服务用于预配 ADC 实例以及稍后与实例通信以检索配置数据的用户凭据。您也可以使用默认管理员配置文件。
2. 将 .xva 映像文件上载到管理服务。
3. 使用管理服务中的“预配 NetScaler”向导添加 NetScaler 实例。管理服务隐式地将 NetScaler 实例部署到 SDX 设备上，然后下载该实例的配置详细信息。

警告

确保您使用管理服务修改实例的已预配网络接口或 VLAN，而不是直接在实例上执行修改。

创建管理员配置文件

管理员配置文件指定管理服务在预配 NetScaler 实例时使用的用户凭据。这些凭据稍后在与实例通信以检索配置数据时使用。客户端通过 CLI 或 GUI 登录 NetScaler 实例时，也会使用管理员配置文件中指定的用户凭据。

管理员配置文件还允许您指定管理服务和 VPX 实例仅通过安全通道或使用 HTTP 彼此通信。

实例的默认管理员配置文件指定默认管理员用户名。此配置文件无法修改或删除。但是，您必须通过创建用户定义的管理员配置文件并在预配实例时将其附加到实例来覆盖默认配置文件。如果用户定义的管理员配置文件未附加到任何 NetScaler 实例，则管理服务管理员可以将其删除。

重要

不要在 VPX 实例上直接更改密码。如果这样做，实例将无法从管理服务访问。要更改密码，请首先创建管理员配置文件，然后修改 NetScaler 实例，从“管理员配置文件”列表中选择此配置文件。

要更改高可用性设置中 NetScaler 实例的密码，请首先更改指定为辅助节点的实例上的密码。然后更改指定为主节点的实例上的密码。请记住，只能通过管理服务更改密码。

创建管理员配置文件

1. 在“配置”选项卡上的导航窗格中，展开“**NetScaler 配置**”，然后单击“**管理员配置文件**”。
2. 在“**管理员配置文件**”窗格中，单击“**添加**”。
3. 将显示“**创建管理员配置文件**”对话框。

管理员配置文件 SNMP(/en-us/sdx/media/admin-profile-snmp-v3-citrix.png)

设置以下参数：

- 配置文件名称：管理员配置文件的名称。默认配置文件名称为 **nsroot**。您可以创建用户定义的配置文件名称。
 - 密码：用于登录 NetScaler 实例的密码。最大长度：31 个字符。
 - SSH 端口：设置 SSH 端口。默认端口为 22。
 - **使用全局设置进行 NetScaler 通信**：如果希望在“系统设置”中定义管理服务与 NetScaler 实例之间通信的设置，请选择此项。您可以清除此复选框并将协议更改为 HTTP 或 HTTPS。
 - 选择“**http**”选项以使用 HTTP 协议进行管理服务与 NetScaler 实例之间的通信。
 - 选择 **https** 选项，以便管理服务和 NetScaler 实例之间使用安全通道进行通信。
4. 在 **SNMP** 下，选择版本。如果选择 v2，请转到步骤 5。如果选择 v3，请转到步骤 6。
 5. 在 SNMP v2 下，添加 **SNMP Community** 名称。
 6. 在 SNMP v3 下，添加 **Security Name** 和 **Security Level**。
 7. 在 **Timeout Settings** 下，指定值。

8\。单击 **Create**，然后单击 **Close**。您创建的管理员配置文件将显示在 **Admin Profiles** 窗格中。

如果 **Default** 列中的值为 true，则默认配置文件是管理员配置文件。如果值为 false，则用户定义的配置文件是管理员配置文件。

如果您不想使用用户定义的管理员配置文件，可以将其从管理服务中删除。要删除用户定义的管理员配置文件，请在 **Admin Profiles** 窗格中，选择要删除的配置文件，然后单击 **Delete**。

上传 NetScaler .xva 映像

添加 NetScaler VPX 实例需要 .xva 文件。

在预配 VPX 实例之前，将 NetScaler SDX .xva 文件上传到 SDX 设备。您还可以将 .xva 映像文件下载到本地计算机作为备份。.xva 映像文件格式为：`NSVPX-XEN-ReleaseNumber-BuildNumber_nc`.xva。

在 **NetScaler XVA Files** 窗格中，您可以查看以下详细信息。

- **名称：**.xva 映像文件的名称。文件名包含版本和内部版本号。例如，文件名 `NSVPX-XEN-12.1-56.22.xva.gz` 指的是版本 12.1 内部版本 56.22。
- **上次修改时间：**.xva 映像文件上次修改的日期。
- **大小：**.xva 映像文件的大小（以 MB 为单位）。

上传 NetScaler .xva 文件

1. 在“**配置**”选项卡中，在导航窗格中，展开“**NetScaler 配置**”，然后单击“**XVA 文件**”。
2. 在“**NetScaler XVA 文件**”窗格中，单击“**上传**”。
3. 在“**上传 NetScaler 实例 XVA**”对话框中，单击“**浏览**”并选择要上传的 XVA 映像文件。
4. 单击“**上传**”。上传后，XVA 映像文件将显示在“**NetScaler XVA 文件**”窗格中。

通过下载 NetScaler .xva 文件创建备份

1. 在“**NetScaler 构建文件**”窗格中，选择要下载的文件，然后单击“**下载**”。
2. 在“**文件下载**”消息框中，单击“**保存**”。
3. 在“**另存为**”消息框中，浏览到要保存文件的位置，然后单击“**保存**”。

添加 NetScaler 实例

从管理服务添加 NetScaler 实例时，需要为某些参数提供值。管理服务会在 NetScaler 实例上隐式配置这些设置。

← Provision Citrix ADC

Name*

 ⓘ × Please enter value

☐ Manage through internal network

☐ IPv4

☐ IPv6

XVA File*

Choose File ▾

Admin Profile*

ns_nsroot_profile ▾

Description

- **名称**：为 NetScaler 实例分配一个名称。
- 选择“**通过内部网络管理**”以在 SDX 管理服务和 VPX 实例之间启用独立的内部始终在线连接。此功能在 SDX 设备上运行的 13.0-36.27 及更高版本的 VPX 实例中受支持。
- 选择 IPv4 或 IPv6 地址，或同时选择 IPv4 和 IPv6 地址，以用于管理目的访问 NetScaler VPX 实例。一个 NetScaler 实例只能有一个管理 IP (NSIP)。您不能删除 NSIP 地址。
- 为 IP 地址分配子网掩码、默认网关和到管理服务的下一跳。
- 当 VPX 配置版本为 13.0–88.9 或 13.1–37.8 及更高版本时，在以下任一条件下，**网关和到管理服务的下一跳**字段是可选的：
 - 启用**通过内部网络管理**时。
 - 当配置的 IPv4 地址与管理服务 IP 地址在同一子网中时。

☒ IPv4

IPv4 Address*

Netmask*

Gateway

Nexthop to Management Service

接下来，添加 XVA 文件、管理员配置文件和实例描述。

注意： 对于高可用性设置（主动-主动或主动-备用），Citrix 建议您在不同的 SDX 设备上配置两个 NetScaler VPX 实例。确保设置中的实例具有相同的资源，例如 CPU、内存、接口、每秒数据包数 (PPS) 和吞吐量。

许可证分配

在本节中，指定您为 NetScaler 采购的许可证。许可证可以是 Standard、Enterprise 和 Platinum。

注意： 星号表示必填字段。

License Allocation			
Feature License*		For more information about Citrix ADC editions, see Citrix ADC Editions	
Standard			
Pool	Total	Available	Allocate
Instance	0	0	1
Bandwidth			Allocation Mode* Fixed
	0 Gbps	0 Gbps	Throughput (Mbps)* 1000

如果您需要带宽突发能力，请在**分配模式**下选择**可突发**。有关更多信息，请参阅 [SDX 中的带宽计量](#)

。

加密分配

从版本 12.1 48.13 开始，管理加密容量的界面已更改。有关更多信息，请参阅 [管理加密容量](#)。

资源分配

在 SDX 上运行的 VPX 实例，默认只有一个管理 CPU。从 13.1 build 53.x 版本开始，如果您有两个或更多专用核心，则在预配或编辑 VPX 实例时可以再添加一个管理 CPU。此功能要求 SDX 和 VPX 都运行 13.1-53.x 及更高版本的软件。

在资源分配下，分配总内存、每秒数据包数和 CPU。

要添加额外的管理 CPU：

1. 从 **CPU** 列表中选择**专用 (2 核)**或更多。
2. 选择**添加额外的管理 CPU**选项。

Resource Allocation

Total Memory (MB)*

2048

Max packets per second*

2147483647

CPU*

Dedicated (2 core)

▼

i

☐ Add an extra management CPU

CPU：为实例分配一个或多个专用核心，或者实例与其他实例共享一个核心。如果选择共享，则会为实例分配一个核心，但如果资源短缺，该核心可能会与其他实例共享。如果重新分配了 CPU 核心，请重新启动受影响的实例。重新启动重新分配了 CPU 核心的实例，以避免任何性能下降。

从 SDX 11.1.x.x (MR4) 版本开始，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。
- 为了获得最佳性能，无论许可证如何，建议为每个数据包引擎 (PE) 分配 4 GB 内存。例如，具有 6 个 PE 的 VPX 必须分配 24 GB 内存。

下表列出了支持的 VPX、单一捆绑包映像版本以及您可以分配给实例的核心数：

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

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 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
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 型号、SDX 14030 40G 型号、SDX 14040 40G 型号、SDX 14060 40G 型号、SDX 14080 40G 型号 以及 SDX 14100 40G 型号	12	10	10

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 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	10
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	16
SDX 26100-50S 型 号、SDX 26160-50S 型号、SDX 26200-50S 型号、 SDX 26250-50S 型 号	28	26	16
SDX 26100-100G， 26160-100G， 26200-100G， 26250-100G	28	26	25
SDX 15000	16	14	14

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 15000-50G	16	14	14
SDX 9100	10	9	9
SDX 16000	32	30	16

注意：

专用核心对应于实例上运行的数据包引擎数量。对于使用专用核心创建的 VPX 实例，会分配一个额外的 CPU 用于管理。

在 SDX 上为 NetScaler VPX 启用额外管理 CPU 的推荐做法

在 NetScaler SDX 部署中，每个 VPX 实例都处理数据平面（数据包处理）和管理平面（控制和管理操作）工作负载。在管理活动频繁的环境中，管理平面中可能会发生 CPU 争用，这可能会影响配置更改、监控和 API 操作等任务的响应速度。

为了提高系统性能和稳定性，Citrix 建议为在 SDX 平台上运行的 NetScaler VPX 实例启用额外管理 CPU（也称为额外管理线程）。

概述

默认情况下，管理平面处理分布在可用的超线程上，并与数据包引擎分时共享。从 NetScaler 13.1 版本开始，SDX 支持启用一个专门用于管理平面任务的额外管理超线程。

注意：

从 NetScaler 13.1 版本 63.16 开始，当您为 VPX 实例选择两个或更多专用核心时，默认情况下会分配一个额外的管理 CPU。

一些主要特性如下：

- 额外的管理 CPU 是通过超线程实现的，而不是物理核心。
- 它为管理平面操作提供专用的处理能力。
- 它不同于在其他平台上使用的传统额外管理 CPU 实现。

优点：

- 改进的管理平面响应能力
 - 更快地执行 CLI 和 API 命令。
 - 降低配置更改的延迟。
 - 改进 GUI 和自动化工作流的响应能力。
- 增强的稳定性
 - 降低负载下管理平面争用的可能性。
 - 尽量减少高监控、日志记录或自动化活动的影响。
- 对数据平面性能没有影响
 - 数据包处理核心（数据包引擎）不会减少或受到影响。
 - 数据平面吞吐量保持不变。

先决条件：

在启用额外的管理 CPU 之前，请确保满足以下先决条件：

- **NetScaler 版本：**SDX 和 VPX 实例上均为 NetScaler 13.1-63.x 或更高版本。
- **VPX 预配：**必须为每个 VPX 实例分配至少 2 个 CPU 核心。
- **平台要求：**必须在 SDX 平台上启用超线程。

何时启用额外的管理 CPU

如果您的环境出现以下任何情况，Citrix 建议启用额外的管理 CPU：

高管理活动	性能问题
持续监控和遥测数据收集	CLI 或 GUI 响应时间慢
频繁的配置更改或自动化	应用配置时出现延迟
高 API 或编排活动	管理 CPU 利用率高

注意：

如果您遇到管理 CPU 压力，请启用此功能。

操作注意事项：

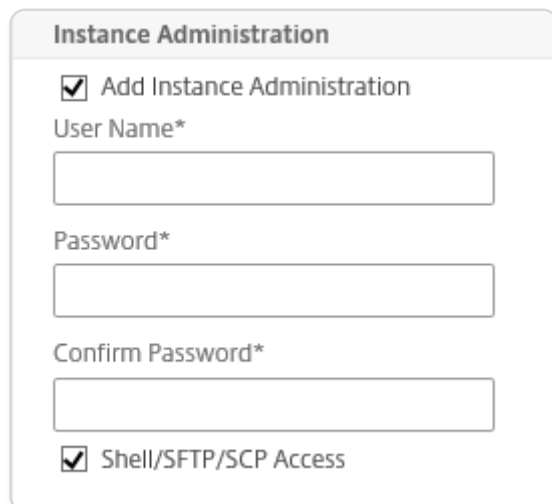
- 启用或禁用额外管理 CPU 后，需要重新启动 VPX。
- 额外管理 CPU 的行为与 NetScaler MPX 和在虚拟机管理程序上运行的 NetScaler VPX 不同。
- 此功能专门适用于在 SDX 上运行的 VPX 实例。

建议摘要：

- 启用额外管理 CPU 是一种推荐的低风险配置。
- 它提高了管理平面的性能和可靠性。
- 它不影响数据平面吞吐量或数据包引擎分配。
- 它被认为是大多数 SDX 部署的最佳实践。

实例管理

您可以通过在**实例管理**下选择**添加实例管理**来为 VPX 实例创建管理员用户。



The screenshot shows a web interface titled "Instance Administration". It contains a form with the following elements:

- A checked checkbox labeled "Add Instance Administration".
- A text input field labeled "User Name*".
- A text input field labeled "Password*".
- A text input field labeled "Confirm Password*".
- A checked checkbox labeled "Shell/SFTP/SCP Access".

添加以下详细信息：

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，但无权访问网络命令以配置 VLAN 和接口。

密码： 该用户名的密码。

Shell/Sftp/Scp 访问： 允许 NetScaler 实例管理员访问的权限。此选项默认选中。

网络设置

- **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**。在您登录实例并启用 L2 模式之前。有关详细信息，请参阅[在 NetScaler 实例上允许 L2 模式](#)。

Network Settings

☐ Allow L2 Mode ?

☒ 0/1

VLAN Tag

☒ 0/2 ?

VLAN Tag

Data Interfaces

Add

Edit

Delete

Interface	Allow Untagged Traffic	Allowed VLANs
No items		

注意：

- 如果您从管理服务禁用实例的 L2 模式，则必须登录该实例并从该实例禁用 L2 模式。否则，在您重新启动实例后，所有其他 NetScaler 模式可能会被禁用
- 在 SDX 上预配 ADC 实例后，您无法从 ADC 实例中删除接口或通道。但是，您可以向 ADC 实例添加接口或通道。

- **接口 0/1 和 0/2**：默认情况下，接口 0/1 和 0/2 被选为管理 LA。
- **VLAN 标记**：为管理接口指定 VLAN ID。接下来，添加数据接口。

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对应。如果您将实例 1 关联的第一个接口是接口 1/4，则在实例上查看接口设置时，它会显示为接口 1/1。编号之所以更改，是因为它是您与实例 1 关联的第一个接口。

Add Data Interface

Interfaces*

1/4

☒ Allow Untagged Traffic

Allowed VLANs

100-110,142,151-155

MAC Address Mode*

Default

▼ VMAC Settings (IPv4 and IPv6 VRIDs to configure Virtual MAC)

VRID IPv4

100-110,142,151-155

VRID IPv6

100-110,142,151-155

Add

Close

- **允许未标记流量**：选中“允许未标记流量”复选框，以使 NetScaler 实例能够处理未标记流量。

注意

当 SDX 设备版本为 13.1-24.x 或更高版本，且 NetScaler 实例版本低于 13.1-24.x 时，即使未选中“允许未标记流量”复选框，ADC 实例也会处理 Mellanox 接口上的未标记流量。

- **允许的 VLAN**：指定可与 NetScaler 实例关联的 VLAN ID 列表。
- **MAC 地址模式**：分配 MAC 地址。从以下选项中选择：
 - **默认**：Citrix Hypervisor™ 分配 MAC 地址。
 - **自定义**：选择此模式可指定一个 MAC 地址，该地址将覆盖生成的 MAC 地址。
 - **生成**：使用之前设置的基本 MAC 地址生成 MAC 地址。有关设置基本 MAC 地址的信息，请参阅“将 MAC 地址分配给接口”。
- **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”。

管理 VLAN 设置

通常，VPX 实例的管理服务和管理地址 (NSIP) 位于同一子网中，并通过管理接口进行通信。但是，如果管理服务 and 实例位于不同的子网中，则在预配 VPX 实例时必须指定 VLAN ID。此 ID 是必需的，以便实例启动时可以通过网络访问。如果您的部署要求 NSIP 只能通过预配 VPX 实例时选择的接口访问，请选择 NSVLAN 选项。

如果选择了 **NSVLAN** 选项，则在预配 NetScaler 实例后无法更改此设置。

VPX 管理 VLAN 设置(/en-us/sdx/media/vpx-mgmt-vlan-setting-citrix.png)

注意：

- HA 心跳仅在属于 NSVLAN 的接口上发送。
- 您只能从 VPX XVA build 9.3 53.4 及更高版本配置 NSVLAN。

重要提示： 如果未选择 NSVLAN，则在 VPX 实例上运行“clear config full”命令会删除 VLAN 配置。

单击 **Done** 以预配 NetScaler VPX 设备。

修改 NetScaler 实例

要修改已预配的 ADC 实例的参数值，请在 **NetScaler instances** 窗格中，选择要修改的实例，然后单击 **Modify**。在“修改 ADC 向导”中，修改参数。

注意：

- 仅当您有两个或更多专用核心，并且 VPX 和 SDX 均在版本 13.1 和 build 53.x 及更高版本时，才能编辑 VPX 实例并添加一个管理 CPU。
- 为版本早于 13.1-53.x 的 VPX 选择 **Add an extra management CPU** 选项会导致错误。请将 VPX 实例升级到 13.1-53.x 及更高版本才能使用此功能。
- 在将 VPX 实例降级到早于 13.1-53.x 的版本之前，必须禁用 **Add an extra management CPU** 选项。否则，VPX 实例的性能会受到影响。
- 如果未禁用 **Add an extra management CPU** 选项，并且 VPX 实例降级到早于 13.1-53.x 的版本，则会生成警报。

注意事项：

- 如果您修改以下参数：SSL 芯片数量、接口、内存和功能许可证，NetScaler 实例将隐式停止并重新启动以使这些参数生效。
- 您无法修改“映像”和“用户名”参数。
- 无法从 ADC 实例中删除接口或通道。但是，可以向 ADC 实例添加新的接口或通道。
- 要删除在 SDX 设备上预置的 ADC 实例，请在“**NetScaler 实例**”窗格中，选择要删除的实例，然后单击“删除”。在“确认”消息框中，单击“是”以删除 NetScaler 实例。

将 VLAN 限制到特定的虚拟接口

SDX 设备管理员可以在与 NetScaler 实例关联的虚拟接口上强制执行特定的 802.1Q VLAN。此功能在限制实例管理员使用 802.1Q VLAN 方面特别有用。如果属于两家不同公司的两个实例托管在 SDX 设备上，您可以限制这两家公司使用相同的 VLAN ID。这样，一家公司就不会看到另一家公司的流量。如果实例管理员尝试将接口分配给 802.1Q VLAN，则会执行验证以确认指定的 VLAN ID 是否在允许列表中。

默认情况下，任何 VLAN ID 都可以在接口上使用。要限制接口上的标记 VLAN，请在预置 NetScaler 实例时在“网络设置”中指定 VLAN ID。您也可以稍后通过修改实例来指定。要指定范围，请使用连字符分隔 ID（例如 10–12）。如果您最初指定了一些 VLAN ID，但后来从允许列表中删除了所有这些 ID，则可以在该接口上使用任何 VLAN ID。实际上，您已恢复默认设置。

创建允许的 VLAN 列表后，SDX 管理员无需登录实例即可创建 VLAN。管理员可以从管理服务中为特定实例添加和删除 VLAN。

重要提示：如果启用了 L2 模式，管理员必须注意不同 NetScaler 实例上的 VLAN ID 不会重叠。

指定允许的 VLAN ID

1. 在“预置 ADC 向导”或“修改 ADC 向导”中，在“网络设置”页面上，在“允许的 VLAN”中，指定此接口上允许的一个或多个 VLAN ID。使用连字符指定范围。例如，2–4094。
2. 按照向导中的说明进行操作。
3. 单击**完成**，然后单击**关闭**。

从管理服务为实例配置 VLAN

1. 在**配置**选项卡上，导航到 NetScaler > 实例。
2. 选择一个实例，然后单击**VLAN**。
3. 在详细信息窗格中，单击**添加**。
4. 在**创建 NetScaler VLAN**对话框中，指定以下参数：
 - VLAN ID — 唯一标识特定帧所属 VLAN 的整数。NetScaler 最多支持 4094 个 VLAN。ID 1 保留给默认 VLAN。
 - IPv6 动态路由 — 在此 VLAN 上启用所有 IPv6 动态路由协议。

注意：要使已启用设置生效，您必须登录实例并从 VTYSH 命令行配置 IPv6 动态路由协议。

5. 选择必须属于此 VLAN 的接口。
6. 单击**创建**，然后单击**关闭**。

管理加密容量

从版本 12.1 48.13 开始，管理加密容量的界面已更改。管理服务提供非对称加密单元 (ACU)、对称加密单元 (SCU) 和加密虚拟接口，以表示 NetScaler SDX 设备上的 SSL 容量。早期，加密容量以 SSL 芯片、SSL 核心和 SSL 虚拟功能为单位进行分配。有关旧版 SSL 芯片如何转换为 ACU 和 SCU 单元的更多信息，请参阅[旧版 SSL 芯片到 ACU 和 SCU 转换表](#)。

通过使用管理服务 GUI，您可以将加密容量以 ACU 和 SCU 为单位分配给 NetScaler VPX 实例。

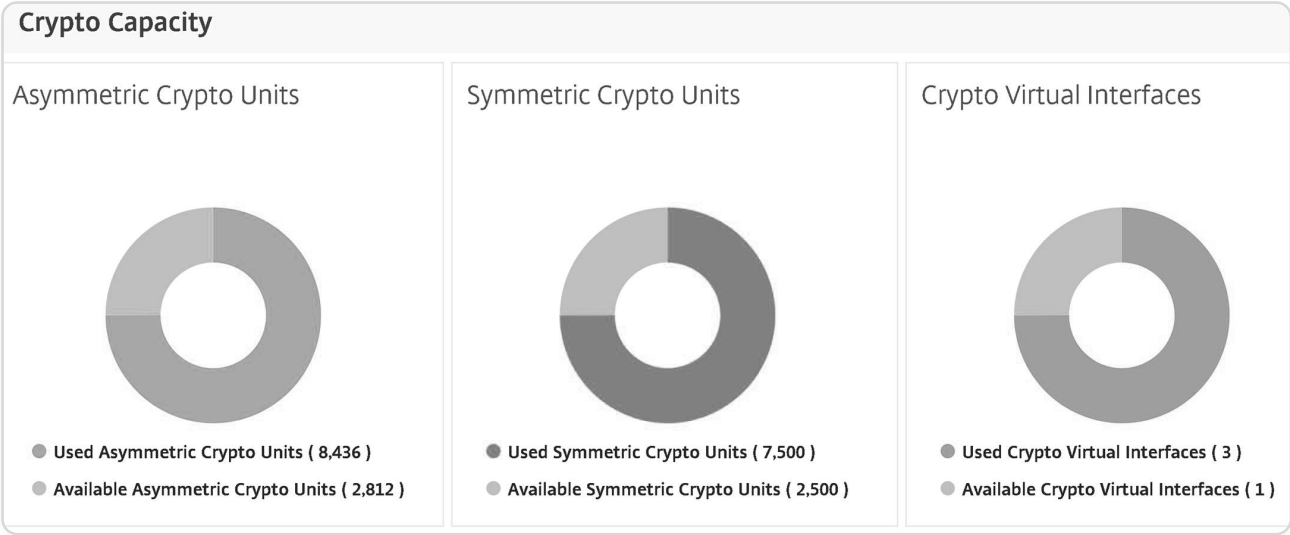
下表提供了有关 ACU、SCU 和加密虚拟实例的简要说明。

表。单位加密单元

新加密单元	描述
非对称加密单元 (ACU)	1 ACU = 1 次每秒操作 (ops) 的 (RSA) 2 K (2048 位密钥大小) 解密。有关更多详细信息，请参阅 ACU 到 PKE 资源转换表 。
对称加密单元 (SCU)	1 SCU = 1 Mbps 的 AES-128-CBC + SHA256-HMAC @ 1024B。此定义适用于所有 SDX 平台。
加密虚拟接口	加密虚拟接口也称为虚拟功能，代表 SSL 硬件的基本单元。在这些接口耗尽后，SSL 硬件无法再分配给 VPX 实例。加密虚拟接口是只读实体，SDX 设备会自动分配这些实体。

查看 SDX 设备的加密容量

您可以在 SDX GUI 的仪表板中查看 SDX 设备的加密容量。仪表板显示 SDX 设备上已使用和可用的 ACU、SCU 和虚拟接口。要查看加密容量，请导航到 **Dashboard > Crypto Capacity**。



在预置 VPX 实例时分配加密容量

在 SDX 设备上预置 VPX 实例时，在“加密分配”下，您可以为 VPX 实例分配 ACU 和 SCU 的数量。有关预置 VPX 实例的说明，请参阅 [预置 NetScaler 实例](#)。

要在预置 VPX 实例时分配加密容量，请执行以下步骤。

1. 登录到管理服务。
2. 导航到“配置 > NetScaler > 实例”，然后单击“添加”。
3. 在“加密分配”下，您可以查看可用的 ACU、SCU 和加密虚拟接口。ACU 和 SCU 的分配方式因 SDX 设备而异：
 - a. 对于 [不同 SDX 设备可用的 ACU 计数器最小值](#) 中列出的设备，您可以按指定数字的倍数分配 ACU。SCU 会自动分配，并且 SCU 分配字段不可编辑。您可以按该型号可用最小 ACU 的倍数增加 ACU 分配。例如，如果最小 ACU 为 4375，则 ACU 增量为 8750、13125 等。

示例。 SCU 自动分配且 ACU 按指定数字的倍数分配的加密分配。

Crypto Allocation			
	Asymmetric Crypto Units	Symmetric Crypto Units	Crypto Virtual Interfaces
Available	70000	56000	16
Total	70000	56000	16

Asymmetric Crypto Units

4375

Symmetric Crypto Units

3500

不同 SDX 设备可用的 ACU 计数器最小值

SDX 平台	ACU 计数器最小值
22040、22060、22080、22100、22120、 24100、24150 (36 端口	2187
8400, 8600, 8010, 8015	2812
17500, 19500, 21500	2812
17550, 19550, 20550, 21550	2812
11500, 13500, 14500, 16500, 18500, 20500	2812
11515, 11520, 11530, 11540, 11542	4375
14xxx	4375
14xxx 40标准	4375
14xxx 40千兆	4375
14xxx FIPS	4375
25xxx	4375
25xxx A 型	4575

b. 对于未在前面表格中列出的其余 SDX 平台，您可以自由分配 ACU 和 SCU。SDX 设备会自动分配加密虚拟接口。

示例。 ACU 和 SCU 均可自由分配的加密分配

Crypto Allocation

	Asymmetric Crypto Units	Symmetric Crypto Units	Crypto Virtual Interfaces
Available	39000	41000	32
Total	39000	41000	32

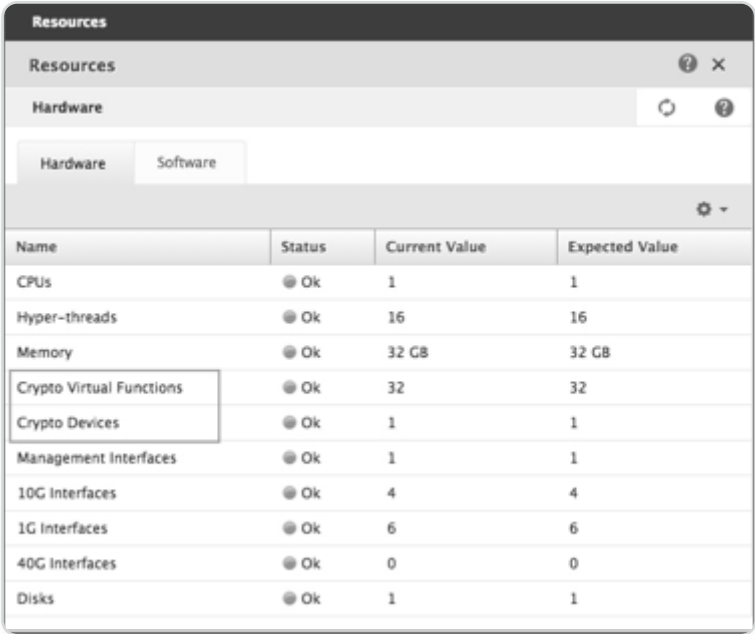
Asymmetric Crypto Units

Symmetric Crypto Units

4./ 完成预置 VPX 实例的所有步骤，然后单击 **Done**。有关详细信息，请参阅[预置 NetScaler 实例](#)。

查看加密硬件运行状况

在 Management Service 中，您可以查看 SDX 设备提供的加密硬件的运行状况。加密硬件的运行状况表示为“加密设备”和“加密虚拟功能”。要查看加密硬件的运行状况，请导航到 **Dashboard > Resources**。

The screenshot shows the 'Resources' window in the NetScaler SDX Management Service. It has tabs for 'Hardware' and 'Software', with 'Hardware' selected. Below the tabs is a table with columns: Name, Status, Current Value, and Expected Value. The table lists various hardware resources and their current status and values.

Name	Status	Current Value	Expected Value
CPUs	● Ok	1	1
Hyper-threads	● Ok	16	16
Memory	● Ok	32 GB	32 GB
Crypto Virtual Functions	● Ok	32	32
Crypto Devices	● Ok	1	1
Management Interfaces	● Ok	1	1
10G Interfaces	● Ok	4	4
1G Interfaces	● Ok	6	6
40G Interfaces	● Ok	0	0
Disks	● Ok	1	1

注意事项

当您将 SDX 设备升级到最新版本时，请记住以下几点。

- 只有 SDX 用户界面会升级，但设备的硬件容量保持不变。
- 加密分配机制保持不变，只有 SDX GUI 上的表示方式会改变。
- 加密接口向后兼容，并且不影响任何使用 NITRO 接口管理 SDX 设备的现有自动化机制。
- SDX 设备升级后，分配给现有 VPX 实例的加密不会改变；只有其在管理服务上的表示方式会改变。

ACU 到 PKE 资源转换表

SDX 平台	ACU	RSA- RSA1K	RSA- RSA2K	RSA- RSA4K	ECDHE- RSA	ECDHE- ECDSA
22040、 22060、 22080、 22100、 22120、 24100、	2187	12497	2187	312	256	190

SDX 平台	ACU	RSA- RSA1K	RSA- RSA2K	RSA- RSA4K	ECDHE- RSA	ECDHE- ECDSA
24150 (36 端口)						
8400, 8600, 8010, 8015	2812	17000	2812	424	330	不适用
11515, 11520, 11530, 11540, 11542	4375	25000	4375	625	512	381
22040, 22060, 22080,22 100, 22120 (24 个端口)	4375	25000	4375	625	512	381
17500, 19500, 21500	2812	17000	2812	424	330	不适用
17550, 19550, 20550, 21550	2812	17000	2812	424	330	不适用
11500, 13500, 14500, 16500, 18500, 20500	2812	17000	2812	424	330	不适用
14000, 14000-40	4375	25000	4375	625	512	381

SDX 平台	ACU	RSA- RSA1K	RSA- RSA2K	RSA- RSA4K	ECDHE- RSA	ECDHE- ECDSA
G, 25000, 25000A						
14000 FIPS	4375	25000	4375	625	512	381
14000-40 S	4375	25000	4375	625	512	381
*8900 (8910, 8920, 8930)	1000	4615	1000	136	397	494
*9100 (9110, 9120, 9130)	1000	4615	1000	136	397	494
*26000-1 00G (26100、 26160、 26200 和 26250)	1000	4615	1000	136	397	494
*15000	1000	4615	1000	136	397	494
*15000-5 0G	1000	4615	1000	136	397	494
*16000	1000	4615	1000	136	397	494
*26000-5 0S	1000	4615	1000	136	397	494

*在这些平台上，PKE 值是最低保证值。

如何解读 ACU 到 PKE 资源转换表

ACU 到 PKE 资源转换表基于以下几点：

- 管理服务帮助将加密资源分配给每个独立的 VPX。管理服务无法分配或保证性能。
- 实际性能因数据包大小、所使用的密码/密钥交换/HMAC（或其变体）等因素而异

以下示例帮助您理解如何阅读和应用 ACU 到 PKE 资源转换表。

示例。适用于 SDX 22040 平台的 ACU 到 PKE 资源转换

在 SDX 22040 平台上，将 2187 个 ACU 分配给一个 VPX 实例，所分配的加密资源相当于 256 次 ECDHE-RSA 操作或 2187 次 RSA-2K 操作等等。

传统 SSL 芯片到 ACU 和 SCU 转换表

有关传统 SSL 芯片如何转换为 ACU 和 SCU 的更多信息，请参阅下表。

[ACU 和 SCU 转换表](#)

预置第三方虚拟机

警告：

从 13.1 版本 37.x 及更高版本开始，NetScaler SDX GUI 中已弃用对 **第三方实例** 的支持。如果您仍想使用第三方实例，Citrix 建议您执行以下操作：

- 登录到管理服务 shell。
- 在目录 `/mpsconfig` 中创建文件 `.thirdPartyVM`。
- 通过运行 `svmd restart` 命令重新启动管理服务。

SDX 设备支持预置以下第三方虚拟机（实例）：

- SECUREMATRIX GSB
- 英特扫描网络安全
- 网星防护
- 蓝猫 DNS/DHCP 服务器
- CA 访问网关
- 派拓 VM 系列

SECUREMATRIX GSB 提供高度安全的密码系统，无需携带任何令牌设备。Websense Protector 提供监控和阻止功能，可防止数据丢失和敏感信息泄露。BlueCat DNS/DHCP Server 为您的网络提供 DNS 和 DHCP。NetScaler SDX 上的 PaloAlto VM-Series 能够在单个平台上整合高级安全和 ADC 功能，为企业和服务提供商客户提供对应用程序的安全可靠访问。NetScaler SDX 上的 VM-Series 组合还为 Citrix Virtual Apps and Desktops 部署提供了完整、经过验证的安全 ADC 解决方案。

您可以从管理服务预置、监控、管理和排查实例故障。所有上述第三方实例都使用 `SDXTools` 守护程序与管理服务通信。该守护程序预装在预置的实例上。当新版本可用时，您可以升级该守护程序。

当您配置第三方虚拟机时，作为通道一部分的 SR-IOV 接口（1/x 和 10/x）不会出现在接口列表中。这些接口缺失是因为第三方虚拟机不支持通道。

注意：

您可以在 SDX 设备上预置的实例总数取决于设备上安装的许可证。

重要提示： 在安装任何第三方实例之前，您必须将 Citrix Hypervisor 版本升级到 6.1.0。

SECUREMATRIX GSB

SECUREMATRIX 是一种高度安全、无令牌、一次性密码 (OTP) 身份验证解决方案，易于使用且经济高效。它使用矩阵表中的位置、序列和图像模式组合来生成一次性密码。SECUREMATRIX GSB 服务器与 SECUREMATRIX 身份验证服务器大幅增强了 VPN/SSL-VPN 端点、基于云的应用程序和资源、桌面/虚拟桌面登录以及 Web 应用程序（带 OTP 的反向代理）的安全性。它提供了一个兼容 PC、虚拟桌面、平板电脑和智能手机的解决方案。

在软件定义网络中使用 NetScaler SDX 多租户平台架构，SECUREMATRIX 的强身份验证功能可以与通过 NetScaler 提供的其他租户或云服务集成，例如 Web Interface、Citrix Virtual Apps and Desktops 以及许多其他需要身份验证的应用程序服务。

预配 SECUREMATRIX GSB 实例

SECUREMATRIX GSB 需要一个 SECUREMATRIX 身份验证服务器，该服务器必须在 SDX 设备外部进行配置。仅选择一个接口并仅为该接口指定网络设置。

注意： 属于通道的 SR-IOV 接口 (1/x 和 10/x) 不会出现在接口列表中。SECUREMATRIX GSB 实例不支持通道。

在开始预配实例之前，请从 SECUREMATRIX 网站下载 XVA 映像并将其上传到 SDX 设备。有关下载 XVA 映像的更多信息，请参阅 SECUREMATRIX 网站。确保您在 SDX 设备上使用的是 Management Service build 118.7 或更高版本。

在“**配置**”选项卡上，导航到“**SECUREMATRIX GSB > 软件映像**”。

要将 XVA 映像上传到 SDX 设备：

1. 在详细信息窗格中，在“**XVA 文件 > 操作**”下，单击“**上传**”。
2. 在出现的对话框中，单击“**浏览**”，然后选择要上传的 XVA 文件。
3. 单击“**上传**”。XVA 文件将显示在“XVA 文件”窗格中。

预配 SECUREMATRIX 实例

1. 在“**配置**”选项卡上，导航到“**SECUREMATRIX GSB > 实例**”。

2. 在详细信息窗格中，单击“添加”。
3. 在“配置 SECUREMATRIX GSB 向导”中，按照屏幕上的说明操作。
4. 单击“完成”，然后单击“关闭”。

配置实例后，登录到实例并执行详细配置。

要修改已配置的 SECUREMATRIX 实例的设置，请在“**SECUREMATRIX 实例**”窗格中，选择要修改的实例，然后单击“修改”。在“修改 SECUREMATRIX GSB 向导”中，修改参数。

注意： 如果您修改任何接口参数或实例名称，实例将停止并重新启动以使更改生效。

生成一个 tar 归档文件以提交给技术支持。有关生成技术支持文件的信息，请参阅[生成技术支持的 Tar 归档文件](#)。

备份 SECUREMATRIX GSB 实例的配置，然后使用备份数据恢复 SDX 设备上实例的配置。有关备份和恢复实例的信息，请参阅[备份和恢复 SDX 设备的配置数据](#)。

监视 SECUREMATRIX GSB 实例

SDX 设备收集 SECUREMATRIX GSB 实例的统计信息，例如 **SDXTools** 的版本、SSH 和 CRON 守护进程的状态以及 Web 服务器状态。

要查看与 SECUREMATRIX GSB 实例相关的统计信息：

1. 导航到“**SECUREMATRIX GSB > 实例**”。
2. 在详细信息窗格中，单击实例名称旁边的箭头。

管理 SECUREMATRIX GSB 实例

您可以从管理服务启动、停止、重新启动、强制停止或强制重新启动 SECUREMATRIX GSB 实例。

在“配置”选项卡上，展开“**SECUREMATRIX GSB**”。

要启动、停止、重启、强制停止或强制重启实例：

1. 单击 **实例**。
2. 在详细信息窗格中，选择要执行操作的实例，然后选择以下选项之一：
 - 启动
 - 关机
 - 重启
 - 强制关机

- 强制重启

3. 在“确认”消息框中，单击 **是**。

升级 SECUREMATRIX GSB 实例的 SDX 工具文件

SDXTools 是在 SECUREMATRIX GSB 实例上运行的守护程序，用于管理服务与实例之间的通信。

升级 **SDXTools** 涉及将文件上传到 SDX 设备，然后在选择实例后升级 **SDXTools**。您可以将 **SDXTools** 文件从客户端计算机上传到 SDX 设备。

上传 SDXTools 文件：

1. 在导航窗格中，展开 **管理服务**，然后单击 **SDXTools 文件**。
2. 在详细信息窗格中，从 **操作** 列表中选择 **上传**。
3. 在“上传 SDXTools 文件”对话框中，单击“浏览”，导航到包含该文件的文件夹，然后双击该文件。
4. 单击“上传”。

升级 SDXTools：

在“配置”选项卡上，展开“SECUREMATRIX GSB”。

1. 单击“实例”。
2. 在详细信息窗格中，选择一个实例。
3. 从“操作”列表中，选择“升级 SDXTools”。
4. 在“升级 SDXTools”对话框中，选择一个文件，单击“确定”，然后单击“关闭”。

升级和降级 SECUREMATRIX GSB 实例

升级 SECUREMATRIX GSB 实例的过程包括将目标版本的软件映像上传到 SDX 设备，然后升级实例。降级会加载实例的早期版本。

在“配置”选项卡上，展开“SECUREMATRIX GSB”。

上传软件映像：

1. 单击“软件映像”。
2. 在详细信息窗格中，从“操作”列表中，选择“上传”。
3. 在对话框中，单击“浏览”，导航到包含生成文件的文件夹，然后双击生成文件。

4. 单击**上传**。

要升级实例：

1. 单击**实例**。
2. 在详细信息窗格中，选择一个实例。
3. 从**操作**列表中，选择**升级**。
4. 在出现的对话框中，选择一个文件，单击**确定**，然后单击**关闭**。

要降级实例：

1. 单击**实例**。
2. 在详细信息窗格中，选择一个实例。
3. 从**操作**列表中，选择**降级**。
4. 在确认消息框中，单击**是**。

排查 SECUREMATRIX GSB 实例

从管理服务 Ping SECUREMATRIX GSB 实例，以检查设备是否可访问。您可以从管理服务跟踪数据包到实例的路由，以确定到达实例所需的跳数。

重新发现实例以查看实例的最新状态和配置。在重新发现期间，管理服务会获取在 SDX 设备上运行的 SECUREMATRIX GSB 的配置和版本。默认情况下，管理服务每 30 分钟安排一次实例重新发现。

在**配置**选项卡上，展开**SECUREMATRIX GSB**。

要 ping 实例：

1. 单击 **实例**。
2. 在详细信息窗格中，选择要 ping 的实例，然后从 **操作** 列表中单击 **Ping**。Ping 消息框会显示 ping 是否成功。

要跟踪实例的路由：

1. 单击 **实例**。
2. 在详细信息窗格中，选择要跟踪路由的实例，然后从 **操作** 列表中单击 **TraceRoute**。Traceroute 消息框会显示到该实例的路由。

要重新发现实例：

1. 单击 **实例**。
2. 在详细信息窗格中，选择要重新发现的实例，然后从 **操作** 列表中单击 **重新发现**。
3. 在确认消息框中，单击 **是**。

趋势科技 InterScan Web 安全

趋势科技 InterScan Web 安全是一款软件虚拟设备，可在互联网网关动态防护传统和新兴的 Web 威胁。它集成了应用程序控制、反恶意软件扫描、实时 Web 信誉、灵活的 URL 过滤和高级威胁防护。因此，它提供了卓越的防护，并对网络上日益增长的基于云的应用程序使用提供了更高的可见性和控制力。实时报告和集中管理为您的管理员提供了主动决策工具，从而实现即时风险管理。

InterScan Web 安全：

- 提供对最终用户互联网活动的更深入可见性
- 集中管理以实现最大程度的控制
- 实时监控 Web 使用情况
- 实现即时补救
- 减少设备蔓延和能源成本
- 提供可选的数据丢失防护和沙盒执行分析

在预配 InterScan Web 安全实例之前，您必须从趋势科技网站下载 XVA 映像。下载 XVA 映像后，将其上传到 NetScaler SDX 设备。

注意： 作为通道一部分的 SR-IOV 接口 (1/x 和 10/x) 不会出现在接口列表中。InterScan Web 安全实例不支持通道。

要将 XVA 映像上传到 SDX 设备：

1. 在“**配置**”选项卡中，导航到“**TrendMicro IWSVA > 软件映像**”。
2. 在详细信息窗格中，在“**XVA 文件**”选项卡下，单击“**上传**”。
3. 在出现的对话框中，单击“**浏览**”，然后选择要上传的 XVA 文件。
4. 单击“**上传**”。XVA 文件将显示在“XVA 文件”窗格中。

配置 TrendMicro IWSVA 实例：

1. 在“**配置**”选项卡上，导航到“**TrendMicro IWSVA > 实例**”。
2. 在详细信息窗格中，单击“**添加**”。
3. 在“**配置 TrendMicro IWSVA**”向导中，按照屏幕上的说明进行操作。

4. 单击**“确定”**，然后单击**“关闭”**。

配置实例后，登录到该实例并执行详细配置。

要修改已配置实例的参数值，请在详细信息窗格中选择要修改的实例，然后单击**“编辑”**。在**“修改 TrendMicro IWSVA”**向导中，将参数设置为适合您环境的值。

卫士通 防护系统

Websense（现称 Forcepoint）数据安全保护器是一个虚拟机，用于拦截出站 HTTP 流量（帖子）。然后，它会分析流量以防止数据丢失和敏感数据通过网络泄露。该保护器与专用 Windows 服务器通信以获取 DLP 策略信息，并在检测到匹配项时监控或阻止数据发布。内容分析在设备上执行，因此在此过程中没有敏感数据离开保护器。

要使用保护器的数据丢失防护 (DLP) 功能，请执行以下操作：

- 购买并安装 Websense 数据安全
- 在数据安全管理器中配置 Web DLP 策略
- 通过管理服务执行初始设置。

预配 Websense Protector 实例

Websense Protector 需要一个数据安全管理服务，该服务器必须在 SDX 设备外部配置。选择一个管理接口和两个数据接口。对于数据接口，必须选择“允许 L2 模式”。确保可以通过 Websense 保护器的管理网络访问数据安全管理服务。对于名称服务器，键入为该保护器提供服务的域名服务器 (DNS) 的 IP 地址。

注意： 作为通道一部分的 SR-IOV 接口（1/x 和 10/x）不会出现在接口列表中。Websense 保护器实例不支持通道。

从 Websense 网站下载保护器映像并将其上传到 SDX 设备，然后才能开始预配实例。有关下载保护器映像的更多信息，请参阅 [Websense 网站]。确保您在 SDX 设备上使用的是管理服务版本 118.7 或更高版本。

在**“配置”**选项卡上，导航到**“Websense Protector > 软件映像”**。

将 XVA 映像上传到 SDX 设备

1. 在详细信息窗格中，在**“XVA 文件 > 操作”**下，单击**“上传”**。
2. 在出现的对话框中，单击**“浏览”**，然后选择要上传的 XVA 文件。
3. 单击**“上传”**。XVA 文件将显示在**“XVA 文件”**窗格中。

预配 Websense protector 实例

1. 在“配置”选项卡上，导航到“**Websense Protector > 实例**”。
2. 在详细信息窗格中，单击“添加”。
3. 在“**预配 Websense Protector**”向导中，按照屏幕上的说明进行操作。
4. 单击“**完成**”，然后单击“**关闭**”。

预配实例后，登录到该实例并执行详细配置。

要修改已预配的 Websense protector 实例的设置，请在 Websense Protector 实例窗格中，选择要修改的实例，然后单击“**修改**”。在“**修改 Websense Protector**”向导中，设置参数。请勿修改在预配 Websense 实例时选择的接口。XVA 文件只能在删除实例并预配新实例后才能更改。

您可以生成一个 tar 存档以提交给技术支持。有关生成技术支持文件的信息，请参阅[生成用于技术支持的 Tar 存档](#)。

监视 Websense Protector 实例

SDX 设备会收集统计信息，例如 **SDXTools** 的版本、Websense Data Security 策略引擎的状态以及 Data Security 代理状态。

要查看与 Websense protector 实例相关的统计信息：

1. 导航到“**Websense Protector > 实例**”。
2. 在详细信息窗格中，单击实例名称旁边的箭头。

管理 Websense Protector 实例

您可以从管理服务启动、停止、重新启动、强制停止或强制重新启动 Websense protector 实例。

在**配置**选项卡上，展开 **Websense Protector**。

启动、停止、重新启动、强制停止或强制重新启动 Websense Protector 实例

1. 单击**实例**。
2. 在详细信息窗格中，选择要执行操作的实例，然后选择以下选项之一：
 - 启动
 - 关机
 - 重新启动
 - 强制关机

- 强制重新启动

3. 在确认消息框中，单击**是**。

升级 Websense Protector 实例的 SDX 工具文件

SDXTools，一个在第三方实例上运行的守护程序，用于管理服务与第三方实例之间的通信。

升级 **SDXTools** 涉及将文件上传到 SDX 设备，然后在选择实例后升级 **SDXTools**。您可以将 **SDXTools** 文件从客户端计算机上传到 SDX 设备。

上传 SDX 工具文件

1. 在导航窗格中，展开**管理服务**，然后单击**SDXTools 文件**。
2. 在详细信息窗格中，从 **Action** 列表中，选择 **Upload**。
3. 在 **Upload SDXTools Files** 对话框中，单击 **Browse**，导航到包含该文件的文件夹，然后双击该文件。
4. 单击 **Upload**。

升级 SDX 工具

在 **Configuration** 选项卡上，展开 **Websense Protector**。

1. 单击 **Instances**。
2. 在详细信息窗格中，选择一个实例。
3. 从 **Action** 列表中，选择 **Upgrade SDXTools**。
4. 在 **Upgrade SDXTools** 对话框中，选择一个文件，单击 **OK**，然后单击 **Close**。

将 Websense Protector 实例升级到更高版本

升级 Websense Protector 实例的过程涉及将目标版本的软件映像上传到 SDX 设备，然后升级该实例。

在 **Configuration** 选项卡上，展开 **Websense Protector**。

上传软件映像

1. 单击 **软件映像**。
2. 在详细信息窗格中，从 **Action** 列表中，选择 **Upload**。
3. 在对话框中，单击“**浏览**”，导航到包含构建文件的文件夹，然后双击该构建文件。
4. 单击“**上传**”。

升级实例

1. 单击“实例”。
2. 在详细信息窗格中，选择一个实例。
3. 从“操作”列表中，选择“升级”。
4. 在出现的对话框中，选择一个文件，单击“确定”，然后单击“关闭”。

对 Websense Protector 实例进行故障排除

从管理服务 Ping Websense Protector 实例，以检查设备是否可达。您可以跟踪从管理服务到实例的数据包路由，以确定到达该实例所需的跳数。

重新发现实例以查看实例的最新状态和配置。在重新发现期间，管理服务会获取在 SDX 设备上运行的 Websense Protector 的配置和版本。默认情况下，管理服务每 30 分钟安排一次实例重新发现。

在“配置”选项卡上，展开“**Websense Protector**”。

Ping 实例

1. 单击“实例”。
2. 在详细信息窗格中，选择要 Ping 的实例，然后从“操作”列表中单击“**Ping**”。Ping 消息框会显示 Ping 是否成功。

跟踪实例的路由

1. 单击 **实例**。
2. 在详细信息窗格中，选择要跟踪路由的实例，然后从 **操作** 列表中，单击 **TraceRoute**。Traceroute 消息框会显示到该实例的路由。

重新发现实例

1. 单击 **实例**。
2. 在详细信息窗格中，选择要重新发现的实例，然后从 **操作** 列表中，单击 **重新发现**。
3. 在确认消息框中，单击 **是**。

BlueCat DNS/DHCP

BlueCat DNS/DHCP 服务器是 NetScaler SDX 设备支持的软件解决方案。它托管在 NetScaler SDX 平台上，可提供可靠、可扩展且安全的 DNS 和 DHCP 核心网络服务，而无需额外管理成本或数据

中心空间。关键 DNS 服务可在单个系统内或跨多个 SDX 设备在多个 DNS 节点之间进行负载均衡，无需更多硬件。

BlueCat DNS/DHCP 服务器的虚拟实例可托管在 SDX 上，以提供更智能的方式连接移动设备、应用程序、虚拟环境和云。

要了解更多关于 BlueCat 和 Citrix 的信息，请访问 BlueCat 网站：<https://citrixready.citrix.com/bluecat-networks.html>。

如果您是 BlueCat 的现有客户，可以通过 BlueCat 支持门户下载软件和文档：<https://care.bluecatnetworks.com/>。

预配 BlueCat DNS/DHCP 实例

从 BlueCat 客户服务中心下载 XVA 映像，网址为 <https://care.bluecatnetworks.com>。下载 XVA 映像后，在开始预配实例之前将其上传到 SDX 设备。请确保您在 SDX 设备上使用的是 Management Service 版本 118.7 或更高版本。

BlueCat DNS/DHCP 虚拟机支持跨 0/1 和 0/2 接口的管理通道。有关详细信息，请参阅[从管理服务配置通道](#)。

注意：作为通道一部分的 SR-IOV 接口（1/x 和 10/x）不会出现在接口列表中，因为 BlueCat DNS/DHCP 实例不支持通道。

在“配置”选项卡上，导航到“**BlueCat DNS/DHCP > 软件映像**”。

要将 XVA 映像上传到 SDX 设备：

1. 在详细信息窗格中，在“**XVA 文件 > 操作**”下，单击“**上传**”。
2. 在出现的对话框中，单击“**浏览**”，然后选择要上传的 XVA 文件。
3. 单击“**上传**”。XVA 文件将显示在“XVA 文件”窗格中。

要预配 BlueCat DNS/DHCP 实例：

1. 在“配置”选项卡上，导航到“BlueCat DNS/DHCP”>“实例”。
2. 在详细信息窗格中，单击“添加”。“预配 BlueCat DNS/DHCP 服务器”页面随即打开。
3. 在“预配 BlueCat DNS/DHCP”向导中，按照屏幕上的说明进行操作。
 - 在“实例创建”下，在“名称”字段中，输入实例的名称，然后从“XVA 文件”下拉菜单中选择上传的映像，然后单击“下一步”。（可选）在“域名”字段中，输入实例的域名。 **注意：**名称不能包含空格。

- 在“网络设置”下，从“管理接口”下拉菜单中，选择用于管理实例的接口，设置该接口的 IP 地址和网关。您可以显式分配接口以实现高可用性和服务。选择参数，然后单击“下一步”。

注意：为管理、高可用性和服务分配接口时，请确保根据支持的接口组合分配接口：

您可以为所有这三项选择相同的接口。您可以为所有这三项选择不同的接口。您可以为管理和服务选择相同的接口，但为高可用性选择不同的接口。单击“完成”，然后单击“关闭”。实例将使用选定的 IP 地址创建、启动和配置。

预配实例后，通过 SSH 登录实例以完成配置。有关配置 BlueCat DNS/DHCP 服务器或将其置于 BlueCat Address Manager 控制下的详细信息，请参阅 BlueCat 文档，该文档可在 <https://care.bluecatnetworks.com> 处获取。

要修改 BlueCat DNS/DHCP 服务器实例的设置，请从“**BlueCat DNS/DHCP 实例**”窗格中，选择要修改的实例，然后单击“修改”。在“修改 BlueCat DNS/DHCP”向导中，修改参数设置。

注意：如果您修改任何接口参数或实例名称，实例将停止并重新启动以使更改生效。

监视 BlueCat DNS/DHCP 实例

SDX 设备会收集 BlueCat DNS/DHCP 实例的统计信息，例如实例上运行的 **SDXTools** 版本。

要查看与 BlueCat DNS/DHCP 实例相关的统计信息：

1. 导航到“BlueCat DNS/DHCP”>“实例”。
2. 在详细信息窗格中，单击实例名称旁边的箭头。

管理 BlueCat DNS/DHCP 实例

您可以从管理服务启动、停止、重新启动、强制停止或强制重新启动 BlueCat DNS/DHCP 实例。

在**配置**选项卡上，展开 **BlueCat DNS/DHCP**。

要启动、停止、重新启动、强制停止或强制重新启动 BlueCat DNS/DHCP 实例：

1. 单击实例。
2. 在详细信息窗格中，选择要执行操作的实例，然后选择以下选项之一：
 - 启动
 - 关机
 - 重新启动
 - 强制关机

- 强制重新启动

3. 在确认消息框中，单击是。

升级适用于 BlueCat DNS/DHCP 实例的 **SDXTools** 文件

SDXTools 是在第三方实例上运行的守护程序，用于管理服务和第三方实例之间的通信。

升级 **SDXTools** 涉及将文件上传到 SDX 设备，然后在选择实例后升级 **SDXTools**。您可以将 **SDXTools** 文件从客户端计算机上传到 SDX 设备。

上传 **SDXTools** 文件：

1. 在导航窗格中，展开“**管理服务**”，然后单击“**SDXTools 文件**”。
2. 在详细信息窗格中，从“**操作**”列表中，选择“**上载**”。
3. 在“**上载 SDXTools 文件**”对话框中，单击“**浏览**”，导航到包含该文件的文件夹，然后双击该文件。
4. 单击“**上载**”。

升级 **SDXTools**：

在“**配置**”选项卡上，展开“**BlueCat DNS/DHCP**”。

1. 单击“**实例**”。
2. 在详细信息窗格中，选择一个实例。
3. 从“**操作**”列表中，选择“**升级 SDXTools**”。
4. 在“**升级 SDXTools**”对话框中，选择一个文件，单击“**确定**”，然后单击“**关闭**”。

重新发现 BlueCat DNS/DHCP 实例

您可以重新发现实例以查看实例的最新状态和配置。在重新发现期间，管理服务会获取配置。默认情况下，管理服务每 30 分钟安排一次所有实例的重新发现。

在“**配置**”选项卡上，展开“**BlueCat DNS/DHCP**”。

1. 单击“**实例**”。
2. 在详细信息窗格中，选择要重新发现的实例，然后从“**操作**”列表中单击“**重新发现**”。
3. 在“**确认**”消息框中，单击“**是**”。

CA 接入网关

CA Access Gateway 是一款可扩展、可管理且可扩展的独立服务器，提供基于代理的访问控制解决方案。CA Access Gateway 采用代理引擎，为企业提供网络网关，并支持不依赖传统基于 Cookie 的技术的多种会话方案。

嵌入式 Web 代理可在整个企业中实现单点登录 (SSO)。CA Access Gateway 为 HTTP 和 HTTPS 请求以及无 Cookie SSO 提供访问控制。此外，该产品还会将会话信息存储在内存会话存储中。代理规则定义 CA Access Gateway 如何将请求转发或重定向到企业内目标服务器上的资源。

通过为网络资源提供单一网关，CA Access Gateway 隔离了企业网络并集中了访问控制。

注意：属于通道的 SR-IOV 接口（1/x 和 10/x）不会出现在接口列表中，因为 CA Access Gateway 实例不支持通道。有关 CA Access Gateway 功能的更多信息，请参阅该产品的文档。

预配 CA Access Gateway 实例

在预配 CA Access Gateway 实例之前，您必须下载 XVA 映像。下载 XVA 映像后，将其上传到 SDX 设备。确保您在 SDX 设备上使用的是 Management Service 10.5 build 52.3.e 或更高版本。要预配 CA Access Gateway，首先需要将 XVA 映像上传到 SDX 设备，然后预配一个实例。

将 XVA 映像上传到 SDX 设备：

1. 在“配置”选项卡上，导航到“CA Access Gateway”>“软件映像”。
2. 在详细信息窗格中，在“XVA 文件”下，从“操作”下拉列表中，单击“上传”。
3. 在出现的对话框中，单击“浏览”，然后选择要上传的 XVA 文件。
4. 单击“上传”。XVA 文件将显示在“XVA 文件”窗格中。

预配 CA Access Gateway 实例：

1. 在“配置”选项卡上，导航到“CA Access Gateway”>“实例”。
2. 在详细信息窗格中，单击“添加”。
3. 在 Provision CA Access Gateway 向导中，按照屏幕上的说明进行操作。
4. 单击“完成”，然后单击“关闭”。

预置实例后，登录到实例并执行详细配置。

要修改已预置实例的参数值，请在详细信息窗格中选择要修改的实例，然后单击“修改”。在 Modify CA Access Gateway 向导中，将参数设置为适合您环境的值。

注意：

如果您修改任何接口参数或实例名称，实例将停止并重新启动以使更改生效。

监视 CA Access Gateway 实例

SDX 设备收集 CA Access Gateway 实例的统计信息，例如实例上运行的 **SDXTools** 版本。

要查看与 CA Access Gateway 实例相关的统计信息：

1. 导航到 **CA Access Gateway > 实例**。
2. 在详细信息窗格中，单击实例名称旁边的箭头。

管理 CA Access Gateway 实例

您可以从 Management Service 启动、停止、重新启动、强制停止或强制重新启动 CA Access Gateway 实例。要完成这些任务，请执行以下步骤：

1. 在“配置”选项卡上，展开“CA Access Gateway”。
2. 导航到 **CA Access Gateway > 实例**。
3. 在详细信息窗格中，选择要对其执行操作的实例，然后选择以下选项之一：
 - 启动
 - 关闭
 - 重新启动
 - 强制关闭
 - 强制重新启动
4. 在“确认”消息框中，单击 **是**。

派拓网络 VM 系列

Palo Alto Networks VM 系列虚拟防火墙使用与该公司物理安全设备中可用的 PAN-OS 功能集相同的功能集，提供所有关键网络安全功能。NetScaler SDX 上的 VM 系列可在单一平台上整合高级安全和 ADC 功能，为企业、业务部门和服务提供商客户提供对应用程序的安全可靠访问。NetScaler SDX 上的 VM 系列组合还为 Citrix Virtual Apps and Desktops 部署提供了完整、经过验证的安全和 ADC 解决方案。

您可以从管理服务调配、监控、管理和故障排除实例。

注意事项：

- 您可以在 SDX 设备上调配的实例总数取决于可用的 SDX 硬件资源。

- 作为通道一部分的 SR-IOV 接口（1/x 和 10/x）不会出现在接口列表中，因为 Palo Alto VM 系列实例不支持通道。有关 Palo Alto Network VM 系列的更多信息，请参阅 [Palo Alto Network 文档](#)。

调配 Palo Alto VM 系列实例

在调配 Palo Alto VM 系列实例之前，您必须从 [Palo Alto Networks 网站](#) 下载 XVA 映像。下载 XVA 映像后，将其上传到 SDX 设备。

要将 XVA 映像上传到 SDX 设备：

1. 在“配置”选项卡上，导航到“**Palo Alto VM 系列 > 软件映像**”。
2. 在详细信息窗格中，在“**XVA 文件**”下，从“操作”下拉列表中，单击“**上传**”。
3. 在出现的对话框中，单击“**浏览**”，然后选择要上传的 XVA 文件。
4. 单击“**上传**”。XVA 文件将显示在“**XVA 文件**”窗格中。

要调配 Palo Alto VM 系列实例：

1. 在“配置”选项卡上，导航到“**Palo Alto VM 系列 > 实例**”。
2. 在详细信息窗格中，单击 **添加**。
3. 在“配置 Palo Alto VM-Series”向导中，按照屏幕上的说明进行操作。
4. 单击 **完成**，然后单击 **关闭**。

配置实例后，登录到实例并执行详细配置。

要修改已配置实例的参数值，请在详细信息窗格中选择要修改的实例，然后单击 **修改**。在“修改 Palo Alto VM-Series”向导中，将参数设置为适合您环境的值。

注意： 如果您修改任何接口参数或实例名称，实例将停止并重新启动以使更改生效。

监视 Palo Alto VM-Series 实例

SDX 设备收集 Palo Alto VM-Series 实例的统计信息，例如实例上运行的 **SDXTools** 版本。

要查看与 Palo Alto VM-Series 实例相关的统计信息：

1. 导航到 **Palo Alto VM-Series > 实例**。
2. 在详细信息窗格中，单击实例名称旁边的箭头。

管理 Palo Alto VM-Series 实例

您可以从管理服务启动、停止、重新启动、强制停止或强制重新启动 Palo Alto VM-Series 实例。

在 **配置** 选项卡上，展开 **PaloAlto VM-Series**。

1. 导航到 **PaloAlto VM-Series > 实例**。
2. 在详细信息窗格中，选择要执行操作的实例，然后选择以下选项之一：
 - 启动
 - 关闭
 - 重启
 - 强制关闭
 - 强制重启
3. 在“确认”消息框中，单击**是**。

排除 PaloAlto VM-Series 实例故障

从管理服务 Ping PaloAlto VM-Series 实例，以检查设备是否可达。您可以跟踪从管理服务到实例的数据包路由，以确定到达实例所需的跳数。

重新发现实例以查看实例的最新状态和配置。在重新发现期间，管理服务会获取在 SDX 设备上运行的 PaloAlto VM-Series 的配置和版本。默认情况下，管理服务每 30 分钟安排一次实例重新发现。

在**配置**选项卡上，展开**PaloAlto VM-Series**。

要 Ping 实例：

1. 单击**实例**。
2. 在详细信息窗格中，选择要 Ping 的实例，然后从**操作**列表中单击**Ping**。“**Ping 消息**”框显示 Ping 是否成功。

要跟踪实例路由：

1. 单击 **实例**。
2. 在详细信息窗格中，选择要 ping 的实例，然后从 **操作** 列表中，单击 **TraceRoute**。**Traceroute** 消息框显示到该实例的路由。

重新发现实例：

1. 单击 **实例**。
2. 在详细信息窗格中，选择要重新发现的实例，然后从 **操作** 列表中，单击 **重新发现**。
3. 在确认消息框中，单击 **是**。

在 NetScaler SDX 设备上部署 Citrix SD-WAN VPX 实例

Citrix SD-WAN 技术将软件定义网络 (SDN) 概念应用于 WAN 连接。该技术将流量管理和监控从网络硬件中抽象出来，并将其应用于单个应用程序。结果是提高了性能，在地理分散的位置提供了高质量的用户体验，并简化了广域网和云访问网络的部署。有关更多信息，请参阅 [Citrix SD-WAN](#)。

注意： 仅支持 SD-WAN VPX 标准版。有关更多信息，请参阅 [SD-WAN VPX 版本](#)。

在 SDX 设备上部署 Citrix SD-WAN™ VPX 实例包括以下任务：

- 安装硬件：确保 SDX 硬件已正确安装。有关更多信息，请参阅 [安装硬件](#)。
- 设置和配置 SDX 管理服务。有关更多信息，请参阅 [管理服务用户界面入门](#) 和 [配置管理服务](#)。
- 在 SDX 设备上预配 SD-WAN VPX 实例。有关更多信息，请参阅 [在 NetScaler SDX 上预配 Citrix SD-WAN VPX 实例](#)。
- 配置 SD-WAN VPX 实例。有关更多信息，请参阅 [配置](#) 文档和 [配置 MCN 与客户端站点之间的虚拟路径服务](#)。

先决条件

确保您拥有以下许可证：

- Citrix SD-WAN VPX 许可证
- NetScaler SDX 平台许可证

Citrix SD-WAN VPX 要求

SDX 平台上的 Citrix SD-WAN VPX 既可以作为站点，也可以作为 MCN。MCN 可以处理 1 Gb/s 的双向吞吐量和 64 个站点。

MCN 和站点支持的吞吐量

- 250 Mb/s 到 1 Gb/s 双向吞吐量
- MCN 支持 64 个站点

支持吞吐量的硬件要求

站点

- 4 到 16 个 CPU
- 4 GB 到 16 GB RAM
- 60 GB 到 250 GB 磁盘存储
- 最少 4 个 NIC：一个用于管理，其余最少 3 个用于数据路径

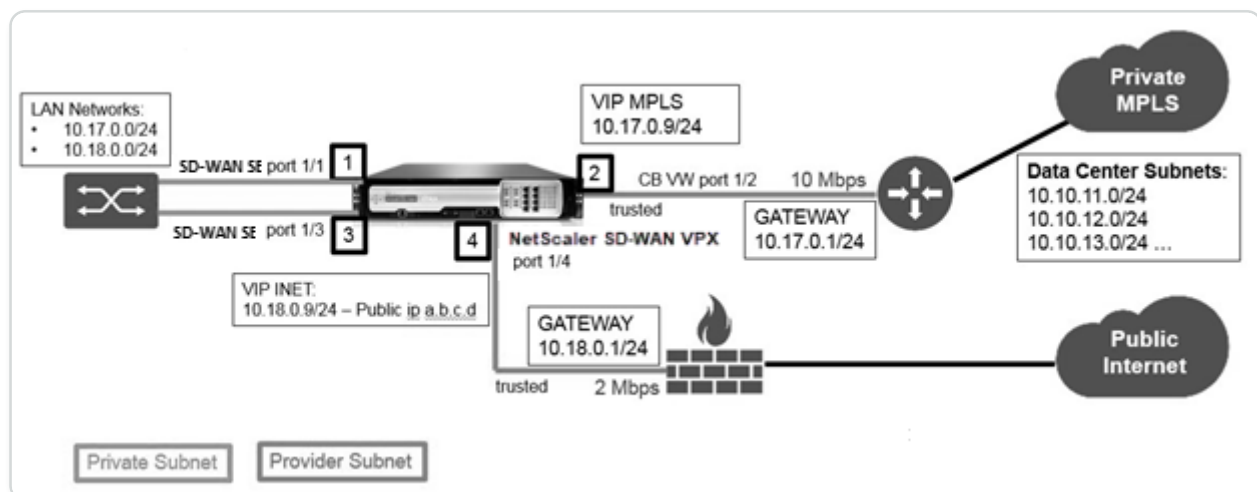
主控制节点 (MCN)

- 4、8 和 16 个 CPU
- 16 GB RAM
- 250 GB 磁盘存储
- 最少 4 个 NIC：一个用于管理，其余 3 个用于数据路径，并为数据路径配备专用 NIC

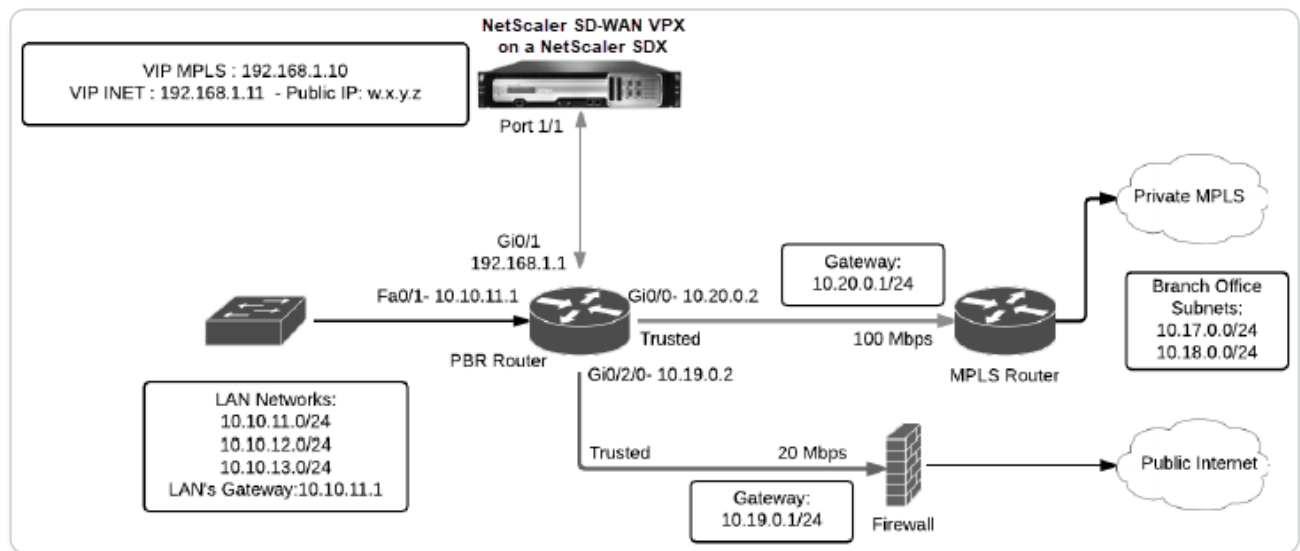
数据中心拓扑

您可以在 NetScaler SDX 上以基于策略的路由 (PBR) 模式或内联模式部署 Citrix SD-WAN VPX 设备。有关这两种支持模式的数据中心拓扑，请参阅场景 1 和 2。有关更多信息，请参阅 [在虚拟内联模式下部署 SD-WAN](#)。

场景 1: 内联模式



场景 2: PBR 模式或虚拟内联模式



在 NetScaler SDX™ 上预置 Citrix SD-WAN VPX 实例

在预置 Citrix SD-WAN VPX 设备之前，请从 NetScaler® 产品下载站点下载 SD-WAN VPX 映像：

<https://www.citrix.com/downloads/netScaler-sd-wan/>。

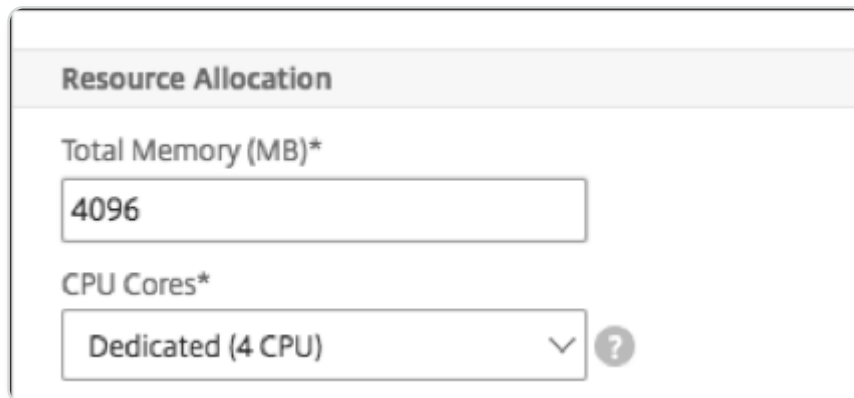
请按照以下步骤预置 Citrix SD-WAN VPX 设备。

1. 登录到 NetScaler SDX 设备。
2. 导航到 **配置 > SD-WAN > 实例**。
3. 选择 **软件映像 > 上载**，然后上载 SD-WAN XVA 文件。



4. 选择 **实例 > 添加**。**预置 SD-WAN 实例** 页面随即显示。
5. 在 **预置 SD-WAN 实例** 页面中，输入以下内容：
 - a. 名称
 - b. IP 地址
 - c. 子网掩码
 - d. 网关地址
 - e. 上传 XVA 文件

f. 在 **资源分配** 下，分配资源。



The image shows a 'Resource Allocation' configuration window. It has two input fields: 'Total Memory (MB)*' with the value '4096' and 'CPU Cores*' with a dropdown menu showing 'Dedicated (4 CPU)'. There is a question mark icon next to the CPU Cores dropdown.

g. 在 **网络设置** 下，预配管理接口，然后选择 **确定** 以在 SDX 设备上创建并预配 SD-WAN VPX 实例。

注意：

SDX 管理服务按照接口名称的升序将接口绑定到 VPX 实例。例如，如果您添加 1/4 和 1/1，管理服务会将其排列为 1/1、1/4。当您添加新接口时，现有序列将保留并创建一个新序列。例如，您添加接口 1/2、10/1、1/3。新序列将是 1/1、1/4；1/2、1/3、10/1。

6. SD-WAN VPX 实例显示在 **实例页面** 下。示例如下。

! [Image](https://docs.netScaler.com/content/dam/netScaler/us/en/sdx/media/sd-wan-vpx-example.png)

要编辑实例，请导航到 **Configuration > SD-WAN > Instances**。选择并单击该实例。完成编辑后，单击 **确定** 以保存更改。

配置 Citrix SD-WAN VPX 实例

在 SDX 设备上创建 SD-WAN 实例后，通过完成以下两项任务来配置 SD-WAN 实例：

1. 为 MCN 和站点设备应用配置。
2. 配置虚拟路径并传输流量。

有关详细信息，请参阅以下主题：

- [配置](#)
- [配置 MCN 和客户端站点之间的虚拟路径服务](#)

相关信息

有关 Citrix SD-WAN 设备入门的更多信息，请参阅 [Citrix SD-WAN](#)。

有关 NetScaler SDX 设备的更多信息，请参阅 [NetScaler SDX](#)。

SDX 中的带宽计量

NetScaler SDX 带宽计量功能为您提供准确、可靠且易于使用的计量方案，使您能够高效地分配处理能力并实现带宽使用货币化。需要计量方案才能在各种资源之间优化分配带宽，同时确保所有用户始终获得分配的带宽。

带宽分配可以通过以下两种模式完成：

- 具有固定吞吐量速率的专用带宽
- 具有最低保证吞吐量和带宽突发能力的专用带宽

具有固定吞吐量速率的专用带宽

在此带宽分配方法中，每个 VPX 实例都分配有专用带宽。实例被允许使用带宽，直至达到设定的限制。在专用模式下，分配的最小和最大带宽是相同的。如果在某个时期，VPX 实例需要的带宽超过了分配的带宽，那么在专用模式下，该实例无法增加其吞吐量。如果 VPX 实例处理关键请求，这可能是一个缺点。

此外，如果 SDX 设备有几个 VPX 实例，其中一些实例没有利用其分配的带宽，则在专用模式下无法共享其未使用的带宽。为了克服所有这些挑战，具有最低保证速率并能够动态增加带宽的专用带宽非常有用。

具有最低保证吞吐量和带宽突发能力的专用带宽

在此带宽分配方法中，VPX 被分配了最低保证带宽，并可灵活地将其带宽增加到预设限制。VPX 可以使用的额外带宽称为突发容量。

当您有一些具有额外容量的实例和一些具有未使用容量的 VPX 时，突发容量的优势就显现出来了。这些 VPX 实例的额外容量可以分配给其他已完全利用其分配带宽并在一段时间内需要更多带宽的 VPX 实例。各种服务提供商也有兴趣向其客户提供需要专用容量的各种附加服务。同时，他们不希望过度预置带宽。可突发带宽有助于解决此类场景，即客户可以获得特定带宽的保证，并可在高需求期间选择增加带宽。

选择带宽分配模式

在选择可突发吞吐量之前，您需要启用动态突发吞吐量分配。要启用此选项，请按照以下步骤操作。

1. 在 SDX 管理控制台中，导航到 **Configuration > System**。
2. 从 **系统设置** 组中，选择 **更改系统设置**。
3. 点击“启用动态突发吞吐量分配”复选框以启用动态吞吐量。

Dashboard Configuration Documentation Downloads

← Configure System Settings

Communication with Citrix ADC Instance*

https

☐ Secure Access Only

☐ Enable Session Timeout

☒ Enable Dynamic Burst Throughput Allocation

☒ Allow Basic Authentication

☒ Enable nsrecover Login

☒ Enable Shell access for non-nsroot User

OK Close

预置 VPX 时，您可以选择带宽突发或动态吞吐量。

1. 在“SDX 管理服务”中，单击“配置 > NetScaler > 实例 > 添加”。
2. “预置 NetScaler”页面打开。在“许可证分配”下，从“分配模式”中选择“可突发”。

License Allocation

Feature License* Standard

For more information about Citrix ADC editions, see Citrix ADC Editions

Pool	Total	Available
Instance	25	0
Bandwidth	100 Gbps	20 Gbps

Allocate

1

Allocation Mode* Burstable

Min (Mbps)* 1000 Max (Mbps) 0 Burst* P0

有关如何预置 NetScaler 实例的更多信息，请参阅[预置 NetScaler 实例](#)。

如果要使用固定吞吐量速率，请选择“固定”。默认情况下，带宽分配设置为固定模式。并非所有 VPX 实例都必须同一模式下工作。每个 VPX 实例都可以配置为不同的模式。

注意：如果您正在从 10.5.e 及更早版本迁移 SDX，则默认情况下所有 VPX 实例都处于固定分配模式。

确定 VPX 实例的最大突发带宽

每个 VPX 允许突发的程度通过算法计算。当您预置具有可突发带宽的 VPX 时，每个此类 VPX 都必须被赋予优先级。可突发带宽的分配取决于此突发优先级。优先级从 P0 到 P4 变化，其中 P0 是最高优先级，P4 是最低优先级。

让我们来看一个有 2 个 VPX（即 VPX1 和 VPX2）的案例。分配给 VPX1 和 VPX2 的最小带宽分别为 4 Gbps 和 2 Gbps，每个 VPX 的可突发带宽分别为 2 Gbps 和 1 Gbps。下表描述了这些参数：

VPX 名称	参数	值	
VPX1	最小保证带宽	4Gbps 带宽	
-	-	最大突发带宽	2Gbps 带宽
-	-	优先级	P0
VPX2	最小保证带宽	2吉比特/秒	
-	-	最大可突发带宽	1 吉比特每秒
-	-	优先级	P1

在这种情况下，我们假设总许可带宽为 8 Gbps。如果两个 VPX 实例都突发到其最大可突发限制，即：

1. VPX1 正在使用其最大可突发带宽，即 2 Gbps，那么它总共使用了 $4 + 2 = 6$ Gbps
2. VPX2 正在使用其最大可突发带宽，即 1 Gbps，那么它总共使用了 $2 + 1 = 3$ Gbps

在这种情况下，使用的最大带宽超过了 8 Gbps 的许可容量。因此，为了将使用量降低到许可容量内的带宽，其中一个 VPX 必须放弃其可突发带宽。在这种情况下，由于 VPX2 的优先级低于 VPX1，因此它放弃了其 1 Gbps 的可突发带宽。VPX1 将继续突发，因为它具有比 VPX2 更高的优先级。在所有此类场景中，都会确保始终遵守最小保证带宽。

检查吞吐量和数据消耗统计信息

对于每个 VPX，您可以在图表中检查吞吐量和数据消耗统计信息。要访问图表，请按照以下步骤操作：

1. 在 SDX 管理服务中，转到“**配置 > NetScaler > 实例**”页面。
2. 选择一个 VPX 实例，然后单击“**操作下拉**”列表。

3. 从列表中选择**吞吐量统计**或**数据使用统计**。

这些图表可让您查看不同时间段内的数据消耗和吞吐量统计，例如：

- 过去 1 小时
- 过去 1 天
- 过去 1 周
- 过去 1 个月，以及
- 上个月

您还可以通过调整图表底部的滑块来选择图表中的特定时间段。将鼠标悬停在图表中的线条上，以查看特定时间的数据消耗或吞吐量数据。

下图显示了为期 1 周的吞吐量数据示例图：

吞吐量数据(/en-us/sdx/media/metering_graph_slider-citrix.png)

配置和管理 NetScaler 实例

在设备上预置 NetScaler 实例后，即可配置和管理这些实例。首先创建子网 IP (SNIP) 地址，然后保存配置。之后，您可以对实例执行基本的管理任务。检查是否需要应用管理配置。

警告： 确保使用管理服务修改实例的预置网络接口或 VLAN，而不是直接在实例上执行修改。

在 NetScaler 实例上创建 SNIP 地址

在 SDX 设备上预置 NetScaler 实例后，您可以为其分配 SNIP 地址。

SNIP 用于连接管理和服务器监控。在首次配置 NetScaler SDX 设备时，并非强制指定 SNIP。您可以从管理服务将 SNIP 分配给 NetScaler 实例。

在 NetScaler 实例上添加 SNIP 地址

1. 在“配置”选项卡上的导航窗格中，单击“**NetScaler**”。
2. 在详细信息窗格中的“**NetScaler 配置**”下，单击“**创建 IP**”。
3. 在“**创建 NetScaler IP**”对话框中，为以下参数指定值。
 - **IP 地址：** 指定用作 SNIP 地址的 IP 地址。
 - **子网掩码：** 指定与 SNIP 地址关联的子网掩码。
 - **类型：** 默认值为 SNIP。
 - **保存配置：** 选择此项可在 NetScaler 上保存配置。默认值为 false。
 - **实例 IP 地址：** 指定 NetScaler 实例的 IP 地址。
4. 单击“**创建**”，然后单击“**关闭**”。

保存配置

您可以从 Management Service 保存 NetScaler 实例的运行配置。

保存 NetScaler 实例上的配置

1. 在“配置”选项卡上的导航窗格中，单击“**NetScaler**”。
2. 在详细信息窗格中的“**NetScaler 配置**”下，单击“**保存配置**”。

3. 在“保存配置”对话框的“实例 IP 地址”中，选择要保存其配置的 NetScaler 实例的 IP 地址。
4. 点击“确定”，然后点击“关闭”。

管理 NetScaler 实例

Management Service 允许您对 NetScaler 实例执行以下操作。您可以从“配置”选项卡中的“NetScaler 实例”窗格或主页上的 NetScaler 实例小工具执行这些操作。

启动 NetScaler 实例：从 Management Service 用户界面启动任何 NetScaler 实例。当 Management Service UI 将此请求转发到 Management Service 时，它会启动 NetScaler 实例。

关闭 NetScaler 实例：从 Management Service 用户界面关闭任何 NetScaler 实例。当 Management Service UI 将此请求转发到 Management Service 时，它会停止 NetScaler 实例。

重新启动 NetScaler 实例：重新启动 NetScaler 实例。

删除 NetScaler 实例：如果您不想使用 NetScaler 实例，可以使用 Management Service 删除该实例。删除实例会永久从 SDX 设备数据库中删除该实例及其相关详细信息。

启动、停止、删除或重新启动 NetScaler 实例

1. 在“配置”选项卡上，在导航窗格中，单击“NetScaler 实例”。
2. 选择要对其执行操作的 NetScaler 实例，然后单击“启动”或“关机”或“删除”或“重新启动”。
3. 在确认消息框中，单击“是”。

删除 NetScaler 实例文件

您可以从设备中删除任何 NetScaler 实例文件，例如 XVA、内部版本、文档、SSL 密钥或 SSL 证书。

删除 NetScaler 实例文件

1. 在“配置”选项卡上，在导航窗格中，展开“NetScaler 配置”，然后单击要删除的文件。
2. 在详细信息窗格中，选择文件名，然后单击“删除”。

应用管理配置

在预配 VPX 实例时，管理服务会在 VPX 实例上创建一些策略、实例管理（管理员）配置文件和其他配置。如果管理服务未能应用管理员配置，您可以显式地将配置从管理服务推送到 VPX 实例。失

败的一个原因可能是管理服务和 VPX 实例位于不同的子网中，并且路由器已关闭。另一个原因可能是两者位于同一子网中，但流量必须通过外部交换机，并且其中一个链接已关闭。

在 NetScaler 实例上应用管理员配置

1. 在“配置”选项卡上，在导航窗格中，单击“NetScaler”。
2. 在详细信息窗格中，在“NetScaler 配置”下，单击“应用管理员配置”。
3. 在“应用管理员配置”对话框中，在“实例 IP 地址”中，选择要应用管理员配置的 VPX 实例的 IP 地址。
4. 单击“确定”。

安装和管理 SSL 证书

安装 SSL 证书的过程首先涉及将证书和密钥文件上传到 NetScaler SDX 设备。然后，在 NetScaler 实例上安装 SSL 证书。在 SDX 设备上安装或更新 SSL 证书时，管理服务会重新启动。

将证书文件上传到 SDX 设备

对于任何 SSL 事务，服务器都需要有效的证书以及相应的私钥和公钥对。在 NetScaler 实例上安装 SSL 证书时，证书文件必须存在于 SDX 设备上。您还可以将 SSL 证书文件下载到本地计算机作为备份。

在 **SSL 证书** 窗格中，您可以查看以下详细信息。

- **名称**

证书文件的名称。

- **上次修改时间**

证书文件上次修改的日期。

- **大小**

证书文件的大小（以字节为单位）。

将 SSL 证书文件上传到 SDX 设备

1. 在导航窗格中，展开“管理服务”，然后单击“SSL 证书文件”。
2. 在“SSL 证书”窗格中，单击“上传”。
3. 在“上传 SSL 证书”对话框中，单击“浏览”并选择要上传的证书文件。
4. 单击“上传”。证书文件将显示在 SSL 证书窗格中。

要通过下载 SSL 证书文件创建备份

1. 在 SSL 证书窗格中，选择要下载的文件，然后单击“下载”。
2. 在消息框中，从“保存”列表中选择“另存为”。
3. 在“另存为”消息框中，浏览到要保存文件的位置，然后单击“保存”。

将 SSL 密钥文件上传到 SDX 设备

对于任何 SSL 事务，服务器都需要有效的证书以及相应的私钥和公钥对。在 NetScaler 实例上安装 SSL 证书时，密钥文件必须存在于 SDX 设备上。您还可以将 SSL 密钥文件下载到本地计算机作为备份。

在 SSL 密钥窗格中，您可以查看以下详细信息。

- **名称**

密钥文件的名称。

- **上次修改时间**

密钥文件上次修改的日期。

- **大小**

密钥文件的大小（以字节为单位）。

要将 SSL 密钥文件上传到 SDX 设备

1. 在导航窗格中，展开“管理服务”，然后单击“SSL 证书文件”。
2. 在“SSL 证书”窗格中，在“SSL 密钥”选项卡上，单击“上传”。
3. 在“上传 SSL 密钥文件”对话框中，单击“浏览”并选择要上传的密钥文件。
4. 单击“上传”将密钥文件上传到 SDX 设备。密钥文件将显示在“SSL 密钥”窗格中。

通过下载 SSL 密钥文件创建备份

1. 在“SSL 证书”窗格中，在“SSL 密钥”选项卡上，选择要下载的文件，然后单击“下载”。
2. 在消息框中，从“保存”列表中选择“另存为”。
3. 在“另存为”消息框中，浏览到要保存文件的位置，然后单击“保存”。

在 NetScaler 实例上安装 SSL 证书

管理服务允许您在一个或多个 NetScaler 实例上安装 SSL 证书。在开始安装 SSL 证书之前，请确保您已将 SSL 证书和密钥文件上传到 SDX 设备。

在 NetScaler 实例上安装 SSL 证书

1. 在导航窗格中，单击“NetScaler”。
2. 在详细信息窗格中，在“NetScaler 配置”下，单击“安装 SSL 证书”。
3. 在“安装 SSL 证书”对话框中，为以下参数指定值。(*) 表示必填字段。
 - 证书文件：指定有效证书的文件名。证书文件必须存在于 SDX 设备上。
 - 密钥文件：指定用于创建证书的私钥的文件名。密钥文件必须存在于 SDX 设备上。
 - 证书名称：指定要添加到 NetScaler 的证书-密钥对的名称。最大长度：31
 - 证书格式：指定 NetScaler 上支持的 SSL 证书格式。NetScaler SDX 设备支持 PEM 和 DER 格式的 SSL 证书。
 - 密码：指定用于加密私钥的密码短语。此选项可用于加载加密的私钥。最大长度：32。

注意：仅 PEM 格式支持受密码保护的私钥。

 - 保存配置：指定是否必须将配置保存到 NetScaler。默认值为 false。
 - 实例 IP 地址：指定要安装 SSL 证书的 NetScaler 实例的 IP 地址。
4. 单击“确定”，然后单击“关闭”。

在 NetScaler 实例上更新 SSL 证书

您可以更新安装在 NetScaler 实例上的 SSL 证书的某些参数，例如证书文件、密钥文件和证书格式。您无法修改 IP 地址和证书名称。

在 NetScaler 实例上更新 SSL 证书

1. 在导航窗格中，展开 NetScaler，然后单击“SSL 证书”。
2. 在“SSL 证书”窗格中，单击“更新”。
3. 在“修改 SSL 证书”对话框中，设置以下参数：
 - 证书文件：有效证书的文件名。证书文件必须存在于 SDX 设备上。
 - 密钥文件：用于创建证书的私钥的文件名。密钥文件必须存在于 SDX 设备上。
 - 证书格式：NetScaler SDX 设备上支持的 SSL 证书格式。设备支持 PEM 和 DER 格式的 SSL 证书。
 - 密码：用于加密私钥的密码短语。此选项可用于加载加密的私钥。最大长度：32 个字符。

注意：仅 PEM 格式支持受密码保护的私钥。

 - 保存配置：指定是否必须将配置保存到 SDX 设备上。默认值为 false。

- 无域检查：更新证书时不要检查域名。

4. 单击“确定”，然后单击“关闭”。

轮询 NetScaler 实例上的 SSL 证书

如果您在登录到 NetScaler 实例后直接在该实例上添加 SSL 证书，管理服务将不会知道此新证书。为避免这种情况，请指定一个轮询间隔，在此间隔之后，管理服务将轮询所有 NetScaler 实例以检查新的 SSL 证书。您也可以随时从管理服务执行轮询。例如，如果您想立即获取所有 NetScaler 实例中的 SSL 证书列表。

配置轮询间隔

1. 在导航窗格中，展开 NetScaler，然后单击“SSL 证书”。
2. 在“SSL 证书”窗格中，单击“配置轮询间隔”。
3. 在“配置轮询间隔”对话框中，设置以下参数：
 - 轮询间隔：管理服务轮询 NetScaler 实例之后的时间。
 - 间隔单位：时间单位。可能的值：小时、分钟。默认值：小时。
4. 单击确定，然后单击关闭。

执行立即轮询

1. 在导航窗格中，展开 NetScaler，然后单击 SSL 证书。
2. 在 SSL 证书窗格中，单击立即轮询。
3. 在确认对话框中，单击是。SSL 证书窗格将刷新，并且新证书（如果有）将显示在列表中。

在 NetScaler 实例上启用 L2 模式

在二层 (L2) 模式下，NetScaler 实例充当学习型网桥，并转发所有非其目的地的报文。某些功能（例如 Citrix CloudBridge）要求在 NetScaler 实例上启用 L2 模式。启用 L2 模式后，实例可以接收并转发除自身 MAC 地址以外的 MAC 地址的报文。但是，要在 NetScaler SDX 设备上运行的 NetScaler 实例上启用 L2 模式，管理员必须首先在该实例上允许 L2 模式。如果允许 L2 模式，则必须采取预防措施以避免桥接环路。

注意事项：

1. 在给定的 1/x 接口上，未标记的报文只能在一个实例上被允许。对于在同一接口上启用的所有其他实例，您必须选择“已标记”。

注意：

Citrix® 建议您为分配给 L2 模式实例的所有接口选择“已标记”。如果选择“已标记”，则无法在该接口上接收未标记的报文。

如果您已为分配给实例的接口选择了“已标记”，请登录到该实例并配置 802.1q VLAN 以在该接口上接收报文。

2. 对于允许 L2 模式的 NetScaler 实例共享的 1/x 和 10/x 接口，请确保满足以下条件：

- 所有接口上均已启用 VLAN 过滤。
- 每个接口都在不同的 802.1q VLAN 上。
- 只有一个实例可以在该接口上接收未标记的报文。如果该接口分配给其他实例，则必须为这些实例在该接口上选择“已标记”。

3. 如果您允许在已启用 L2 模式的实例的 1/x 接口上接收未标记的报文，则其他任何实例都不能在该接口上接收未标记的报文。无论其他实例上是否允许 L2 模式，此条件都适用。

4. 如果您允许在已禁用 L2 模式的实例的 1/x 接口上接收未标记的报文，则已启用 L2 模式的实例不能在该接口上接收未标记的报文。

5. 如果 0/x 接口分配给在 L2 模式下配置的 instance1，并且该接口也分配给 instance2，则为分配给 instance2 的所有其他接口选择“已标记”。

注意： 如果两个管理接口都分配给一个 L2 模式实例，则这些接口中只有一个可以分配给另一个已启用 L2 模式的 ADC 实例。也就是说，您不能将两个管理接口与多个已启用 L2 模式的 NetScaler 实例相关联。

允许实例上的 L2 模式

1. 在“配置 ADC 向导”或“修改 ADC 向导”中，在“网络设置”页面上，选择“允许 L2 模式”。**注意：** 您可以在预配实例时或实例运行时激活实例上的“允许 L2 模式”设置。
2. 按照向导中的说明进行操作。
3. 单击“完成”，然后单击“关闭”。

在接口上配置虚拟 MAC

NetScaler 实例使用虚拟 MAC (VMAC) 进行高可用性（主动-主动或主动-备用）配置。虚拟 MAC 地址 (VMAC) 是高可用性设置中主节点和辅助节点共享的浮动实体。

在高可用性设置中，主节点拥有所有浮动 IP 地址，例如 MIP、SNIP 和 VIP 地址。主节点使用自己的 MAC 地址响应这些 IP 地址的地址解析协议 (ARP) 请求。因此，外部设备（例如上游路由器）的 ARP 表会使用浮动 IP 地址和主节点的 MAC 地址进行更新。

发生故障转移时，辅助节点将接管成为新的主节点。然后，它使用无偿 ARP (GARP) 来通告从主节点获取的浮动 IP 地址。但是，新主节点通告的 MAC 地址是其自身接口的 MAC 地址。

某些设备（特别是少数路由器）不接受 NetScaler SDX 设备生成的 GARP 消息。此类设备会保留旧主节点通告的旧 IP 到 MAC 映射，结果可能导致站点停机。

您可以通过在 HA 对的两个节点上配置 VMAC 来克服此问题。两个节点都将拥有相同的 MAC 地址。因此，当发生故障转移时，辅助节点的 MAC 地址保持不变，外部设备上的 ARP 表无需更新。

配置 VMAC 是一个两步过程：

1. 在 SDX 管理服务上配置 VMAC。您为接口或 LA 通道添加 VRID。 [在 SDX 管理服务上配置 VMAC](#)。
2. 在 Citrix 实例上配置 VMAC。有关信息，请参阅 [在通道上配置 VMAC](#) 组支持文章。

在 SDX 管理服务上配置 VMAC

要配置 VMAC，请从管理服务向接口或 LA 通道添加 IPv4 或 IPv6 VRID。管理服务在内部生成 VMAC。在 NetScaler 实例上配置主动-主动模式时，请指定相同的 VRID。Mellanox 接口不支持此主动-主动配置。

请记住以下几点：

1. 从管理服务添加 VRID 并在 NetScaler 实例中指定相同的 VRID。如果直接在 NetScaler 实例中添加 VRID，则该实例无法接收以 VMAC 地址作为目标 MAC 地址的数据包。
2. 您不能在同一 SDX 设备中运行的不同实例上使用相同的 VRID。
3. 您可以在实例运行时添加或删除分配给实例的接口的 VRID。
4. 在主动-主动配置中，您可以为分配给实例的接口指定多个 VRID。Mellanox 接口不支持主动-主动部署。
5. 10G 接口上最多允许 86 个 VMAC，1G 接口上最多允许 16 个 VMAC。如果没有更多 VMAC 过滤器可用，请减少另一个实例上的 VRID 数量。

您可以在添加 NetScaler VPX 实例时添加 VRID，也可以修改现有 NetScaler 实例以添加 VRID。

将 IPv4 或 IPv6 VRID 添加到接口或 LA 通道

1. 在 SDX 上添加 VPX 实例时，在“网络设置”下，选择“数据接口”。有关如何在 SDX 上添加 VPX 实例的更多信息，请参阅[添加 NetScaler 实例](#)。
2. 从“接口”下拉菜单中，选择接口或 LA 通道。
3. 在 VMAC 设置下，设置以下一个或两个值：
 - VRID IPv4 — 标识 VMAC 的 IPv4 VRID。可能的值：1–255。
 - VRID IPv6 — 标识 VMAC 的 IPv6 VRID。可能的值：1–255。注意：使用逗号分隔多个 VRID。例如，12,24。
4. 单击“添加”将 VMAC 设置添加到接口。
5. 单击“完成”，然后单击“关闭”。

Add Data Interface

Interfaces*

LA/1 (LACP) ▼

The option "Allow Untagged Traffic" needs to be always enabled on a

☒ Allow Untagged Traffic

VLANs

100-110,142,151-155

MAC Address Mode*

Default ▼

▼ VMAC Settings (IPv4 and IPv6 VRIDs to configure Virtual MAC)

VRID IPv4

2,10,111

VRID IPv6

2,10,111

Add Close

如果实例已预置，要添加 IPv4 或 IPv6 VRID，请按照以下步骤操作。

1. 在 SDX 管理服务中，转到“配置 > NetScaler > 实例”。

2. 选择实例，然后单击“**编辑**”。
3. 在 **数据接口** 下，选择接口并单击编辑。
4. 在 VMAC 设置下，设置 VRID 值。单击 **添加**，然后单击 **完成**。

生成分区 MAC 地址以在 SDX 设备上的 NetScaler 实例中配置管理分区

NetScaler SDX 设备上的 NetScaler 实例可以划分为称为管理分区的逻辑实体。每个分区都可以配置并用作独立的 NetScaler 实例。有关管理分区的更多信息，请参阅[管理分区](#)。

要将管理分区与共享 VLAN 配置结合使用，您需要为每个分区提供一个虚拟 MAC 地址。这种虚拟 MAC 地址称为分区 MAC (PMAC) 地址，用于对在共享 VLAN 上接收的流量进行分类。此 PMAC 地址用于绑定到该分区的所有共享 VLAN。

在使用管理分区之前，请使用管理服务用户界面生成并配置 PMAC 地址。管理服务允许您通过以下方式生成分区 MAC 地址：

- 使用基本 MAC 地址
- 指定自定义 MAC 地址
- 随机生成 MAC 地址

注意 生成分区 MAC 地址后，必须先重新启动 NetScaler 实例，然后才能配置管理分区。

要使用基本 MAC 地址生成分区 MAC 地址，请执行以下操作：

1. 在**配置**选项卡上的左侧窗格中，展开 **NetScaler**，然后单击**实例**。
2. 在**实例**窗格中，选择要为其生成分区 MAC 地址的 NetScaler 实例。
3. 在**操作**下拉列表中，单击**分区 MAC**。
4. 在**分区 MAC**窗格中，单击**生成**。
5. 在**生成分区 MAC**对话框的**生成方法**部分中，选择**使用基本地址**。
6. 在**基本 MAC 地址**字段中，输入基本 MAC 地址。
7. 在“**递增量**”字段中，输入每个后续 MAC 地址的基本 MAC 地址必须递增的值。

例如，如果您已将基本 MAC 地址指定为 00:A1:C9:11:C8:11，并将递增值指定为 2，则下一个 MAC 地址将生成为 00:A1:C9:11:C8:13。

8. 在“**计数**”字段中，输入要生成的分区 MAC 地址数量。
9. 单击“**生成**”。

要通过指定自定义 MAC 地址来生成分区 MAC 地址：

1. 在“配置”选项卡上的左侧窗格中，展开“**NetScaler**”，然后单击“**实例**”。
2. 在“**实例**”窗格中，选择要为其生成分区 MAC 地址的 NetScaler 实例。
3. 在“**操作**”下拉列表中，单击“**分区 MAC**”。
4. 在“**分区 MAC**”窗格中，单击“**生成**”。
5. 在“**生成分区 MAC**”对话框的“**生成方法**”部分中，选择“**用户指定**”。
6. 在“**MAC 地址**”字段中，输入 MAC 地址。
7. 单击“+”图标，然后输入下一个 MAC 地址。重复此操作以指定更多自定义 MAC 地址。
8. 单击“**生成**”。

要随机生成分区 MAC 地址：

1. 在“配置”选项卡上的左侧窗格中，展开“**NetScaler**”，然后单击“**实例**”。
2. 在“**实例**”窗格中，选择要为其生成分区 MAC 地址的 NetScaler 实例。
3. 在“**操作**”下拉列表中，单击“**分区 MAC**”。
4. 在“**分区 MAC**”窗格中，单击“**生成**”。
5. 在“**生成分区 MAC**”对话框中，在“**生成方法**”部分中，选择“**随机**”。
6. 在“**计数**”字段中，输入要生成的分区 MAC 地址数量。
7. 单击“**生成**”。

在 SDX 设备中生成分区 MAC 地址后，使用生成的分区 MAC 地址在 NetScaler 实例上配置管理分区。

适用于 VPX 实例的变更管理

您可以从管理服务跟踪 NetScaler VPX 实例上配置的任何更改。详细信息窗格列出了设备名称、IP 地址以及上次更新的日期和时间。它还列出了保存的配置和正在运行的配置之间是否存在任何差异。选择一个设备以查看其正在运行的配置、保存的配置、配置更改历史记录以及升级前后配置之间的任何差异。您可以将 VPX 实例的配置下载到本地计算机。默认情况下，管理服务每 24 小时轮询所有实例，但您可以更改此间隔。您可以通过从现有配置文件复制命令来创建审计模板。稍后，您可以使用此模板查找实例配置中的任何更改，并在必要时采取纠正措施。

查看适用于 VPX 实例的变更管理

1. 在“配置”选项卡上，导航到“**NetScaler > 变更管理**”。
2. 在“**变更管理**”窗格中，选择一个 VPX 实例，然后从“**操作**”列表中选择以下选项之一：

- 正在运行的配置 — 在新窗口中显示所选 VPX 实例的正在运行的配置。
- 已保存的配置 — 在新窗口中显示所选 VPX 实例的已保存配置。
- 已保存与正在运行的差异 — 显示已保存的配置、正在运行的配置以及纠正命令（差异）。
- 修订历史差异 — 显示基本配置文件和第二个配置文件之间的差异。
- 升级前与升级后差异 — 显示升级前后配置差异以及纠正命令（差异）。
- 模板差异 — 显示已保存或正在运行的配置与模板之间的差异。您可以将此差异保存为批处理文件。要将模板中的配置应用到实例，请将此批处理文件应用到实例。
- 下载 — 下载所选 VPX 实例的配置并将其保存到本地设备。

轮询任何 NetScaler 实例配置的更新

1. 在“配置”选项卡上，导航到“**NetScaler > 变更管理**”。
2. 在“变更管理”窗格中，从“操作”列表中选择以下选项之一：
 - 立即轮询 — 管理服务立即轮询设备上安装的任何 VPX 实例的配置 (ns.conf) 更新。
 - 配置轮询间隔 — 管理服务轮询设备上安装的任何 VPX 实例的配置 (ns.conf) 更新的时间。默认轮询间隔为 24 小时。

配置 NetScaler 实例的审计模板

1. 打开现有配置文件并复制其命令列表。
2. 在“配置”选项卡上，导航到“**NetScaler > 更改管理 > 审计模板**”。
3. 在详细信息窗格中，单击“添加”。
4. 在“添加模板”对话框中，为模板添加名称和描述。
5. 在“命令”文本框中，粘贴您从配置文件中复制的命令列表。
6. 单击“创建”，然后单击“关闭”。

监控 NetScaler 实例

设备及其上预置的 VPX 实例的性能概览显示在管理服务用户界面的“监控”页面上。预置和配置 NetScaler 实例后，您可以执行各种任务来监控 NetScaler 实例。

查看 VPX 实例的属性

管理服务用户界面显示 SDX 设备上预置的所有 VPX 实例的列表和描述。使用“**NetScaler 实例**”窗格查看详细信息，例如实例名称和 IP 地址、CPU 和内存利用率、吞吐量以及分配给实例的总内存。

单击 VPX 实例的 IP 地址将在新选项卡或浏览器中打开该实例的配置实用程序 (GUI)。

查看 VPX 实例的属性

1. 在“配置”选项卡中，在左侧窗格中，展开“NetScaler 配置”，然后单击“实例”。注意：您也可以从“主页”选项卡查看 VPX 实例的属性。
2. 在“NetScaler 实例”窗格中，您可以查看 NetScaler 实例的以下详细信息：
 - **名称**：预置 NetScaler 实例时分配的主机名。
 - **VM 状态**：虚拟机的状态。
 - **NetScaler 状态**：NetScaler 实例的状态。
 - **IP 地址**：NetScaler 实例的 IP 地址。单击 IP 地址将在新选项卡或浏览器中打开此实例的 GUI。
 - **接收 (Mbps)**：NetScaler 实例上接收的数据包。
 - **发送 (Mbps)**：NetScaler 实例发送的数据包。
 - **HTTP 请求/秒**：NetScaler 实例每秒接收的 HTTP 请求总数。
 - **CPU 使用率 (%)**：NetScaler 上的 CPU 使用率百分比。
 - **内存使用率 (%)**：NetScaler 上的内存使用率百分比。
3. 单击 NetScaler 实例名称旁边的箭头以查看该实例的属性。您还可以单击“**全部展开**”以查看所有 NetScaler 实例的属性。您可以查看以下属性：
 - **子网掩码**：NetScaler 实例的子网掩码 IP 地址。
 - **网关**：默认网关的 IP 地址，即在其中安装实例的子网之外转发流量的路由器。
 - **每秒数据包数**：每秒通过的数据包总数。

- **网卡**：NetScaler 实例使用的网卡名称，以及分配给每个接口的虚拟功能。
- **版本**：实例上当前运行的 NetScaler 软件的内部版本号、内部版本日期和时间。
- **主机名**：NetScaler 实例的主机名。
- **总内存 (GB)**：分配给 NetScaler 实例的总内存。
- **吞吐量 (Mbps)**：NetScaler 实例的总吞吐量。
- **启动时间**：实例持续处于“启动”状态的日期和时间。
- **SSL 芯片**：分配给实例的 SSL 芯片总数。
- **对等 IP 地址**：如果此 NetScaler 实例处于 HA 设置中，则为该实例的对等 IP 地址。
- **状态**：在 NetScaler 实例上执行的操作的状态，例如实例清单是否完成的状态。
- **HA 主状态**：设备的当前状态。该状态指示实例是配置为独立设置、主设置，还是高可用性设置的一部分。在高可用性设置中，该状态还显示它是处于主模式还是辅助模式。
- **HA 同步状态**：HA 同步状态的模式，例如已启用或已禁用。
- **描述**：预置 NetScaler 实例时输入的描述。

注意：

当 ADC 实例因身份验证失败而停止服务时，如果满足以下条件，实例状态颜色将变为灰色：

- 直接使用实例 CLI 更改了 ADC 实例密码。
- 密码与管理服务中存储的实例管理员配置文件密码不匹配。
- 首次重新启动实例后，之前的会话丢失。

通常，当实例停止服务时，实例状态颜色为黄色。

要恢复实例，请执行以下操作之一：

- 从实例 CLI 中，修改实例密码以匹配实例管理员配置文件中的密码。然后从管理服务中重新发现实例。
- 创建与 ADC 实例当前密码相同的管理员配置文件。然后，使用新的管理员配置文件更新 ADC 实例。

查看 NetScaler 实例的运行配置和已保存配置

通过使用管理服务，您可以查看 NetScaler 实例的当前运行配置。您还可以查看 NetScaler 实例的已保存配置以及配置保存的时间。

查看 NetScaler 实例的运行配置和已保存配置

1. 在“配置”选项卡上，在左侧窗格中，展开“NetScaler 配置”，然后单击“实例”。
2. 在“NetScaler 实例”窗格中，单击要查看其运行配置或已保存配置的 NetScaler 实例。
3. 要查看运行配置，请单击“运行配置”；要查看已保存配置，请单击“已保存配置”。
4. 在“NetScaler 运行配置”窗口或“NetScaler 已保存配置”窗口中，您可以查看 NetScaler 实例的运行配置或已保存配置。

Ping NetScaler 实例

您可以从管理服务 Ping NetScaler 实例，以检查设备是否可访问。

Ping NetScaler 实例

1. 在“配置”选项卡上，在左侧窗格中，展开“NetScaler 配置”，然后单击“实例”。
2. 在“NetScaler 实例”窗格中，单击要 Ping 的 NetScaler 实例，然后单击“Ping”。在“Ping”消息框中，您可以查看 Ping 是否成功。

跟踪 NetScaler 实例的路由

您可以从管理服务跟踪数据包到 NetScaler 实例的路由，方法是确定到达该实例所用的跳数。

跟踪 NetScaler 实例的路由

1. 在“配置”选项卡上，在左侧窗格中，展开“NetScaler 配置”，然后单击“实例”。
2. 在“NetScaler 实例”窗格中，单击要跟踪的 NetScaler 实例，然后单击“TraceRoute”。在“Traceroute”消息框中，您可以查看 NetScaler 的路由。

重新发现 NetScaler 实例

当您需要查看 NetScaler 实例的最新状态和配置时，可以重新发现 NetScaler 实例。

在重新发现期间，管理服务会获取配置。默认情况下，管理服务每 30 分钟调度一次设备以进行重新发现。

重新发现 NetScaler 实例

1. 在“配置”选项卡上，在左侧窗格中，展开“**NetScaler 配置**”，然后单击“**实例**”。
2. 在“**NetScaler 实例**”窗格中，单击要重新发现的 NetScaler 实例，然后单击“**重新发现**”。
3. 在“确认”消息框中，单击“**是**”。

使用日志监控操作和事件

使用审计日志和任务日志监控在管理服务 and NetScaler SDX 实例上执行的操作。您还可以使用事件日志跟踪在管理服务和 Citrix Hypervisor 上执行的所有任务事件。

查看审计日志

通过管理服务执行的所有操作都记录在设备数据库中。使用审计日志查看管理服务用户执行的操作、日期和时间以及每个操作的成功或失败状态。您还可以通过单击相应的列标题，按用户、操作、审计时间、状态等对详细信息进行排序。

审计日志窗格支持分页。选择每页显示的记录数。默认情况下，每页显示 25 条记录。

要查看审计日志，请执行以下步骤：

1. 在导航窗格中，展开“系统”，然后单击“审计”。
2. 在“审计日志”窗格中，您可以查看以下详细信息。
 - **用户名**：执行操作的管理服务用户。
 - **IP 地址**：执行操作的系统的 IP 地址。
 - **端口**：执行操作时系统运行的端口。
 - **资源类型**：用于执行操作的资源类型，例如 xen_vpx_image 和 login。
 - **资源名称**：用于执行操作的资源的名称，例如 vpx_image_name 和用于登录的用户名。
 - **审计时间**：生成审计日志的时间。
 - **操作**：执行的任务，例如添加、删除和注销。
 - **状态**：审计的状态，例如“成功”或“失败”。
 - **消息**：如果操作失败，则描述失败原因的消息；如果操作成功，则描述任务状态的消息，例如“完成”。
3. 要按特定字段对日志进行排序，请单击列标题。

查看任务日志

使用任务日志查看和跟踪由管理服务在 NetScaler 实例上运行的任务，例如升级实例和安装 SSL 证书。任务日志可让您查看任务是正在进行、已失败还是已成功。

任务日志窗格支持分页。选择每页要显示的记录数。默认情况下，每页显示 25 条记录。

要查看任务日志，请执行以下步骤：

1. 在导航窗格中，展开“**诊断**”，然后单击“**任务日志**”。
2. 在“**任务日志**”窗格中，您可以查看以下详细信息。
 - **名称**：正在运行或已运行的任务的名称。
 - **状态**：任务的状态，例如“正在进行”、“已完成”或“失败”。
 - **执行者**：执行此操作的管理服务用户。
 - **开始时间**：任务开始的时间。
 - **结束时间**：任务结束的时间。

查看任务设备日志

使用任务设备日志查看和跟踪在每个 SDX 实例上执行的任务。任务设备日志可让您查看任务是正在进行、已失败还是已成功。它还显示执行任务的实例的 IP 地址。

要查看任务设备日志，请执行以下步骤：

1. 在导航窗格中，展开“**诊断**”，然后单击“**任务日志**”。
2. 在“**任务日志**”窗格中，双击任务以查看任务设备详细信息。
3. 在“**任务设备日志**”窗格中，要按特定字段对日志进行排序，请单击列标题。

查看任务命令日志

使用任务命令日志查看在 NetScaler 实例上运行的任务中每个命令的状态。任务命令日志可让您查看命令是已成功运行还是已失败。它还显示运行的命令以及命令失败的原因。

要查看任务命令日志，请执行以下步骤：

1. 在导航窗格中，展开“**诊断**”，然后单击“**任务日志**”。
2. 在“**任务日志**”窗格中，双击任务以查看任务设备详细信息。
3. 在“**任务设备日志**”窗格中，双击任务以查看任务命令详细信息。
4. 在“**任务命令日志**”窗格中，要按特定字段对日志进行排序，请单击列标题。

查看事件

使用 Management Service 用户界面中的“**事件**”窗格来监视 Management Service 为在 Management Service 上执行的任务生成的事件。

要查看事件，请执行以下步骤：

1. 导航到 **System > Events**。
2. 在 **事件** 窗格中，您可以查看以下详细信息。
 - **严重性**：事件的严重性，可能包括关键、主要、次要、清除和信息。
 - **源**：生成事件的 IP 地址。
 - **日期**：生成事件的日期。
 - **类别**：事件的类别，例如 PolicyFailed 和 DeviceConfigChange。
 - **消息**：描述事件的消息。
3. 要按特定字段对事件进行排序，请单击列标题。

NetScaler SDX 设备的用例

对于网络组件（例如防火墙和应用交付控制器），对多租户的支持历来涉及将单个设备划分为多个逻辑分区的功能。这种方法允许为每个租户实施不同的策略集，而无需大量独立的设备。然而，传统上，它在实现隔离程度方面受到严重限制。

从设计上讲，SDX 设备不受相同限制。在 SDX 架构中，每个实例都作为独立的虚拟机 (VM) 运行，拥有自己专用的 NetScaler 内核、CPU 资源、内存资源、地址空间和带宽分配。SDX 设备上的网络 I/O 不仅保持了聚合系统性能，而且还实现了每个租户的数据平面和管理平面流量的完全隔离。管理平面包括 0/x 接口。数据平面包括 1/x 和 10/x 接口。数据平面也可以用作管理平面。

SDX 设备的主要用例与整合相关，旨在减少所需的网络数量，同时保持管理隔离。以下是基本的整合方案：

- 当管理服务 and NetScaler 实例位于同一网络中时的整合。
- 当管理服务 and NetScaler 实例位于不同网络中但所有实例都位于同一网络中时的整合。
- 跨安全整合。
- 为每个实例配备专用接口的整合。
- 多个实例共享一个物理端口的整合。

当管理服务 and NetScaler 实例位于同一网络时进行整合

SDX 设备上的一种简单整合情况是将管理服务 and NetScaler 实例配置为同一网络的一部分。此用例适用于以下情况：

- 设备管理员也是实例管理员。
- 您的组织的合规性要求未指定管理服务 and 不同实例的 NSIP 地址需要单独的管理网络。

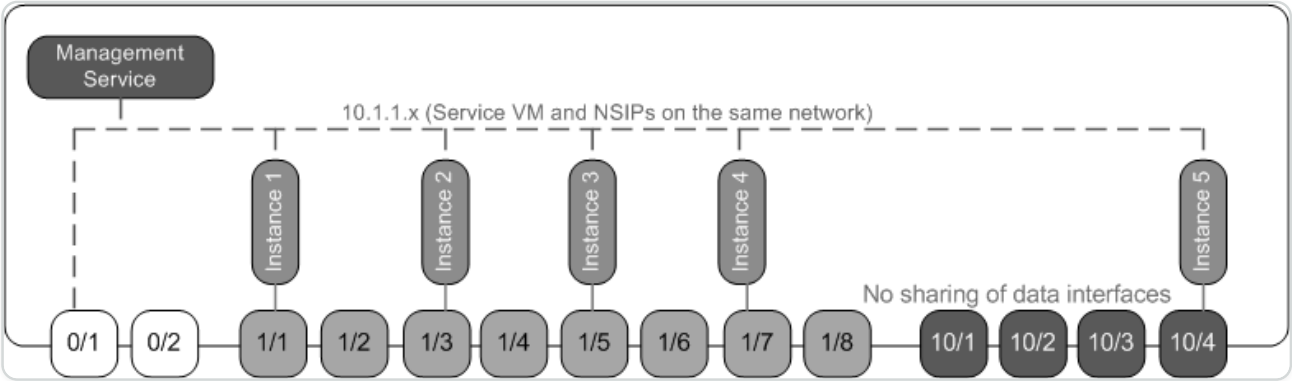
实例可以在同一网络中进行预配（用于管理流量）。VIP 地址可以在不同的网络中配置（用于数据流量），从而位于不同的安全区域。

在以下示例中，管理服务 and NetScaler 实例是 10.1.1.x 网络的一部分。接口 0/1 和 0/2 是管理接口，1/1 到 1/8 是 1G 数据接口，10/1 到 10/4 是 10G 数据接口。每个实例都有自己专用的物理接口。因此，实例的数量受限于设备上可用的物理接口数量。默认情况下，SDX 设备的每个接口都启用了 VLAN 过滤。1G 接口上的 VLAN 数量限制为 32 个，10G 接口上的 VLAN 数量限制为 63 个。可以为每个接口启用和禁用 VLAN 过滤。禁用 VLAN 过滤可在每个实例的每个接口上配置多达 4096 个 VLAN。在此示例中，不

需要VLAN过滤，因为每个实例都有自己专用的接口。有关VLAN过滤的更多信息，请参阅[管理和监控SDX设备](#)中的“VLAN 过滤”部分。

下图说明了上述用例。

图1. SDX设备网络拓扑，其中管理服务和服务实例的NSIP位于同一网络中



下表列出了在上述示例中用于预配NetScaler实例1的参数名称和值。

参数名称	实例1的值
名称	vpv8
IP地址	10.1.1.2
子网掩码	255.255.255.0
网关	10.1.1.1
XVA 文件	NS-VPX-XEN-10.0-51.308.a_nc.xva
功能许可证	白金版
管理员配置文件	ns_nsroot_profile
用户名	vpv8
密码	Sdx1
确认密码	Sdx1
Shell/Sftp/Scp 访问	是
总内存 (MB)	2048
#SSL 芯片	1

参数名称	实例1的值
吞吐量 (Mbps)	1000
每秒数据包	1000000
CPU	共享
接口	0/1 和 1/1

按此示例所示置备 NetScaler 实例 1

1. 在“配置”选项卡上的导航窗格中，展开“NetScaler 配置”，然后单击“实例”。
2. 在“NetScaler 实例”窗格中，单击“添加”。
3. 在“置备 Citrix® 向导”中，按照向导中的说明指定上表中所示的参数值。
4. 单击“创建”，然后单击“关闭”。您置备的 NetScaler 实例将显示在“NetScaler 实例”窗格中。

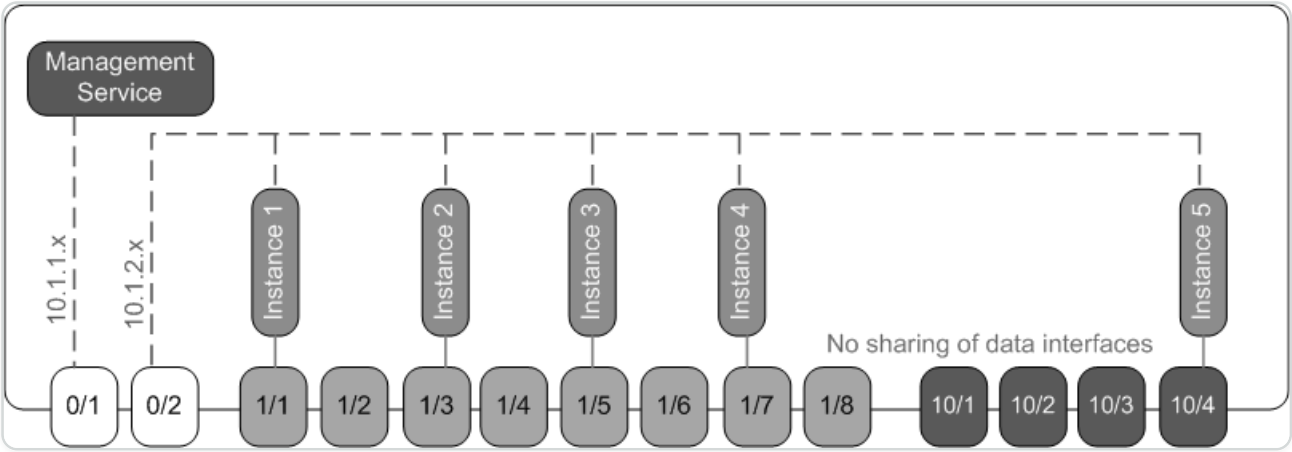
当管理服务与NetScaler实例位于不同网络时进行整合

在某些情况下，设备管理员可能允许其他管理员对单个实例执行管理任务。这可以通过仅向单个实例管理员授予该实例的登录权限来安全地完成。但是，出于安全原因，设备管理员可能不希望允许实例与管理服务位于同一网络中。这在服务提供商环境中很常见，并且随着企业采用虚拟化和云架构，这种情况在企业中也变得越来越普遍。

在以下示例中，管理服务位于 10.1.1.x 网络中，NetScaler 实例位于 10.1.2.x 网络中。接口 0/1 和 0/2 是管理接口，1/1 到 1/8 是 1G 数据接口，10/1 到 10/4 是 10G 数据接口。每个实例都有自己专用的管理员和自己专用的物理接口。因此，实例的数量受限于设备上可用的物理接口数量。不需要 VLAN 过滤，因为每个实例都有自己专用的接口。或者，禁用 VLAN 过滤以配置每个接口每个实例最多 4096 个 VLAN。在此示例中，您无需配置 NSVLAN，因为实例不共享物理接口，并且没有标记的 VLAN。有关 NSVLAN 的更多信息，请参阅 [添加 NetScaler 实例](#)

下图说明了上述用例。

图 1. 具有管理服务和不同网络中实例的 NSIP 的 SDX 设备网络拓扑



作为设备管理员，您可以将管理服务 和 SDX 设备上的 NSIP 地址之间的流量保留在设备上。或者，如果您希望流量通过外部防火墙或其他安全中介，然后返回到设备，则可以强制流量离开设备。

下表列出了在此示例中用于预配 NetScaler 实例 1 的参数名称和值。

参数名称	实例 1 的值
名称	vpx1
IP 地址	10.1.2.2
子网掩码	255.255.255.0
网关	10.1.2.1
XVA 文件	NS-VPX-XEN-10.0-51.308.a_nc.xva
功能许可证	白金
管理员配置文件	ns_nsroot_profile
用户名	vpx1
密码	Sdx1
确认密码	Sdx1
Shell/Sftp/Scp 访问	是
总内存 (MB)	2048
#SSL 芯片	1
吞吐量 (Mbps)	1000

参数名称	实例 1 的值
每秒数据包	1000000
CPU	共享
接口	0/2 和 1/1

预配 NetScaler 实例 1，如本例所示

1. 在“配置”选项卡上，在导航窗格中，展开“**NetScaler 配置**”，然后单击“实例”。
2. 在 NetScaler 实例窗格中，单击“添加”。
3. 在“**预配 NetScaler 向导**”中，按照向导中的说明将参数设置为上表中显示的值。
4. 单击“创建”，然后单击“关闭”。您预配的 NetScaler 实例将显示在 NetScaler 实例窗格中。

跨安全区域整合

SDX 设备通常用于跨安全区域进行整合。DMZ 为组织内部网络增加了一层额外的安全性，因为攻击者只能访问 DMZ。它无法访问组织的内部网络。在高合规性环境中，单个 NetScaler 实例在 DMZ 和内部网络中同时拥有 VIP 地址是不可接受的。借助 SDX，您可以预配在 DMZ 中托管 VIP 地址的实例，以及在内部网络中托管 VIP 地址的其他实例。

有时，您可能需要为每个安全区域设置独立的管理网络。DMZ 中实例的 NSIP 地址可以在一个网络中。内部网络中具有 VIP 的实例的 NSIP 地址可以在不同的管理网络中。此外，管理服务与实例之间的通信通常可能需要通过外部设备（例如路由器）进行路由。您可以配置防火墙策略来控制发送到防火墙的流量并记录流量。

SDX 设备具有两个管理接口（0/1 和 0/2），并且根据型号，最多可有八个 1G 数据端口和八个 10G 数据端口。您还可以将数据端口用作管理端口（例如，当您需要配置标记的 VLAN 时，因为管理接口上不允许标记）。如果这样做，来自管理服务的流量必须离开设备，然后返回设备。您可以路由此流量，或者选择性地在分配给实例的接口上指定一个 NSVLAN。如果管理接口在实例和管理服务之间是通用的，则两者之间的流量不必路由。但是，如果您的设置明确要求，则可以路由流量。

注意 Citrix Hypervisor 6.0 版支持标记。

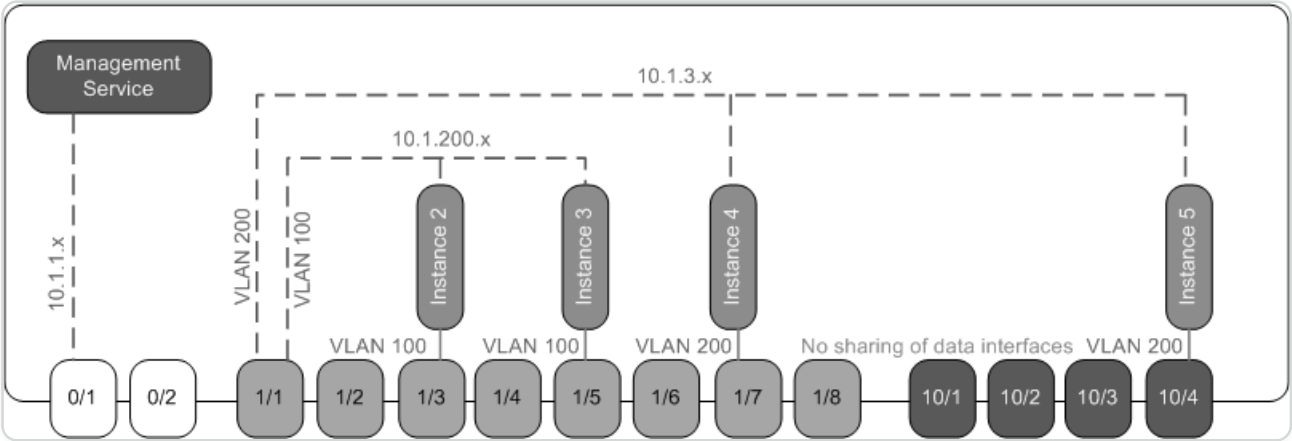
为每个实例使用专用接口进行整合

在以下示例中，实例是多个网络的一部分。接口 0/1 分配给管理服务，该服务是内部 10.1.1.x 网络的一部分。NetScaler 实例 2 和 3 是 10.1.200.x 网络（VLAN 100）的一部分。NetScaler 实例 4 和 5 是 10.1.3.x 网络（VLAN 200）的一部分。

(可选) 您可以在所有实例上配置 NSVLAN。

下图说明了上述用例。

图 1. 具有多个网络中 NetScaler 实例的 SDX 设备网络拓扑



SDX 设备连接到交换机。请确保在设备端口 1/1 连接到的交换机端口上配置了 VLAN ID 100 和 200。

下表列出了在此示例中用于预配 NetScaler 实例 5 和 3 的参数名称和值。

参数名称	实例 5 的值	实例 3 的值
名称	vpx5	vpx3
IP 地址	10.1.3.2	10.1.200.2
子网掩码	255.255.255.0	255.255.255.240
网关	10.1.3.1	10.1.200.1
XVA 文件	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
功能许可证	白金版	白金版
管理员配置文件	ns_nsroot_profile	ns_nsroot_profile
用户名	vpx5	vpx3
密码	Sdx1	根
确认密码	Sdx1	根

参数名称	实例 5 的值	实例 3 的值
Shell/Sftp/Scp 访问	是	是
总内存 (MB)	2048	2048
#SSL 芯片	1	1
吞吐量 (Mbps)	1000	1000
每秒数据包数	1000000	1000000
CPU	共享	共享
接口	1/1 和 10/4	1/1 和 1/5
NSVLAN	200	100
添加 (接口)	1/1	1/1
已标记接口	选择 已标记	选择 已标记

配置 NetScaler 实例 5 和 3，如本示例所示

1. 在“配置”选项卡上的导航窗格中，展开“**NetScaler 配置**”，然后单击“实例”。
2. 在 NetScaler 实例窗格中，单击“添加”。
3. 在“**预配 NetScaler 向导**”中，按照向导中的说明将参数设置为上表中显示的值。
4. 单击 **创建**，然后单击 **关闭**。您配置的 NetScaler 实例将显示在 NetScaler 实例窗格中。

多个实例共享物理端口的整合

您可以根据需要启用和禁用接口上的 VLAN 过滤。例如，要在实例上配置 100 多个 VLAN，请为该实例分配一个专用物理接口，并禁用该接口上的 VLAN 过滤。在共享物理接口的实例上启用 VLAN 过滤，以便一个实例无法看到另一个实例的流量。

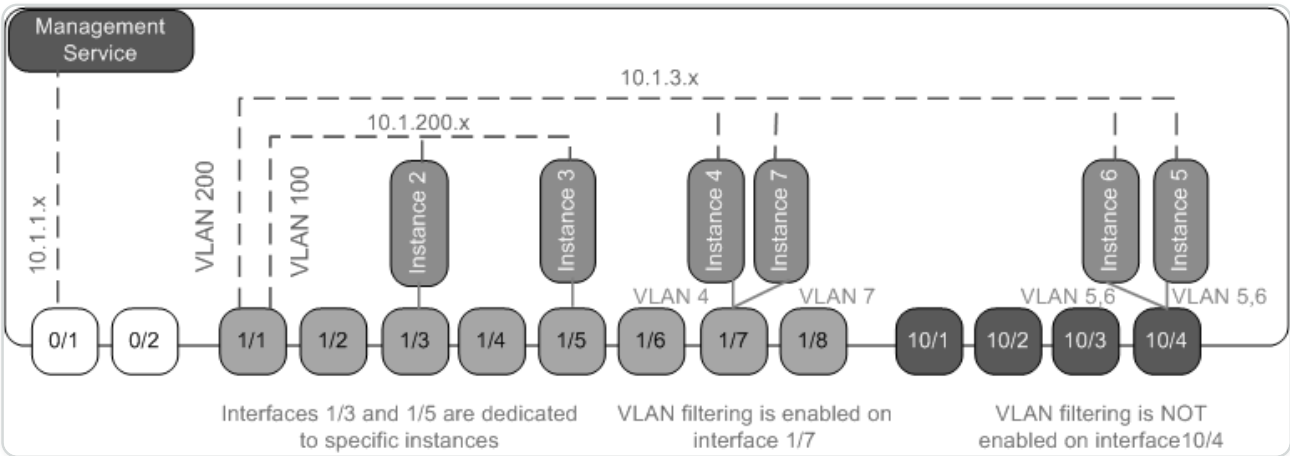
注意： VLAN 过滤不是设备上的全局设置。您可以在接口上启用或禁用 VLAN 过滤，该设置适用于与该接口关联的所有实例。如果禁用 VLAN 过滤，则最多可以配置 4096 个 VLAN。如果启用 VLAN 过滤，则可以在 10G 接口上配置最多 63 个标记 VLAN，在 1G 接口上配置最多 32 个标记 VLAN。

在以下示例中，实例属于多个网络。

- 接口 1/1 被分配为所有实例的管理接口。接口 0/1 被分配给管理服务，该服务是内部 10.1.1.x 网络的一部分。
- NetScaler 实例 2 和 3 位于 10.1.200.x 网络中，实例 4、5、6 和 7 位于 10.1.3.x 网络中。实例 2 和 3 各有一个专用物理接口。实例 4 和 7 共享物理接口 1/7，实例 5 和 6 共享物理接口 10/4。
- 接口 1/7 上启用了 VLAN 过滤。实例 4 的流量标记为 VLAN 4，实例 7 的流量标记为 VLAN 7。因此，实例 4 的流量对实例 7 不可见。反之，实例 7 的流量对实例 4 不可见。接口 1/7 上最多可以配置 32 个 VLAN。
- 接口 10/4 上禁用了 VLAN 过滤，因此您可以在该接口上配置最多 4096 个 VLAN。在实例 5 上配置 VLAN 500–599，在实例 6 上配置 VLAN 600–699。实例 5 可以看到来自 VLAN 600–699 的广播和多播流量，但数据包在软件级别被丢弃。同样，实例 6 可以看到来自 VLAN 500–599 的广播和多播流量，但数据包在软件级别被丢弃。

下图说明了上述用例。

图 1. 具有管理服务和分布在多个网络中的 NetScaler 实例的 SDX 设备网络拓扑



下表列出了在此示例中用于预配 NetScaler 实例 7 和 4 的参数名称和值。

参数名称	实例 7 的值	实例 4 的值
名称	vpx7	vpx4
IP 地址	10.1.3.7	10.1.3.4
子网掩码	255.255.255.0	255.255.255.240
网关	10.1.3.1	10.1.3.1
XVA 文件	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva

参数名称	实例 7 的值	实例 4 的值
功能许可证	白金	白金
管理员配置文件	ns_nsroot_profile	ns_nsroot_profile
用户名	vpx4	vpx4
密码	Sdx1	Sdx1
确认密码	Sdx1	Sdx1
Shell/Sftp/Scp 访问	是	是
总内存 (MB)	2048	2048
SSL 芯片数量	1	1
吞吐量 (Mbps)	1000	1000
每秒数据包数	1000000	1000000
CPU	共享	共享
接口	1/1 和 1/7	1/1 和 1/7
NSVLAN	200	200

在此示例中预配 NetScaler 实例 7 和 4

1. 在“配置”选项卡上，在导航窗格中，展开“NetScaler 配置”，然后单击“实例”。
2. 在“NetScaler 实例”窗格中，单击“添加”。
3. 在“预配 NetScaler 向导”中，按照向导中的说明将参数设置为上表中显示的值。
4. 单击“创建”，然后单击“关闭”。您预配的 NetScaler 实例将显示在“NetScaler 实例”窗格中。

NITRO API

NetScaler SDX NITRO 协议允许您以编程方式配置和监控 SDX 设备。

NITRO 通过表述性状态传输 (REST) 接口公开其功能。因此，NITRO 应用程序可以用任何编程语言开发。此外，对于必须用 Java、.NET 或 Python 开发的应用程序，NITRO 协议以相关库的形式公开，这些库作为单独的软件开发工具包进行打包。

注意：在使用 NITRO 之前，您必须对 SDX 设备有基本的了解。

要使用 NITRO 协议，客户端应用程序需要满足以下条件：

- 访问 SDX 设备。
- 要使用 REST 接口，您必须有一个系统来向 SDX 设备生成 HTTP 或 HTTPS 请求（JSON 格式的有效负载）。您可以使用任何编程语言或工具。
- 对于 Java 客户端，您必须有一个系统，其中 Java Development Kit (JDK) 1.5 或更高版本可用。可以从 <http://www.oracle.com/technetwork/java/javase/downloads/index.html> 下载 JDK。
- 对于 .NET 客户端，您必须有一个系统，其中 .NET framework 3.5 或更高版本可用。可以从 <http://www.microsoft.com/downloads/en/default.aspx> 下载 .NET framework。
- 对于 Python 客户端，您必须有一个系统，其中已安装 Python 2.7 或更高版本以及 Requests 库（位于 `<NITRO\_SDK\_HOME>/lib` 中）。

获取 NITRO 包

NITRO 包以 tar 文件的形式在 SDX 设备配置实用程序的下载页面上提供。您必须将该文件下载并解压到本地系统上的一个文件夹中。此文件夹在本文档中称为 `<NITRO\_SDK\_HOME>`。

该文件夹包含 NITRO 库，位于 `lib` 子文件夹中。必须将这些库添加到客户端应用程序的类路径中才能访问 NITRO 功能。该 `<NITRO\_SDK\_HOME>` 文件夹还提供了示例和文档，可帮助您理解 NITRO SDK。

注意：

```
<div id="sdx-nitro-obtain-con__li_5716E0FF34204411A267E100E8A92067">
```

The REST package contains only documentation for using the REST interfaces.

</div>

<div id="sdx-nitro-obtain-con__li_A72149DD47854CE9B82A5DA88B705828">

For the Python SDK, the library must be installed on the client path. For installation instructions, read the \<NITRO_SDK_HOME\>/README.txt file.

</div>

.NET SDK

SDX NITRO API 根据其范围和用途分为系统 API 和配置 API。您还可以对 NITRO 操作进行故障排除。

系统 API

使用 NITRO 的第一步是与 SDX 设备建立会话，然后使用管理员凭据对会话进行身份验证。

通过指定设备的 IP 地址以及连接到设备的协议（HTTP 或 HTTPS）来创建 `nitro_service` 类的对象。然后，您可以使用此对象，并通过指定管理员的用户名和密码登录到设备。

注意：您必须在该设备上拥有一个用户帐户。您可以执行的配置操作受分配给您帐户的管理角色的限制。

以下示例代码使用 HTTPS 协议连接到 IP 地址为 10.102.31.16 的 SDX 设备：

```
//Specify the IP address of the appliance and service type

nitro_service nitroservice = new nitro_service ("10.102.31.16", "https");
```

```
//Specify the login credentials

nitroservice.login("nsroot", "verysecret");
```

注意： 请使用 nitro_service 对象在设备上的所有后续 NITRO 操作中。

要断开与设备的连接，请按如下方式调用 logout() 方法：

```
nitroservice.logout();
```

配置 API

NITRO 协议可用于配置 SDX 设备的资源。

用于配置资源的 API 被分组到包或命名空间中，其格式为 com.citrix.sdx.nitro.resource.config.<resource_type>。这些包或命名空间中的每一个都包含一个名为 <resource_type> 的类，该类提供用于配置资源的 API。

例如，NetScaler 资源具有 com.citrix.sdx.nitro.resource.config.ns 包或命名空间。

资源类提供用于执行其他操作的 API。这些操作可以是创建资源、检索资源和资源属性、更新资源、删除资源以及对资源执行批量操作。

创建资源

要在 SDX 设备上创建资源（例如，NetScaler 实例）：

1. 通过使用相应的属性名称设置资源的所需属性值。结果是一个资源对象，其中包含资源所需的详细信息。注意：这些值在客户端本地设置。在对象上传之前，这些值不会反映在设备上。
2. 使用静态 add() 方法将资源对象上传到设备。

以下示例代码在 SDX 设备上创建了一个名为“ns_instance”的 NetScaler 实例：

```
ns newns = new ns();

//Set the properties of the NetScaler locally

newns.name = "ns_instance";
```

```
newns.ip_address = "10.70.136.5";

newns.netmask = "255.255.255.0";

newns.gateway = "10.70.136.1";

newns.image_name = "nsvpx-9.3.45_nc.xva";

newns.profile_name = "ns_nsroot_profile";

newns.vm_memory_total = 2048;

newns.throughput = 1000;

newns.pps = 1000000;

newns.license = "Standard";

newns.username = "admin";

newns.password = "admin";


int number_of_interfaces = 2;

network_interface[] interface_array = new
network_interface[number_of_interfaces];


//Adding 10/1

interface_array[0] = new network_interface();

interface_array[0].port_name = "10/1";


//Adding 10/2

interface_array[1] = new network_interface();
```

```
interface_array[1].port_name = "10/2";

newns.network_interfaces = interface_array;

//Upload the NetScaler instance

ns result = ns.add(nitroservice, newns);
```

检索资源详细信息

要检索 SDX 设备上资源的属性，请执行以下操作：

1. 使用 get() 方法从设备检索配置。结果是一个资源对象。
2. 使用相应的属性名称从对象中提取所需的属性。

以下示例代码检索所有 NetScaler® 资源的详细信息：

```
//Retrieve the resource object from the SDX appliance

ns[] returned_ns = ns.get(nitroservice);

//Extract the properties of the resource from the object

Console.WriteLine(returned_ns[i].ip_address);

Console.WriteLine(returned_ns[i].netmask);
```

检索资源统计信息

SDX 设备会收集其功能使用情况的统计信息。您可以使用 NITRO 检索这些统计信息。

以下示例代码检索 ID 为 123456a 的 NetScaler 实例的统计信息：

```
ns obj = new ns();

obj.id = "123456a";

ns stats = ns.get(nitroservice, obj);

Console.WriteLine("CPU Usage:" + stats.ns_cpu_usage);

Console.WriteLine("Memory Usage:" + stats.ns_memory_usage);

Console.WriteLine("Request rate/sec:" +stats.http_req);
```

更新资源

要更新设备上现有资源的属性，请执行以下操作：

1. 将 id 属性设置为要更新的资源的 ID。
2. 使用相应的属性名称设置资源的必需属性值。结果是一个资源对象。注意：这些值在客户端本地设置。在对象上传之前，这些值不会反映在设备上。
3. 使用 update() 方法将资源对象上传到设备。

以下示例代码将 ID 为 123456a 的 NetScaler 实例的名称更新为“ns_instance_new”：

```
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated

update_obj.id = "123456a";

//Get existing NetScaler details

update_obj = ns.get(nitroservice, update_obj);

//Update the name of the NetScaler to "ns_instance_new" locally

update_obj.name = "ns_instance_new";
```

```
//Upload the updated NetScaler details

ns result = ns.update(nitroservice, update_obj);
```

删除资源

要删除现有资源，请通过传递要删除资源的 ID 作为参数，在资源类上调用静态方法 `delete()`。

以下示例代码删除 ID 为 1 的 NetScaler 实例：

```
ns obj = new ns();

obj.id = "123456a";

ns.delete(nitroservice, obj);
```

批量操作

您可以同时查询或更改多个资源，从而最大限度地减少网络流量。例如，您可以在同一操作中添加多个 NetScaler SDX 设备。

每个资源类都有用于添加、更新和删除资源的接受资源数组的方法。要执行批量操作，请在本地指定每个操作的详细信息，然后一次性将详细信息发送到服务器。

为了处理批量操作中某些操作的失败，NITRO 允许您配置以下行为之一：

- **退出。** 当遇到第一个错误时，执行停止。错误之前运行的命令将被提交。
- **继续。** 即使某些命令失败，列表中的所有命令也会运行。

注意： 在与设备建立连接时，通过设置 `onerror` 参数，在 `nitro_service()` 方法中配置所需行为。

以下示例代码在一个操作中添加两个 ADC 设备：

```
ns[] newns = new ns[2];

//Specify details of first NetScaler

newns[0] = new ns();
```

```
newns[0].name = "ns_instance1";

newns[0].ip_address = "10.70.136.5";

newns[0].netmask = "255.255.255.0";

newns[0].gateway = "10.70.136.1";

...

...

//Specify details of second NetScaler

newns[1] = new ns();

newns[1].name = "ns_instance2";

newns[1].ip_address = "10.70.136.8";

newns[1].netmask = "255.255.255.0";

newns[1].gateway = "10.70.136.1";

...

...

//upload the details of the ADC appliances to the NITRO server

ns[] result = ns.add(nitroservice, newns);
```

异常处理

错误代码字段指示操作的状态。

- 错误代码为 0 表示操作成功。
- 非零错误代码表示处理 NITRO 请求时出错。

错误消息字段提供了简要说明和故障性质。

`com.citrix.sdx.nitro.exception.nitro_exception` 类捕获 NITRO API 执行中的所有异常。要获取有关异常的信息，可以使用 `getErrorCode()` 方法。

有关错误代码的更详细说明，请参阅 `<NITRO_SDK_HOME>/doc` 文件夹中提供的 API 参考。

REST Web 服务

REST（表征性状态传输）是一种基于客户端和服务端之间简单 HTTP 请求和响应的架构风格。

REST 用于查询或更改服务器端对象的状态。在 REST 中，服务器端被建模为一组实体，其中每个实体都由唯一的 URL 标识。

每个资源还具有一个状态，可以对其执行以下操作：

- **创建。** 客户端可以在“容器”资源上创建新的服务器端资源。您可以将容器资源视为文件夹，将子资源视为文件或子文件夹。调用客户端提供要创建资源的状态。状态可以通过使用 XML 或 JSON 格式在请求中指定。客户端还可以指定标识新对象的唯一 URL。或者，服务器可以选择并返回标识所创建对象的唯一 URL。用于创建请求的 HTTP 方法是 POST。
- **读取。** 客户端可以通过使用 HTTP GET 方法指定资源的 URL 来检索其状态。响应消息包含以 JSON 格式表示的资源状态。
- **更新。** 您可以使用 PUT HTTP 方法，通过指定标识该对象的 URL 及其在 JSON 或 XML 中的新状态来更新现有资源的状态。
- **删除。** 您可以使用 DELETE HTTP 方法和标识要删除资源的 URL 来销毁服务器端存在的资源。

除了这四个 CRUD 操作（创建、读取、更新和删除）之外，资源还可以支持其他操作或动作。这些操作使用 HTTP POST 方法，请求正文以 JSON 格式指定要执行的操作及其参数。

SDX NITRO API 根据其范围和目的分为系统 API 和配置 API。

系统 API

使用 NITRO 的第一步是与 SDX 设备建立会话，然后使用管理员凭据对会话进行身份验证。

在登录对象中指定用户名和密码。创建的会话 ID 必须在会话中所有后续操作的请求头中指定。

注意：您必须在该设备上拥有一个用户帐户。您可以执行的配置受分配给您帐户的管理角色的限制。

要使用 HTTPS 协议连接到 IP 地址为 10.102.31.16 的 SDX 设备：

- **URL** `https://10.102.31.16/nitro/v2/config/login/`

- HTTP 方法 POST
- 请求
 - 标头

```
Content-Type:application/vnd.com.citrix.sdx.login+json
```

注意：也可以使用早期版本 NITRO 支持的内容类型，例如“application/x-www-form-urlencoded”。请确保负载与早期版本中使用的负载相同。本文档中提供的负载仅适用于内容类型为“application/vnd.com.citrix.sdx.login+json”的情况。

- 负载

```
{  
  
  "login":  
  
    {  
  
      "username":"nsroot",  
  
      "password":"verysecret"  
  
    }  
  
}
```

- 响应负载

- 标头

```
HTTP/1.0 201 Created  
  
Set-Cookie:  
  
NITRO_AUTH_TOKEN=##87305E9C51B06C848F0942; path=/nitro/v2
```

注意：在设备上的所有后续 NITRO 操作中，请使用会话 ID。

注意：默认情况下，与设备的连接在 30 分钟不活动后过期。您可以通过在登录对象中指定新的超时时间（以秒为单位）来修改超时时间。例如，要将超时时间修改为 60 分钟，请求负载为：

```
{  
  "login":  
  {  
    "username": "nsroot",  
    "password": "verysecret",  
    "timeout": 3600  
  }  
}
```

您还可以通过在操作的请求标头中指定用户名和密码来连接到设备以执行单个操作。例如，在创建 NetScaler 实例时连接到设备：

- **URL**
- **HTTP 方法**
- **请求**

- **标头**

```
X-NITRO-USER:nsroot
```

```
X-NITRO-PASS:verysecret
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

- **负载**

```
{  
  "ns":  
  {  
    ...  
  }  
}
```

```
}
}
```

- 响应。
- 标头

```
HTTP/1.0 201 Created
```

要从设备断开连接，请使用 DELETE 方法：

- URL
- HTTP 方法 DELETE
- 请求
- 标头

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue

Content-Type:application/vnd.com.citrix.sdx.login+json
```

配置 API

NITRO 协议可用于配置 SDX 设备资源。

每个 SDX 资源都有一个与其关联的唯一 URL，具体取决于要执行的操作类型。配置操作的 URL 格式为：`http://<IP>/nitro/v2/config/<resource_type>`

创建资源

要在 SDX 设备上创建资源（例如，NetScaler 实例），请在特定资源对象中指定资源名称和其他相关参数。例如，要创建名为 vpx1 的 NetScaler 实例：

- URL
- HTTP 方法
- 请求
- 标头

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

- 有效负载

```
{  
  
  "ns":  
  
    {  
  
      "name": "vpx1",  
  
      "ip_address": "192.168.100.2",  
  
      "netmask": "255.255.255.0",  
  
      "gateway": "192.168.100.1",  
  
      "image_name": "nsvpx-9.3-45_nc.xva",  
  
      "vm_memory_total": 2048,  
  
      "throughput": 1000,  
  
      "pps": 1000000,  
  
      "license": "Standard",  
  
      "profile_name": "ns_nsroot_profile",  
  
      "username": "admin",  
  
      "password": "admin",  
  
      "network_interfaces":  
  
        [  
  
          {  
  

```

```

        "port_name": "10/1"
    },
    {
        "port_name": "10/2"
    }
]
}
}

```

获取资源详细信息和统计信息

SDX 资源详细信息可以按如下方式检索：

- 要在 SDX 设备上检索特定资源的详细信息，请在 URL 中指定资源的 ID。
- 要根据某些筛选器检索资源的属性，请在 URL 中指定筛选条件。

URL 格式为：`http://<IP>/nitro/v2/config/<resource_type>?filter=<property1>:<value>,<property2>:<value>`

- 如果您的请求可能会从设备返回许多资源，您可以将这些结果分成“页面”并逐页检索，从而分块检索这些结果。

例如，假设您要检索 SDX 上所有 53 个 NetScaler 实例。与其在一个大型响应中检索所有 53 个实例，不如将结果配置为每页 10 个 NetScaler 实例（总共 6 页）。然后，逐页从服务器检索它们。

您可以使用页面大小查询字符串参数指定页面计数，并使用页码查询字符串参数指定要检索的页码。URL 格式为：`http://<IP>/nitro/v2/config/<resource_type>?pageno=<value>&pagesize=<value>`

您不必检索所有页面，也不必按顺序检索页面。每个请求都是独立的，您甚至可以在请求之间更改页面大小设置。

注意： 为了了解请求可能返回的资源数量，您可以使用 count 查询字符串参数来请求返回资源的计数，而不是资源本身。要获取可用 NetScaler 实例的数量，URL 将是 `http://<IP>/nitro/v2/config/<resource_type>?count=yes`

要检索 ID 为 123456a 的 NetScaler 实例的配置信息：

- URL
- HTTP 方法 GET

更新资源

要更新现有 SDX 资源，请使用 PUT HTTP 方法。在 HTTP 请求负载中，指定名称和需要更改的其他参数。例如，要将 ID 为 123456a 的 NetScaler 实例的名称更改为 vpx2：

- URL
- HTTP 方法
- 请求负载
 - 标头

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

- 负载

```
{
  "ns":
  {
    "name": "vpx2",
    "id": "123456a"
  }
}
```

删除资源

要删除现有资源，请在 URL 中指定要删除的资源名称。例如，要删除 ID 为 123456a 的 NetScaler 实例：

- URL
- HTTP 方法
- 请求
 - 标头

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

批量操作

您可以同时查询或更改多个资源，从而最大限度地减少网络流量。例如，您可以在同一操作中添加多个 NetScaler SDX 设备。您还可以在一个请求中添加不同类型的资源。

为了处理批量操作中某些操作的失败，NITRO 允许您配置以下行为之一：

- **退出。** 当遇到第一个错误时，执行停止。错误发生之前运行的命令将被提交。
- **继续。** 即使某些命令失败，列表中的所有命令也会运行。

注意： 使用 `X-NITRO-ONERROR` 参数在请求头中配置所需行为。

要在一次操作中添加 2 个 NetScaler 资源，并在一个命令失败时继续执行：

- URL。
- HTTP 方法。
- 请求负载。
 - 请求头

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

```
X-NITRO-ONERROR:continue
```

。 负载

```
{
  "ns":
  [
    {
      "name": "ns_instance1",
      "ip_address": "10.70.136.5",
      "netmask": "255.255.255.0",
      "gateway": "10.70.136.1"
    },
    {
      "name": "ns_instance2",
      "ip_address": "10.70.136.8",
      "netmask": "255.255.255.0",
      "gateway": "10.70.136.1"
    }
  ]
}
```

要在一次操作中添加多个资源（NetScaler 和两个 MPS 用户），并在一个命令失败时继续执行：

- **URL。**
- **HTTP 方法。** POST
- **请求负载。**

- 请求头

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

```
X-NITRO-ONERROR:continue
```

- 有效负载

```
{  
  "ns":  
  [  
    {  
      "name":"ns_instance1",  
      "ip_address":"10.70.136.5",  
      "netmask":"255.255.255.0",  
      "gateway":"10.70.136.1"  
    },  
    {  
      "name":"ns_instance2",  
      "ip_address":"10.70.136.8",  
      "netmask":"255.255.255.0",  
      "gateway":"10.70.136.1"  
    }  
  ],  
}
```

```
    "mpuser":  
    [  
        {  
            "name": "admin",  
            "password": "admin",  
            "permission": "superuser"  
        },  
        {  
            "name": "admin",  
            "password": "admin",  
            "permission": "superuser"  
        }  
    ]  
}
```

异常处理

错误代码字段指示操作的状态。

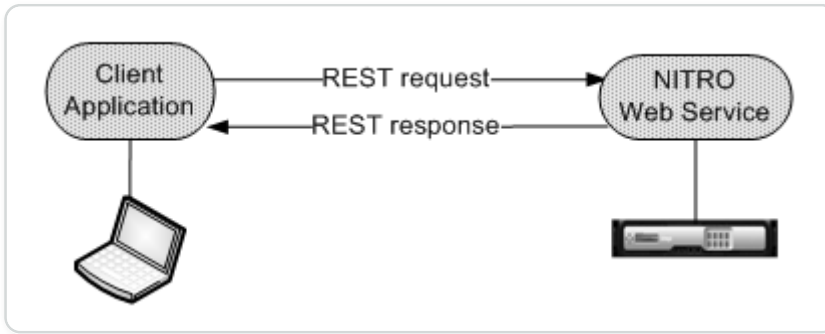
- 错误代码为 0 表示操作成功。
- 非零错误代码表示处理 NITRO 请求时出错。

错误消息字段提供简要说明以及故障的性质。

NITRO 的工作原理

NITRO 基础设施由客户端应用程序和运行在 NetScaler SDX 设备上的 NITRO Web 服务组成。客户端应用程序和 NITRO Web 服务之间的通信基于使用 HTTP 或 HTTPS 的 REST 架构。

图 1. NITRO 工作流程



工作流程的详细步骤：

1. 客户端应用程序向 NITRO Web 服务发送 REST 请求消息。使用 SDK 时，API 调用会被转换为相应的 REST 请求消息。
2. Web 服务处理 REST 请求消息。
3. NITRO Web 服务将相应的 REST 响应消息返回给客户端应用程序。使用 SDK 时，REST 响应消息会被转换为 API 调用的相应响应。

为了最大限度地减少网络流量，请从服务器检索资源的完整状态。在本地修改资源的状态。然后通过一次网络事务将其上传回服务器。

注意： 对资源进行的本地操作（更改其属性）不会影响其在服务器上的状态，直到明确上传对象的状态。

NITRO API 本质上是同步的。也就是说，客户端应用程序在运行另一个 NITRO API 之前会等待 NITRO Web 服务的响应。

Java 开发工具包

SDX NITRO API 根据其范围和目的分为系统 API 和配置 API。您还可以对 NITRO 操作进行故障排除。

系统 API

使用 NITRO 的第一步是与 SDX 设备建立会话，然后使用管理员凭据对会话进行身份验证。

通过指定设备的 IP 地址和连接到设备的协议（HTTP 或 HTTPS），创建 `nitro_service` 类的对象。然后，您可以使用此对象并通过指定管理员的用户名和密码登录到设备。

注意： 您必须在该设备上拥有一个用户帐户。您可以执行的配置操作受分配给您帐户的管理角色的限制。

以下示例代码使用 HTTPS 协议连接到 IP 地址为 10.102.31.16 的 SDX 设备：

```
//Specify the IP address of the appliance and service type

nitro_service nitroservice = new nitro_service ("10.102.31.16", "https");


//Specify the login credentials

nitroservice.login("nsroot", "verysecret");
```

注意： 请使用 nitro_service 对象在设备上的所有后续 NITRO 操作中。

要断开与设备的连接，请按如下方式调用 `logout()` 方法：

```
nitroservice.logout();
```

配置 API

NITRO 协议可用于配置 SDX 设备的资源。

用于配置资源的 API 分组到包或命名空间中，其格式为

`com.citrix.sdx.nitro.resource.config.<resource_type>`。这些包或命名空间中的每一个都包含一个名为 `<resource_type>` 的类，该类提供用于配置资源的 API。

例如，NetScaler 资源具有 `com.citrix.sdx.nitro.resource.config.ns` 包或命名空间。

资源类提供用于执行许多其他操作的 API。这些操作可以是创建资源、检索资源详细信息和统计信息、更新资源、删除资源以及对资源执行批量操作。

创建资源

要在 SDX 设备上创建资源（例如，NetScaler 实例），请执行以下操作：

1. 使用相应的属性名称设置资源的必需属性值。结果是一个资源对象，其中包含资源所需的详细信息。注意：这些值在客户端本地设置。在对象上传之前，这些值不会反映在设备上。
2. 使用静态 `add()` 方法将资源对象上传到设备。

以下示例代码在 SDX 设备上创建了一个名为“ns_instance”的 NetScaler 实例：

```
ns newns = new ns();
```

```
//Set the properties of the NetScaler locally

newns.set_name("ns_instance");

newns.set_ip_address("10.70.136.5");

newns.set_netmask("255.255.255.0");

newns.set_gateway("10.70.136.1");

newns.set_image_name("nsvpx-9.3.45_nc.xva");

newns.set_profile_name("ns_nsroot_profile");

newns.set_vm_memory_total(new Double(2048));

newns.set_throughput(new Double(1000));

newns.set_pps(new Double(1000000));

newns.set_license("Standard");

newns.set_username("admin");

newns.set_password("admin");


int number_of_interfaces = 2;

network_interface[] interface_array = new
network_interface[number_of_interfaces];


//Adding 10/1

interface_array[0] = new network_interface();

interface_array[0].set_port_name("10/1");
```

```
//Adding 10/2

interface_array[1] = new network_interface();

interface_array[1].set_port_name("10/2");


newns.set_network_interfaces(interface_array);


//Upload the NetScaler instance

ns result = ns.add(nitroservice, newns);
```

检索资源详细信息

要在 SDX 设备上检索资源的属性，请执行以下操作：

1. 使用 `get()` 方法从设备检索配置。结果是一个资源对象。
2. 使用相应的属性名称从对象中提取所需的属性。

以下示例代码检索所有 NetScaler® 资源的详细信息：

```
//Retrieve the resource object from the SDX appliance

ns[] returned_ns = ns.get(nitroservice);


//Extract the properties of the resource from the object

System.out.println(returned_ns[i].get_ip_address());

System.out.println(returned_ns[i].get_netmask());
```

检索资源统计信息

SDX 设备会收集其功能使用情况的统计信息。您可以使用 NITRO 检索这些统计信息。

以下示例代码检索 ID 为 123456a 的 NetScaler 实例的统计信息：

```
ns obj = new ns();

obj.set_id("123456a");

ns stats = ns.get(nitroservice, obj);

System.out.println("CPU Usage:" + stats.get_ns_cpu_usage());

System.out.println("Memory Usage:" + stats.get_ns_memory_usage());

System.out.println("Request rate/sec:" +stats.get_http_req());
```

更新资源

要更新设备上现有资源的属性，请执行以下操作：

1. 将 id 属性设置为要更新的资源的 ID。
2. 通过使用相应的属性名称，为资源的必需属性设置值。结果是一个资源对象。注意：这些值是在客户端本地设置的。在对象上传之前，这些值不会反映在设备上。
3. 使用 update() 方法将资源对象上传到设备。

以下示例代码将 ID 为 123456a 的 NetScaler 实例的名称更新为 'ns_instance_new'：

```
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated

update_obj.set_id("123456a");

//Get existing NetScaler details

update_obj = ns.get(nitroservice, update_obj);

//Update the name of the NetScaler to "ns_instance_new" locally

update_obj.set_name("ns_instance_new");
```

```
//Upload the updated NetScaler details

ns result = ns.update(nitroservice, update_obj);
```

删除资源

要删除现有资源，请在资源类上调用静态方法 `delete()`，并将要删除资源的 ID 作为参数传递。

以下示例代码删除 ID 为 1 的 NetScaler 实例：

```
ns obj = new ns();

obj.set_id("123456a");

ns.delete(nitroservice, obj);
```

批量操作

您可以同时查询或更改多个资源，从而最大限度地减少网络流量。例如，您可以在同一操作中添加多个 NetScaler SDX 设备。

每个资源类都有接受资源数组的方法，用于添加、更新和删除资源。要执行批量操作，请在本地指定每个操作的详细信息，然后一次性将详细信息发送到服务器。

为了处理批量操作中某些操作的失败，NITRO 允许您配置以下行为之一：

- **退出。** 当遇到第一个错误时，执行停止。错误之前运行的命令将被提交。
- **继续。** 即使某些命令失败，列表中的所有命令也会运行。

注意： 在与设备建立连接时，通过设置 `onerror` 参数，在 `nitro_service()` 方法中配置所需行为。

以下示例代码在一个操作中添加两个 ADC 设备：

```
ns[] newns = new ns[2];

//Specify details of first NetScaler

newns[0] = new ns();
```

```
newns[0].set_name("ns_instance1");

newns[0].set_ip_address("10.70.136.5");

newns[0].set_netmask("255.255.255.0");

newns[0].set_gateway("10.70.136.1");

...

...

...

//Specify details of second NetScaler

newns[1] = new ns();

newns[1].set_name("ns_instance2");

newns[1].set_ip_address("10.70.136.8");

newns[1].set_netmask("255.255.255.0");

newns[1].set_gateway("10.70.136.1");

...

...

//upload the details of the NetScalers to the NITRO server

ns[] result = ns.add(nitroservice, newns);
```

异常处理

错误代码字段指示操作的状态。

- 错误代码为 0 表示操作成功。
- 非零错误代码表示处理 NITRO 请求时出错。

错误消息字段提供了简要说明和故障性质。

`com.citrix.sdx.nitro.exception.nitro_exception` 类捕获 NITRO API 执行中的所有异常。要获取有关异常的信息，可以使用 `getErrorCode()` 方法。

有关错误代码的更详细说明，请参阅 `<NITRO_SDK_HOME>/doc` 文件夹中提供的 API 参考。

fix

This is the content for the sample heading topic. It is hidden from the main table of contents but remains accessible via links.