NetScaler SDX 13.1

Machine translated content

Disclaimer

Contents

简介

November 23, 2023

NetScaler SDX 设备是一个多租户平台，您可以在其中预置和管理多个 NetScaler 虚拟机（实例）。SDX 设备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委托给租户，从而满足云计算和多租户需求。SDX 设备使设备管理员能够为每个租户提供以下好处：

- 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
  - 实体的单独空间
  - 自己选择的发布版本和构建的独立性
  - 生命周期独
- 一个完全隔离的网络。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置的管理服务。管理服务提供用户界面（HTTP 和 HTTPS 模式）和用于配置、管理和监视设备、管理服务和实例的 API。Citrix 自签名证书已预先打包以支持 HTTPS。Citrix 建议您使用 HTTPS 模式访问管理服务用户界面。

发行说明

November 23, 2023

发行说明介绍了 NetScaler 的某个特定版本或内部版本的增强功能、变更、缺陷修复和已知问题。NetScaler SDX 发行说明作为 ADC 发行说明的一部分进行了介绍。

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

November 23, 2023

要开始配置、管理和监视设备、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。然后在设备上配置虚拟实例。

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：

- Internet Explorer

- Google Chrome
- Apple Safari
- Mozilla Firefox

登录到管理服务用户界面

1. 在 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”页面的“用户名 和 密码”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背面。首次使用默认凭据登录后，必须更改默认 `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“开始”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”、“监视”、“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“开始”列表中选择“配置”。
   b) 在 超时中，键入您希望会话过期的时间长度（以分钟、小时或天为单位）。最小超时值为 15 分钟。

   “开始”和“超时”设置在会话之间保持不变。只有在清除缓存后，它们的默认值才会恢复。

4. 单击“登录”登录到管理服务用户界面。

初始设置向导

您可以使用安装向导在单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。

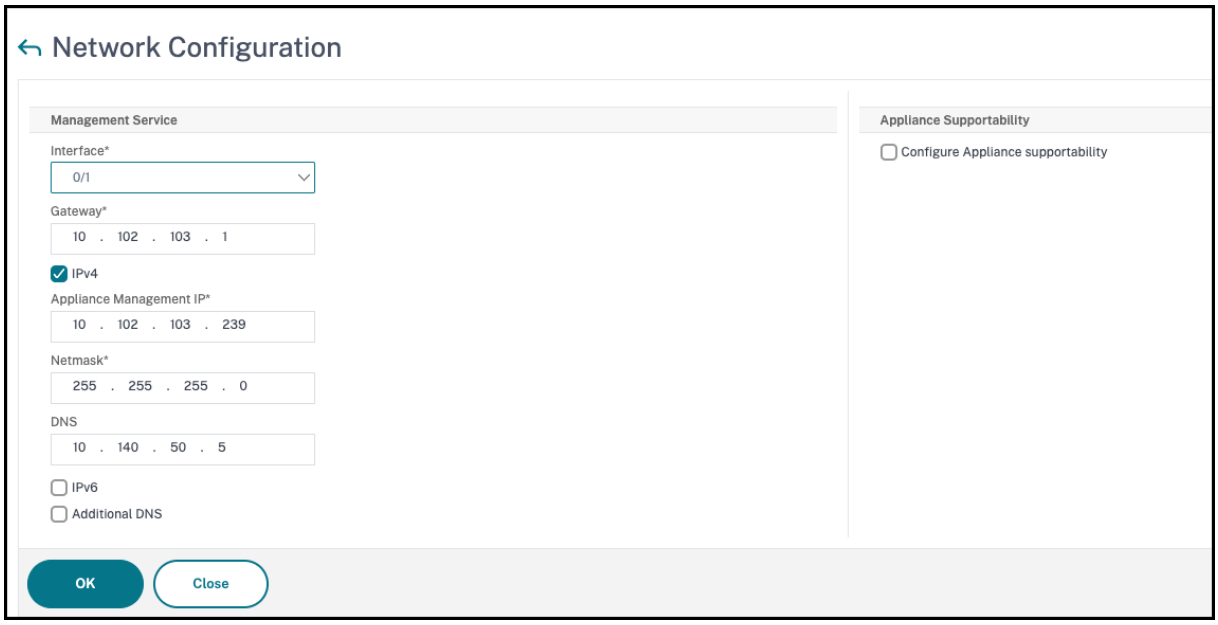
您还可以使用此向导修改在初始配置期间为 SDX 设备指定的网络配置详细信息。

要访问该向导，请导航到“配置”**>**“系统”，然后在“设置设备”下单击“安装向导”。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界面。可能的值：0/1、0/2。默认值：0/1。
- 网关：将流量转发出设备子网的路由器的 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**：用于使用 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。
- 如果要使用管理服务的 IPv 6 地址，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：用于使用 Web 浏览器访问管理服务的 IPv6 地址。
  - 网关 **IPv6** 地址：将流量转发出设备子网的路由器的 IPv4 地址。

- 选择其他 **DNS** 可将 DNS 服务器 IP 地址添加为主 DNS 服务器之外的额外 DNS 服务器。IP 地址可以是 IPv4 或 IPv6。



> 重要提示！
>
> Citrix 建议您禁用“设备支持性”以提高安全性。要禁用设备支持性，请导航到“系统”>“网络配置”，然后清除“配置设备支持性”复选框。

在“系统设置”下，您可以指定管理服务和 NetScaler 实例只能通过安全通道相互通信。您还可以限制对管理服务用户界面的访问。客户端只能使用 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。您可以通过选中“更改密码”复选框并键入新密码来更改管理密码。

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，如果本地计算机上已存在许可证，则可以将其上载到设备。

在设备上选择许可证，然后单击“完成”以完成初始配置。

在 **SDX** 设备上置备实例

您可以使用管理服务在 SDX 设备上置备一个或多个 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。

有关置备第三方实例的信息，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。此访问权限有助于对 SDX 设备上托管的实例进行调试和故障排除。

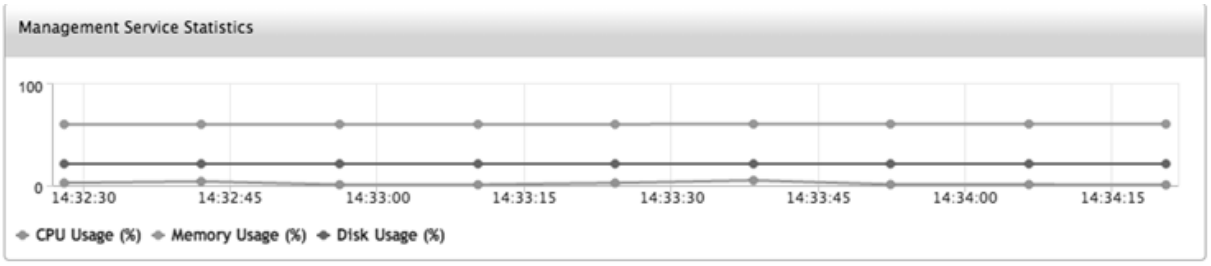
要访问虚拟机的控制台，请导航到实例列表，从列表中选择虚拟机，然后在 操作 列表中单击 控制台访问。

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

仪表板现在包括管理服务统计信息，用于监视 SDX 设备上的管理服务对内存、CPU 和磁盘资源的使用情况。



单点登录管理服务和 **NetScaler** 实例

使用用户凭证登录到管理服务后，您不必再次提供登录实例的用户凭证。默认情况下，“超时”值设置为 30 分钟，并在新的浏览器窗口中打开配置选项卡。

管理主页

管理服务主页为您提供 SDX 设备和设备上置备的实例的性能的高级视图。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。

默认情况下，主页上提供以下小工具。

- 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)**：在实时绘制并定期更新的图表中显示 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、虚拟机状态、实例状态、IP 地址、接收 (Mbps)、Tx (Mbps)、HTTP Req/s、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置任何实例。
- 运行状况监视事件：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 实例的详细信息

  您可以通过在“名称”列中单击特定 NetScaler 实例的名称来查看和隐藏该实例的详细信息。
  您也可以单击全部展开展开所有实例节点，单击全部折叠以折叠所有实例节点。

- 添加和移除小工具

  您还可以添加小工具以查看其他系统信息。

  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，然后单击开始。允许使用的字符为：a-z、A-Z、0—9、^、$、* 和 _。单击“开始”而不在搜索框中键入任何字符，以显示所有可用的小工具。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”页面：

  - 虚拟机管理程序详细信息：“虚拟机管理程序详细信息”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、构建日期和内部版本号的详细信息。
  - 许可证：许可证小工具显示以下详细信息：SDX 硬件平台、平台上支持的最大实例数、支持的最大吞吐量（以 Mbps 为单位）和可用吞吐量（以 Mbps 为单位）。

  如果删除默认情况下在主页上可用的小工具，则可以通过搜索小工具将其添加回主页。

端口

必须在 SDX 设备上打开以下端口才能正常工作。

类型	端口	详细信息
TCP	80	用于传入的 HTTP（图形用户界面和 NITRO）请求。用于访问 SDX 管理服务接口的主要接口之一。
TCP	443	用于传入的安全 HTTP（GUI 和 NITRO）请求。用于访问 SDX 管理服务接口的主要接口之一。
TCP	22	用于对 SDX 管理服务接口的 SSH 和 SCP 访问。

类型	端口	详细信息
UDP	162	SDX 管理服务接口监听来自 SDX 设备上托管的 NetScaler 实例的 SNMP 陷阱。
UDP	161	SDX 管理服务界面监听 SNMP 行走/获取请求。

数据治理

November 23, 2023

什么是 **NetScaler ADM** 服务连接

NetScaler Application Delivery Management (ADM) 服务连接是一项功能，可让 NetScaler SDX 设备无缝接入 NetScaler ADM 服务。此功能允许 NetScaler SDX 设备自动安全地连接到 NetScaler ADM 服务，并将系统、使用情况和遥测数据发送给该服务。根据这些数据，您可以获得有关 NetScaler ADM 服务上的 NetScaler 基础架构的见解和建议。

通过使用 NetScaler ADM 服务连接功能并将您的 NetScaler SDX 设备引入 NetScaler ADM 服务，您可以管理所有 NetScaler 和 NetScaler Gateway 资产，无论是在本地还是在云中。此外，您还可以获得一组丰富的可见性功能，这些功能有助于快速识别性能问题、高资源使用率、严重错误等。NetScaler ADM 服务为您的 NetScaler 实例和应用程序提供广泛的功能。有关 NetScaler ADM 服务的更多信息，请参阅 NetScaler Application Delivery Management Service。

> 重要提示
>
> - 本文档与 NetScaler SDX 设备有关。有关 NetScaler 设备的更多信息，请参阅NetScaler 设备的 NetScaler ADM 服务连接简介。
> - NetScaler Gateway 还支持 NetScaler ADM 服务连接功能。为了方便起见，在连续的部分中没有明确调用 NetScaler Gateway 设备。

注意：
NetScaler 实例和 NetScaler Gateway 实例的 NetScaler ADM 服务连接功能已经发布。但是，NetScaler ADM 服务的相应功能在即将发布的版本中可用。随着 NetScaler ADM 服务的发布，此功能的价值将很快得到释放。发生此情况时，Citrix 将更新此注释。
这项新功能的优势在 NetScaler ADM 服务上发布后即可使用。

什么是 **NetScaler ADM** 服务

NetScaler ADM 服务是一种基于云的解决方案，通过提供有关 NetScaler SDX 实例以及应用程序运行状况、性能和安全性的分析见解和基于机器学习的精选建议，帮助您管理、监视、编排、自动化和故障排除。有关更多信息，请参阅 NetScaler ADM 服务概述。

NetScaler ADM 服务连接是如何启用的

在您安装或升级 NetScaler SDX 到版本 13.1 之后，NetScaler ADM 服务连接默认处于启用状态。

使用 **NetScaler ADM** 服务连接捕获了哪些数据

以下详细信息是使用 NetScaler ADM 服务连接捕获的：

- **NetScaler SDX** 详情
  - Management IP address（管理 IP 地址）
  - 平台说明
  - 平台类型
  - 主机名
  - 系统 ID
  - 编码的序列号
  - 版本
  - 序列 ID
  - 主机 ID
  - 类型
  - 生成类型
- 关键使用指标
  - 管理 CPU 百分比
  - 内存使用百分比
  - CPU 使用率百分比
  - 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 安装的及时而深入的见解，其中包括以下内容：

- 关键指标。与 CPU、内存、吞吐量、SSL 吞吐量相关的关键指标的详细信息，并重点介绍 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。
- 部署咨询。识别在独立模式下部署但吞吐量高且易受单点故障影响的 NetScaler 实例。

收集的数据保留多长时间?

收集的任何数据的保留时间都不超过 13 个月。

如果您决定通过禁用 NetScaler 的 NetScaler ADM 服务连接功能来终止使用该服务，则先前收集的所有数据都将在 30 天后删除。

数据存储在何处及其安全性如何?

NetScaler ADM 服务连接收集的所有数据都存储在三个地区之一——美国、欧盟以及澳大利亚和新西兰 (ANZ)。有关详细信息，请参阅地理方面的注意事项。

数据安全地存储在数据库层，执行严格的租户隔离。

如何禁用 **NetScaler ADM** 服务连接

如果您想通过 NetScaler ADM 服务连接禁用数据收集，请参阅如何启用和禁用 NetScaler ADM 服务连接。

适用于 **NetScaler SDX** 设备的 **NetScaler ADM** 服务连接简介

November 23, 2023

NetScaler ADM 服务是一种基于云的解决方案，可帮助您管理、监视、协调、自动化您的 NetScaler SDX 设备并对其进行故障排除。它还为您的应用程序运行状况、性能和安全性提供分析见解和精心策划的基于机器学习的建议。有关更多信息，请参阅 NetScaler ADM 服务。

NetScaler Application Delivery Management (ADM) 服务连接是一项功能，可让 NetScaler SDX 设备无缝接入 NetScaler ADM 服务。此功能有助于 NetScaler SDX 设备和 NetScaler ADM 服务充当整体解决方案，为客户提供多重好处。

NetScaler ADM 服务连接功能允许 NetScaler SDX 实例自动连接到 NetScaler ADM 服务，并将系统、使用情况和遥测数据发送给该服务。利用这些数据，NetScaler ADM 服务为您提供一些有关 NetScaler SDX 基础架构的见解和建议，例如快速识别性能问题和高资源使用率。

要利用 NetScaler ADM 服务的强大功能，您可以选择将 NetScaler SDX 设备加入 NetScaler ADM 服务。载入流程使用 ADM 服务连接，为您提供速度更快的无缝体验。

> 注意事项
>
> - NetScaler ADM 服务连接现已在 NetScaler MPX、SDX 和 VPX 实例以及 NetScaler Gateway 设备上可用。
> - NetScaler ADM 服务连接在 NetScaler ADM 服务上尚不可用。

有关详细信息，请参阅数据治理。

NetScaler ADM 服务如何将支持与 NetScaler ADM 服务联系起来

以下是 NetScaler 上的 NetScaler ADM 服务连接功能如何与 NetScaler ADM 服务交互的高级工作流程。

1. NetScaler SDX 设备上的 NetScaler ADM 服务连接功能使用定期探测请求自动连接到 NetScaler ADM 服务。
2. 此请求包含系统、使用情况和遥测数据，NetScaler ADM 服务使用这些数据为您提供有关 NetScaler 基础架构的一些见解和建议，例如快速识别性能问题和高资源使用率。
3. 您可以查看见解和建议，决定将您的 NetScaler SDX 设备加入 NetScaler ADM 服务，开始管理您的 NetScaler SDX 设备。
4. 当您决定加入时，NetScaler ADM 服务连接功能可帮助您无缝完成载入。

NetScaler ADM 服务连接支持哪些版本的 NetScaler

所有 NetScaler 平台和所有设备型号（MPX、VPX 和 SDX）都支持 NetScaler ADM 服务连接。从 NetScaler 版本 13.0 Build 64.xx 开始，NetScaler SDX 设备默认启用 NetScaler ADM 服务连接。

如何启用 NetScaler ADM 服务连接

如果您是 NetScaler 的现有客户，并且升级到 NetScaler 版本 13.0 Build 64.xx，则在升级过程中会默认启用 NetScaler ADM 服务连接。

如果您是 NetScaler 的新客户，正在安装 NetScaler 版本 13.0 Build 64.xx，NetScaler ADM 服务连接在安装过程中默认处于启用状态。

> 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 找到路线。

如何启用和禁用 NetScaler ADM 服务连接

您可以通过 CLI、GUI 或 NITRO API 方法启用和禁用 NetScaler ADM 服务连接。

使用 **CLI**

要启用 NetScaler ADM 服务，请使用 CLI 进行连接

在命令提示符下，键入：

```
set autoreg_setting autoreg=true
```

要禁用 NetScaler ADM 服务，请使用 CLI 进行连接

在命令提示符下，键入：

```
set autoreg_setting autoreg=false
```

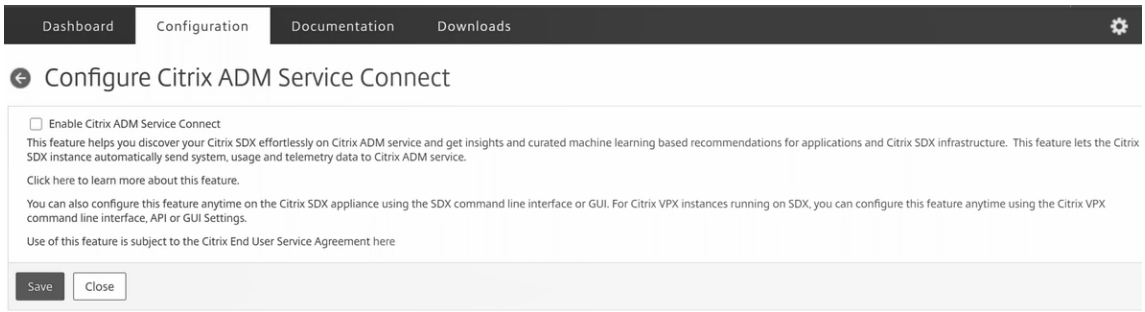
使用 CLI 显示 NetScaler ADM 服务连接设置

```
show autreg_setting

                autoreg: true

    is_banner_displayed: true

Done
```

使用 **GUI**

要禁用 NetScaler ADM 服务，请使用 NetScaler GUI 进行连接

1. 导航到“系统”。在“系统”页面上，单击“系统设置”部分下的“配置 **NetScaler ADM** 服务连接”。
2. 在“配置 **ADM** 参数”页面上，清除“启用 **NetScaler ADM** 服务连接”，然后单击“确定”。



使用 **NITRO API**

您可以使用 NITRO 命令禁用 NetScaler ADM 服务连接。

```
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 ADM 内置代理行为

从 NetScaler 版本 13.0 Build 61.xx 及更高版本开始，NetScaler SDX 实例内置了具有 ADM 服务连接功能的代理。NetScaler SDX 实例上可用的 NetScaler ADM 内置代理像活动守护程序一样启动，与 ADM 服务通信。与 ADM 服务建立通信后，内置代理会定期自动升级到最新软件版本。

引用

有关 NetScaler ADM 服务连接的更多信息，请参阅以下主题：

- 数据治理：数据治理。
- NetScaler ADM 服务：NetScaler Application Delivery Management。

单捆绑包升级

November 23, 2023

注意：在您安装或升级 NetScaler SDX 设备到 13.1 版后，NetScaler ADM 服务连接默认处于启用状态。有关更多详细信息，请参阅 数据治理 和 NetScaler ADM 服务连接。

从 11.0 及更高版本开始提供的单包升级将除 NetScaler VPX 实例映像和 LOM 固件之外的所有组件合并到一个映像文件中。此文件称为 SDX 映像。

> 注意
>
> 从版本 12.0 Build 57.19 开始，熄灯管理 (LOM) 固件将添加到 SBI 中，Citrix 客户不必单独升级 LOM。LOM 固件不是由 Citrix 编写的。

使用此映像，您可以一步升级所有组件，从而消除各个组件之间出现不兼容的可能性。单个套件升级还可以确保您的设备始终运行 Citrix 测试和支持的版本。因为所有 SDX 组件都合并到一个文件中，所以 SDX 映像文件比管理服务映像文件大。

图像的文件名格式为 `build-sdx-13.1-<build_number>.tgz`。管理服务升级到 SDX 13.1 后，新 GUI 不会显示用于上载 Citrix Hypervisor 映像文件、补充包或修补程序的选项。缺少这些选项，因为 SDX 13.1 不支持升级单个组件。

注意事项

- 单包升级是一个多步骤的过程，可能需要长达 90 分钟的时间。
- 首先，将管理服务升级到更新的提供的版本。在升级过程中，与管理服务的连接可能会丢失。重新连接到管理服务以监视升级状态。

- 接下来，新的管理服务会升级 Citrix Hypervisor 并完成设备升级的剩余部分。11.0 版及更高版本的管理服务可以执行完整的 Citrix Hypervisor 升级。
- 请勿在 Citrix Hypervisor 升级期间重新启动设备。
- Citrix 建议您使用 Citrix Hypervisor 串行控制台（或 LOM 控制台）来监视 Citrix Hypervisor 的升级。

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 实例位于高可用性设置中，请将所有主 HA 节点故障转移到辅助节点。如果您没有高可用性部署，请相应地规划停机时间。

要升级设备，请执行以下操作：

1. 上载单个分发包映像文件，导航到 配置 **>** 管理服务 **>** 软件映像，然后单击 上载。
2. 导航到 配置 **>** 系统 **>** 系统管理。
3. 在“系统管理”组中，单击“升级设备”。
   升级过程需要几分钟。

升级之前，管理服务会显示以下信息：

- 单包映像文件名。
- 设备上运行的当前版本的 SDX。
- 设备要升级到的选定版本。
- 升级设备的大概时间。
- 杂项信息。

在单击“升级设备”之前，请确保已查看屏幕上显示的所有信息。升级过程一旦启动，就无法中止。

支持的升级路径

	11.1	12.0	12.1	13.0	13.1	14.1
10.5 或 11.0	Y	Y	Y	N*	N*	N*
11.1—65.x 及更高版本	不适用	不推荐	12.1-56.x 及更高版本	Y	Y	Y
12.1	不适用	不适用	不推荐	Y	Y	Y

* 从 10.5、11.0 和 11.1 版本的较早版本中，您必须先升级到 11.1 或 12.1 版，然后再升级到 13.0、13.1 或 14.1 版。

相关信息

NetScaler SDX 硬件软件兼容性列表

揭开 NetScaler SDX 设备升级过程的神秘面纱

升级 **NetScaler** 实例

November 23, 2023

> 备注
>
> - 在您安装或升级 NetScaler SDX 设备到 13.1 版后，NetScaler ADM 服务连接默认处于启用状态。有关更多详细信息，请参阅 数据治理 和 NetScaler ADM 服务连接。
> - 从版本 13.1 Build 37.x 开始，NetScaler SDX 设备升级过程需要一次重启，而不是两次重启。

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

> 重要提示
>
> 不支持使用管理服务降级 ADC 实例。使用实例 CLI 降级。

在升级 NetScaler 实例之前，将 NetScaler 软件映像上载到 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：上次修改文件的日期。
- 大小：文件的大小（以 MB 为单位）。

上载软件映像

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“上载”。
3. 在上 载 **NetScaler** 软件映像 对话框中，单击 浏览，然后选择要上载的 NetScaler 映像文件。
4. 单击上载。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. 在消息框的“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”。

上载 **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”窗格的“**XVA** 文件”选项卡上，单击“上载”。
3. 在“上载 **NetScaler XVA** 文件”对话框中，单击“浏览”，然后选择要上载的 NetScaler XVA 文件。
4. 单击上载。XVA 文件出现在 **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，请确保已将正确的版本上载到 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（例如从标准版升级到企业版或从企业版升级到铂金版）可能需要新的许可证。另请注意以下事项：

- 为防止配置丢失，请在升级任何实例之前在每个实例上保存配置。
- 您还可以从 Instances 节点升级单个实例。为此，请从“实例”节点中选择实例。在详细信息窗格中，选择实例，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 来升级 VPX 实例，则升级映像是备份文件的一部分，可让您顺利恢复实例。

升级 **VPX** 实例

1. 在 配置 选项卡的导航窗格中，单击 **NetScaler**。
2. 在详细信息窗格中的 **NetScaler** 配置下，单击 升级。
3. 在 升级 **NetScaler** 对话框的 软件映像中，选择要升级到的版本的 NetScaler 升级构建文件。

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 硬件软件兼容性列表

揭开 NetScaler SDX 设备升级过程的神秘面纱

管理和监视 **SDX** 设备

February 16, 2024

NetScaler SDX 设备启动并运行后，您可以执行各种任务，从管理服务用户界面管理和监视设备。

修改 **SDX** 设备的网络配置

您可以在初始配置期间修改为 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 的访问权限时，会显示一条警告消息“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。为确保安全性，请仅在必要时使用默认管理员帐户。只有其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。如果丢失了密码，则可以通过将设备设置恢复为出厂默认值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。

修改设备上的时区

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 筛选可在共享物理端口的 VPX 实例之间进行数据分离。例如，如果您在两个不同的 VLAN 上配置了两个 VPX 实例，并且启用了 VLAN 过滤，则一个实例将无法查看另一个实例的流量。如果禁用了 VLAN 过滤，则所有实例都能看到标记或未标记的广播数据包，但在软件级别丢弃这些数据包。如果启用了 VLAN 过滤，则每个带标记的广播数据包将仅到达属于相应标记的 VLAN 的实例。如果所有实例都不属于相应的已标记 VLAN，则数据包将在硬件级别 (NIC) 丢弃。

如果在接口上启用了 VLAN 过滤，则可以在该接口上使用有限数量的带标记的 VLAN。10G 接口上有 63 个带标记的 VLAN，在 1G 接口上使用 32 个带标记的 VLAN。VPX 实例仅接收具有已配置 VLAN ID 的数据包。如果将与某个接口关联的 VLAN 筛选器的状态从“已禁用”更改为“已启用”，请重新启动该接口的 VPX 实例。

默认情况下，SDX 设备上启用 VLAN 过滤。如果在接口上禁用 VLAN 过滤，则可以在该接口上配置多达 4096 个 VLAN。

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

要在接口上启用 VLAN 过滤，请单击 系统 > 接口。选择一个接口，然后单击 **VLAN** 过滤器，然后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) 同步后，管理服务将重新启动。您可以将 SDX 设备配置为将其本地时钟与 NTP 服务器同步。因此，SDX 设备上的时钟与网络上的其他服务器具有相同的日期和时间设置。如果重新启动、升级或降级设备，时钟同步配置不会更改。但是，在高可用性设置中，配置不会传播到辅助 NetScaler 实例。

如果添加 NTP 服务器或更改任何身份验证参数，时钟将立即同步。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 NTP 官方网站 http://www.ntp.org 上找到公共开放访问的 NTP 服务器列表。在将 NetScaler 配置为使用公共 NTP 服务器之前，请务必阅读“接洽规则”页面（所有公共时间服务器页面上都包含链接）。

要配置 NTP 服务器，请单击“系统”**>**“**NTP** 服务器”。

启用 **NTP** 同步

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 **NTP** 同步。

3. 在“**NTP** 同步”对话框中，选择“启用 **NTP** 同步”。
4. 单击“**** 确定”，然后单击“关闭 ****”。

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。
    - 可信密钥 **ID**—可信密钥 ID。添加 NTP 服务器时，您可以从此列表中选择密钥标识符。最小值：1。最大值：65534。
    - 撤消时间间隔 - 自动密钥方案使用的某些加密值的重新随机化间隔（以 2 的幂为单位），以秒为单位。默认值：17（2^17=36 小时）。
    - **Automax In**terval —重新生成与 Autokey 协议一起使用的会话密钥列表之间的间隔（以 2 为幂），以秒为单位。默认值：12（2^12=1.1 小时）。
4. 单击“**** 确定”，然后单击“关闭 ****”。

查看 **SDX** 设备的属性

在“配置”选项卡上查看系统属性，例如 CPU 内核和 SSL 芯片数量、可用内存总量和可用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、虚拟机管理程序、许可证和系统的以下信息：

系统资源：

- **CPU** 内核总数； SDX 设备上的 CPU 内核数。
- **SSL** 芯片总数： SDX 设备上的 SSL 芯片总数。
- 免费 **SSL** 芯片：尚未分配给实例的 SSL 芯片总数。
- 总内存 **(GB)**：装置总内存 (GB)。
- 可用内存 **(GB)**：可用设备内存（以 GB 为单位）。

虚拟机管理程序信息：

- 正常运行时间：设备上次重新启动以来的时间，以天数、小时数和分钟数表示。
- 版本：安装在 SDX 设备上的 Citrix Hypervisor 的版本。
- 版本：安装在 SDX 设备上的 Citrix Hypervisor 的版本。
- **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。
- 构建日期： Citrix Hypervisor 的构建日期。
- 内部版本号： Citrix Hypervisor 的内部版本号。
- 补充包： SDX 设备上安装的补充包的版本。

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：根据已安装的许可证，您可以在 SDX 设备上设置的最大实例数。
- 可用实例（共享）：可配置的实例数量，具体取决于仍然可用的 CPU 内核数。
- 最大吞吐量 **(Mbps)**：根据已安装的许可证，在设备上可实现的最大吞吐量。
- 可用吞吐量 **(Mbps)**：基于已安装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。
- 构建：在 SDX 设备上运行的 NetScaler 发布和构建版本。
- **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：以日月日期小时数: 分钟: 秒时区年格式显示的系统时间。
- 正常运行时间：自上次重新启动管理服务以来的时间，以天数、小时数和分钟数表示。
- **BIOS** 版本： BIOS 版本。

查看实时设备吞吐量

传入和传出流量的 SDX 设备总吞吐量在定期更新的图表中实时绘制。默认情况下，传入和传出流量的吞吐量将一起绘制在图形上。

要查看 SDX 设备的吞吐量，请在 GUI 上单击控制板，然后选中系统吞吐量 **(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。图表是实时绘制的，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 控制板，然后选中 管理服务统计信息。

查看所有内核的 **CPU** 使用率

您可以查看 SDX 设备上每个 CPU 内核的使用情况。

CPU 核心使用率 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**：该内核的物理 CPU 编号。
- 超线程：与该 CPU 核心关联的超线程。
- 实例：使用该 CPU 内核的实例。
- 平均核心使用量：平均核心使用量，以百分比表示。

要查看 SDX 设备上所有内核的 CPU 使用率，请在 GUI 上单击控制板，然后选中系统 **CPU** 使用率 **(%)**。

在 **SDX** 设备上安装 **SSL** 证书

SDX 设备附带默认 SSL 证书。出于安全考虑，您可能希望将此证书替换为您自己的 SSL 证书。为此，您必须先将 SSL 证书上载到管理服务，然后再安装证书。安装 SSL 证书将终止当前与管理服务的所有客户端会话。登录到管理服务以执行任何其他配置任务。

要安装 SSL 证书，请单击“系统”。在 设置设备 组中，单击 安装 **SSL** 证书，然后在向导中输入详细信息。

在管理服务上查看 **SSL** 证书

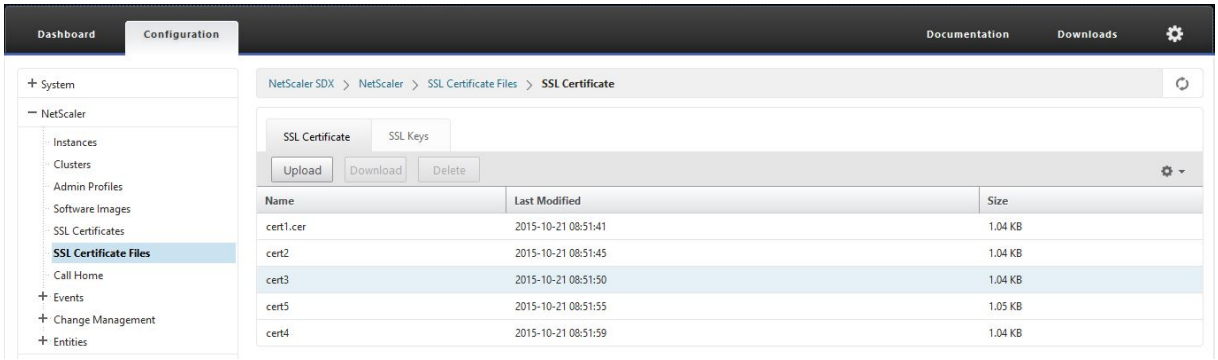
管理服务使用 SSL 证书进行安全的客户端连接。查看此证书的详细信息，例如有效性状态、颁发者、主题、过期天数、有效起始日期和终止日期、版本和序列号。

要查看 SSL 证书，请单击 系统，然后在 设置设备 组中单击 查看 **SSL** 证书。

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增强了可用性。使用新的管理服务节点 SSL 证书文件上载和管理 SSL 证书以及可安装在 NetScaler 实例上的相应公钥和私钥对。

要访问 NetScaler 实例的 SSL 证书和密钥，请导航到配置 **> NetScaler > SSL** 证书文件。



修改系统设置

出于安全原因，您可以指定管理服务和 VPX 实例只能通过安全通道相互通信。您还可以限制对管理服务用户界面的访问。客户端只能使用 https 登录管理服务用户界面。

要修改系统设置，请单击 配置 **>** 系统，然后在系统设置组中单击 更改系统设置。

重启设备

管理服务提供了重新启动 SDX 设备的选项。在重启期间，设备将关闭所有托管实例，然后重新启动 Citrix Hypervisor。当 Citrix Hypervisor 重新启动时，它将启动所有托管实例以及管理服务。

要重新启动设备，请单击 配置 **>** 系统，然后在系统管理组中单击 重新启动设备。

关闭设备

您可以从管理服务中关闭 SDX 设备。

要关闭设备，请单击 配置 **>** 系统，然后在系统管理组中单击 关闭设备。

SDX 管理域

November 23, 2023

SDX 管理域功能可帮助您创建多个管理域。您可以使用管理域为不同部门隔离资源。因此，管理域可以改善对资源的控制，并且可以在各个域之间分配资源以实现最佳利用。

SDX 设备附带固定资源，例如 CPU 内核、数据吞吐量、内存、磁盘空间、SSL 芯片以及可以预配的特定数量的实例。您可以创建的实例数量取决于许可证。

SDX 设备最多支持三个级别的管理域。设备出厂时，所有资源都将分配给所有者。

您创建的任何管理域都是所有者域的子域。在每种情况下，子域的资源都是从父域的资源池中分配的。管理域中的用户有权访问该域的资源。他们无法访问同一层次结构级别的其他域的资源，也无法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的子域的资源。

向子域分配资源的示例

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。在这种情况下，管理员最多可以分配 10 个 CPU 核心和 840 GB 的磁盘空间。

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。该子域已被分配给其父域的 10 个 CPU 核心中的 5 个，剩下的 5 个核心可以分配给所有者的其他子域。

表 2. 测试域的资源

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。

下图显示了在子域之间进行资源分配的另一个示例，它使用的值与表 1 和表 2 中列出的值不同。

要创建管理域，请导航到 配置 **>** 系统 **>** 管理域，然后选择所需的选项。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到此域，并提供域名和用户名。例如，如果您使用用户 NewUser 创建了一个名为 NewDomain 的域，则以 NewDomain\NewUser 的身份登录。

将用户分配到域

创建子域时，将自动创建两个用户组：管理员组和只读组。默认情况下，每个用户都是管理员组的一部分。可以将一个用户添加到多个群组。

在 **SDX 22000** 平台上管理 **RAID** 磁盘分配

November 23, 2023

NetScaler SDX 22040/22060/22080/22100/22120 设备现在包括独立磁盘冗余阵列 (RAID) 控制器，它最多可以支持八个物理磁盘。多个磁盘不仅提高了性能，而且还增强了可靠性。可靠性对于 SDX 设备尤为重要，因为该设备托管许多虚拟机，而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，两个磁盘维护着相同的数据。如果 RAID 1 阵列中的某个磁盘出现故障，其镜像将立即提供所有需要的数据。

RAID 1 磁盘镜像将两个物理驱动器合并到一个逻辑驱动器中。逻辑驱动器的可用容量等于其中一个物理驱动器的容量。例如，合并两个 1 TB 的驱动器将创建一个总可用容量为 1 TB 的逻辑驱动器。在设备看来，这种驱动器组合显示为单个逻辑驱动器。

SDX 设备附带的配置包括逻辑驱动器 0 和逻辑驱动器 1。逻辑驱动器 0 分配给管理服务，Citrix Hypervisor 和逻辑驱动器 1 分配给您预置的 NetScaler 实例。要使用更多的物理驱动器，必须创建新的逻辑驱动器。

查看驱动器的属性和操作

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。必须先使物理驱动器成为逻辑驱动器的一部分，然后才能使用该物理驱动器。

在管理服务中，“配置” **>** “系统” **>** “**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 配置 **>** 系统 **> RAID >** 逻辑驱动器 选项卡上，您可以查看每个逻辑驱动器的名称、状态、大小以及有关其组件物理驱动器的信息。下表描述了虚拟驱动器的状态。

状态	说明
最佳	虚拟驱动器运行状况良好。所有配置的驱动器都处于联机状态。
已降级	虚拟驱动器的运行状况不是最佳。其中一个配置的驱动器出现故障或处于脱机状态。
失败	虚拟驱动器出现故障。
脱机	RAID 控制器无法使用虚拟驱动器。

您还可以通过选择逻辑驱动器并单击“显示物理驱动器”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 配置 > 系统 > **RAID**，然后选择 逻辑驱动器 选项卡。
2. 单击添加。
3. 在“创建逻辑磁盘”对话框中，选择两个包含正常运行的物理驱动器的插槽，然后单击“创建”。

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
配置 **>** 系统 **> RAID >** 物理驱动器 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，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，无法作为逻辑驱动器的一部分添加。
- 外国：—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。如果物理驱动器未处于良好状态，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：—启动驱动器的重建。当驱动器组中的驱动器发生故障时，您可以通过重新创建驱动器出现故障之前存储在驱动器上的数据来重建该驱动器。RAID 控制器重新创建存储在驱动器组中其他驱动器上的数据。
- 定位：—在设备上找到驱动器，通过使与驱动器关联的驱动器活动 LED 闪烁来指示。
- 停止定位：—停止在设备上查找驱动器。
- 准备移除：—停用选定的物理驱动器，以便将其移除。

存储库

在 配置 **>** 系统 **> RAID >** 存储库 选项卡上，可以查看 SDX 设备上存储库的状态。您还可以查看有关未连接的存储库驱动器的信息，然后选择该驱动器，然后单击“删除”可以将其 删除。“存储库”选项卡显示有关每个存储库的以下信息：

- 名称：—存储库驱动器的名称。
- 是否已连接驱动器：—存储库是否已连接。如果未连接驱动器，则可以单击“删除”进行删除。
- 大小：—存储库的大小。
- 已使用：—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 设备的背面，将两个空白固态硬盘插入插槽编号 4 和 5 中。您可以在正在运行的系统中添加 SSD。
   注意：确保固态硬盘已通过 NetScaler 认证。
4. 在管理服务中，导航到配置 **>** 系统 **> RAID** 和 物理驱动器选项卡。您会看到您添加的固态硬盘。
5. 导航到“逻辑驱动器”选项卡，然后单击“添加”。
6. 在“创建逻辑磁盘”页面中：
   a) 在 第一个插槽下拉列表中，选择 4。
   b) 在 第二个插槽下拉列表中，选择 5。
   c) 单击 **Create**（创建）。
      注意：在管理服务中，插槽编号以零开头。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。

逻辑驱动器随即创建并列在“
逻辑驱动器”选项卡下。单击刷新图标可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，请将固态硬盘插入插槽编号 6 和 7 中。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。

用空白的 **SSD** 驱动器更换有故障的 **SSD** 驱动器　要将有故障的 SSD 驱动器替换为空白的 SSD 驱动器：

1. 导航到“配置” **>** “系统” **>** “**RAID**”。
2. 在“物理驱动器”选项卡上，选择要更换的有故障的驱动器。
3. 单击“准备拆除”以卸下驱动器。
4. 单击刷新图标以刷新物理驱动器列表。
5. 从插槽中实际卸下有故障的驱动器。
6. 将经过 Citrix 验证的新 SSD 插入卸下有缺陷固态硬盘的插槽中。
7. 在管理服务中，导航到 配置 **>** 系统 **> RAID**。新的固态硬盘列在物理驱动器 部分。驱动器重建过程将自动启动。

单击刷新图标可检查重建进程的状态。重建过程完成后，您可以在“
固件 状态”列中看到“联机，正在启动”状态。

SDX 许可概述

February 16, 2024

在 NetScaler SDX Management Service 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，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。

或者，如果本地计算机上已存在许可证，则可以将其上载到设备。

对于所有其他功能（例如返回或重新分配许可证），则必须使用许可门户。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：

- 选择合适的平台和版本选项。
- 许可模式

注意：安装永久许可证或池许可证不需要重新启动 SDX 设备。

必备条件

要使用硬件序列号或许可证访问代码分配许可证，请执行以下操作：

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。许可证分配软件在内部访问您的许可证的 Citrix 许可证门户。要访问公共域，必须配置管理服务 IP 地址并设置 DNS 服务器。
2. 您的许可证必须链接到您的硬件，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

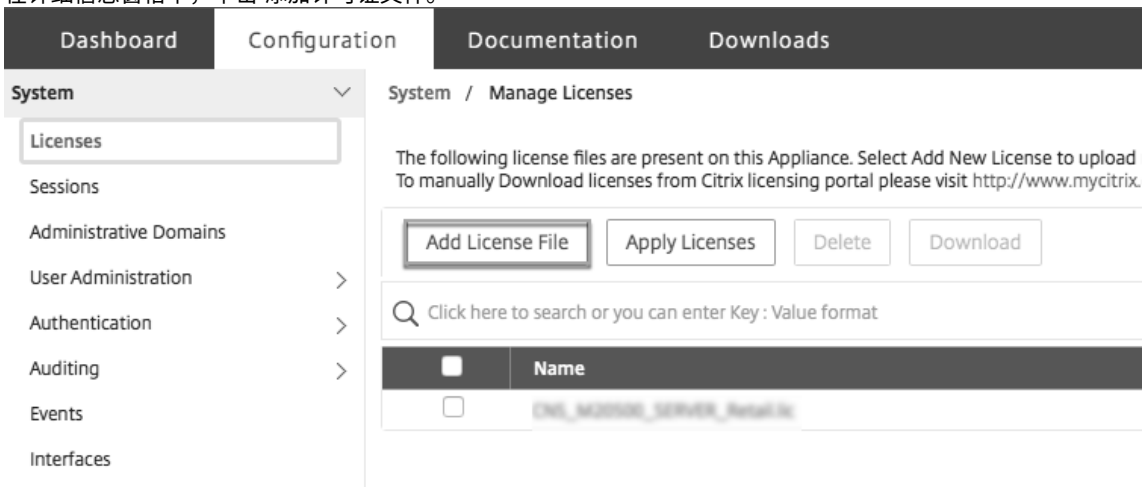
如果您的许可证已链接到您的硬件，则许可证分配过程可以使用硬件序列号。否则，必须键入许可证访问代码。

可以根据您的部署的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 6 个许可证，现在可以分配 6 个许可证，以后再分配更多许可证。分配的数量不能超过许可证文件中存在的许可证总数。

分配许可证

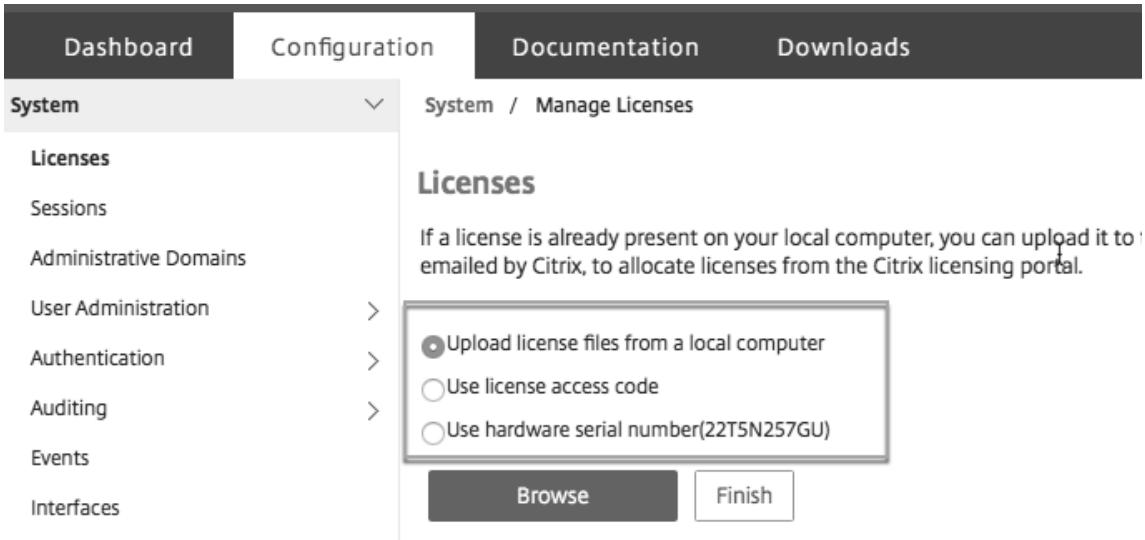
1. 在 Web 浏览器中，键入 SDX 设备管理服务的 IP 地址（例如 http://10.102.126.251）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，键入管理员凭据。

3. 在 **Configuration**（配置）选项卡上，导航到 **System**（系统）**> Licenses**（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，选择其中一个选项：

   - 从本地计算机上载许可证文件（默认情况下选中此选项）
   - 使用许可证访问代码
   - 使用硬件序列号



- 从本地计算机上载许可证文件：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”。

  1. 成功应用零容量许可证后，许可证模式 部分将显示在 许可证 页面上。
  2. 您可以选择共享许可证或自管理池许可证。
  3. 在 授权服务器名称或 **IP** 地址 字段中，输入许可证服务器详细信息。
  4. 在 端口号 字段中，输入许可证服务器端口。默认值：27000。
  5. 单击 **Get Licenses**（获取许可证）。

6. 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”。
7. 在“管理许可证”页面上，您可以查看许可证服务器、许可证版本以及池中分配的实例和带宽的详细信息。

> 注意：
>
> 从 NetScaler 版本 13.1 Build 30.x 起，NetScaler SDX 设备支持自助管理池许可证。使用此许可证，您可以简化和自动将许可证文件上载到许可证服务器。您可以使用 NetScaler ADM 创建包含公共带宽或 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** ，或者选中复选框以通过代理服务器进行连接。接下来，单击 获取许可证。
  - 选择要用于分配许可证的许可证文件。
  - 在 **Allocate**（分配）列中，输入要分配的许可证数。接下来，单击“下载”。

  如果下载了许可证，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，软件将在内部获取设备的序列号，并使用该序列号来显示您的许可证。
  - 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，然后单击 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为 NetScaler 池容量。

SDX 资源可视化工具

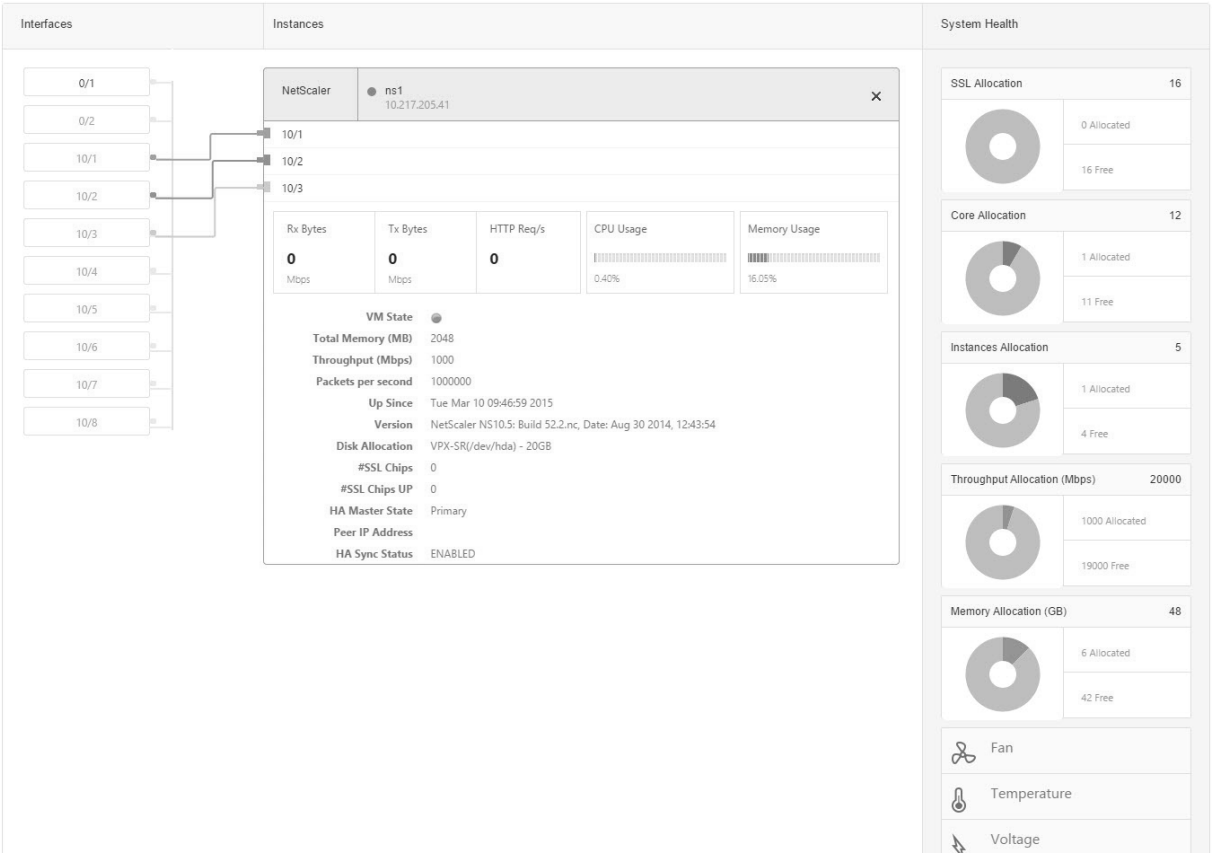
February 16, 2024

在 NetScaler SDX 设备上配置 NetScaler 实例时，需要为实例分配 CPU、吞吐量、内存等各种资源。对于当前的 SDX，不会显示有关各种可用资源的信息。

使用资源可视化工具，可用于置备实例的所有可用资源都显示在单个控制板中。所有可用和已使用的资源都以图形格式显示。除了可以分配的资源外，资源可视化工具还会显示其他参数，例如电源状态和温度。

资源可视化工具还会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使用的资源。

下图显示了资源可视化工具中捕获的详细信息：



管理接口

November 23, 2023

在 接口 窗格中，您可以显示 VPX 实例上的虚拟接口到 SDX 设备的映射，并为接口分配 MAC 地址。

注意：直接连接电缆 (DAC) 的接口不支持自动协商。

在“接口”窗格的“接口”列表中，在“状态”列中，UP 表示该接口正在正常接收流量。DOWN 表示存在网络问题，因此接口无法发送或接收流量。

重要提示：不建议对超过 1 GB 的连接进行流量控制。

配置接口

1. 在“配置”选项卡的导航窗格中，展开“系统”，然后单击“接口”。
2. 在 接口 窗格中，单击要配置的接口，然后单击 编辑。
3. 在“配置接 口”窗口中，指定以下参数的值：

- 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，以 MB/s 为单位。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”。

将接口的参数重置为默认值

1. 在“配置”选项卡的导航窗格中，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 显示了实例上的虚拟接口与设备上的物理接口的映射。

登录 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和设备上相应的物理接口号将显示在 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.
...
<!--NeedCopy-->
```

为接口分配 **MAC** 地址

在 SDX 设备上配置 ADC 实例时，Citrix Hypervisor 会在内部为与该实例关联的虚拟接口分配一个 MAC 地址。可能会将相同的 MAC 地址分配给与同一设备或其他设备上的另一个实例关联的虚拟接口。要防止分配重复的 MAC 地址，您可以强制使用唯一的 MAC 地址。

为接口分配 MAC 地址有两种方法：

1. 为接口分配基本 MAC 地址和范围：管理服务使用基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。如果设置全局基本 MAC 地址，则 1G 接口的范围将设置为 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，请参阅下表中的基本 MAC 地址示例。

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 地址生成的基本 MAC 地址示例

管理端口的基本 MAC 地址仅供参考。管理服务仅根据基本 MAC 地址为 1/x 和 10/x 端口生成 MAC 地址。

注意：您无法为通道分配基本 MAC 地址。

要使用 MAC 地址执行各种操作，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

如果未使用 SDX 设备上的任何物理接口，则可以使用管理服务禁用物理接口。出于安全考虑，此操作很有帮助。

注意：默认情况下，SDX 设备上的所有物理接口都处于启用状态。此外，如果某个接口被 VPX 或频道使用，则无法禁用该接口。

要禁用物理接口，请执行以下操作：

1. 在“配置”选项卡的导航窗格中，展开“系统”，然后单击“接口”。
2. 在 接口 窗格中，选择要禁用的接口。

3. 在“操作”下拉列表中，单击“禁用”。

如果要使用禁用的物理接口，可以使用管理服务启用该接口。

要启用禁用的物理接口，请执行以下操作：

1. 在“配置”选项卡的导航窗格中，展开“系统”，然后单击“接口”。
2. 在“接口”窗格中，选择要启用的禁用接口。
3. 在“操作”下拉列表中，单击“启用”。

SDX 设备上的巨型帧

November 23, 2023

NetScaler SDX 设备支持接收和传输包含多达 9216 字节 IP 数据的巨型帧。相比于 1500 字节的标准 IP MTU 大小，巨型帧可以更有效地传输大文件。

NetScaler SDX 设备可以在以下部署场景中使用巨型帧：

- **Jumbo to Jumbo**：设备以巨型帧的形式接收数据，然后将其作为巨型帧发送。
- 非巨型到巨型帧：设备以非巨型帧的形式接收数据，然后将其作为巨型帧发送。
- 巨型到非巨型帧：设备以巨型帧的形式接收数据，然后将其作为非巨型帧发送。

在 SDX 设备上配置的 NetScaler 实例支持以下协议的负载平衡配置中的巨型帧：

- TCP
- 通过 TCP 的任何其他协议
- SIP

有关巨型帧的更多信息，请参阅使用案例。

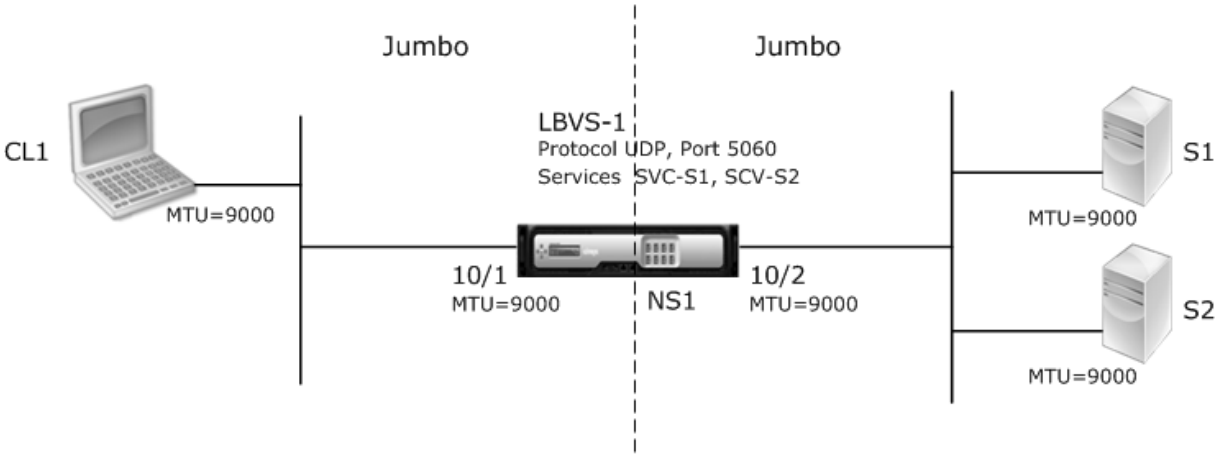
使用案例：巨型到巨型设置

举一个从巨型到巨型设置的示例，其中使用在 NetScaler 实例 NS1 上配置的 SIP 负载平衡虚拟服务器 LBVS-1 来对服务器 S1 和 S2 之间的 SIP 流量进行负载平衡。客户端 CL1 和 NS1 之间的连接以及 NS1 和服务器之间的连接都支持巨型帧。

NS1 的接口 10/1 接收或发送来往客户端 CL1 的流量。NS1 的接口 10/2 接收或发送来自服务器 S1 或 S2 的流量。NS1 的接口 10/1 和 10/2 分别是 VLAN 10 和 VLAN 20 的一部分。

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

本设置示例中的所有其他网络设备（包括 CL1、S1、S2）也配置为支持巨型帧。



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
为接口（通过使用管理服务界面）和 NS1 上的 VLAN（使用 CLI）指定的 MTU。	10/1	9000
		10/2
		VLAN 10
		VLAN 20
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
在 VLAN 10 上对虚拟服务器进行负载平衡	LBVS-1	IP 地址：203.0.113.15；协议：SIP；端口：5060；SVC-S1、SVC-S2

以下是 CL1 向 NS1 发出的请求的流量：

1. CL1 为 LBVS1 创建了一个 20000 字节的 SIP 请求。
2. CL1 以 IP 分段的形式将请求数据发送到 NS1 的 LBVS1。每个 IP 片段的大小等于或小于 CL1 将这些片段发送到 NS1 的接口上设置的 MTU (9000)。
    - 第一个 IP 片段的大小 = [IP 标头 + UDP 标头 + SIP 数据段] = [20 + 8 + 8972] = 9000
    - 第二个 IP 分段的大小 = [IP 标头 + SIP 数据段] = [20 + 8980] = 9000

- 最后一个 IP 片段的大小 = [IP 标头 + SIP 数据段] = [20 + 2048] = 2068

3. NS1 在接口 10/1 接收请求 IP 片段。NS1 接受这些分段，因为每个分段的大小等于或小于接口 10/1 的 MTU (9000)。
4. NS1 重新组装这些 IP 分段以构成 27000 字节的 SIP 请求。NS1 正在处理此请求。
5. LBVS-1 的负载平衡算法选择服务器 S1。
6. 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)。这些 IP 数据包的来源是 SNIP 地址 NS1。

   - 第一个 IP 片段的大小 = [IP 标头 + UDP 标头 + SIP 数据段] = [20 + 8 + 8972] = 9000
   - 第二个 IP 分段的大小 = [IP 标头 + SIP 数据段] = [20 + 8980] = 9000
   - 最后一个 IP 片段的大小 = [IP 标头 + SIP 数据段] = [20 + 2048] = 2068

以下是本示例中 S1 对 CL1 的响应的通信流：

1. 服务器 S1 创建一个 30000 字节的 SIP 响应，以发送到 NS1 的 SNIP 地址。
2. S1 将 IP 分段中的响应数据发送到 NS1。每个 IP 分段的大小等于或小于 S1 将这些分段发送到 NS1 的接口上设置的 MTU (9000)。

   - 第一个 IP 片段的大小 = [IP 标头 + UDP 标头 + SIP 数据段] = [20 + 8 + 8972] = 9000
   - 第二个和第三个 IP 分段的大小 = [IP 标头 + SIP 数据段] = [20 + 8980] = 9000
   - 最后一个 IP 片段的大小 = [IP 标头 + SIP 数据段] = [20 + 3068] = 3088

3. NS1 在接口 10/2 接收响应 IP 片段。NS1 接受这些分段，因为每个分段的大小等于或小于接口 10/2 的 MTU (9000)。
4. NS1 重新组装这些 IP 分段以构成 27000 字节的 SIP 响应。NS1 会处理此响应。
5. NS1 以 IP 分段的形式将响应数据发送到 CL1。每个 IP 分段的大小等于或小于 NS1 将这些分段发送到 CL1 的接口 10/1 的 MTU (9000)。这些 IP 片段源自 LBVS-1 的 IP 地址。这些 IP 数据包来自 LBVS-1 的 IP 地址，并注定到 CL1 的 IP 地址。

   - 第一个 IP 片段的大小 = [IP 标头 + UDP 标头 + SIP 数据段] = [20 + 8 + 8972] = 9000
   - 第二个和第三个 IP 分段的大小 = [IP 标头 + SIP 数据段] = [20 + 8980] = 9000

最后一个 IP 片段的大小 = [IP 标头 + SIP 数据段] = [20 + 3068] = 3088

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 **Edit**（编辑）。设置 MTU 值，然后单击 确定。

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 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 并设置所需的 VLAN 的 MTU 以支持巨型帧。	add vlan <id> -mtu <positive_integer>;show vlan <id>	add vlan 10 -mtu 9000; add vlan 20 -mtu 9000
将接口绑定到 VLAN。	bind vlan <id> -ifnum <interface_name>; show vlan <id>	bind vlan 10 -ifnum 10/1; bind vlan 20 -ifnum 10/2
添加一个 SNIP 地址。	add ns ip <IPAddress> <netmask> -type SNIP; show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP
创建代表 SIP 服务器的服务。	add service <serviceName> <ip> SIP_UDP <port>; show service <name>	add service SVC-S1 198.51.100.19 SIP_UDP 5060; dd service SVC-S2 198.51.100.20 SIP_UDP 5060
创建 SIP 负载平衡虚拟服务器并将服务绑定到它	add lb vserver <name> SIP_UDP <ip> <port> ;bind lb vserver <vserverName> <serviceName>; show lb vserver <name>	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
bind lb vserver LBVS -1 SVC-S2	save ns config; show ns config	

用例：非巨型到巨型设置

以非巨型到巨型设置为例，在该设置中，在 NetScaler 实例 NS1 上配置的负载平衡虚拟服务器 LBVS1 用于对服务器 S1 和 S2 之间的流量进行负载平衡。客户端 CL1 和 NS1 之间的连接支持非巨型帧，NS1 和服务器之间的连接支持巨型帧。

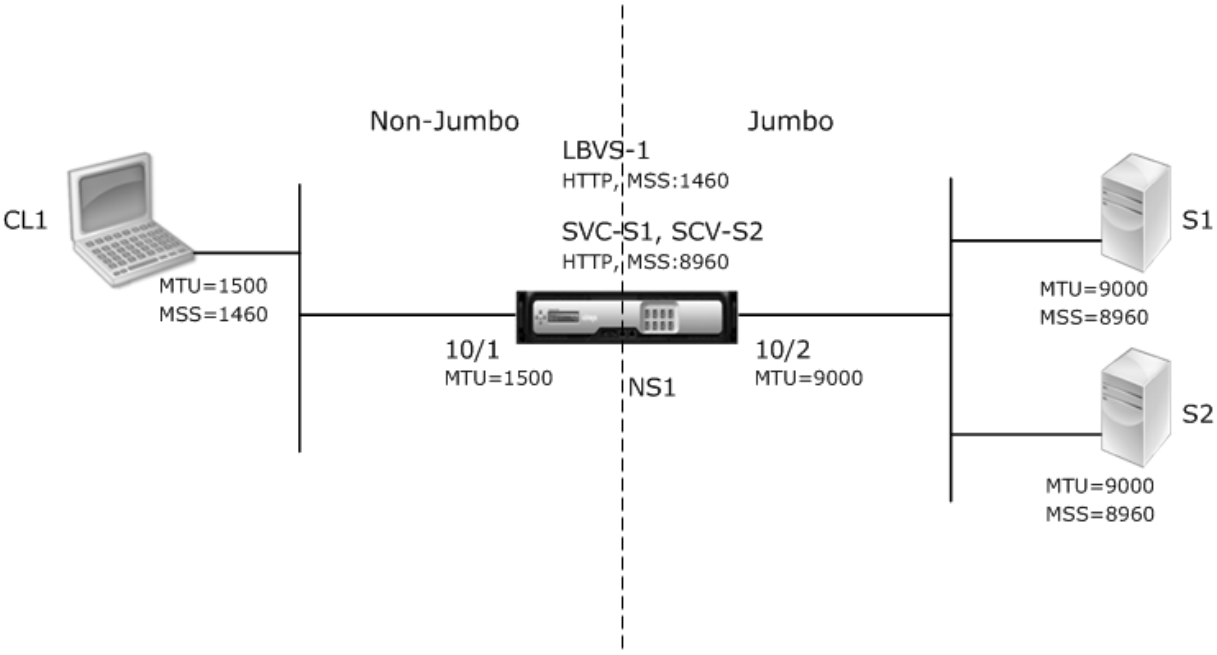
NS1 的接口 10/1 接收或发送来往客户端 CL1 的流量。NS1 的接口 10/2 接收或发送来自服务器 S1 或 S2 的流量。

NS1 的接口 10/1 和 10/2 分别是 VLAN 10 和 VLAN 20 的一部分。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 和服务器之间的巨型帧，接口 10/2 和 VLAN 20 的 MTU 设置为 9000。

NS1 和服务器之间的服务器和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，因此会在每个端点相应设置 MSS 以支持巨型帧：

- 对于 CL1 和 NS1 的虚拟服务器 LBVS1 之间的连接，NS1 上的 MSS 将在 TCP 配置文件中设置，然后该配置文件绑定到 LBVS1。
- 对于 NS1 和 S1 的 SNIP 地址之间的连接，在 TCP 配置文件中设置 NS1 上的 MSS，然后将其绑定到 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
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
NS1 上的 VLAN 10 的 MTU（通过使用 ADC 命令行界面）。		1500
在 NS1 上为 VLAN 20 设置了 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	

实体	名称	详细信息
在 VLAN 10 上对虚拟服务器进行负载平衡	LBVS-1	IP 地址：203.0.113.15；协议：HTTP；端口：80。绑定服务：SVC-S1、SVC-S2；MSS：1460

以下是本示例中 CL1 向 S1 发出的请求的流量：

1. 客户端 CL1 创建一个 200 字节的 HTTP 请求以发送到 NS1 的虚拟服务器 LBVS-1。
2. CL1 打开了与 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，因此 CL1 将请求数据以单个 IP 数据包的形式发送到 NS1。
   1.

```
<div id="concept_57AEA1C9D3DA47948B6D834341388D29__d978e142">

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 的负载平衡算法选择服务器 S1，然后 NS1 在其中一个 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。
6. 由于 S1 的 MSS 大于 HTTP 请求，NS1 将单个 IP 数据包中的请求数据发送到 S1。

   a) 请求数据包的大小 = [IP 标头 + TCP 标头 + [TCP 请求] = [20 + 20 + 200] = 240

以下是本示例中 S1 对 CL1 的响应的通信流：

1. 服务器 S1 创建一个 18000 字节的 HTTP 响应以发送到 NS1 的 SNIP 地址。
2. S1 将响应数据分成多个 NS1 的 MSS，然后将这些数据段以 IP 数据包的形式发送到 NS1。这些 IP 数据包来自 S1 的 IP 地址，并指定到 NS1 的 SNIP 地址。
   - 前两个数据包的大小 = [IP 标头 + TCP 标头 + (TCP 分段 =NS1 的 MSS 大小)] = [20 + 20 + 8960] = 9000
   - 最后一个数据包的大小 = [IP 标头 + TCP 标头 + (剩余的 TCP 数据段)] = [20 + 20 + 2080] = 2120
3. NS1 在接口 10/2 接收响应数据包。
4. 从这些 IP 数据包中，NS1 将所有 TCP 数据段组合起来，构成 18000 字节的 HTTP 响应数据。NS1 会处理此响应。
5. NS1 将响应数据分割为 CL1 的 MSS 的倍数，然后通过 IP 数据包将这些数据段从接口 10/1 发送到 CL1。这些 IP 数据包来自 LBVS-1 的 IP 地址，并注定到 CL1 的 IP 地址。

- 除最后一个数据包之外的所有数据包的大小 = [IP 标头 + TCP 标头 + (TCP 有效负载 =CL1 的 MSS 大小)] = [20 + 20 + 1460] = 1500
- 最后一个数据包的大小 = [IP 标头 + TCP 标头 + (剩余的 TCP 分段)] = [20 + 20 + 480] = 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 **Edit**（编辑）。设置 MTU 值，然后单击 确定。

示例：

设置以下 MTU 值：

- 对于 10/1 接口作为 1500
- 对于 10/2 接口作为 9000

登录 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 并设置所需的 VLAN 的 MTU 以支持巨型帧。	add vlan <id> -mtu <positive_integer>; show vlan <id>	add vlan 10 -mtu 1500; add vlan 20 -mtu 9000
将接口绑定到 VLAN。	bind vlan <id> -ifnum <interface_name>; show vlan <id>	bind vlan 10 -ifnum 10/1; bind vlan 20 -ifnum 10/2
添加一个 SNIP 地址。	add ns ip <IPAddress> <netmask> -type SNIP; show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP
创建表示 HTTP 服务器的服务	add service <serviceName> <ip> HTTP <port>; show service <name>	add service SVC-S1 198.51.100.19 http 80; add service SVC-S2 198.51.100.20 http 80
创建 HTTP 负载平衡虚拟服务器并将服务绑定到该虚拟服务器	add lb vserver <name> HTTP <ip> <port>;bind lb vserver <vserverName> <serviceName>; show lb vserver <name>	add lb vserver LBVS-1 http 203.0.113.15 80; bind lb vserver LBVS-1 SVC-S1
创建自定义 TCP 配置文件并设置其 MSS 以支持巨型帧。	add tcpProfile <name> -mss <positive_integer>; show tcpProfile <name>	add tcpprofile NS1-SERVERS-JUMBO -mss 8960
将自定义 TCP 配置文件绑定到所需的服务。	set service <Name> -tcpProfileName <string>; show service <name>	set service SVC-S1 -tcpProfileName NS1-SERVERS-JUMBO; set service SVC-S2 -tcpProfileName NS1-SERVERS-JUMBO
保存配置	save ns config; show ns config

用例：巨型和非巨型流在同一组接口上共存

举一个在 NetScaler 实例 NS1 上配置负载平衡虚拟服务器 LBVS1 和 LBVS2 的示例。LBVS1 用于对服务器 S1 和 S2 之间的 HTTP 流量进行负载平衡，全局用于在服务器 S3 和 S4 之间对流量进行负载均衡。

CL1 在 VLAN 10 上，S1 和 S2 在 VLAN20 上，CL2 在 VLAN 30 上，S3 和 S4 在 VLAN 40 上。VLAN 10 和 VLAN 20 支持巨型帧，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 之间的连接都支持巨型帧。CL2 和 NS1 之间的连接以及 NS1 与服务器 S3 或 S4 之间的连接仅支持非巨型帧。

NS1 的接口 10/1 接收或发送来自客户端的流量。NS1 的接口 10/2 接收或发送来自服务器的流量。

接口 10/1 作为标记接口同时绑定到 VLAN 10 和 VLAN 20。接口 10/2 作为标记接口同时绑定到 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 的 MTU 设置为 9000，支持巨型帧的 VLAN 30 设置为 VLAN 30。VLAN 20 的 MTU 设置为默认值 1500，如果仅支持非巨型帧，则将 VLAN 40 设置为默认值。

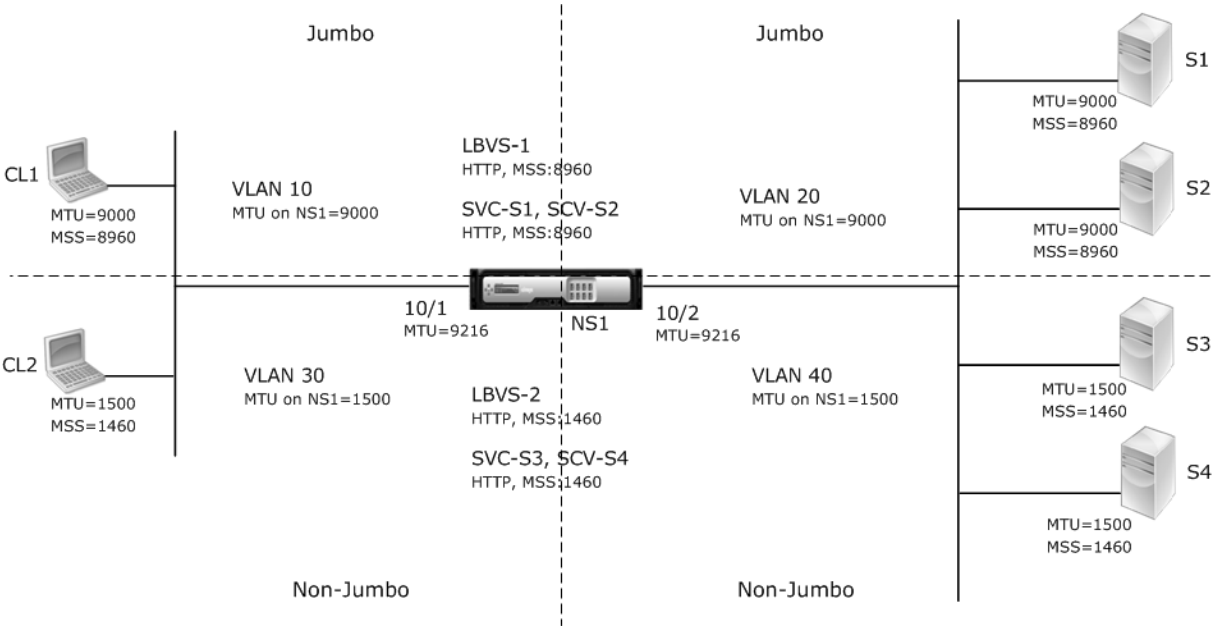
ADC 接口上用于标记为 VLAN 的数据包的有效 MTU 是该接口的 MTU 或 VLAN 的 MTU（以较低者为准）。例如：

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

CL1、S1、S2 以及 CL1 和 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，因此会在每个端点相应设置 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 将在 TCP 配置文件中设置，然后该配置文件绑定到 LBVS1。
- 对于 NS1 和 S1 的 SNIP 地址之间的连接，在 TCP 配置文件中设置 NS1 上的 MSS，然后将其绑定到 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
客户端的 IP 地址	CL1	192.0.2.10
	CL2	192.0.2.20
服务器的 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
为 NS1 上的接口和 VLAN 指定了 MTU	10/1	9216
	10/2	9216
VLAN 10	9000
VLAN 20	9000
VLAN 30	9000
VLAN 40	1500
Default TCP profile	nstcp_default_profile	MSS: 1460
Custom TCP profile	ALL-JUMBO	MSS: 8960
Services on NS1 representing servers	SVC-S1	IP address: 198.51.100.19; Protocol: HTTP; Port: 80; TCP profile: ALL-JUMBO (MSS: 8960)
	SVC-S2	IP address: 198.51.100.20; Protocol: HTTP; Port: 80; TCP profile: ALL-JUMBO (MSS: 8960)
	SVC-S3	IP address: 198.51.101.19; Protocol: HTTP; Port: 80; TCP profile: nstcp_default_profile (MSS: 1460)
	SVC-S4	IP address: 198.51.101.20; Protocol: HTTP; Port: 80; TCP profile: nstcp_default_profile (MSS:

1460)
|Load balancing virtual servers on NS1|LBVS-1|IP address = 203.0.113.15; Protocol: HTTP; Port: 80. Bound services: SVC-S1, SVC-S2; TCP profile: ALL-JUMBO (MSS: 8960)
||LBVS-2|IP address = 203.0.114.15; Protocol: HTTP; Port: 80. 绑定服务：SVC-S3、SVC-S4；TCP 配置文件：nstcp_default_profile（MSS：1460）

以下是 CL1 向 S1 发出的请求的流量：

1. 客户端 CL1 创建一个 20000 字节的 HTTP 请求以发送到 NS1 的虚拟服务器 LBVS-1。
2. CL1 打开了与 NS1 的 LBVS-1 的连接。CL1 和 NS1 在建立连接时交换它们的 TCP MSS 值。
3. 由于 NS1 的 MSS 值小于 HTTP 请求，因此 CL1 将请求数据分割成 NS1 MSS 的倍数，并将这些段标记为 VLAN 10 的 IP 数据包发送到 NS1。
    - 前两个数据包的大小 = [IP 标头 + TCP 标头 + (TCP 分段 =NS1 MSS)] = [20 + 20 + 8960] = 9000
    - 最后一个数据包的大小 = [IP 标头 + TCP 标头 + (剩余的 TCP 数据段)] = [20 + 20 + 2080] = 2120
4. NS1 在接口 10/1 接收这些数据包。NS1 接受这些数据包是因为这些数据包的大小等于或小于带有 VLAN 10 标记的数据包的接口 10/1 的有效 MTU (9000)。
5. 从这些 IP 数据包中，NS1 将所有 TCP 数据段组合起来构成 20000 字节的 HTTP 请求。NS1 正在处理此请求。
6. LBVS-1 的负载平衡算法选择服务器 S1，然后 NS1 在其中一个 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 将请求数据分割成 S1 MSS 的倍数，并将这些段以标记为 VLAN 20 的 IP 数据包发送到 S1。
    - 前两个数据包的大小 = [IP 标头 + TCP 标头 + (TCP 有效负载 =S1 MSS)] = [20 + 20 + 8960] = 9000
    - 最后一个数据包的大小 = [IP 标头 + TCP 标头 + (剩余的 TCP 数据段)] = [20 + 20 + 2080] = 2120

以下是 S1 响应 CL1 的流量：

1. 服务器 S1 创建一个 30000 字节的 HTTP 响应以发送到 NS1 的 SNIP 地址。
2. S1 将响应数据分成多个 NS1 的 MSS，然后将这些数据段以标记为 VLAN 20 的 IP 数据包的形式发送到 NS1。这些 IP 数据包来自 S1 的 IP 地址，并指定到 NS1 的 SNIP 地址。
    - 前三个数据包的大小 = [IP 标头 + TCP 标头 + (TCP 分段 =NS1 的 MSS 大小)] = [20 + 20 + 8960] = 9000
    - 最后一个数据包的大小 = [IP 标头 + TCP 标头 + (剩余的 TCP 分段)] = [20 + 20 + 3120] = 3160
3. NS1 在接口 10/2 接收响应数据包。NS1 接受这些数据包，因为对于带有 VLAN 20 标记的数据包，它们的大小等于或小于接口 10/2 的有效 MTU 值 (9000)。
4. 从这些 IP 数据包中，NS1 汇集所有 TCP 数据段以构成 30000 字节的 HTTP 响应。NS1 会处理此响应。
5. NS1 将响应数据分割为 CL1 的 MSS 的倍数，然后将这些数据段以标记为 VLAN 10 的 IP 数据包的形式从接口 10/1 发送到 CL1。这些 IP 数据包来自 LBVS 的 IP 地址，并注定到 CL1 的 IP 地址。
    - 前三个数据包的大小 = [IP 标头 + TCP 标头 + [(TCP 有效负载 =CL1 的 MSS 大小)] = [20 + 20 + 8960] = 9000
    - 最后一个数据包的大小 = [IP 标头 + TCP 标头 + (剩余的 TCP 分段)] = [20 + 20 + 3120] = 3160

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 **Edit**（编辑）。设置 MTU 值，然后单击 确定。

示例：

设置以下 MTU 值：

- 对于 10/1 接口作为 9216
- 对于 10/2 接口作为 9216

登录 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 并设置所需的 VLAN 的 MTU 以支持巨型帧。	add vlan <id> -mtu <positive_integer>; show vlan <id>	add vlan 10 -mtu 9000;add vlan 20 -mtu 9000;add vlan 30 -mtu 1500;add vlan 40 -mtu 1500
将接口绑定到 VLAN。	bind vlan <id> -ifnum <interface_name>;show vlan <id>	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
添加一个 SNIP 地址。	add ns ip <IPAddress> <netmask> -type SNIP;show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP;add ns ip 198.51.101.18 255.255.255.0 -type SNIP
创建表示 HTTP 服务器的服务。	add service <serviceName> <ip> HTTP <port>;show service <name>	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
创建 HTTP 负载平衡虚拟服务器并将服务绑定到该虚拟服务器	add lb vserver <name> HTTP <ip> <port>; bind lb vserver <vserverName> <serviceName>;show lb vserver <name>	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
		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
创建自定义 TCP 配置文件并设置其 MSS 以支持巨型帧。	add tcpProfile <name> -mss <positive_integer>;show tcpProfile <name>	add tcpprofile ALL-JUMBO -mss 8960
将自定义 TCP 配置文件绑定到所需的负载平衡虚拟服务器和服务。	set service <Name> -tcpProfileName <string>;show service <name>	set lb vserver LBVS-1 - tcpProfileName ALL-JUMBO; set service SVC-S1 - tcpProfileName ALL-JUMBO;set service SVC-S2 - tcpProfileName ALL-JUMBO

|Save the configuration|save ns config; show ns config|

在 **SDX** 设备上配置 **SNMP**

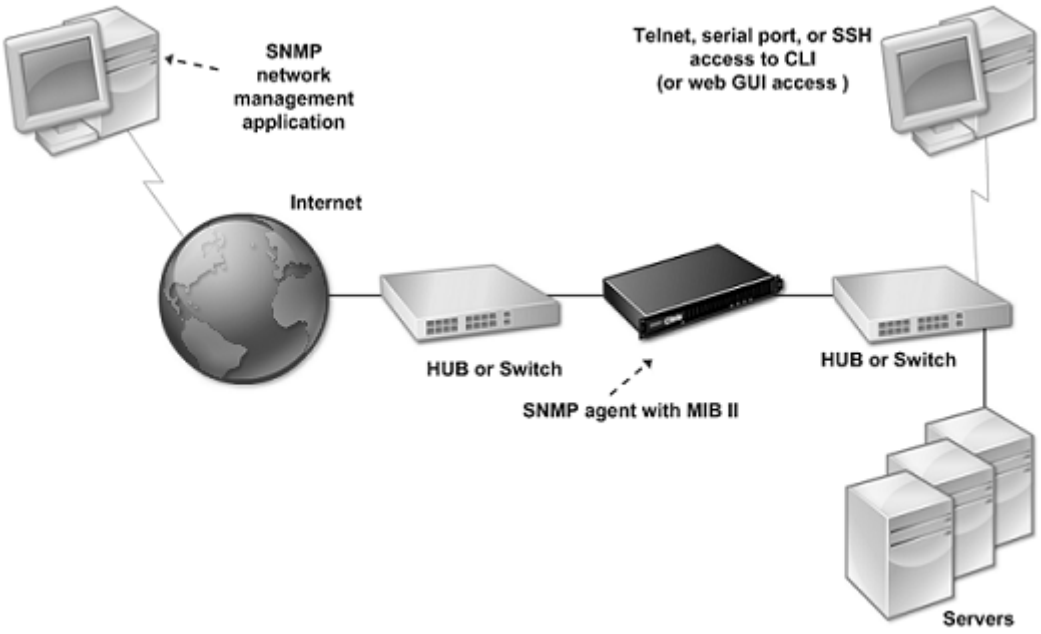
November 23, 2023

您可以在 NetScaler SDX 设备上配置 SNMP 代理以生成异步事件，这些事件称为陷阱。每当 SDX 设备出现异常情况时，就会生成陷阱。然后，这些陷阱被发送到名为 t *rap li*stener 的远程设备，该设备向 SDX 设备上的异常情况发出信号。

除了配置 SNMP 陷阱目的地、下载 MIB 文件和配置一个或多个 SNMP 管理器外，您还可以为 SNMPv3 查询配置 NetScaler SDX 设备。

下图说明了具有启用并配置了 SNMP 的 SDX 设备的网络。在图中，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 代理会生成仅符合 SNMPv2 的陷阱。支持的陷阱可以在 SDX MIB 文件中查看。您可以从 SDX 用户界面的“下载”页面下载此文件。

添加 **SNMP** 陷阱目的地

1. 在配置选项卡的导航窗格中，展开“系统”**>**“**SNMP**”，然后单击“SNMP 陷阱目标”。
2. 在 SNMP 陷阱目的地窗格中，单击添加。

3. 在“配置 SNMP 陷阱目标”页中，指定以下参数的值：

   - 目标服务器-要向其发送 SNMP 陷阱消息的陷阱侦听器的 IPv4 地址。
   - port-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相匹配，否则监听器将丢弃消息。最小值：1。默认值：162。
   - 社区-随陷阱消息一起发送的密码（字符串），以便陷阱侦听器可以对其进行身份验证。可以包含字母、数字和连字符 (-)、句点 (.) 哈希 (#)、空格 ()、at (@)、等于 (=)、冒号 (:) 和下划线 (_) 字符。
     注意：在陷阱侦听器设备上指定相同的团体字符串，否则监听器将丢弃消息。默认值：公开。

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 陷阱目的地”窗格中选择要修改的陷阱目的地，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 陷阱目的地”窗格中选择要删除的陷阱目的地，然后单击“删除”。在“确认”消息框中，单击以删除 SNMP 陷阱目标。

正在下载 **MIB** 文件

在开始监视 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。

该文件包括提供特定于 SDX 的事件的 NetScaler 企业 MIB。

下载 **MIB** 文件

1. 登录 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，以查询和监视设备上托管的装置和受管设备。此外，您必须向 SNMP 管理器提供所需的特定于设备的信息。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，则必须添加一个将 SNMP 管理器的主机名解析为其 IP 地址的 DNS 名称服务器。

至少配置一个 SNMP 管理器。如果未配置 SNMP 管理器，则设备不会接受或响应来自网络上任何 IP 地址的 SNMP 查询。如果配置一个或多个 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”选项卡的导航窗格中，展开“系统”，然后展开“SNMP”。
2. 单击“管理员”。

3. 在详细信息窗格中，单击 Add（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，则必须添加一个将 SNMP 管理器的主机名解析为其 IP 地址的 DNS 名称服务器。
    - 团体—SNMP 团体字符串。可以包含 1 到 31 个字符，包括大写和小写字母、数字、连字符 (-)、句点 (.) 磅 (#)、at (@)、等于 (=)、冒号 (:) 和下划线 (_) 字符。
    - 选中 启用管理网络 复选框以使用子网掩码指定 SNMP 管理器。
    - 在“网络掩码”字段中，输入 SNMP 团体的子网掩码。

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、数据来源验证、消息及时性检查和数据机密性。

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

- SNMP 视图
- SNMP 用户

这些实体协同工作以实现 SNMPv3 安全功能。创建视图是为了允许访问 MIB 的子树。

添加 **SNMP** 管理器

配置 SDX 设备以允许相应的 SNMP 管理器对其进行查询。还要向 SNMP 管理器提供所需的特定于设备的信息。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，则必须添加一个将 SNMP 管理器的主机名解析为其 IP 地址的 DNS 名称服务器。

至少配置一个 SNMP 管理器。如果未配置 SNMP 管理器，则设备不会接受或响应来自网络上任何 IP 地址的 SNMP 查询。如果配置一个或多个 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。

要配置 **SNMP** 管理器，请执行以下操作：

1. 导航到 系统 **>** 配置 页面。
2. 在“配置”选项卡的导航窗格中，展开“系统”，然后展开“SNMP”。
3. 单击“管理员”。
4. 在详细信息窗格中，单击 Add（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，则必须添加一个将 SNMP 管理器的主机名解析为其 IP 地址的 DNS 名称服务器。

- 团体—SNMP 团体字符串。可以包含 1 到 31 个字符，包括大写和小写字母、数字、连字符 (-)、句点 (.) 磅 (#)、at (@)、等于 (=)、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 视图用于实现访问控制。

配置视图

1. 在“配置”选项卡的导航窗格中，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 Add（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、连字符 (-)、句点 (.) 磅 (#)、at (@)、等于 (=)、冒号 (:) 和下划线 (_) 字符。选择有助于识别 SNMPv3 视图的名称。
   - 子树-要与此 SNMPv3 视图关联的 MIB 树的特定分支（子树）。将子树指定为 SNMP OID。
   - 类型 (Type)-在此视图中或从该视图中包括或排除由子树参数指定的子树。如果在 SNMPv3 视图中包含了子树（如 A），并且想要从 SNMPv3 视图中排除 A 的特定子树（如 B），则此设置非常有用。

配置 **SNMP** 用户

创建 SNMP 视图后，请添加 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”选项卡的导航窗格中，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 Add（添加）。
4. 在“创建 SNMP 用户”页中，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、连字符 (-)、句点 (.) 磅 (#)、at (@)、等于 (=)、冒号 (:) 和下划线 (_) 字符。
   - 安全级别-设备与 SNMPv3 用户之间的通信所需的安全级别。选择以下选项之一：
     - noAuthNoPriv —既不需要身份验证也不需要加密。
     - authNoPriv—需要身份验证但不需要加密。
     - authPriv—需要身份验证和加密。

- 身份验证协议-设备和 SNMPv3 用户用于对他们之间的通信进行身份验证的身份验证算法。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-身份验证算法要使用的密码短语。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 (.) 磅 (#)、空格 ()、at (@)、等于 (=)、冒号 (:) 和下划线 (_) 字符。
- 隐私协议-设备和 SNMPv3 用户用于加密他们之间的通信的加密算法。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 用户可以以 INCLUDED 类型访问绑定到此 SNMPv3 视图的子树，但无法访问类型为 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。当满足为 SNMP 警报设置的条件时，设备会生成 SNMP 陷阱消息，这些消息将发送到已配置的陷阱侦听器。例如，启用 deviceAdded 警报后，只要在设备上配置了设备（实例），就会生成一条陷阱消息并将其发送到陷阱侦听器。您可以为 SNMP 警报分配严重级别。执行此操作时，相应的陷阱消息将分配给该严重性级别。

以下是设备上定义的严重性级别（按严重性递减顺序排列）：

- 严重
  - 重大
- 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”严重性级别，则会为添加设备时生成的陷阱消息分配警告严重性级别。

您还可以配置 SNMP 警报，以便在满足该警报上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 系统 **> SNMP >** 警报。

配置系统日志通知

November 23, 2023

SYSLOG 是一种标准的日志记录协议。它有两个组件：在 NetScaler SDX 设备上运行的 SYSLOG 审计模块和可以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中之前对其进行过滤。SYSLOG 服务器可以从多个 SDX 设备接收日志信息，SDX 设备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的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

可以使用此信息分析警报来源并在需要时采用纠正措施。首先配置设备向其发送日志信息的 syslog 服务器，然后指定用于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”**>**“系统日志服务器”。
2. 在详细信息窗格中，单击“添加”。
3. 在“创建 **Syslog** 服务器”页中，指定 syslog 服务器参数的值。有关参数的描述，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”**>**“系统日志服务器”。
2. 在详细信息窗格中，单击 **Syslog** 参数。
3. 在“配置 **Syslog** 参数”页中，指定日期和时间格式。
4. 单击“确定”，然后单击“关闭”。

配置邮件通知

November 23, 2023

将 SMTP 服务器配置为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“电子邮件服务器”选项卡，然后单击“添加”。
3. 在“创建电子邮件服务器”页中，指定服务器参数的值。

- 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。
- 端口：输入端口号。默认值为 25。
- 身份验证：选择此选项可验证对电子邮件服务器的访问权限。
- 安全：选择此选项可创建安全的电子邮件连接。默认情况下，使用 TLS 1.2 来加密电子邮件通信。

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“电子邮件”选项卡，然后单击“添加”。
3. 在“创建电子邮件通讯组列表”页面中，为参数指定值。有关参数的描述，请将鼠标悬停在相应字段上。
4. 单击 **Create**（创建）。

配置短信通知

November 23, 2023

将短消息服务 (SMS) 服务器配置为在每次发出警报时接收 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的地址。

配置 **SMS** 服务器

1. 导航到 **System**（系统）**> Notifications**（通知）**> SMS**。
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”。

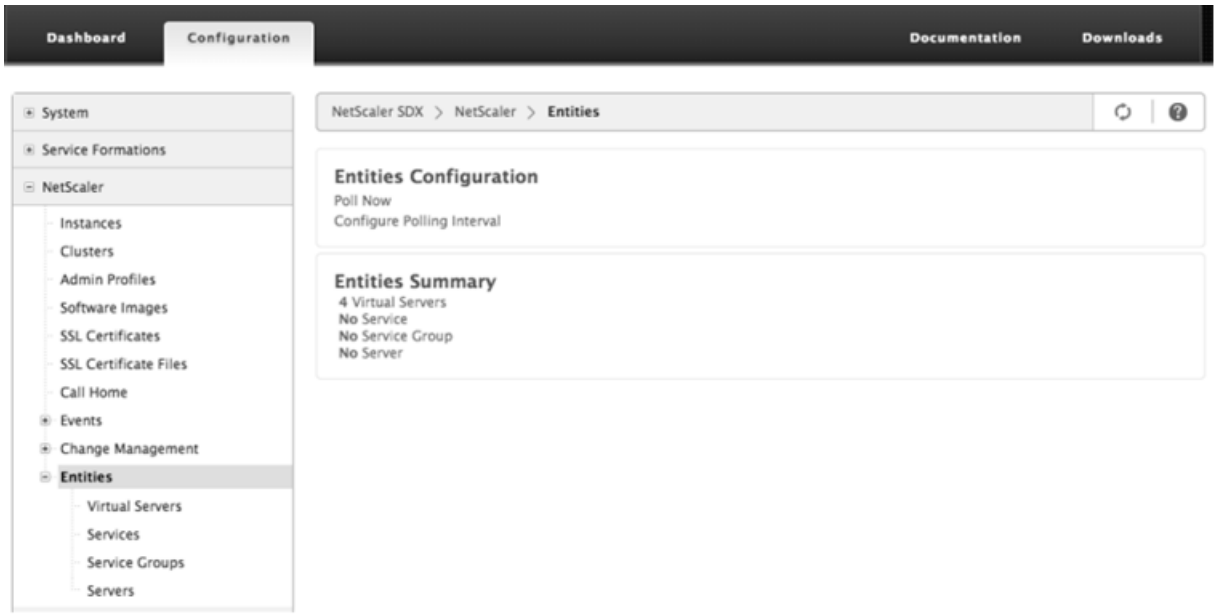
配置 **SMS** 配置文件

1. 导航到 **System**（系统）**> Notifications**（通知）**> SMS**。
2. 在详细信息窗格中，单击 **SMS** 通讯组列表，然后单击 添加。
3. 在“创建 **SMS** 通讯组列表”页中，指定邮件配置文件参数的值。有关参数的描述，请将鼠标悬停在相应字段上。
4. 单击“创建”，然后单击“关闭”。

监视和管理 **SDX** 设备上配置的实体的实时状态

February 16, 2024

NetScaler SDX 设备可以监视和管理 SDX 设备上托管的虚拟设备上的虚拟服务器、服务、服务组和服务器的状态。您可以监视值，例如虚拟服务器的运行状况以及自服务或服务组上次状态更改以来经过的时间。这种监视使您可以查看实体的实时状态，当您在 NetScaler 实例上配置了许多实体时，可以轻松管理这些实体。



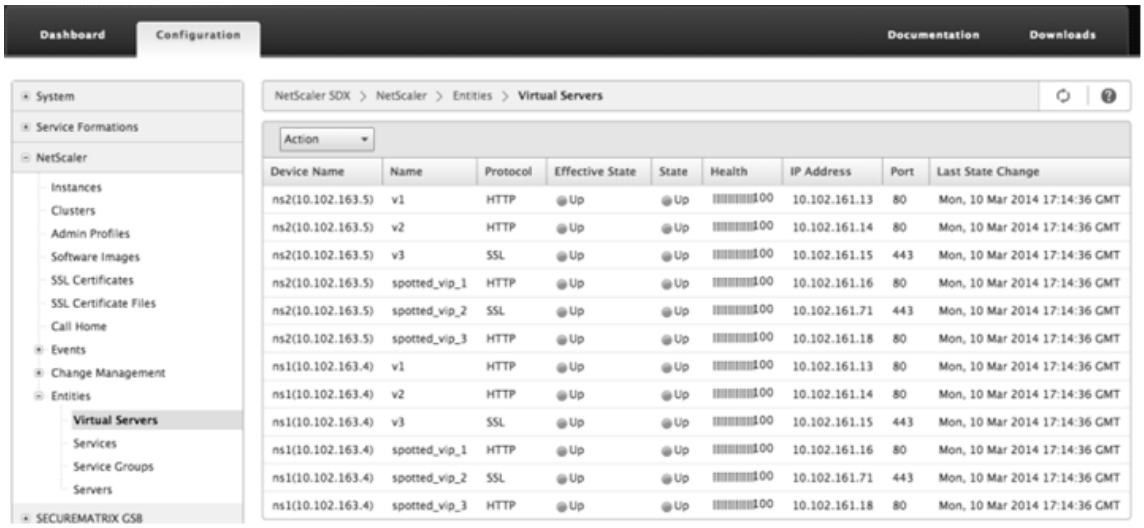
查看虚拟服务器的状态

您可以监视虚拟服务器的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，例如虚拟服务器的名称、IP 地址和类型。

- 查看虚拟服务器的状态

  1. 在配置选项卡的导航窗格中，单击 **NetScaler >** 实体 **>** 虚拟服务器。
  2. 在右窗格中的“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-虚拟服务器的有效状态，基于备份虚拟服务器的状态。例如，向上、向下或停止服务。
     - 状态-虚拟服务器的当前状态。例如，向上、向下或停止服务。
     - 运行状况-处于 UP 状态且绑定到虚拟服务器的服务的百分比。以下公式用于计算运行状况百分比：（绑定服务数量 x 100）/绑定服务总数
     - IP 地址-虚拟服务器的 IP 地址。客户端向此 IP 地址发送连接请求。

- 端口—虚拟服务器侦听客户端连接的端口。
- 上次状态更改—自上次更改虚拟服务器状态以来经过的时间（以天、小时、分钟和秒为单位）。也就是说，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 版及更高版本上配置的虚拟服务器。

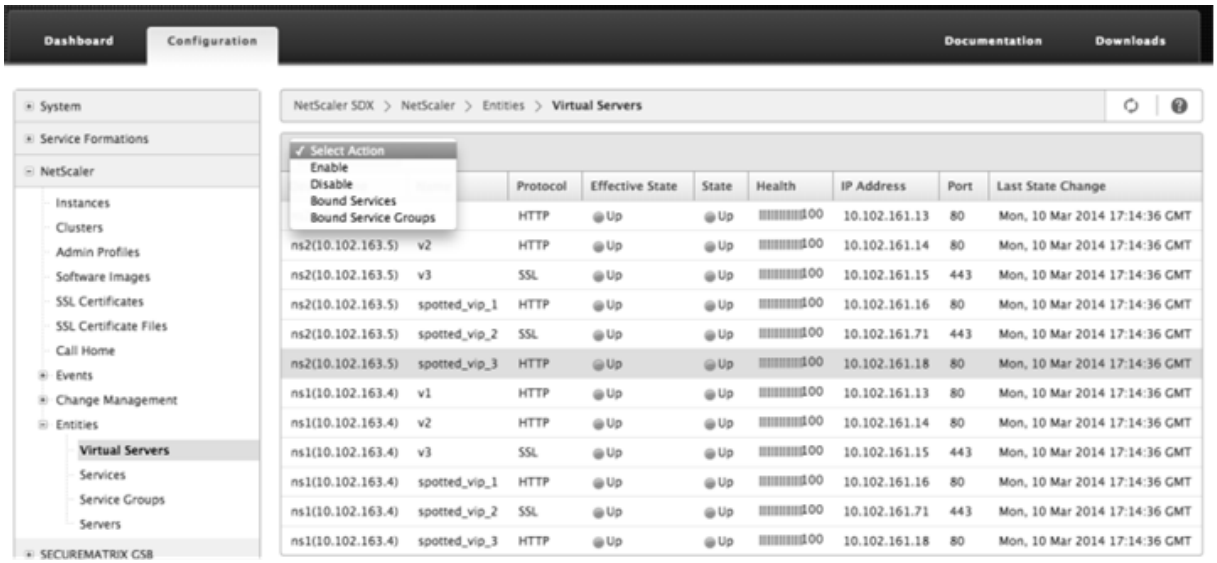


- 查看绑定到虚拟服务器的服务和服务组

  您可以监视绑定到虚拟服务器的服务和服务组的实时状态。通过此监视，您可以检查可能导致虚拟服务器运行状况百分比变低的服务的状态，以便采取适当的措施。

  查看绑定到虚拟服务器的服务和服务组

  1. 在配置选项卡的左侧窗格中，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，单击要为其显示绑定服务和服务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。



查看服务的状态

您可以监视服务状态的实时值以及服务处于当前状态的持续时间。

查看虚拟服务器的状态

1. 在配置选项卡的导航窗格中，单击 **NetScaler >** 实体 **>** 服务。
2. 在详细信息窗格的服务下，查看以下统计信息：

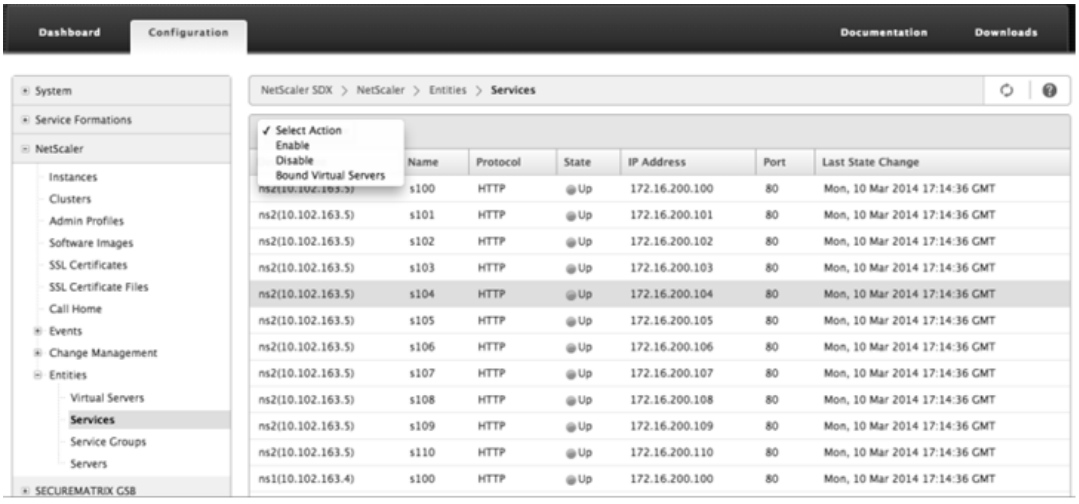
   - 设备名称-配置服务的设备的名称。
   - 名称-服务的名称。
   - 协议-服务类型，用于确定服务的行为。例如，HTTP、TCP、UDP 或 SSL。
   - 状态-服务的当前状态。例如，向上、向下或停止服务。
   - IP 地址-服务的 IP 地址。
   - 端口-服务侦听的端口。
   - 上次状态更改—自上次更改服务状态以来经过的时间（以天、小时、分钟和秒为单位）。也就是说，服务处于当前状态的持续时间。

- 查看服务绑定到的虚拟服务器

  您可以查看服务绑定到的虚拟服务器，并监视虚拟服务器的实时状态。

  查看服务绑定到的虚拟服务器

  1. 在配置选项卡的导航窗格中，单击 **NetScaler >** 实体 **>** 服务。
  2. 在详细信息窗格的服务下，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。



查看服务组的状态

您可以通过 SDX 界面监视服务组成员的实时状态。

查看服务组的状态

1. 在配置选项卡的导航窗格中，单击 **NetScaler >** 实体 **>** 服务组。
2. 在详细信息窗格的服务组下，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，用于确定服务组的行为。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，向上、向下或停止服务
    - 状态-服务组的有效状态，基于服务组成员的状态。例如，向上、向下或停止服务。
    - 上次状态更改-自上次更改服务组成员状态以来经过的时间（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持续时间。此信息仅适用于在 NetScaler 9.0 版及更高版本上配置的服务组成员。

- 查看服务绑定到的虚拟服务器

  您可以查看服务绑定到的虚拟服务器，并监视虚拟服务器的实时状态。

  查看服务绑定到的虚拟服务器

  1. 在配置选项卡的左侧窗格中，单击 **NetScaler >** 实体 **>** 服务器。
  2. 在右窗格的“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，右键单击该服务，然后单击绑定虚拟服务器。

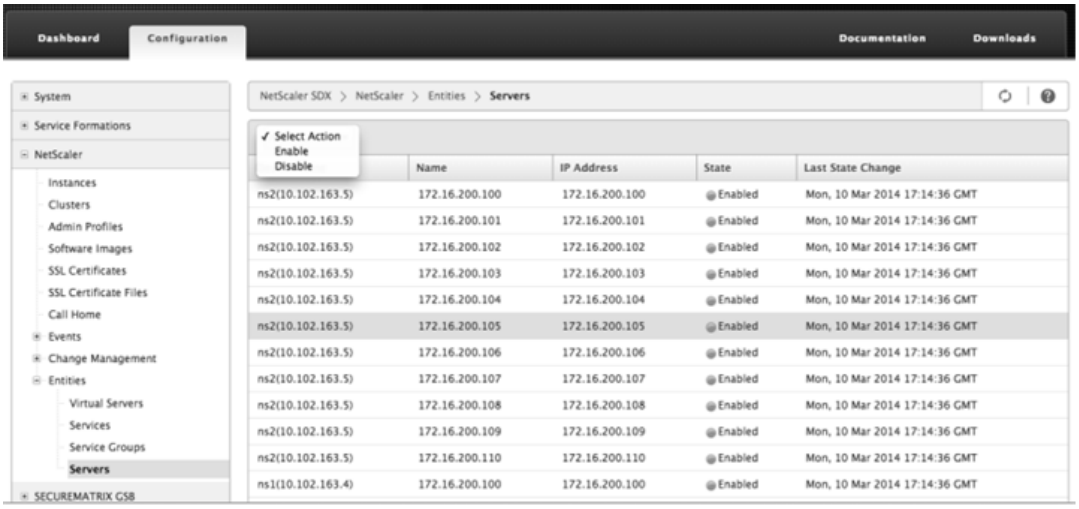
查看服务器的状态

您可以监视和管理 NetScaler 实例中的服务器状态。通过这种监视，您可以查看服务器的实时状态，并在拥有许多服务器时轻松管理这些服务器。

查看服务器的状态

1. 在配置选项卡的导航窗格中，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。客户端向此 IP 地址发送连接请求。
    - 状态：指定服务器的当前状态。例如，向上、向下和停止服务。
    - 上次状态更改：指定自上次更改服务器状态以来经过的时间（以天、小时、分钟和秒为单位）。也就是说，服务器处于当前状态的持续时间。



配置轮询间隔

您可以设置希望 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，键入要设置为 SDX 必须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。

监视和管理在 **NetScaler** 实例上生成的事件

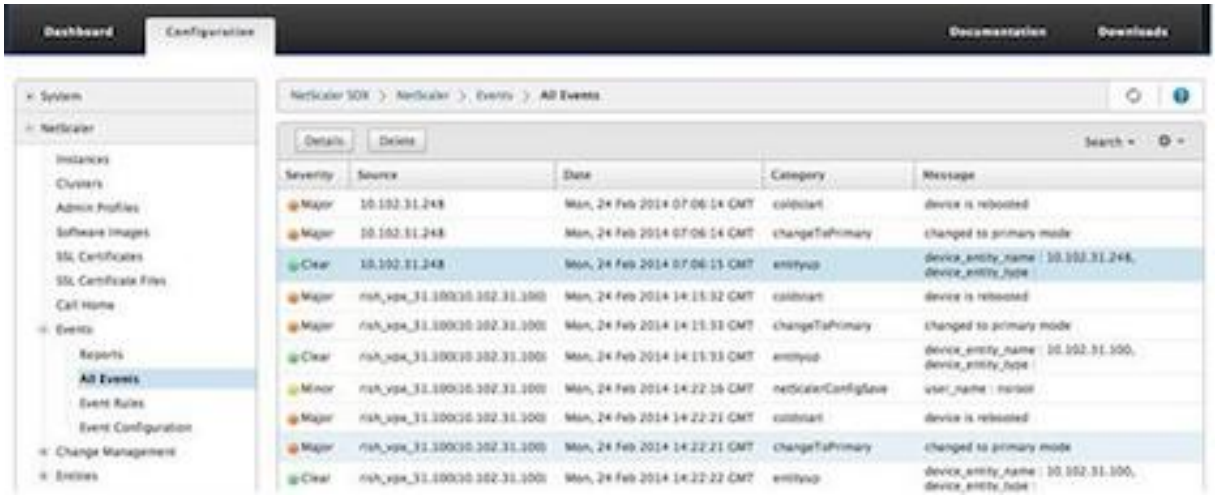
February 16, 2024

使用事件功能监视和管理 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 实例的有效运行。您还可以配置事件规则以筛选生成的事件，并获得对筛选的事件列表采取操作的通知。

查看所有活动

您可以查看在 NetScaler SDX 设备上配置的 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、来源和消息。

要查看事件，请导航到“配置”**>**“**NetScaler**”**>**“事件”**>**“所有事件”。



通过选择事件并单击详细信息按钮，可以查看事件历史记录和实体 详细信息。您也可以搜索特定事件或将其从此页面中删除。

注意：删除事件后，将无法恢复它们。

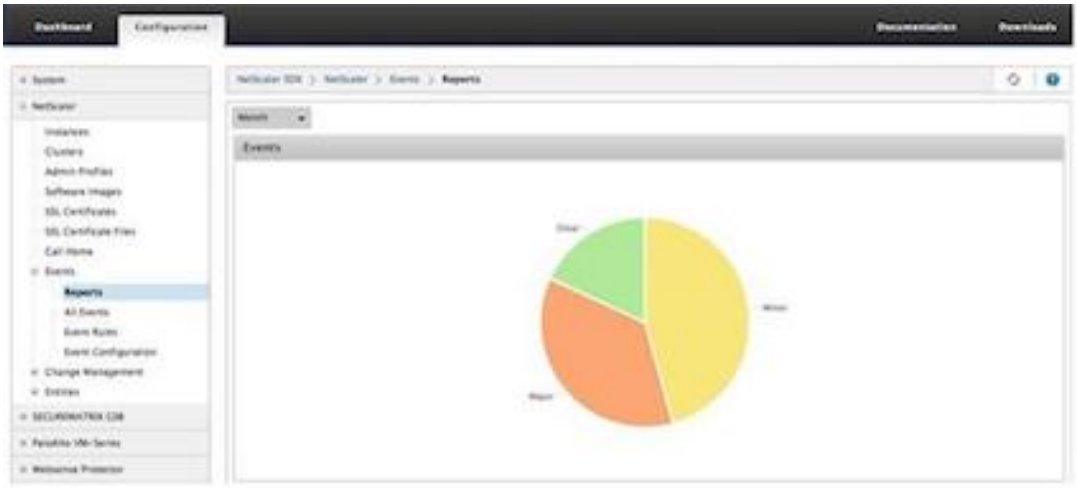
- 查看报告

  “报告”页面以图形格式显示事件摘要。您的报告视图可以基于不同的时间尺度。默认情况下，时间尺度为 Day。

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

  - 事件

    “事件”报告以饼图形式表示事件的数量，并根据事件的严重性进行分段和颜色编码。

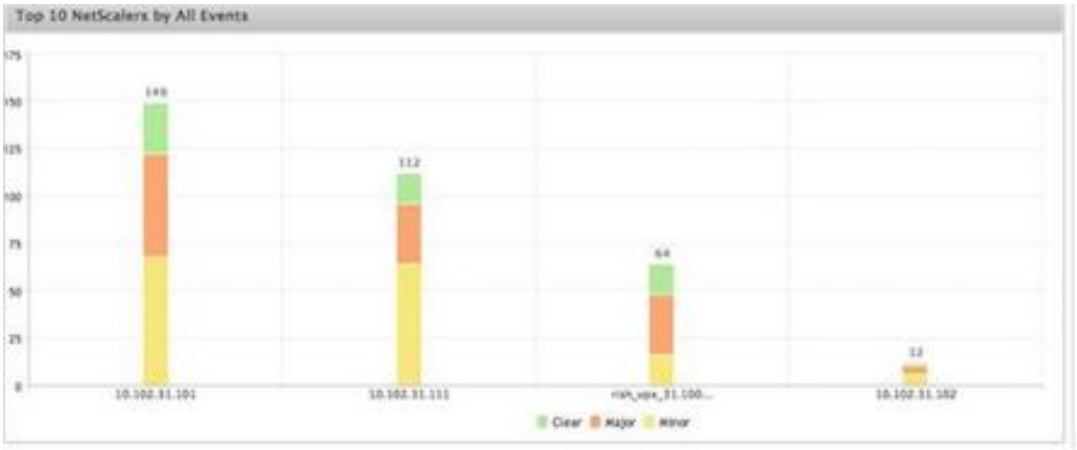


    要查看特定严重性的事件的详细信息，请单击饼图的相应部分，即可查看以下详细信息：

    * 来源：系统名称、主机名或生成事件的 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：事件的描述。

– 按所有事件排列的前 **10** 个 **NetScaler** 实例

此报告是一个条形图，它根据所选时间范围内的事件数显示前 10 个 NetScaler 实例。



– 按实体状态变更事件排列的前 **10** 个 **NetScaler** 实例

此报告是一个条形图，它根据所选时间范围内的实体状态更改次数显示前 10 个 NetScaler 实例。实体状态更改反映实体启动、实体关闭或停止服务事件。

– 按阈值违规事件排列的前 **10** 个 **NetScaler** 实例

此报告是一个条形图，它根据所选时间范围内的阈值违规事件数量显示前 10 个 NetScaler 实例。阈值违规事件反映了以下事件：

* cpuUtilization
* memoryUtilization
* diskUsageHigh
* temperatureHigh
* voltageLow
* voltageHigh
* fanSpeedLow
* temperatureCpuHigh

  * interfaceThroughputLow
  * interfaceBWUseHigh
  * aggregateBWUseHigh

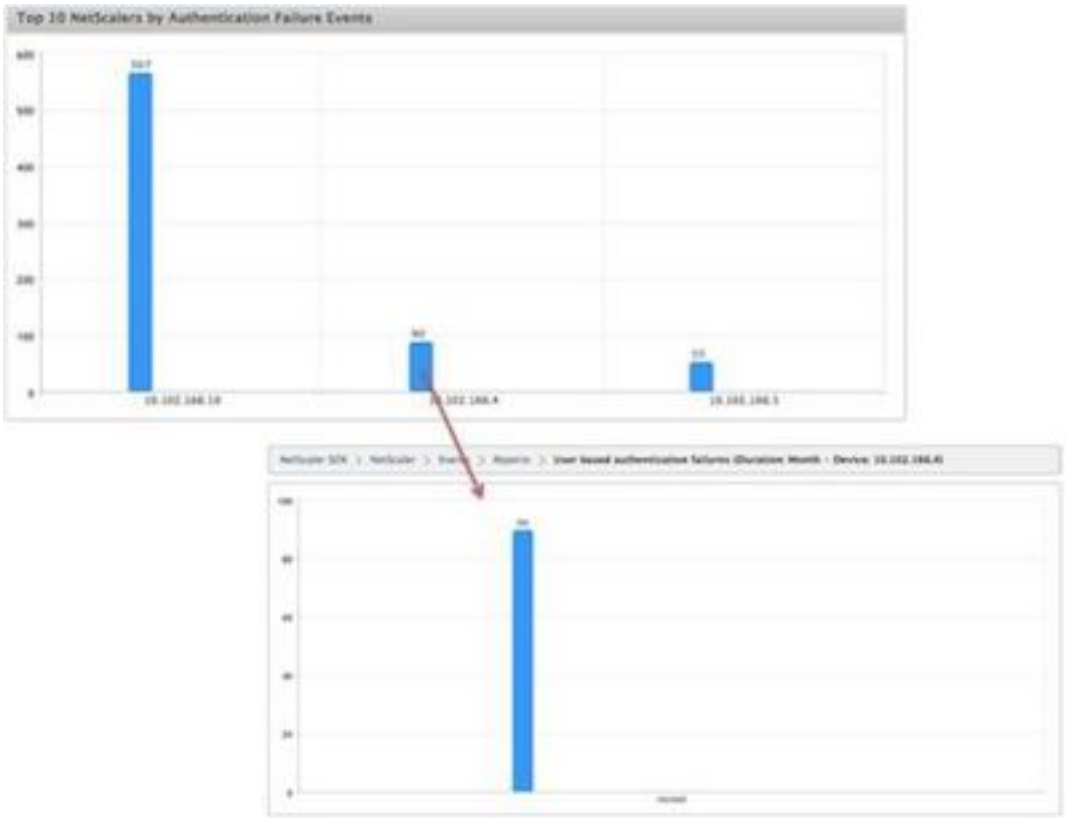
- 按硬件故障事件排列的前 **10** 个 **NetScaler** 实例
  此报告是一个条形图，根据所选时间范围内的硬件故障事件数显示前 10 个 NetScaler 实例。硬件故障事件反映了以下事件：
  * hardDiskDriveErrors
  * compactFlashErrors
  * powerSupplyFailed
  * “sslCardFailed”

- 按配置变更事件排列的前 **10** 个 **NetScaler** 实例

  此报告是一个条形图，它根据所选时间范围内的配置更改事件数量反映了前 10 个 NetScaler 实例。您可以单击图表向下钻取并查看实例基于用户的配置更改。通过单击此图表，您可以进一步查看授权和执行状态的详细信息。

- < 按身份验证失败事件排列的前 **10** 个 **NetScaler** 实例

  此报告是一个条形图，根据所选时间范围内的身份验证失败事件数显示前 10 个 NetScaler 实例。您可以单击图表深入查看实例的基于用户的身份验证失败。



- 配置事件规则

  可以通过为规则配置特定条件及为规则分配操作来过滤一组事件。当生成的事件符合规则中的筛选条件时，将执行与规则关联的操作。您可以为其创建过滤器的条件包括：严重性、设备、故障对象和类别。

  可以为事件分配以下操作：

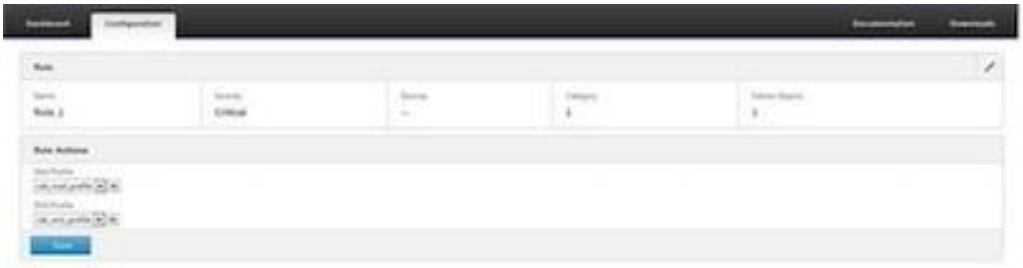
  - 发送电子邮件操作 针对符合筛选条件的事件发送电子邮件。
  - 发送 **SMS** 操作 为符合筛选条件的事件发送短消息服务 (SMS)。

  添加事件规则

  1. 导航到“配置”**>**“**NetScaler**”**>**“事件”**>**“事件规则”，然后单击“添加”。
  2. 在“规则”页面上，设置以下参数：
     - Name（名称）- 事件规则的名称。
     - Enabled（启用）- 启用事件规则。
     - Severity（严重性）- 要为其添加事件规则的事件的严重性。
     - 设备-您要为其定义事件规则的 NetScaler 实例的 IP 地址。
     - Category（类别）- NetScaler 实例生成的事件的类别。
     - Failure Objects（失败对象）- 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证书相关事件的证书名称。

3. 单击保存。
4. 在“规则操作”下，您可以为事件分配通知操作。
   a) Mail Profile（邮件配置文件）- 邮件服务器和邮件配置文件详细信息。当事件满足定义的过滤条件时，将触发电子邮件。
   b) SMS Profile（SMS 配置文件）- SMS 服务器和 SMS 配置文件详细信息。当事件满足定义的过滤条件时，将触发短信。

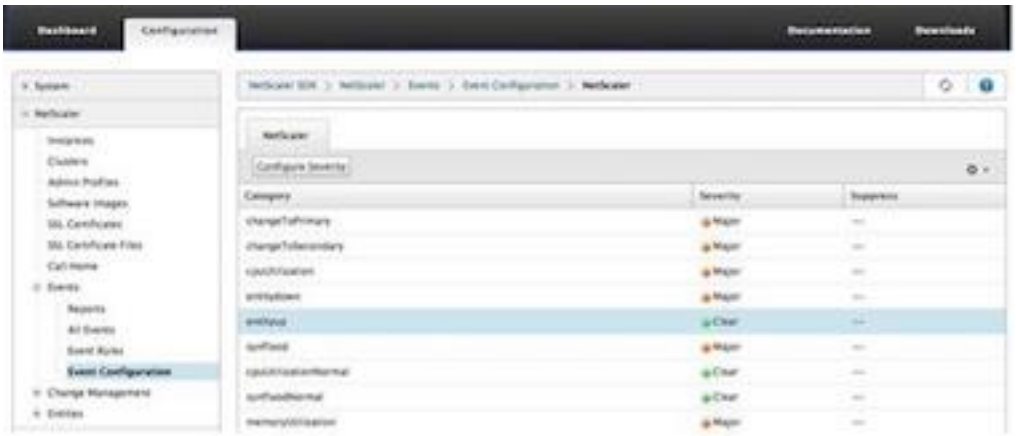


5. 单击 Done（完成）。

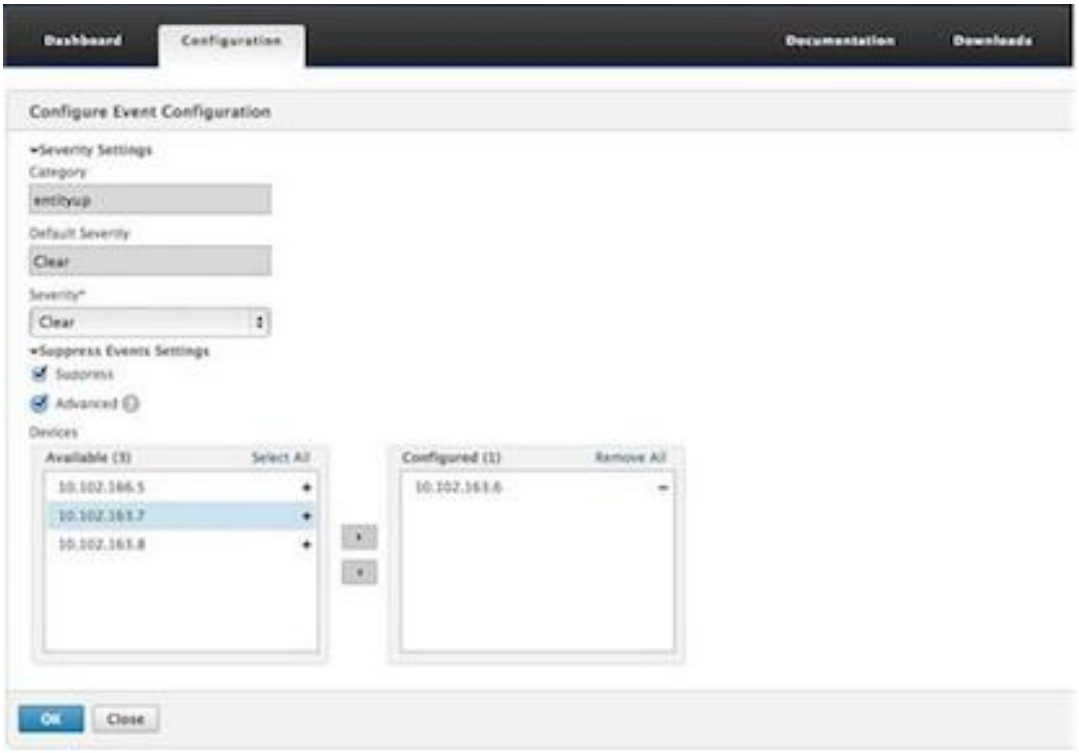
- 配置事件

  您可以为在 SDX 设备上为 NetScaler 实例生成的事件分配严重性级别。您可以定义以下类型的严重性级别：严重、主要、次要、警告、清除和信息。您还可以在特定时间内禁止这些事件。
  要配置严重性：

  1. 导航到“配置”**>**“**NetScaler**”**>**“事件”**>**“事件配置”，从列表中选择事件，然后单击“配置严重性”。



  2. 在“配置事件配置”页面上，从下拉列表中选择所需的严重性级别。
  3. 或者，您可以通过选中抑制复选框来隐藏事件。您也可以使用“高级”选项指定要抑制此事件的 NetScaler 实例。



4. 单击确定。

SDX 设备上的 NetScaler 实例的 Call Home 支持

February 16, 2024

Call Home 功能会监视您的 NetScaler 实例是否存在常见的错误情况。现在，您可以从管理服务用户界面配置、启用或禁用 NetScaler 实例上的 Call Home 功能。

注意：设备 上出现预定义的错误情况时，必须先在 Citrix 技术支持服务器上注册 NetScaler 实例，然后 Call Home 才能将系统数据上载到服务器。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

  您可以通过管理服务在 NetScaler 实例上启用 Call Home 功能。当您启用 Call Home 功能时，Call Home 流程会向 Citrix 技术支持服务器注册 NetScaler 实例。注册需要一些时间才能完成。在此期间，管理服务将显示注册进度。

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

  要禁用 Call Home 功能，请导航到 配置 **> 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”。

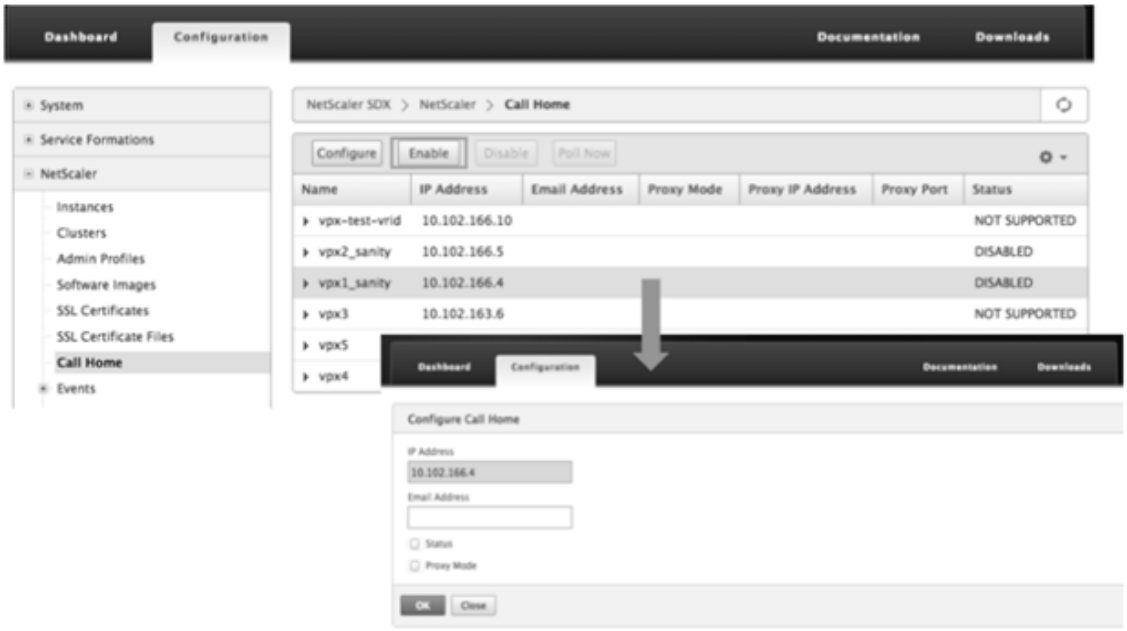
如果启用 Call Home，则可以配置以下选项：

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，并将其存储在该位置，以备将来有关 Call Home 的通信之用。
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 实例的数据上载到 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）的所有流量都是通过 SSL 和加密的，因此数据安全和隐私不会受到损害。

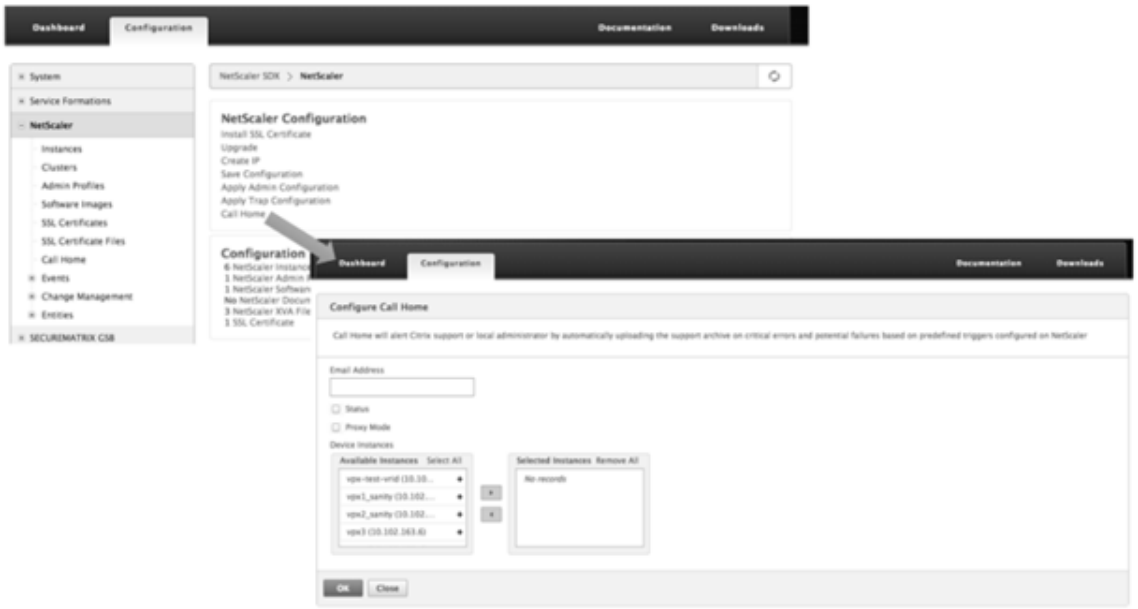
- 通过管理服务在 NetScaler 实例上配置 Call Home

  您可以在单个实例上配置 Call Home 功能，也可以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 配置 **> NetScaler > Call Home**，选择 NetScaler 实例，然后单击“配置”按钮。在“配置 Call Home”中，单击“确定”。



要在多个 NetScaler 实例上配置 Call Home 功能，请导航到配置 **> NetScaler**。在右窗格中，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”。



– 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**”，然后单击“立即轮询”。在确认页面上，单击“是”。

系统运行状况监视

November 23, 2023

系统运行状况监视会检测受监视组件中的错误，以便您可以采取纠正措施来避免故障。在 NetScaler SDX 设备上监视以下组件：

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

在“监视”选项卡中，单击“系统运行状况”。此时将显示所有组件的摘要。要查看受监视组件的详细信息，请展开“系统运行状况”，然后单击要监视的组件。

- 监视 SDX 设备上的资源

  您可以监视 SDX 设备上的硬件和软件组件，并在必要时采取纠正措施。若要查看监视的组件，请在“监视”选项卡中展开“系统运行状况”，然后单击“资源”。此时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，除了 BMC 固件版本外，当前值和预期值将显示为不适用 (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（状况）。对于
  硬件和 BMC 固件版本，ERROR 表示与预期值的偏差。对于对 Citrix Hypervisor 的调用，错误表示管理服务无法使用 API、HTTP、PING 或 SSH 调用与 Citrix Hypervisor 进行通信。对于
  运行状况监视器插件，ERROR 表示插件未安装在 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。

监视 **SDX** 设备上的存储资源

您可以监视 SDX 设备上的磁盘，并在必要时采取纠正措施。要查看监视的组件，请在“监视”选项卡中展开“系统运行状况”，然后单击“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（磁盘），将显示以下详细信息：

- 名称 物理磁盘的名称。
- 大小：磁盘的大小，以 GB 为单位。
- 已使用：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。这个数字是从 `iostat` 输出中读取的。
- 块读/秒：每秒读取的块数。您可以使用此值来测量磁盘的输出速率。
- 写入的块数：每秒写入的块数。您可以使用此值来测量磁盘的输入速率。
- 读取的总块数：自设备上次启动以来读取的块数。
- 写入的总块数：自设备上次启动以来写入的块数。

对于虚拟磁盘或分区（存储库），将显示以下详细信息：

- 驱动器托架：驱动器托架中的驱动器编号。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（状况）。可能的值：
  - GOOD：驱动器状态良好，可以使用。
  - FAIL：驱动器出现故障，必须更换。
  - MISSING：驱动器托架中未检测到驱动器。
  - UNKNOWN：驱动器托架中存在一个新的未格式化的驱动器。
- 名称：系统定义的存储库名称。
- 大小：存储库的大小（以 GB 为单位）。
- 已使用：存储库中的数据量（以 GB 为单位）。

监视 **SDX** 设备上的硬件传感器

您可以监视 SDX 设备上的硬件组件，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“硬件传感器”。监视功能显示有关不同风扇的速度、不同组件的温度和电压以及电源状态的详细信息。

对于风扇转速，将显示以下详细信息：

- 名称：风扇的名称。
- 状态：风扇的状态（状况）。ERROR 表示偏离预期值。NA 表示风扇不存在。
- 当前值 **(RPM)**：每分钟的当前旋转次数。

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（状况）。ERROR 表示当前值超出范围。
- 当前值（摄氏度）：组件的当前温度（以度为单位）。

电压信息包括以下详细信息：

- 名称：组件的名称，例如 CPU 内核。
- 状态：组件的状态（状况）。ERROR 表示当前值超出范围。
- 电流值（**Volts**）：元件上存在的电流电压。

有关电源的信息包括以下详细信息：

- 名称：组件的名称。
- 状态：组件的状态（状况）。可能的值：
  - 错误：只有一个电源已连接或工作正常。
  - 正常：两个电源均已连接，并且工作正常。

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”。监视函数详细说明每个接口的以下信息：

- 接口： SDX 设备上的接口号。
- 状态：接口的状态。可能的值：UP, DOWN。
- 分配的虚拟功能/总数：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。
- **Tx** 数据包：自设备上次启动以来传输的数据包数。
- **Rx** 数据报：自上次启动设备以来收到的数据包数。
- **Tx** 字节：自设备上次启动以来传输的字节数。
- **Rx** 字节：自上次启动设备以来接收的字节数。
- **Tx** 错误：自上次启动设备以来传输数据的错误数。
- **Rx** 错误：自上次启动设备以来接收数据的错误数。

配置系统通知设置

November 23, 2023

您可以发送通知，以便与选定的用户组就许多与系统相关的功能进行通信。您可以在 SDX Management Service 中设置通知服务器，以配置电子邮件和短信服务 (SMS) 网关服务器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 版后，系统会为所有事件类别启用系统通知，并将通知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”页中，输入以下详细信息：
   - 类别—SDX Management Service 生成的事件的类别。
   - 电子邮件**-** 从下拉菜单中选择电子邮件分发列表。您还可以通过单击“**+** ”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通讯组列表。
   - **SMS**（短信） -从下拉菜单中选择 SMS 分发列表。您还可以通过单击 **+** 图标并在相应字段中输入新的 SMS 服务器详细信息来创建新的 SMS 通讯组列表。
3. 单击“确定”。

启用和禁用管理服务的功能

November 23, 2023

> 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 实例以进行操作，例如 SSL 证书、网络功能和配置审计。根据您的要求，可以使用选项来启用或禁用此轮询。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 启用 或 禁用。

配置管理服务

November 23, 2023

管理服务允许您管理客户端会话和执行配置任务，例如创建和管理用户帐户以及根据需要调整备份和修剪策略。您还可以重新启动管理服务并升级管理服务的版本。您可以进一步创建管理服务和 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，会创建客户端会话。您可以在“会话”窗格中查看设备上的所有客户端 会话。

在“会话”窗格中，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：从中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：上次在会话中检测到用户活动的时间。
- 会话过期时间：会话到期的剩余时间。

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”。

您无法从已启动该会话的客户端结束会话。

配置策略

为了将记录的数据大小保持在可管理的限制范围内，SDX 设备会在指定时间自动运行备份和数据修剪策略。

修剪策略在每天凌晨 00:00 运行，并指定要在设备上保留数据的天数。默认情况下，设备会修剪 3 天以上的数据，但您可以指定要保留的数据的天数。只会修剪事件日志、审核日志和任务日志。

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

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

要指定删减记录数据的天数，请执行以下操作：

1. 在 配置 选项卡的导航窗格中，单击 系统。
2. 在“系统”窗格的“策略管理”下，单击“修剪策略”。

3. 在 修改修剪策略 对话框的 要保留的数据（天数）中，指定设备在任何给定时间必须保留的数据天数。
4. 单击确定。

要配置备份策略，请执行以下操作：

1. 在 配置 选项卡的导航窗格中，单击 系统。
2. 在“系统”窗格的“策略管理”下，单击“备份策略”。
3. 在 修改备份策略 对话框的要保留的 先前备份 中，指定设备在任何给定时间必须保留的备份数。
4. 选择“加密备份文件”以加密备份文件。
5. 选择“外部传输”，然后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，输入用于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，选择要用来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的路径。

6. 传输后从 **Management Service** 中删除文件：如果要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

可以从“系统”窗格中重新启动管理服务。重启管理服务不会影响实例的运行。实例在管理服务重启过程中继续运行。

要重新启动管理服务，请执行以下操作：

1. 在 配置 选项卡的导航窗格中，单击 系统。
2. 在“系统”窗格的“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。

要删除管理服务文件，请执行以下操作：

1. 在 配置 选项卡的导航窗格中，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”。

为技术支持生成 **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。可以为管理服务或 Citrix Hypervisor 或同时为两者生成此 tar。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：上次修改此文件的日期。
- 大小： tar 文件的大小。

要为技术支持生成 **tar** 存档，请执行以下操作：

1. 在 配置 选项卡上，导航到 诊断 **>** 技术支持。
2. 在 详细信息 窗格的“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”对话框的“模式”列表中，选择相应的选项。
4. 单击确定。

要下载 **tar** 存档以获得技术支持，请执行以下操作：

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”。该文件将保存到您的本地计算机。

管理服务的 **CLI** 支持

现在，您可以使用 CLI 对管理服务执行操作。支持以下操作：

- 添加、设置、删除-配置资源。
- Do-执行系统级操作。例如，管理服务升级或关闭，或重新启动。
- 保存-添加用于置备的接口。

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：通过控制台访问不支持 CLI。

配置身份验证和授权设置

November 23, 2023

使用 NetScaler SDX Management Service 进行身份验证可以是本地的，也可以是外部的。使用外部身份验证时，管理服务会根据来自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)
- 终端门禁控制器访问控制系统 (TACACS)
- 轻型目录访问协议 (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，然后配置身份验证服务器。

通过管理服务进行的授权是本地的。管理服务支持两个级别的授权。允许具有管理员权限的用户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。

组提取支持对 RADIUS 和 LDAP 的授权。您可以在管理服务上配置 RADIUS 或 LDAP 服务器期间设置组提取属性。提取的组名与管理服务上的组名相匹配，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。将此组与提取的组一起考虑进行授权。

在 TACACS 授权中，TACACS 服务器管理员必须允许特殊命令，即具有管理员权限的用户的 admin 命令，对具有只读权限的用户拒绝此命令。当用户登录到 SDX 设备时，管理服务会检查用户是否有权运行此命令。如果用户具有权限，则会为该用户分配管理员权限，否则将为该用户分配只读权限。

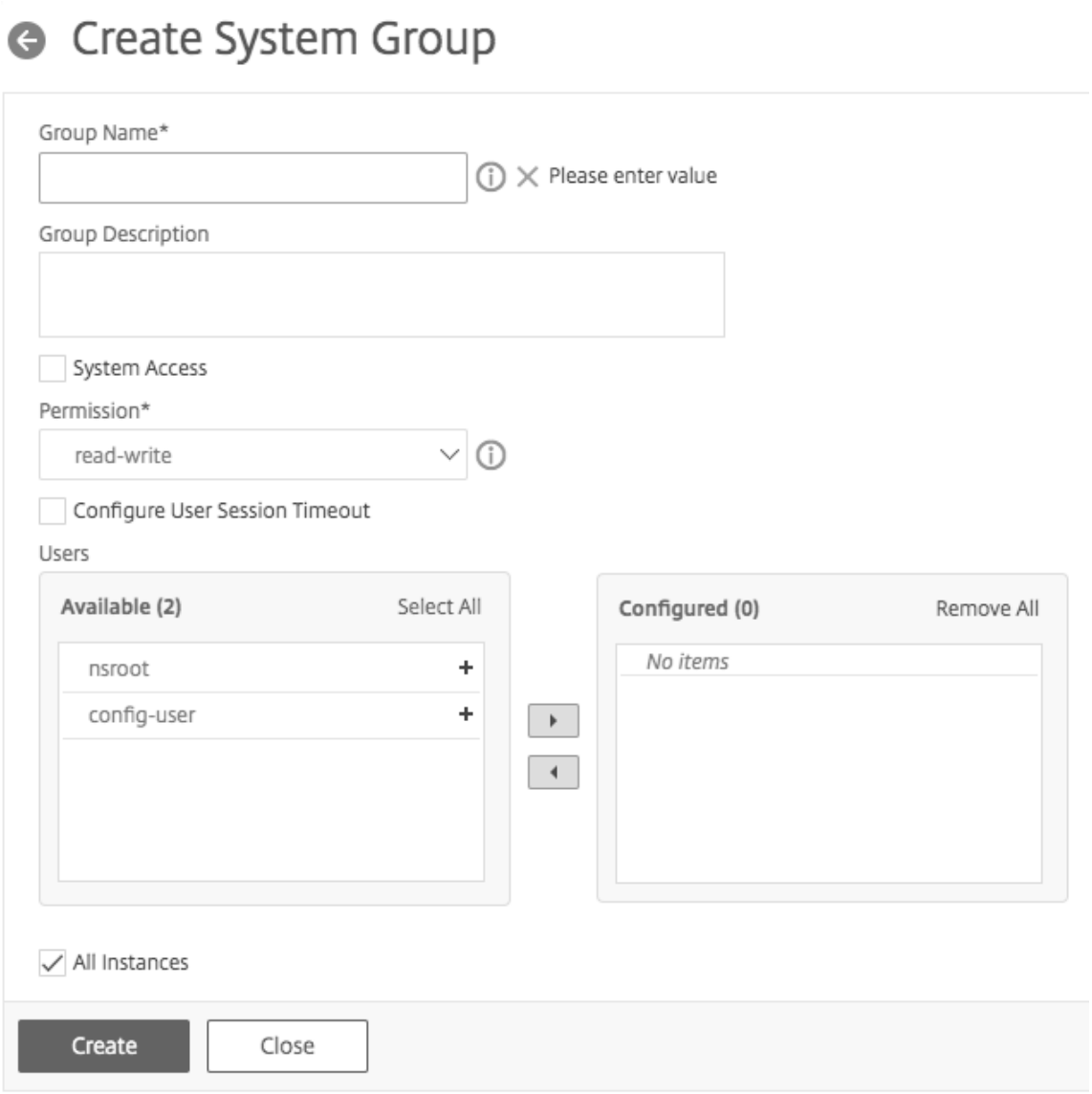
添加用户组

组是需要访问公共信息或执行类似任务的逻辑用户组。您可以将用户组织到由一组常见操作定义的组中。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。如果用户所属的组的名称与身份验证服务器上的组相匹配，则登录并通过身份验证，则该用户将继承该组的设置。

添加用户组

1. 在“配置”选项卡上的“系统”下，展开“用户管理”，然后单击“组”。
2. 在详细信息窗格中，单击“添加”。



3. 在“创建系统组”页中，设置以下参数：

   - 组名
   - 群组描述
   - 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 Instances 下指定 实例。
   - 权限
   - 配置用户会话超时
   - 用户：属于组的数据库用户。选择要添加到组中的用户。

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，请选中“读写”权限和“系统访问权限”复选框。在 SDX 10.5 中，此复选框不可用，权限的值为“admin”和“read-only”。

配置用户帐户

用户登录到 SDX 设备以执行设备管理任务。要允许用户访问设备，必须在 SDX 设备上为该用户创建一个用户帐户。用户在设备上进行本地身份验证。

重要：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“配置”选项卡上的“系统”下，展开“管理”，然后单击“用户”。“用户”窗格显示现有用户帐户及其权限的列表。
2. 在“用户”窗格中，执行以下操作之一：
   - 要创建用户帐户，请单击“添加”。
   - 要修改用户帐户，请选择该用户，然后单击 修改。
3. 在“创建系统用户”或“修改系统用户”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。此名称无法更改。
   - 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。
     - 只读-用户只能监视系统并更改帐户的密码。
       默认值：管理员。
   - 启用外部身份验证-为此用户启用外部身份验证。管理服务在进行数据库用户身份验证之前尝试进行外部身份验证。如果禁用此参数，则不会使用外部身份验证服务器对用户进行身份验证。
     注意：如果无法访问远程身份验证服务器，则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 user (`nsroot`)。
   - 配置会话超时-允许您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。

   * 必需的参数
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，对本地用户禁用外部身份验证。在添加本地用户或修改用户的设置时，可以通过选中
启用外部身份验证选项来启用它。

重要：只有在设置 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的类型。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。该菜单列出了为所选身份验证类型配置的所有服务器。
    - 启用后备本地身份验证-或者，您也可以选择在外部身份验证失败时使用本地身份验证对用户进行身份验证。默认情况下启用此选项。
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向管理服务 NITRO 接口进行身份验证。默认情况下，在 SDX 设备中启用基本身份验证。要使用管理服务界面禁用基本身份验证，请执行以下操作。

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，清除“允许基本身份验证”复选框。
4. 单击确定。

配置外部身份验证服务器

November 23, 2023

NetScaler SDX Management Service 可以使用本地用户帐户或使用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。用户数据存储在本地管理服务上。
- RADIUS —向外部 RADIUS 身份验证服务器进行身份验证。
- LDAP-向外部 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，然后配置 RADIUS 身份验证服务器。

管理服务根据 RADIUS 规范支持 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“配置”选项卡上的“系统”下，展开“身份验证”，然后单击“**Radius**”。
2. 在详细信息窗格中，单击“添加”。
3. 在“创建 **Radius** 服务器”对话框中，键入或选择参数值：
    - 名称 *-服务器的名称。
    - 服务器名称/ IP 地址 *-完全限定的域名 (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“为 FQDN 名称解析添加主 DNS”部分。“
    - 端口 *—运行 RADIUS 服务器的端口。默认值：1812。
    - 超时 * —系统等待来自 RADIUS 服务器的响应的秒数。默认值：3。
    - 密钥 * - 客户端与服务器之间共享的密钥。此信息是系统与 RADIUS 服务器之间的通信所必需的。
    - 启用 NAS IP 地址提取—如果启用，将根据 RADIUS 协议将管理服务 IP 地址作为发送到服务器。`nasip`
    - NASID —如果已配置，则会根据 RADIUS 协议将此字符串作为发送到 RADIUS 服务器。`nasid`
    - 组前缀-用于提取 RADIUS 组的 RADIUS 属性中组名称前面的前缀字符串。
    - 组供应商 ID-用于使用 RADIUS 组提取的供应商 ID。
    - 组属性类型-RADIUS 组提取的属性类型。
    - 组分隔符-用于分隔 RADIUS 组提取的 RADIUS 属性内的组名称的组分隔符字符串。

- IP 地址供应商标识符—RADIUS 中表示内部网 IP 的属性的供应商 ID。值为 0 表示该属性不是供应商编码的。
- 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—如何在从系统传输到 RADIUS 服务器的 RADIUS 数据包中对密码进行编码。可能的值：pap、chap、mschapv1 和 mschapv2。
- 默认身份验证组 - 除提取的组外，身份验证成功时选择的默认组。
- 记帐-启用管理服务以使用 RADIUS 服务器记录审核信息。

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，然后配置 LDAP 身份验证服务器。

添加 **LDAP** 服务器

1. 在“配置”选项卡的“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“为 FQDN 名称解析添加主 DNS”部分。“
   - 端口 *—运行 LDAP 服务器的端口。默认值：389。
   - 超时 *-系统等待来自 LDAP 服务器的响应的秒数。
   - 基本 DN-必须启动 LDAP 搜索的基本节点或节点。
   - 类型-LDAP 服务器的类型。可能的值：Active Directory (AD) 和 Novell 目录服务 (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-选中此选项可验证从 LDAP 服务器接收的证书。
   - LDAP 主机名-LDAP 服务器的主机名。如果启用了 validateServerCert 参数，则此参数将指定 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。
   - 搜索过滤器-要与默认 LDAP 用户搜索字符串组合以构成值的字符串。例如，使用 ldaploginame `samaccount` 和用户提供的用户名 bob 的 vpnallowed=true 会生成一个 LDAP 搜索字符串:(&(vpnallowed=true) (samaccount=bob)。

- 组属性-从 LDAP 服务器中提取组的属性名称。
- 子属性名称-用于从 LDAP 服务器中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：不需要加密。

  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 - 除提取的组外，身份验证成功时选择的默认组。
- 引用-启用对从 LDAP 服务器接收的 LDAP 引用的关注。
- 最大的 LDAP 引用次数-可跟随的最大 LDAP 引用数。
- 启用更改密码-允许用户在密码过期时修改密码。仅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-允许组提取的级别数。
- 组名标识符-唯一标识 LDAP 服务器中组的名称。
- 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-要与默认 LDAP 组搜索字符串组合以构成搜索值的字符串。

4. 单击 Create（创建），然后单击 Close（关闭）。

LDAP 用户的 **SSH** 公钥身份验证支持

SDX 设备现在可以通过用于登录的 SSH 公钥身份验证对 LDAP 用户进行身份验证。公钥列表存储在 LDAP 服务器中的用户对象上。在身份验证过程中，SSH 会从 LDAP 服务器中提取 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存在于 LDAP 服务器和 NetScaler SDX 设备中。

> 重要提示
>
> 对于基于密钥的身份验证，您必须通过在以下方面设置 /etc/sshd_config 文件中的 Authorizedkeysfile 的值来指定公钥的位置：
>
> ```
> AuthorizedKeysFile .ssh/authorized_keys
> ```

系统用户。通过设置 /etc/sshd_config*‘ 文件中的 Authorizedkeysfile 的值，可以为任何系统用户指定公钥的位置。

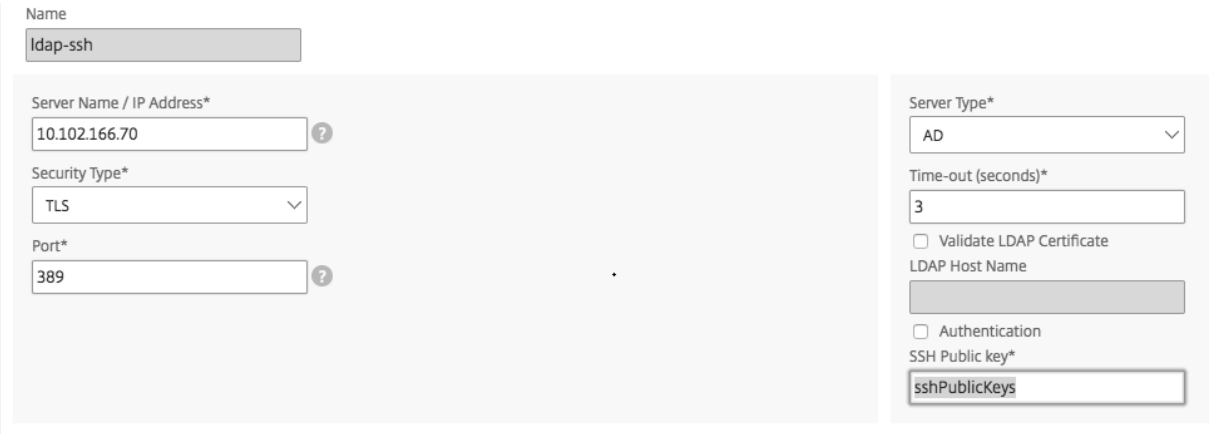
LDAP 用户。检索到的公钥存储在 /var/pubkey/<user_name>/tmp_authorized_keys-<pid> 目录中。pid 是添加的唯一编号，用于区分来自同一用户的并发 SSH 请求。此位置是在身份验证过程中保存公钥的临时位置。验证完成后，公共密钥将从系统中删除。

要使用用户登录，请在 shell 提示符下运行以下命令：

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

要使用 **GUI** 配置 **LDAP** 服务器，请执行以下操作：

1. 导航到 系统 **>** 身份验证 **> 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。



> 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 IP 地址来定义 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 系统 **>** 网络配置 **> DNS**。

要使用 CLI 设置主 DNS，请执行以下步骤。

1. 打开安全外壳 (SSH) 控制台。
2. 使用管理员凭据登录 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。

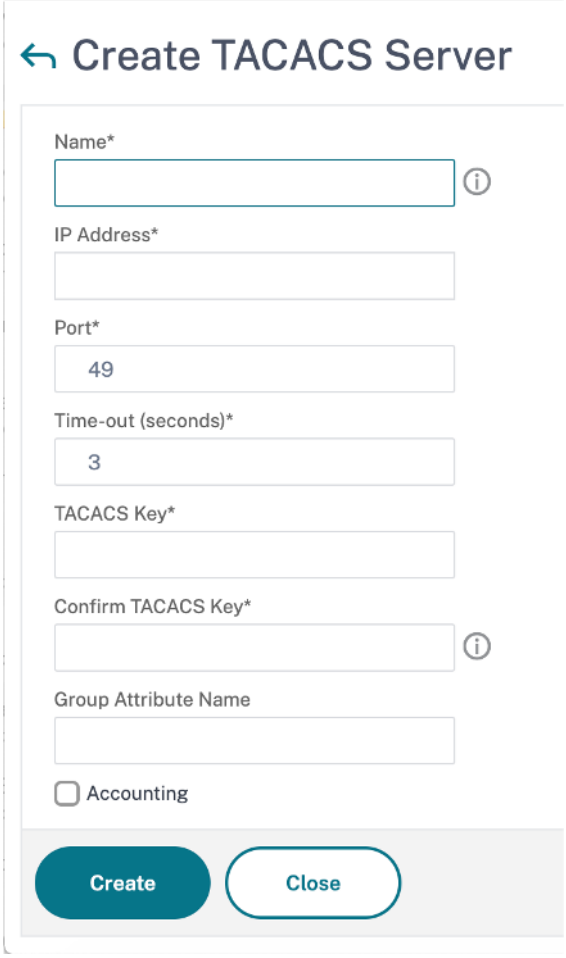
如果再次运行 `networkconfig` 命令，您将看到更新后的 DNS 地址。

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，然后配置 TACACS 身份验证服务器。

添加 **TACACS** 服务器

1. 在 配置 选项卡的 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，键入或选择参数值：
   - 名称—TACAS 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—系统等待来自 TACACS 服务器的响应的最大秒数
   - TACACS 密钥—客户端和服务器之间共享的密钥。此信息是系统与 TACACS 服务器通信所必需的
   - 记帐-使管理服务能够使用 TACACAS 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



4. 单击“创建”，然后单击“关闭”。

从管理服务配置链路聚合

November 23, 2023

链路聚合将多条以太网链路组合成一条高速链路。配置链路聚合可增加 NetScaler SDX 设备与其他连接设备之间通信通道的容量和可用性。聚合链接也称为“通道”。“

如果将网络接口绑定到通道，则通道参数优先于网络接口参数。也就是说，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 中删除，并添加到默认 VLAN 中。但是，您可以将该通道绑定回原来的 VLAN，或绑定到新的 VLAN。例如，如果将网络接口 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。
- 配置一个通道至少需要两个接口。
- 添加或修改 NetScaler 实例时，“网络设置”视图中未列出构成通道一部分的接口。列出的不是接口，而是列出了通道。

如果您使用分配给一个实例的三个接口来配置通道，而另一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，然后重启实例。例如，假设两个实例，即实例 1 和实例 2。置备这些实例后，接口 10/1、10/2 和 10/3 将分配给实例 1，接口 10/1 和 10/2 将分配给实例 2。如果使用接口 10/1、10/2 和 10/3 创建了 LA 通道，则 instance1 不会重新启动。但是，管理服务会关闭实例 2，将接口 10/3 分配给实例 2，然后重新启动 Instance2。

如果从 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，该接口将显示在 Network Settings 视图中。在删除接口之前，只会列出该接口所属的通道。

从管理服务配置频道

November 23, 2023

您可以手动配置通道，也可以使用链路聚合控制协议 (LACP)。您无法将 LACP 应用于手动配置的通道，也无法手动配置 LACP 创建的通道。从管理服务配置频道。然后在预置或修改 NetScaler 实例时选择频道。

LA 通道是提供链路冗余和带宽聚合的逻辑实体。作为通道一部分的接口无法分配单独的 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 版本 13.1 Build 27.x 及更高版本中，在 NetScaler SDX 设备上托管的 NetScaler VPX 实例上明确不支持链路冗余配置。

从管理服务配置频道

1. 导航到“系统”**>**“频道”。
2. 在详细信息窗格中，单击“添加”。
3. 在添加通道对话框中，设置以下参数：

    - 通道 ID-要创建的 LA 频道的 ID。用 LA/x 表示法指定 LA 通道，其中 x 的范围可以是 1 到等于接口数量一半的数字。创建 LA 通道后无法更改。
    - 类型-频道的类型。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（以 Mbps 为单位）。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，则会触发故障切换。
    - 带宽高（仅适用于静态通道和 LACP）—LA 通道带宽使用率的高阈值，以 Mbps 为单位。当 LA 通道的带宽使用量等于或大于指定的高阈值时，设备会生成 SNMP 陷阱消息。
    - 带宽正常（仅适用于静态通道和 LACP）—LA 通道带宽使用情况的正常阈值，以 Mbps 为单位。当超出高阈值后 LA 通道的带宽使用量等于或小于指定的正常阈值时，NetScaler SDX 设备会生成 SNMP 陷阱消息，表明带宽使用已恢复正常。

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）—如果链路未接收 LACPDU，则链路在此时间后不会聚合。在 SDX 设备和伙伴节点上参与链路聚合的所有端口上，该值必须匹配。
    - HA 监视—在高可用性 (HA) 配置中，监视通道是否存在故障事件。启用了 HA MON 的任何 LA 通道出现故障都会触发 HA 故障切换。
    - 标记全部-在此通道上发送的每个数据包中添加一个四字节的 802.1q 标记。开设置为绑定到此通道的所有 VLAN 应用标记。“关”将标记应用到除本地 VLAN 之外的所有 VLAN。
    - 别名—洛杉矶频道的别名。仅用于增强可读性。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 接口都是 VPX 实例的一部分，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，则无法删除该管理 LA。

访问控制列表

February 16, 2024

访问控制列表 (ACL) 是一组条件，您可以将这些条件应用于网络设备，以过滤 IP 流量并保护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：
>
> 从版本 12.0 57.19 起支持 SDX 设备上的 ACL。

本主题包括以下几个部分：

- 用法指南
- 如何配置 ACL
- ACL 规则的其他操作
- 故障排除

用法指南

在设备上创建 ACL 时，请记住以下几点：

- 将 SDX 设备升级到版本 11.0 57.19 时，默认情况下会禁用 ACL 功能。
- 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 SDX 设备，则必须创建适当的 ACL 规则以允许 MAS 与 SDX 管理服务之间的通信。
- SDX 设备上的任何其他配置（如置备或删除 VPX、添加/删除外部服务器、SNMP 管理）都不需要对现有 ACL 配置进行任何更改。与这些实体的沟通由管理处负责。

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，则无法在创建 ACL 规则后启用该规则。

启用 **ACL** 功能

1. 要启用 ACL 功能，请登录 SDX 管理服务 GUI，然后导航到 配置 **>** 系统 **> ACL**。
2. 通过使用切换按钮，打开 ACL 功能。

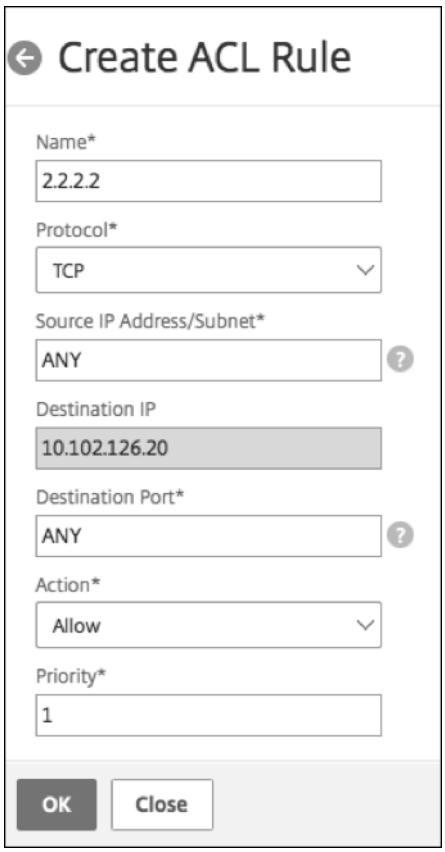
创建 **ACL** 规则

1. 在 ACL 页面上，单击 创建规则。
2. 此时将打开创建规则窗口。添加下表中列出的详细信息。

属性	说明
名称	添加一个名字。
协议	从菜单中选择协议。默认情况下，TCP 处于选中状态。您可以选择 **ANY** 以允许所有协议。
源 IP 地址/子网	指定应用规则的源 IP 地址或源子网。如果必须将规则应用于所有传入通信，请选择 **ANY**。
目标 IP	SDX 管理服务 IP 地址将自动填充为目标 IP。无法编辑此字段。
目的端口	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	分配优先级以指定评估规则的顺序。优先级编号决定了 ACL 规则与传入数据包的匹配顺序。优先级较低的数字具有较高的优先级。例如，优先级编号 1 的优先级高于优先级编号 1。如果没有任何规则与传入的数据包匹配，则该数据包将被阻止。

3. 单击“确定”创建规则。

图： ACL 规则的示例



创建规则后，它将处于禁用状态。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。如果禁用了该功能，并且您尝试启用 ACL 规则，则会显示一条消息“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. 出现提示时，单击“是”进行确认。

ACL 规则的其他操作

您可以对 ACL 规则应用以下操作：

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. 单击是进行确认。

> 注意：
>
> 禁用规则后，该规则将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。
2. 在列表中单击 编辑规则。修改规则窗口随即打开。
3. 或者，选择该规则的单选按钮，然后单击 编辑规则 选项卡。修改规则窗口随即打开
4. 进行编辑，然后单击“确定”。

> 注意：
>
> 您可以编辑处于启用和禁用状态的规则。如果编辑的规则已经启用，编辑内容将立即应用。对于处于禁用状态的规则，启用规则时将应用编辑内容。

删除 **ACL** 规则

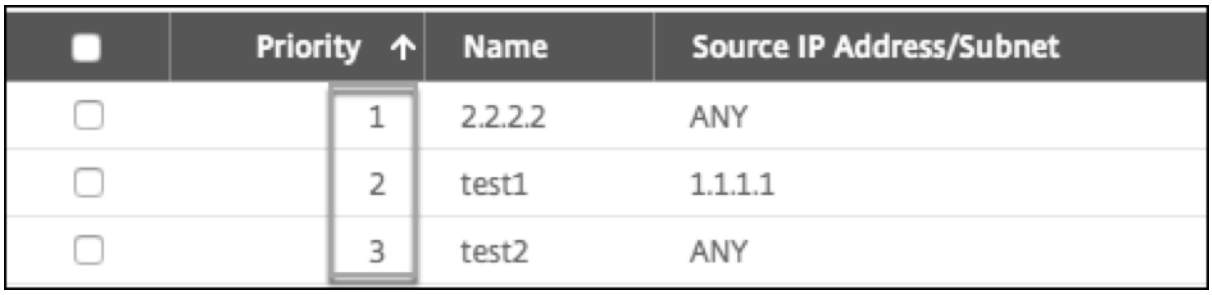
1. 确保规则处于禁用状态。
2. 将鼠标悬停在要删除的规则上，然后选择带有三个点的圆圈。单击列表中的 删除规则。
3. 或者，选择该规则的单选按钮，然后单击 删除规则 选项卡。
4. 单击是进行确认。

> 注意：
>
> 您无法删除处于启用状态的规则。

重新编号 **ACL** 规则的优先级

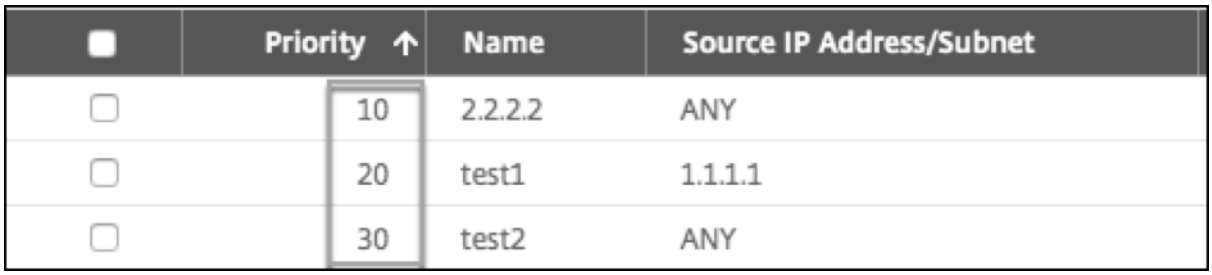
1. 将鼠标悬停在要为其重新编号优先级的规则上，然后选择带有三个点的圆圈。从列表中单击“重新编号优先级”。
2. 或者，选择该规则的单选按钮，然后单击 选择操作 选项卡。
3. 选择“重新编号优先级”。
4. SDX 管理服务会自动为所有现有规则分配新的优先级编号，即 10 的倍数。
5. 编辑规则以根据需要分配优先级编号。有关如何编辑规则的更多信息，请参阅“编辑 ACL 规则”部分。

图。现有优先级号码的示例



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

图。优先级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。如果由于 ACL 设置不当而无意中失去了对 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 Citrix Hypervisor 管理 IP 地址。
2. 使用管理员权限登录管理服务虚拟机的控制台。
3. 运行命令 `pfctl -d`。
4. 通过 GUI 登录到管理服务，然后相应地重新配置 ACL。

设置 **NetScaler** 实例群集

November 23, 2023

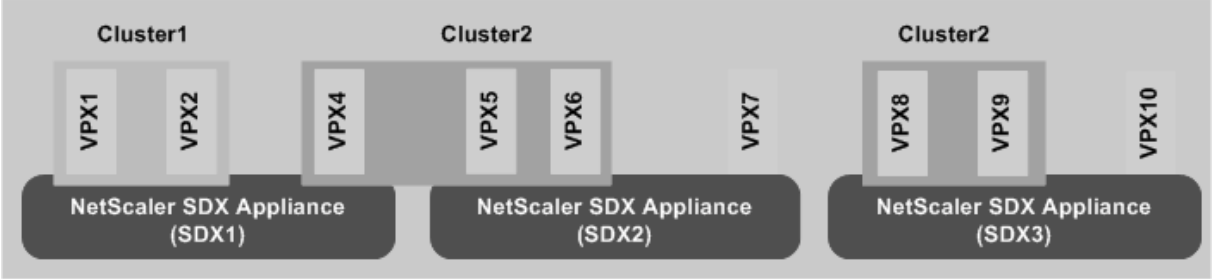
在一个或多个 SDX 设备上配置 NetScaler 实例后，您可以创建 NetScaler 实例群集。

Citrix 建议您从管理服务执行群集配置。当您从 VPX 实例执行群集配置时，管理服务会每 30 分钟在自动发现期间了解一次配置。在最坏的情况下，30 分钟内不会发现群集信息。尽管群集可能正常工作，但遗漏了一些针对群集依赖项的基本验证检查。在 ADC 实例上配置群集之前，管理服务会执行这些检查。因此，您必须从管理服务执行任何群集配置。

注意：

- 要设置群集，您必须了解 NetScaler 群集。有关更多信息，请参阅 聚类。
- 对于在 SDX 设备上拥有 NetScaler 实例的群集，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) 个节点的群集标准。

图 1. SDX NetScaler 实例群集



上图显示了同一子网中的三个 SDX 设备 SDX1、SDX2 和 SDX3。这些设备上的 NetScaler 实例用于形成两个群集：Cluster1 和 Cluster2。

- 群集 1 在 SDX1 上包含两个实例。
- Cluster2 包括 SDX1 上的一个实例、SDX2 上的两个实例和 SDX3 上的另外两个实例。

需要记住的几个要点

- SDX 平台不支持使用 Mellanox 接口（50G 和 100G）进行 CLAG 形成。
- 群集的所有节点必须是同一类型。您无法使用以下组合形成群集：
  - 硬件和虚拟设备。
  - NetScaler VPX 实例和 NetScaler SDX 实例。
  - 不同 SDX 硬件平台上的 ADC 实例。
- NetScaler 实例的版本必须相同，版本必须为 10.1 或更高版本。
- NetScaler 实例必须都具有相同的功能许可证。
- 将单个 NetScaler 实例添加到群集后，无法更新这些实例上的任何配置。所有更改都必须通过群集 IP 地址执行。

- NetScaler 实例必须都具有相同的资源（内存、CPU、接口等）。
- 背板 MTU 必须比数据接口 MTU 多 78 字节。
- 确保所有数据接口 MTU 都在 9138 字节以内。
- 从版本 13.0 Build 82.x 开始，系统会在向群集添加节点时提示您添加 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的源 IP 地址检查中的安全问题。
- 重要提示！请谨慎使用“移除群集”选项。单击 移除群集时，群集将被删除，不会出现任何警告。

在 **SDX** 设备上设置群集

1. 登录到 SDX 设备。
2. 在 配置 选项卡上，导航到 **NetScaler >** 群集 **>** 群集实例。
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。要描述参数，请将鼠标光标悬停在相应的字段上。
   c) 单击“下一步”查看配置摘要。
   d) 单击“完成”创建群集。
   注意：将配置了 L2 VLAN 的 NetScaler 实例添加到群集时，
   添加 VLAN 命令将保存，
   `sdxvlan` 参数设置为“是”。此参数是一个内部参数，用于避免在 SDX 群集形成过程中断开连接。

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。有关参数的描述，请将鼠标光标悬停在相应字段上。
   c) 单击“下一步”查看配置摘要。
   d) 单击“完成”将节点添加到群集。
   e) 重复步骤 1 到 4 向群集添加另一个节点。

   创建群集后，您必须通过群集 IP 地址访问群集来配置它。

如果群集实例中的节点属于同一 Citix NetScaler SDX 设备，则当 NetScaler SDX 设备出现故障时，我们可能会失去法定人数。

您可以使用以下方法部署群集节点：

1. 使用每台 NetScaler SDX 设备中的一个 VPX 实例创建多个群集实例。

示例：

SDX1	SDX2	InstanceID
VPX1	VPX1	1
VPX2	VPX2	2

1. 如果有两个以上 NetScaler SDX 设备，则使用来自`quorumType Majority` 的所有设备的 VPX 实例创建一个群集实例。在这种情况下，请确保 VPX 实例平均分布在所有 NetScaler SDX 设备上。

示例 **1**：

SDX1	SDX2	SDX3	InstanceID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	不适用
VPX3	VPX3	VPX3	不适用

示例 **2**：

SDX1	SDX2	SDX3	InstanceID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	不适用
VPX3	VPX3	VPX3	不适用
VPX4	不适用	不适用	不适用

1. 使用来自所有 NetScaler SDX 设备的所有 VPX 实例创建单个群集实例。但是使用 `quorum type NONE`。这有一些局限性。

示例：

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

-quorumType 参数设置为时的限制 **NONE**：

- 拓扑在群集节点之间必须有冗余链路，以避免因单点故障而导致网络分区。
- 在任何群集操作（例如添加或删除节点）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，每个群集至少有一个 SDX 设备的 NetScaler 实例，请使用“重新发现”选项。

将存在于一个 **SDX** 设备上的 **NetScaler** 实例添加到另一个 **SDX** 设备上配置的群集中

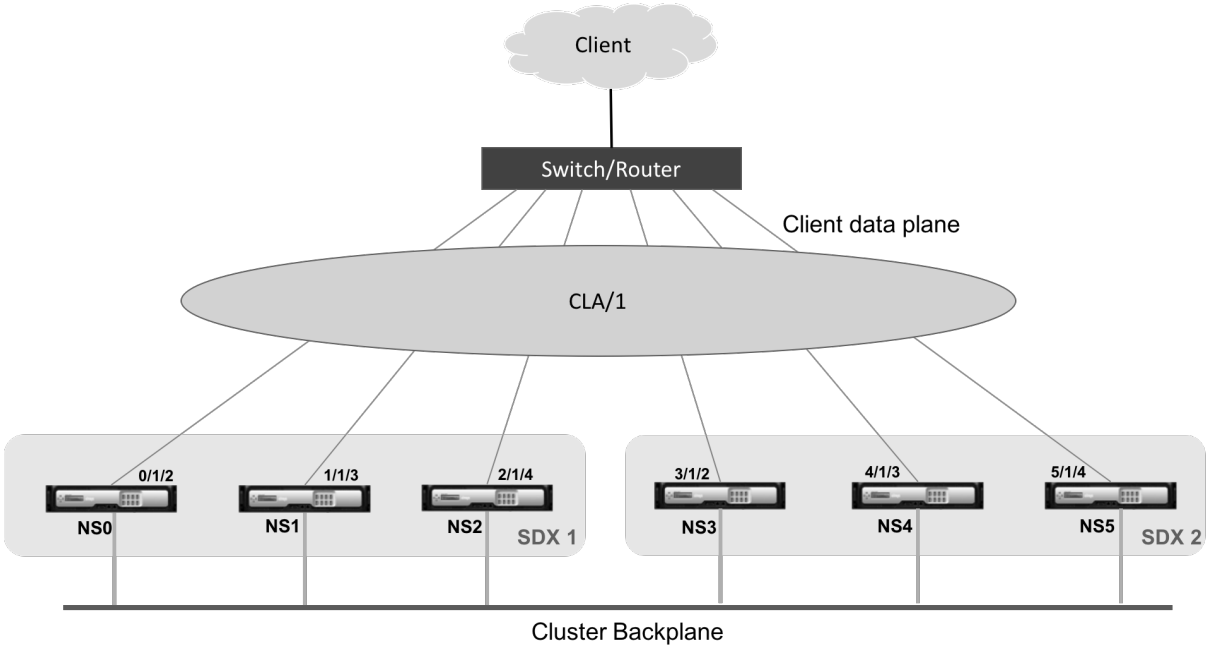
1. 登录到要从中添加 NetScaler 实例的 SDX 设备。
2. 在“配置”选项卡上，导航到 **NetScaler**，然后单击“群集”。
3. 单击 添加节点。
4. 在 添加节点 对话框中，配置添加群集节点所需的参数。有关参数的描述，请将鼠标光标悬停在相应字段上。
   注意：确保“
   群集 IP 地址”和“
   群集 IP 密码”参数的值适用于要向其添加节点的群集。
5. 单击“下一步”查看配置摘要。
6. 单击“完成”将节点添加到群集。

配置群集链路聚合

February 16, 2024

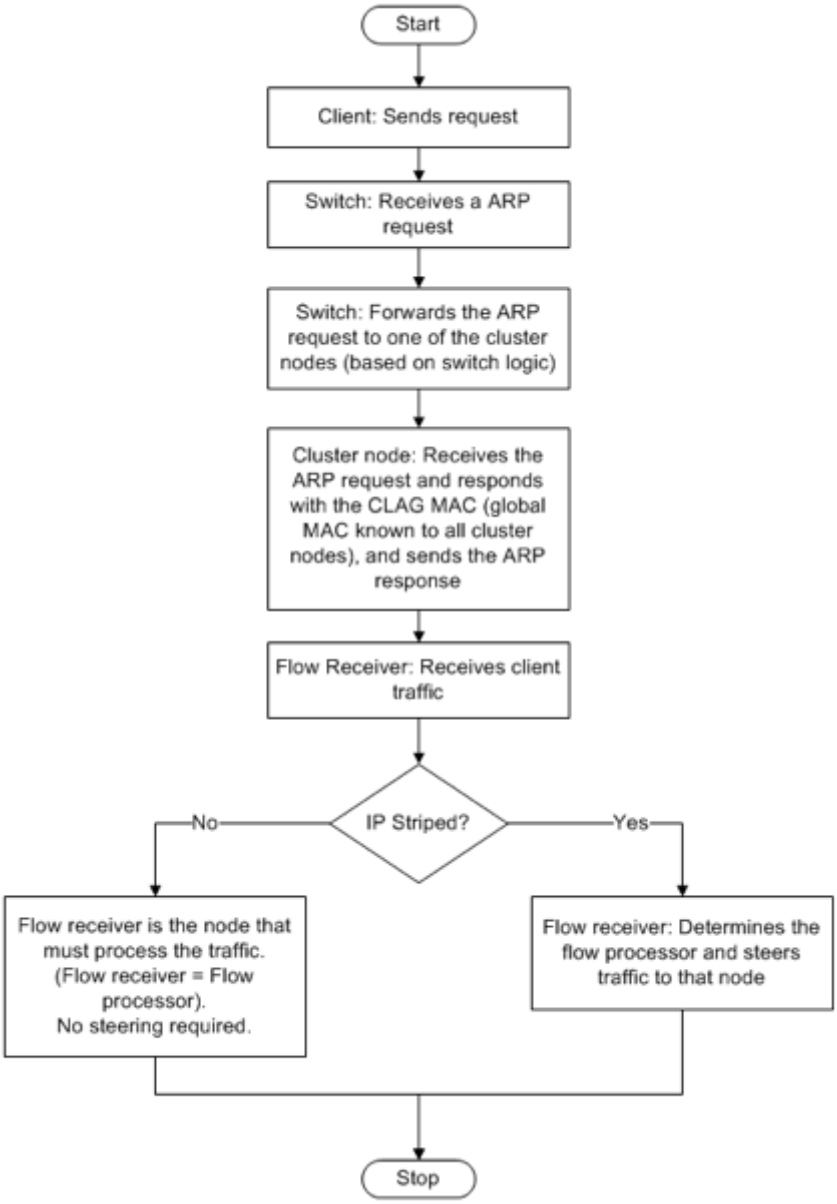
顾名思义，群集链路聚合将一组群集节点接口组合成一个通道。它是 NetScaler 链路聚合 (LA) 的扩展。唯一的区别是，虽然链路聚合要求接口位于同一设备上，但在群集链路聚合中，接口位于群集的不同节点上。有关链接聚合的详细信息，请参阅 配置链路聚合。

例如，假设一个跨两个 SDX 设备的六节点群集，其中所有六个节点都连接到上游交换机。群集 LA 通道 (CLA/1) 由绑定接口 0/1/2、1/1/3、2/1/4、3/1/2、4/1/3 和 5/1/4 组成。



群集 LA 通道具有以下属性：

- 每个通道都有一个由群集节点同意的唯一 MAC 地址。
- 该通道可以绑定本地和远程 SDX 节点的接口。
- 一个群集最多支持四个群集 LA 通道。
- 每个群集 LA 通道最多可以绑定 16 个接口。
- 背板接口不能是群集 LA 通道的一部分。
- 当接口绑定到群集 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。
- 请勿配置对群集 LA 通道（例如 CLA/1）或其成员接口上的群集节点的管理访问权限。当节点处于 INACTIVE 状态时，相应的群集 LA 接口将被标记为 POWER OFF，这会导致其失去管理访问权限。



在群集 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 地址分配流量。

需要记住的几个要点：

- 启用 LACP（通过将 LACP 模式指定为 ACTIVE 或 PASSIVE）。
  注意：确保在 NetScaler 群集和外部连接设备上均未将 LACP 模式设置为被动。
- 要创建群集 LA 通道，LACP 密钥的值可以介于 5 到 8 之间。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

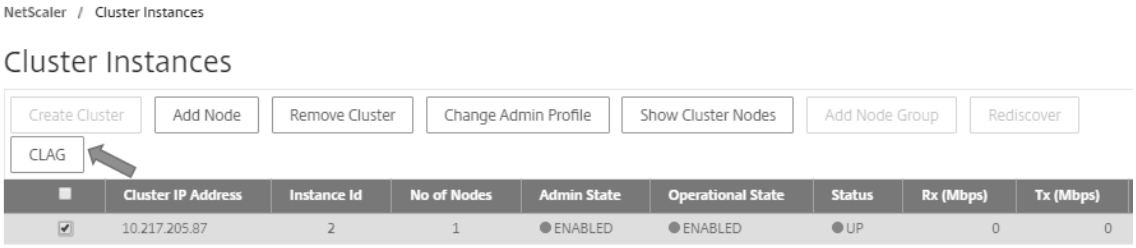
超时之后才收到有关 CLAG 及其成员接口断电的通知时，此设置非常有用。

必备条件：

创建一个 NetScaler 实例群集。群集的节点可以是同一 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。

要使用管理服务配置群集 **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，然后单击 **CLAG**。

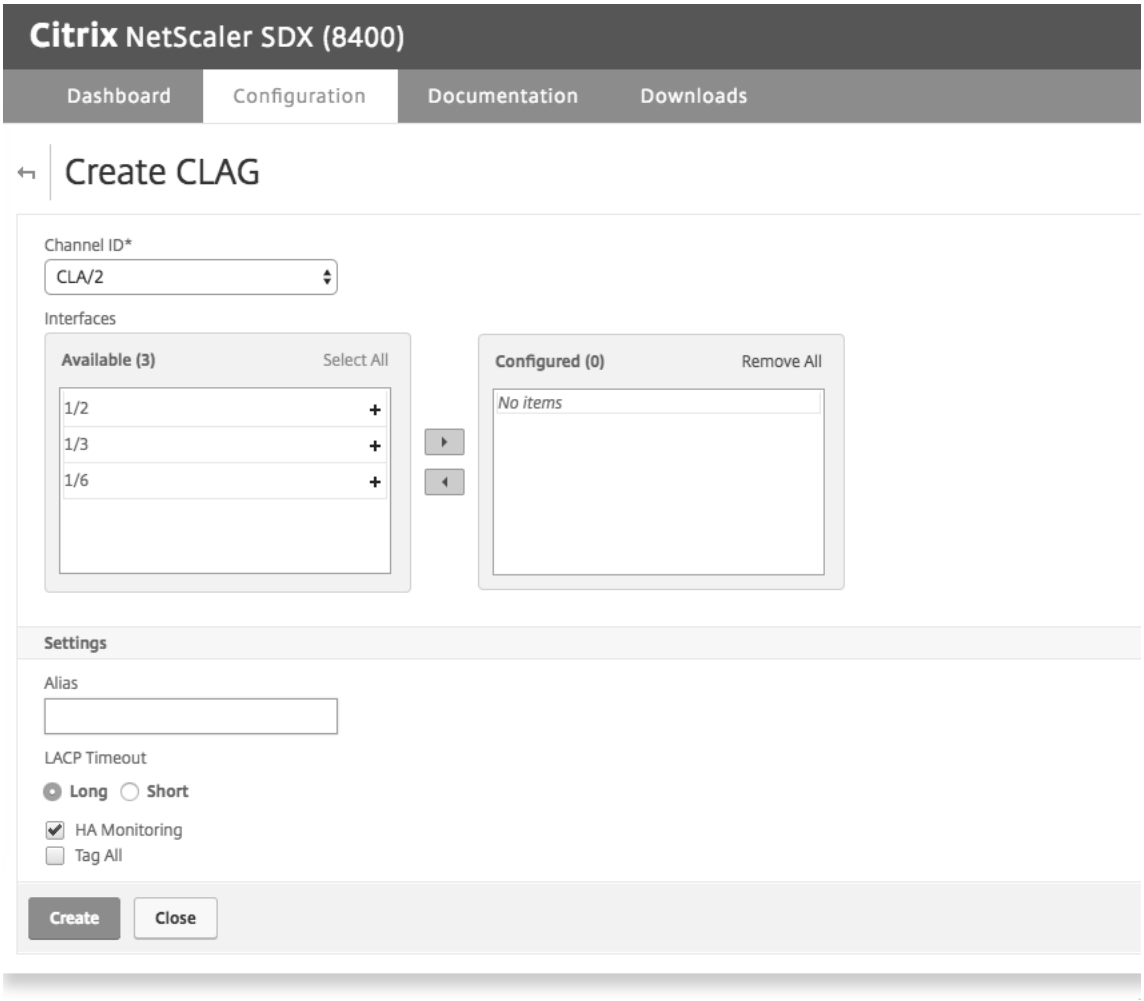


4. 在“创建 **CLAG**”对话框中，执行以下操作：
   a) 在 通道 **ID** 下拉列表中，选择群集 LA 通道 ID。
   b) 在“接口”部分中，从“可用”选择框中选择接口，然后单击 **+**。
   c) 所选接口显示在“已配置”选择框下。
5. 在“设置”部分中，执行以下操作：
   a) 在“别名”字段中，输入群集 LA 通道的备用名称。
   b) 在“**LACP** 超时”字段中，选择以下值之一以定义链路未收到 LACPDU 时链路不聚合的时间间隔。

      该值必须与参与 SDX 设备和伙伴节点上链路聚合的所有端口上的值相匹配：

      - 长—30 秒
      - 短—1 秒

   c) 对于高可用性 (HA) 配置，选中 **HA** 监视 复选框以监视通道的故障事件。启用了 HA MON 的任何 LA 通道出现故障都会触发 HA 故障切换。
   d) 选择 **Tag All** ，将一个四字节的 802.1q 标记添加到此通道上发送的每个数据包。开设置为绑定到此通道的所有 VLAN 应用标记。OFF 会将标记应用于除本地 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”刷新其他 SDX 设备中的 CLAG 设置。

   备注：

   - 如果选择“否”，则未配置 CLAG。
   - 手动刷新其他 SDX 设备中的 CLAG 设置。
   - 两台 SDX 设备上的 MTU 设置必须相同。必须在任一 SDX 设备上手动更改 MTU 设置。

8. 要在 **CLAG** 对话框中更改 MTU 设置，请执行以下操作：

   a) 选择 **CLA/1**，然后单击“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

February 16, 2024

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 个预定义密码组，它们是类似密码的组合，您可以从支持的 SSL 密码列表中创建自定义密码组。

限制

- 不支持使用密钥交换 =“DH”或“ECC-DHE”绑定密码。
- 不支持使用身份验证 =“DSS”绑定密码。
- 不支持绑定不在支持的 SSL 密码列表中的密码，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，如果列出了 SSLv3，则全部支持 SSLv3/TLSv1/TLSv1.1/TLSv1.2。

Citrix 密码名称	OpenSSL 密码名	十六进制码	协议	密钥交换算法	身份验证算法	消息验证码 (MAC) 算法
TLS1-AES-256-CBC-SHA	AES256-SHA	0x0035	SSLv3	RSA	RSA	AES(256)
TLS1-AES-128-CBC-SHA	AES128-SHA	0x002F	SSLv3	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)
TLS1.2-AES256-GCM-SHA384	AES256-GCM-SHA384	0x009D	TLSv1.2	RSA	RSA	AES-GCM(256)

Citrix 密码名称	OpenSSL 密码名	十六进制码	协议	密钥交换算法	身份验证算法	消息验证码 (MAC) 算法
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	SSLv3	ECC-DHE	RSA	AES(256)
TLS1-ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA	0xC013	SSLv3	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-GCM-SHA384	ECDHE-RSA-AES256-GCM-SHA384	0xC030	TLSv1.2	ECC-DHE	RSA	AES-GCM(256)
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)

Citrix 密码名称	OpenSSL 密码名	十六进制码	协议	密钥交换算法	身份验证算法	消息验证码 (MAC) 算法
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-AES-256-CBC-SHA	DHE-RSA-AES256-SHA	0x0039	SSLv3	DH	RSA	AES(256)
TLS1-DHE-RSA-AES-128-CBC-SHA	DHE-RSA-AES128-SHA	0x0033	SSLv3	DH	RSA	AES(128)
TLS1-DHE-DSS-AES-256-CBC-SHA	DHE-DSS-AES256-SHA	0x0038	SSLv3	DH	DSS	AES(256)
TLS1-DHE-DSS-AES-128-CBC-SHA	DHE-DSS-AES128-SHA	0x0032	SSLv3	DH	DSS	AES(128)
TLS1-ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA-DES-CBC3-SHA	0xC012	SSLv3	ECC-DHE	RSA	3DES(168)
SSL3-EDH-RSA-DES-CBC3-SHA	EDH-RSA-DES-CBC3-SHA	0x0016	SSLv3	DH	RSA	3DES(168)
SSL3-EDH-DSS-DES-CBC3-SHA	EDH-DSS-DES-CBC3-SHA	0x0013	SSLv3	DH	DSS	3DES(168)

Citrix 密码名称	OpenSSL 密码名	十六进制码	协议	密钥交换算法	身份验证算法	消息验证码 (MAC) 算法
TLS1-ECDHE-RSA-RC4-SHA	ECDHE-RSA-RC4-SHA	0xC011	SSLv3	ECC-DHE	RSA	RC4(128)
SSL3-DES-CBC3-SHA	DES-CBC3-SHA	0x000A	SSLv3	RSA	RSA	3DES(168)
SSL3-RC4-SHA	RC4-SHA	0x0005	SSLv3	RSA	RSA	RC4(128)
SSL3-RC4-MD5	RC4-MD5	0x0004	SSLv3	RSA	RSA	RC4(128)
SSL3-DES-CBC-SHA	DES-CBC-SHA	0x0009	SSLv3	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	RSA (512)	RSA	RC2(40)
SSL2-DES-CBC-MD5	DHE-DSS-AES128-SHA256	0x0040	SSLv2	RSA	RSA	DES (56)
SSL3-EDH-DSS-DES-CBC-SHA	EDH-DSS-DES-CBC-SHA	0x0012	SSLv3	DH	DSS	DES (56)
SSL3-EXP-EDH-DSS-DES-CBC-SHA	EXP-EDH-DSS-DES-CBC-SHA	0x0011	SSLv3	DH (512)	DSS	DES (40)
SSL3-EDH-RSA-DES-CBC-SHA	EDH-RSA-DES-CBC-SHA	0x0015	SSLv3	DH	RSA	DES (56)
SSL3-EXP-EDH-RSA-DES-CBC-SHA	EXP-EDH-RSA-DES-CBC-SHA	0x0014	SSLv3	DH (512)	RSA	DES (40)
SSL3-ADH-RC4-MD5	ADH-RC4-MD5	0x0018	SSLv3	DH	无	RC4(128)

Citrix 密码名称	OpenSSL 密码名	十六进制码	协议	密钥交换算法	身份验证算法	消息验证码 (MAC) 算法
SSL3-ADH-DES-CBC3-SHA	ADH-DES-CBC3-SHA	0x001B	SSLv3	DH	无	3DES(168)
SSL3-ADH-DES-CBC-SHA	ADH-DES-CBC-SHA	0x001A	SSLv3	DH	无	DES (56)
TLS1-ADH-AES-128-CBC-SHA	ADH-AES128-SHA	0x0034	SSLv3	DH	无	AES(128)
TLS1-ADH-AES-256-CBC-SHA	ADH-AES256-SHA	0x003A	SSLv3	DH	无	AES(256)
SSL3-EXP-ADH-RC4-MD5	EXP-ADH-RC4-MD5	0x0017	SSLv3	DH (512)	无	RC4(40)
SSL3-EXP-ADH-DES-CBC-SHA	EXP-ADH-DES-CBC-SHA	0x0019	SSLv3	DH (512)	无	DES (40)
SSL3-NULL-MD5	NULL-MD5	0x0001	SSLv3	RSA	RSA	无
SSL3-NULL-SHA	NULL-SHA	0x0002	SSLv3	RSA	RSA	无

预定义的密码组

下表列出了 SDX 设备提供的预定义密码组。

密码组名	说明
ALL	SDX 设备支持的所有密码，不包括空密码
DEFAULT	加密强度 >= 128 位的默认密码列表
kRSA	使用 Key-ex 算法作为 RSA 的密码
kEDH	使用 Key-ex 算法作为 Ephemeral-DH 的密码
DH	使用 Key-ex 算法作为 DH 的密码
EDH	使用 Key-ex/Auth 算法作为 DH 的密码

密码组名	说明
aRSA	使用身份验证算法作为 RSA 的密码
aDSS	使用身份验证算法作为 DSS 的密码
aNULL	使用身份验证算法为空的密码
DSS	使用身份验证算法作为 DSS 的密码
DES	使用 Enc 算法作为 DES 的密码
3DES	使用 Enc 算法作为 3DES 的密码
RC4	使用 Enc 算法作为 RC4 的密码
RC2	使用 Enc 算法作为 RC2 的密码
NULL	使用 Enc 算法为空的密码
MD5	使用 MAC 算法作为 MD5 的密码
SHA1	使用 MAC 算法作为 SHA-1 的密码
SHA	使用 MAC 算法作为 SHA 的密码
NULL	使用 Enc 算法为空的密码
RSA	使用 key-ex/Auth 算法作为 RSA 的密码
ADH	使用 Key-ex 算法作为 DH 和 Auth 算法为 NULL 的密码
SSLv2	SSLv2 协议密码
SSLv3	SSLv3 协议密码
TLSv1	SSLv3/TLSv1 协议密码
TLSv1_ONLY	TLSv1 协议密码
EXP	导出密码
EXPORT	导出密码
EXPORT40	使用 40 位加密导出密码
EXPORT56	导出带有 56 位加密的密码
LOW	低强度密码（56 位加密）
MEDIUM	中等强度的密码（128 位加密）
HIGH	高强度密码（168 位加密）
AES	AES 密码
FIPS	FIPS 批准的密码
ECDHE	椭圆曲线短暂的 DH 密码

密码组名	说明
AES-GCM	使用 Enc 算法作为 AES-GCM 的密码
SHA2	使用 MAC 算法作为 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

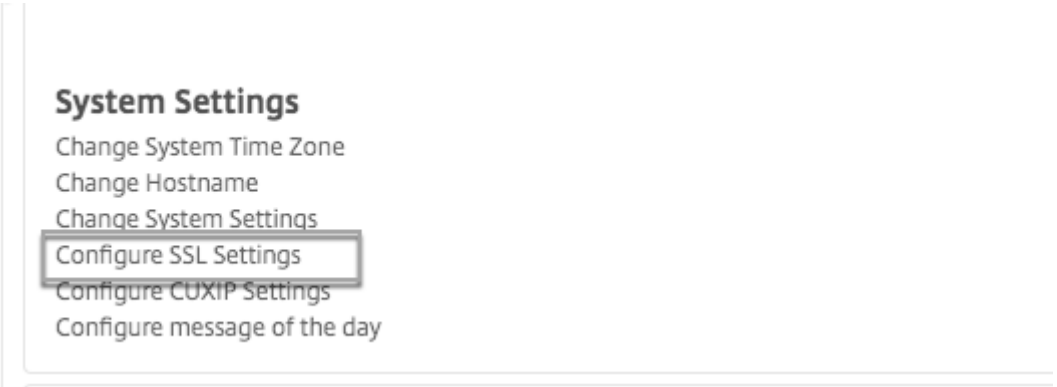
您可以从支持的 SSL 密码列表中创建自定义密码组。

要创建自定义密码组，请执行以下操作：

1. 在 配置 选项卡的导航窗格中，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”字段中，输入自定义密码组的名称。
    b) 在“密码组说明”字段中，输入自定义密码组的简要说明。
    c) 在“密码套件”部分中，单击“添加”，然后选择要包括在支持的 SSL 密码列表中的密码。
    d) 单击创建。

查看现有的 **SSL** 密码绑定

若要查看现有的密码绑定，请在“配置”选项卡的导航窗格中，展开“系统”，然后单击“系统设置”下的“配置 SSL 设置”。



> 注意：
>
> 升级到最新版本的管理服务后，现有密码套件列表将显示 OpenSSL 名称。绑定升级后的管理服务中的密码后，显示将使用 Citrix 命名约定。

将密码绑定到 **HTTPS** 服务

1. 在 配置 选项卡的导航窗格中，单击 系统。
2. 在“系统”窗格的“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：
   - 要从预定义的密码组中选择密码组，请选择“密码组”，从“密码组”列表中选择 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”。

备份和还原 **SDX** 设备的配置数据

February 16, 2024

NetScaler SDX 设备备份过程是一个单步过程，用于创建包含以下内容的备份文件：

- 单捆绑包图片：
  - Citrix Hypervisor 映像
  - Citrix Hypervisor 的修补程序和补充包
  - 管理服务映像
- XVA 图片
- 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。
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括管理服务的当前 IP 地址和进行备份的时间戳。要检查备份文件可能存在的任何差异，请从 SDX GUI 导航到 配置 **>** 系统 **>** 事件**/**警报。

定时备份

默认情况下，SDX 使用备份策略每 24 小时创建一次备份。使用备份策略，您可以定义要在 SDX 设备中保留的备份文件的数量。此外，您可以使用密码对定时备份文件进行加密，以确保备份文件的安全。

编辑备份策略

1. 在“配置”选项卡上，单击“系统”。
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“要保留的先前备份”字段中，键入要保留的备份文件数。
    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，键入并确认密码以加密备份文件。

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，选择要用来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的路径。
8. 选择 从管理服务删除文件，在将备份文件传输到外部备份服务器后，将备份文件从 SDX 设备中删除。
9. 单击确定。

还原设备

您可以将 SDX 设备还原为备份文件中提供的配置。在设备还原期间，将删除所有当前配置。

注意事项：

- 在使用其他 SDX 设备的备份文件还原 SDX 设备之前，请根据备份文件中的可用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。不支持在两个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还原 SDX 备份。您可以为 SVM 指定以下网络设置：
  - 支持向量机 IP 地址
  - 虚拟机管理程序 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“装置还原”，然后单击“继续”。

   将显示应用程序还原的不同组件：

   - 许可证
   - SDX 图片
   - XVA 文件
   - NetScaler 配置
   - 总结

   如果备份文件中缺少任何必需的组件，系统将提示您上载缺少的元素，然后再继续操作。

   要了解是否可以在当前 SDX Single Bundle 映像版本上还原备份文件，请参阅下表。作为单包映像的经验法则，任何较低版本的备份都无法在更高版本上恢复。

当前的 SDX 单捆绑包映像版本	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	12.1、13.0 支持、11.0、11.1、12.0 不支持
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，检查是否存在有效的许可证，然后单击 下一步。
5. 此时将显示“**SDX** 映像”页面。如果执行还原时不需要 SDX 映像，请单击“下一步”。否则，当系统提示时，请上载有效的 SDX 映像，然后单击下一步。

6. 此时将打开 **XVA** 文件 页面。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，您可以上载该文件或跳过还原此实例。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。您可以在不恢复其配置的情况下预配置实例。如果备份文件中缺少 NetScaler 配置文件，则只能继续进行实例置备，也可以跳过还原实例。单击“下一步”转到下一页。
8. 此时将显示摘要页面，其中包含有关备份文件中存在的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恢复，则会出现复选标记。如果不是，则会出现一个十字标记。
   - 错误消息：如果设备或实例尚未准备好恢复，则会显示一条错误消息以解释原因。
9. 单击“还原”以完成应用程序还原过程。

恢复 **NetScaler** 实例

您可以将 SDX 设备中的 NetScaler 实例恢复到备份文件中可用的 NetScaler 实例。

注意事项：如果出现以下 情况，VPX 实例将无法还原：

- 实例没有分配管理 NIC，并且
- 该实例只能通过 LACP 从 SDX 管理服务进行管理。
  恢复失败，因为 SDX 管理服务无法自动恢复通道配置。为避免此问题，请手动还原通道配置以完成 VPX 实例还原。

要在备份文件中还原 **NetScaler** 实例，请执行以下操作：

1. 在配置选项卡的导航窗格中，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：
>
> 确保运行正在恢复的实例的 SDX 设备上存在相应的 XVA、编译映像和通道配置。

执行设备重置

November 23, 2023

NetScaler SDX 设备允许您：

- 重置设备的配置。

  > 注意：
  >
  > 重置配置时，必须使用装置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，包括在设备上配置的所有 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当前与管理服务的所有客户端会话。重新登录到管理服务以执行任何其他配置任务。准备好还原数据时，请使用管理服务导入备份文件。

管理服务提供以下选项来重置设备：

- 配置重置
- 恢复出厂设置
- 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默认设置。
- 删除管理服务映像。
- 删除 NetScaler SDX 映像。
- 删除除在设备上访问的最后一个映像文件之外的所有 XVA 映像。
- 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 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“装置重置”。
3. 在“装置重置”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以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。

确保备份设备上存储的所有数据，包括设备上配置的所有 NetScaler 实例的设置。Citrix 建议您将文件存储在设备外部。执行恢复出厂设置会终止当前与管理服务的所有客户端会话。重新登录到管理服务以执行任何其他配置任务。准备好还原数据时，请使用管理服务导入备份文件。

> 重要提示
>
> 在执行恢复出厂设置之前，请确保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“装置重置”。
3. 在“装置重置”对话框中，从“重置类型”列表中选择“恢复出厂 设置”。
4. 单击确定。

将设备重置为单包映像版本

管理服务提供了“全新安装”选项，允许您在设备上安装任意版本的单个分发包映像。它使您能够全新安装单个软件包映像作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（网络设置除外）。

> 注意：
>
> 如果您的 SDX 设备随软件版本 11.0 或更早版本一起提供，则全新安装到版本 13.1 或更高版本将失败。

以下版本支持全新安装选项：

单捆绑包映像版本	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，则支持全新安装选项。

单捆绑包映像版本	SDX 平台
11.1.xx	SDX 14xxx、SDX 25xxx。注意：如果其他 SDX 平台具有 10G 出厂分区，则支持全新安装选项
11.1.51.x	所有的 SDX 平台。
12.1.xx	所有的 SDX 平台。
13.0.xx	所有的 SDX 平台。
13.1.xx	所有的 SDX 平台。

必备条件

请确保：

- 将所有主高可用性节点故障切换到其他 SDX 设备。如果您没有高可用性功能，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：
>
> 确保在使用“全新安装”选项时不要重新启动或重启设备。
> 设备会多次重新启动。

将设备重置为单包映像版本

1. 导航到“配置”**>**“系统”**>**“系统管理”组。
2. 单击“装置重置”。
3. 在“装置重置”对话框中，从“重 置类型”列表中选择“全新 安装”。
4. 单击确定。

级联外部身份验证服务器

February 16, 2024

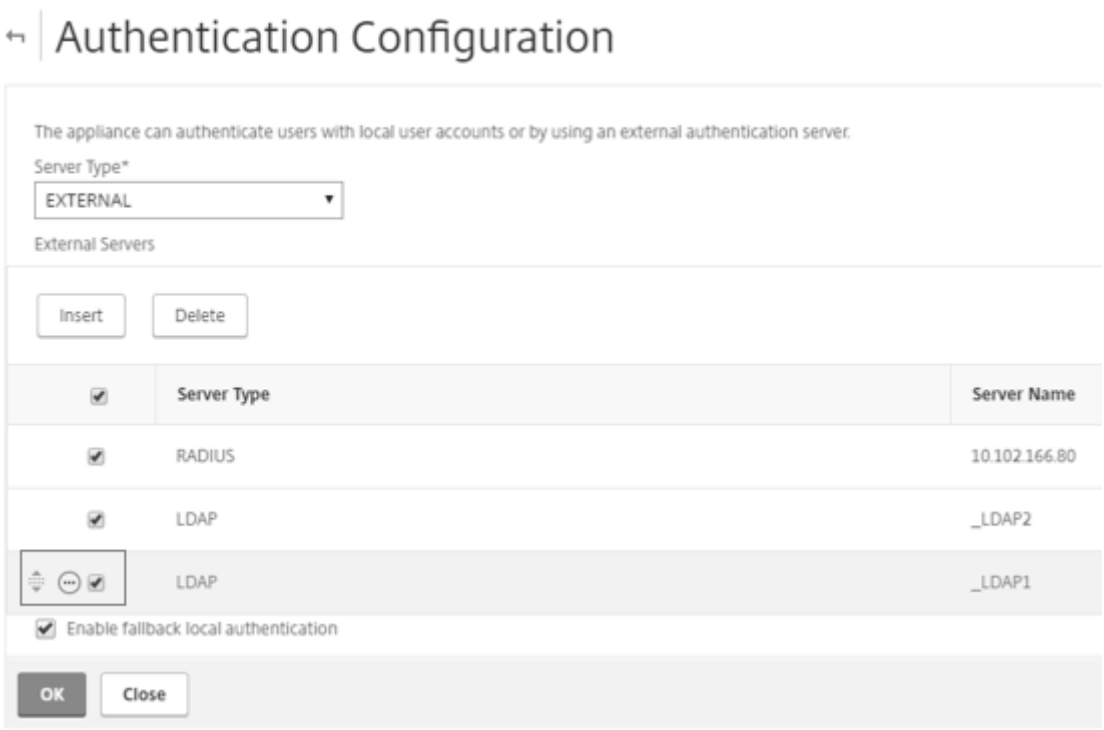
级联多个外部身份验证服务器为对外部用户进行身份验证和授权提供了一个连续、可靠的过程。如果第一个身份验证服务器上的身份验证失败，管理服务将尝试使用第二个外部身份验证服务器对用户进行身份验证。

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。可以添加任何类型的受支持的外部身份验证服务器（RADIUS、LDAP 和 TACACS）。例如，要添加四个用于级联身份验证的外部身份验证服务器，可以添加 RADIUS、LDAP 和 TACACS 服务器的任意组合。您还可以添加同一类型的所有四台服务器。您可以在 NetScaler Application Delivery Management 中配置多达 32 个外部身份验证服务器。

级联外部身份验证服务器

1. 在 配置 选项卡的 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 **EXTERNAL**（只能级联外部服务器）。
4. 单击“插入”，然后在打开的“外部服务器”页上，选择要级联的一个或多个身份验证服务器。
5. 单击确定。

所选服务器将显示在“身份验证服务器”页面上，如下图所示。要更改身份验证的顺序，请使用服务器名称旁边的图标在列表中上移或下移服务器。



解锁用户

November 23, 2023

NetScaler SDX 管理员可以在封锁间隔到期之前解锁用户。如果用户通过控制台登录管理服务，则不适用锁定。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“解锁”。

使用 **CLI** 解锁用户

在命令提示符下，键入：

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

配置 **NetScaler** 实例

November 23, 2023

> 注意
>
> 在您安装或升级 NetScaler SDX 设备到 13.1 版后，NetScaler ADM 服务连接默认处于启用状态。有关更多详细信息，请参阅 数据治理 和 NetScaler ADM 服务连接。

您可以使用管理服务在 SDX 设备上预置一个或多个 NetScaler 实例。您可以安装的实例数量取决于您购买的许可证。如果添加的实例数等于许可证中指定的数量，则管理服务不允许配置更多 NetScaler 实例。

> 注意：
>
> 您最多可以在独立于底层硬件平台的网络接口上配置 20 个 VPX 实例。

在 SDX 设备上预配 NetScaler VPX 实例包括以下步骤。

1. 定义要连接到 NetScaler 实例的管理员配置文件。此配置文件指定管理服务用于置备 ADC 实例以及稍后与实例通信以检索配置数据的用户凭证。您还可以使用默认的管理员配置文件。
2. 将.xva 映像文件上载到管理服务。
3. 使用管理服务中的“配置 NetScaler”向导添加 NetScaler 实例。管理服务在 SDX 设备上隐式部署 NetScaler 实例，然后下载该实例的配置详细信息。

> 警告
>
> 请确保使用管理服务修改实例的预配置网络接口或 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了管理服务在配置 NetScaler 实例时使用的用户凭证。稍后在与实例通信以检索配置数据时会使用这些凭证。客户端通过 CLI 或 GUI 登录 NetScaler 实例时也使用管理员配置文件中指定的用户凭证。

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 进行通信。

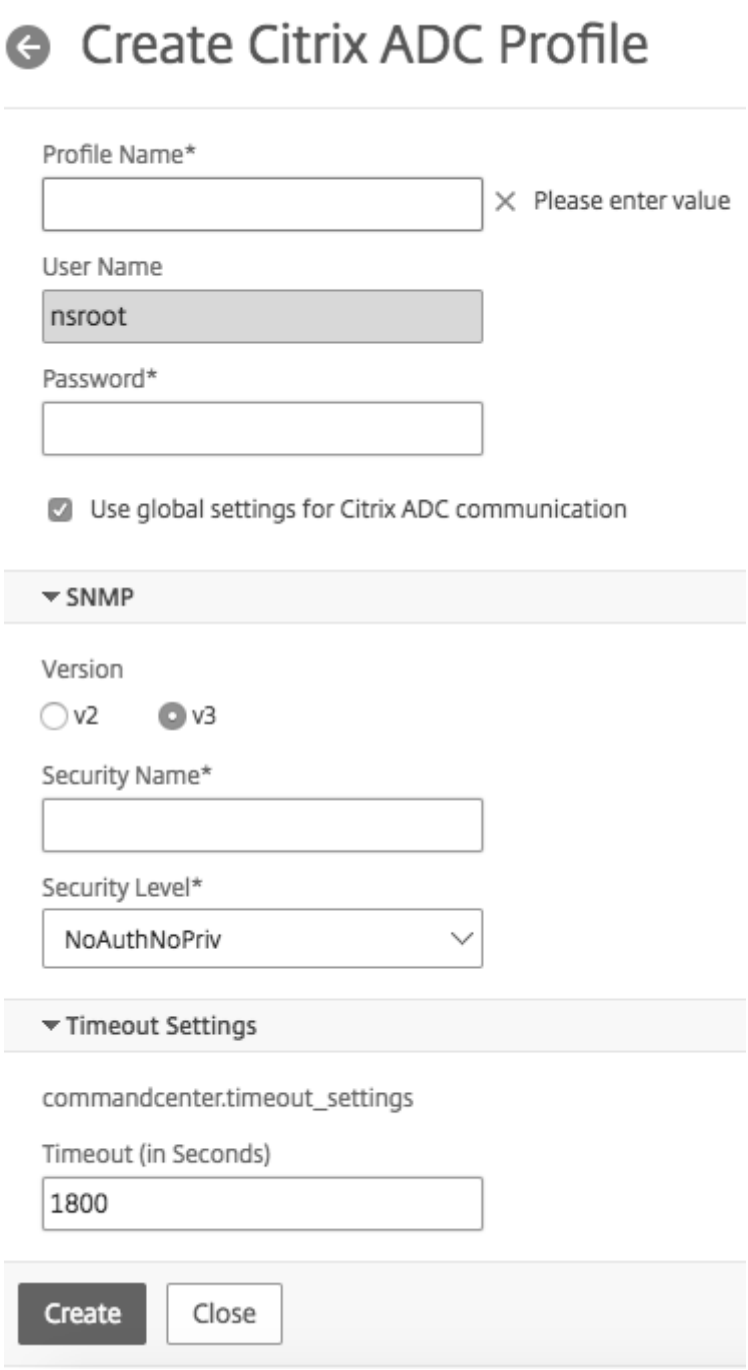
实例的默认管理员配置文件指定默认管理员用户名。无法修改或删除此配置文件。但是，您必须通过创建用户定义的管理员配置文件并在置备实例时将其附加到实例来覆盖默认配置文件。如果用户定义的管理员配置文件未附加到任何 NetScaler 实例，则管理服务管理员可以删除该配置文件。

> 重要提示
>
> 请勿直接在 VPX 实例上更改密码。如果这样做，则无法从管理服务访问实例。要更改密码，请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。

要在高可用性设置中更改 NetScaler 实例的密码，请先更改指定为辅助节点的实例的密码。然后在指定为主节点的实例上更改密码。请记住，只能使用管理服务来更改密码。

创建管理员配置文件

1. 在配置选项卡的导航窗格中，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. 此时将显示“创建管理员配置文件”对话框。



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 **NetScaler** 通信的全局设置：如果要在“系统设置”中定义管理服务与 NetScaler 实例之间通信的设置，请选择此选项。您可以清除此复选框，然后将协议更改为 HTTP 或 HTTPS。

- 选择 **http** 选项，使用 HTTP 协议在管理服务与 NetScaler 实例之间进行通信。
- 选择 **https** 选项，使用安全通道在管理服务与 NetScaler 实例之间进行通信。

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 团体 名称。

6. 在 SNMP v3 下，添加 安全名称 和 安全级别。

7. 在“超时设置”下，指定值。

8. 单击“创建”，然后单击“关闭”。您创建的管理员配置文件显示在“管理员配置文件”窗格中。

如果“默认”列中的值为 true，则默认配置文件为管理员配置文件。如果值为 false，则用户定义的配置文件就是管理员配置文件。

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“管理员配置文件”窗格中选择要删除的配置文件，然后单击“删除”。

上载 **NetScaler .xva** 图片

添加 NetScaler VPX 实例需要.xva 文件。

在配置 VPX 实例之前，将 NetScaler SDX .xva 文件上载到 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 图像文件格式为：`NSVPX-XEN-ReleaseNumber-BuildNumber_nc`.xva。

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

- 名称：.xva 映像文件的名称。文件名包含发行版和内部版本号。例如，文件名 `NSVPX-XEN-12.1-56.22.xva.gz` 是指发行版 12.1 版本 56.22。
- 上次修改时间：上次修改.xva 映像文件的日期。
- 大小：.xva 图像文件的大小（以 MB 为单位）。

上载 **NetScaler .xva** 文件

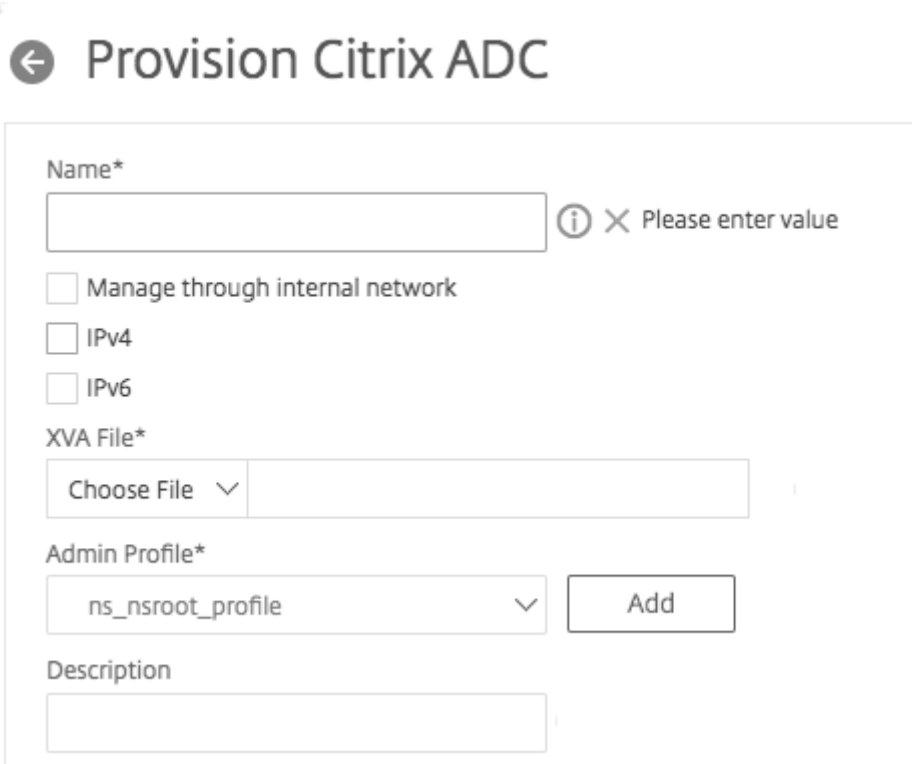
1. 在“配置”选项卡的导航窗格中，展开“**NetScaler** 配置”，然后单击“**XVA** 文件”。
2. 在 **NetScaler XVA** 文件 窗格中，单击 上载。
3. 在上 传 **NetScaler** 实例 **XVA** 对话框中，单击 浏览，然后选择要上载的 XVA 映像文件。
4. 单击上载。上载后，XVA 映像文件将显示在 **NetScaler XVA** 文件 窗格中。

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。管理服务在 NetScaler 实例上隐式配置这些设置。



- 名称：为 NetScaler 实例指定一个名称。
- 选择“通过内部网络管理”，在 SDX 管理服务与 VPX 实例之间启用独立的内部常开连接。在 SDX 设备上运行的 13.0-36.27 及更高版本的 VPX 实例支持此功能。
- 出于管理目的，选择 IPv4 或 IPv6 地址或同时选择 IPv4 和 IPv6 地址来访问 NetScaler VPX 实例。一个 NetScaler 实例只能有一个管理 IP (NSIP)。无法删除 NSIP 地址。
- 为该 IP 地址分配网络掩码、默认网关和 nexthop 给管理服务。
- 在以下任一条件下，当 VPX 配置版本为 13.0—88.9 或 13.1—37.8 及其更高版本时，网关和 **Nexthop** 到管理服务字段是可选的：
  - 启用了“通过内部网络管理”时。
  - 当配置的 IPv4 地址与管理服务 IP 地址位于同一子网时。

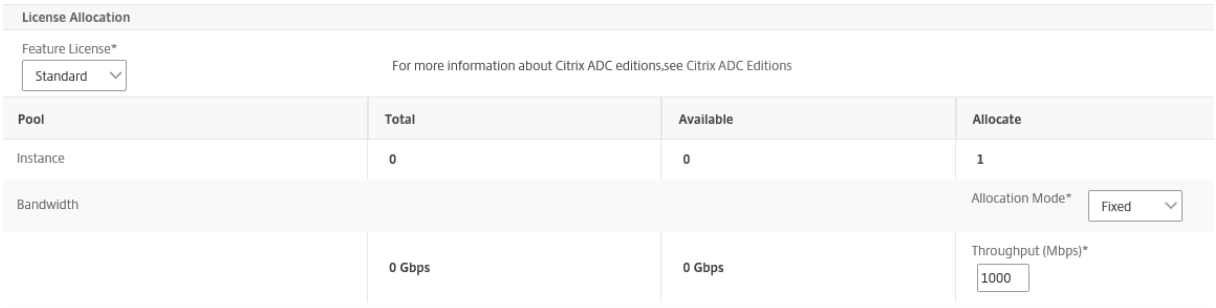
接下来，添加 XVA 文件、管理员配置文件和实例描述。

注意：对于高可用性设置（主动-主动或活动-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 购买的许可证。许可证可以是标准版、企业版和白金版。

注意：星号表示必填字段。



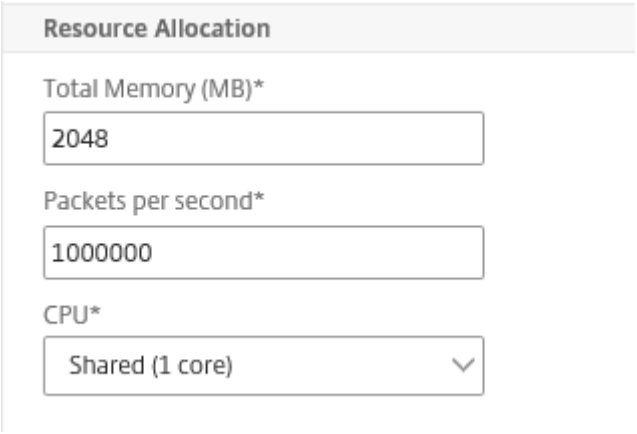
如果您需要带宽突增能力，请在分配模式下选择可突增。有关更多信息，请参阅 SDX 中的带宽计量。

加密货币分配

从版本 12.1 48.13 开始，管理加密容量的接口已经改变。有关更多信息，请参阅 管理加密容量。

资源分配

在资源分配下，分配总内存、每秒数据包数和 CPU。



CPU

为实例分配一个或多个专用内核，或者实例与其他实例共享一个核心。如果您选择 shared，则会将一个核心分配给实例，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 CPU 核心，请重启受影响的实例。重启已重新分配 CPU 核心的实例，以避免性能下降。

从 SDX 11.1.x.x (MR4) 版本开始，如果您使用的是 SDX 25000xx 平台，则最多可以为一个实例分配 16 个内核。此外，如果您使用的是 SDX 2500xxx 平台，则最多可以为实例分配 11 个内核。

注意：对于实例，您配置的最大吞吐量为 180 Gbps。

下表列出了受支持的 VPX、Single bundle 映像版本以及可以分配给实例的内核数：

平台名称	核心总数	可用于 VPX 预配的内核总数	可分配给单个实例的最大核心数
SDX 8015、SDX 8400 和 SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500、SDX 13500、SDX 14500、SDX 16500、SDX 18500 和 SDX 20500	12	10	5
SDX 11515、SDX 11520、SDX 11530、SDX 11540 和 SDX 11542	12	10	5
SDX 17500、SDX 19500 和 SDX 21500	12	10	5
SDX 17550、SDX 19550、SDX 20550 和 SDX 21550	12	10	5

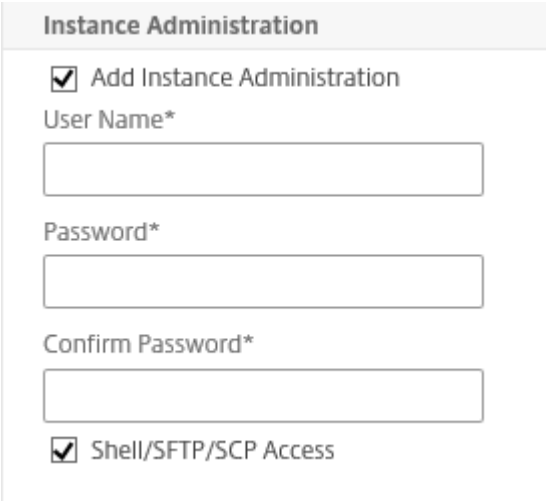
平台名称	核心总数	可用于 VPX 预配的内核总数	可分配给单个实例的最大核心数
SDX 14020、SDX 14030、SDX 14040、SDX 14060、SDX 14080 和 SDX 14100	12	10	5
SDX 22040、SDX 22060、SDX 22080、SDX 22100 和 SDX 22120	16	14	7
SDX 24100 和 SDX 24150	16	14	7
SDX 14020 40G、SDX 14030 40G、SDX 14040 40G、SDX 14060 40G、SDX 14080 40G 和 SDX 14100 40G	12	10	10
SDX 14020 FIPS、SDX 14030 FIPS、SDX 14040 FIPS、SDX 14060 FIPS、SDX 14080 FIPS 和 SDX 14100 FIPS	12	10	5
SDX 14040 40S、SDX 14060 40S、SDX 14080 40S 和 SDX 14100 40S	12	10	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 或更高版本）；9（如果版本为 11.1-50.x 或更低；所有版本为 11.0 和 10.5）
SDX 26100、26160、26200、26250	28	26	16
SDX 26100-50S、26160-50S、26200-50S、26250-50	28	26	16
SDX 26100-100G、26160-100G、26200-100G、26250-100G	28	26	25

平台名称	核心总数	可用于 VPX 预配的内核总数	可分配给单个实例的最大核心数
SDX 15000	16	14	14
SDX 15000-50G	16	14	14
SDX 9100	10	9	9
SDX 16000	32	30	16

> 注意：
>
> 专用内核映射到实例上运行的数据包引擎的数量。对于使用专用内核创建的 VPX 实例，将额外分配一个 CPU 用于管理。

实例管理

您可以通过选择“实例管理”下的“添加实例管理”来为 VPX 实例创建管理员用户。



添加以下详细信息：

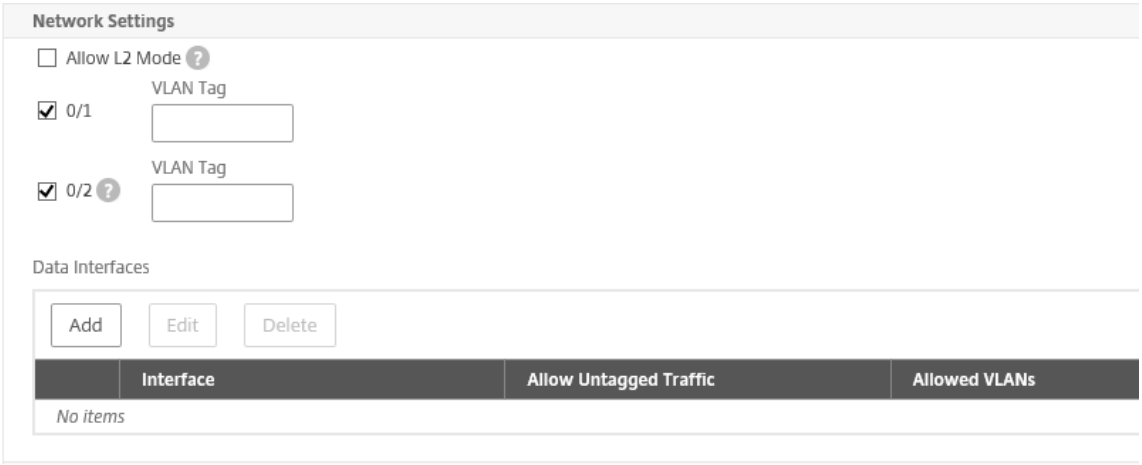
用户名： NetScaler 实例管理员的用户名。此用户具有超级用户访问权限，但无权访问联网命令来配置 VLAN 和接口。

密码：用户名的密码。

Shell/Sftp/Scp 访问权限： NetScaler 实例管理员的访问权限。此选项默认处于选中状态。

网络设置

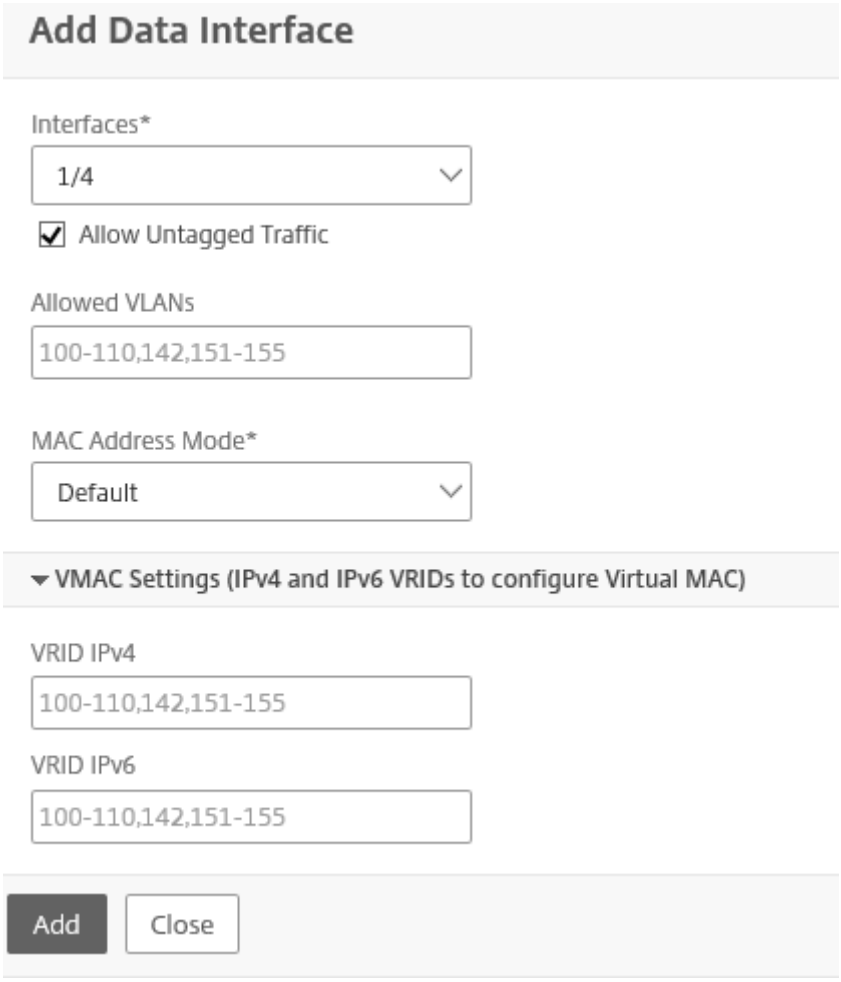
- 允许 **L2** 模式：您可以在 NetScaler 实例上允许 L2 模式。在“网络设置”下选择“允许 **L2** 模式”。在登录实例并启用 L2 模式之前。有关更多信息，请参阅在 NetScaler 实例上允许 L2 模式。



> 注意：
>
> – 如果您通过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。如果不这样做，可能会导致在重启实例后禁用所有其他 NetScaler 模式
> – 在 SDX 上配置 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，为管理 LA 选择接口 0/1 和 0/2。
- **VLAN** 标记：为管理接口指定一个 VLAN ID。接下来，添加数据接口。

> 注意：
>
> 添加到实例的接口的接口 ID 不一定与 SDX 设备上的物理接口编号相对应。如果您与实例 1 关联的第一个接口是接口 1/4，则当您查看实例上的接口设置时，它将显示为接口 1/1。编号会发生变化，因为它是您与实例 1 关联的第一个接口。



- 允许未标记的流量：选中“允许未标记流量”复选框以允许 NetScaler 实例处理未标记的流量。

  > 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，即使清除“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。

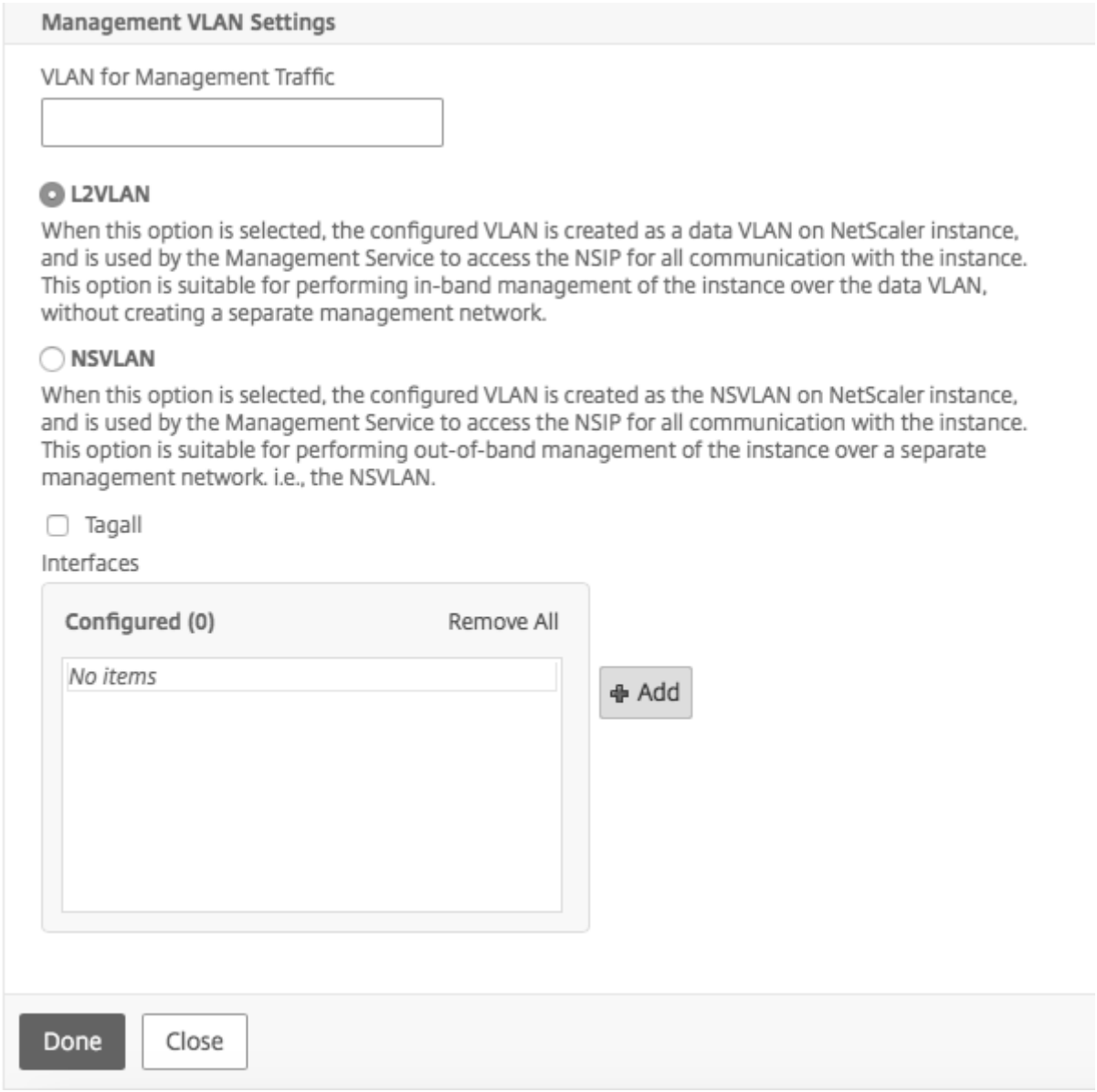
- 允许的 **VLAN**：指定可以与 NetScaler 实例关联的 VLAN ID 列表。
- **MAC** 地址模式：分配一个 MAC 地址。选择以下选项之一：
  - 默认值： Citrix Hypervisor 分配一个 MAC 地址。
  - 自定义：选择此模式可指定覆盖生成的 MAC 地址的 MAC 地址。
  - 已生成：使用先前设置的基本 MAC 地址生成 MAC 地址。有关设置基本 MAC 地址的信息，请参阅 为接口分配 MAC 地址。
- VMAC 设置（用于配置虚拟 MAC 的 IPv4 和 IPv6 VRID）
  - **VRID IPV4**：用于标识 VMAC 的 IPv4 VRID。可能的值：1—255。有关更多信息，请参阅在接口上配置 VMAC。

- **VRID IPV6**：用于标识 VMAC 的 IPv6 VRID。可能的值：1—255。有关更多信息，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) 位于同一个子网中，并且通过管理接口进行通信。但是，如果管理服务和实例位于不同的子网中，则必须在置备 VPX 实例时指定 VLAN ID。此 ID 是必需的，以便实例在启动时可以通过网络进行访问。如果您的部署要求只有在置备 VPX 实例时选择的接口才能访问 NSIP，请选择 NSVLAN 选项。

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



注意：

- HA 检测信号仅在属于 NSVLAN 的接口上发送。
- 只能从 VPX XVA 版本 9.3 53.4 及更高版本中配置 NSVLAN。

重要：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 完成 以配置 NetScaler VPX 设备。

修改 **NetScaler** 实例

要修改已配置 ADC 实例的参数值，请在 **NetScaler** 实例窗格中选择要修改的实例，然后单击修改。在“修改 ADC 向导”中，修改参数。

注意事项：

- 如果您修改以下参数：SSL 芯片数量、接口数量、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 设备上配置的 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** 限制在特定的虚拟接口上

SDX 设备管理员可以在与 NetScaler 实例关联的虚拟接口上强制实施特定的 802.1Q VLAN。此功能在限制实例管理员使用 802.1Q VLAN 时特别有用。如果属于两个不同公司的两个实例托管在 SDX 设备上，则可以限制两家公司使用相同的 VLAN ID。这样，一家公司就看不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，则会执行验证以验证指定的 VLAN ID 是否属于允许列表的一部分。

默认情况下，任何 VLAN ID 都可以在接口上使用。要限制接口上带标签的 VLAN，请在配置 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它。要指定范围，请用连字符分隔 ID（例如 10-12）。如果您最初指定了一些 VLAN ID，但后来又从允许列表中删除了所有这些 VLAN ID，则可以使用该接口上的任何 VLAN ID。实际上，您已经恢复了默认设置。

创建允许的 VLAN 列表后，SDX 管理员无需登录实例即可创建 VLAN。管理员可以在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. 在配置 ADC 向导或修改 ADC 向导中，在网络设置页面的 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的 VLAN 的整数。NetScaler 最多支持 4094 个 VLAN。ID 1 是为默认 VLAN 保留的。
   - IPV6 动态路由—在此 VLAN 上启用所有 IPv6 动态路由协议。注意：要使 **ENABLED** 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. 选择必须是 VLAN 一部分的接口。
6. 单击“创建”，然后单击“关闭”。

管理加密容量

November 23, 2023

从版本 12.1 48.13 开始，管理加密容量的接口已经改变。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。早期的加密容量是以 SSL 芯片，SSL 核心和 SSL 虚拟功能为单位分配的。有关传统 SSL 芯片如何转换为 ACU 和 SCU 单元的更多信息，请参阅传统 SSL 芯片到 ACU 和 SCU 的转换表。

通过使用管理服务 GUI，您可以以 ACU 和 SCU 为单位向 NetScaler VPX 实例分配加密容量。

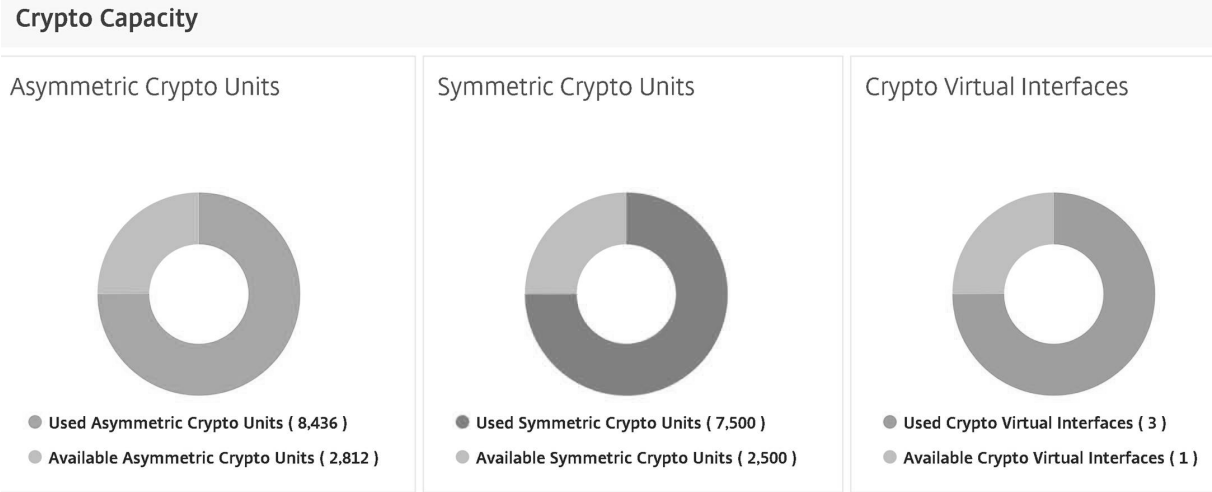
下表提供了有关 ACU、SCU 和加密虚拟实例的简要说明。

桌子。单位加密单位

新的加密单位	说明
非对称加密单元 (ACU)	1 ACU = (RSA) 2 K（2048 位密钥大小）解密的每秒 1 次操作 (ops)。有关更多详细信息，请参阅 ACU 到 PKE 的资源转换表。
对称加密单元 (SCU)	1 个 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函数，代表 SSL 硬件的基本单元。在这些接口用尽后，无法再将 SSL 硬件分配给 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 控制面板 **>** 加密容量。



在预配 **VPX** 实例时分配加密容量

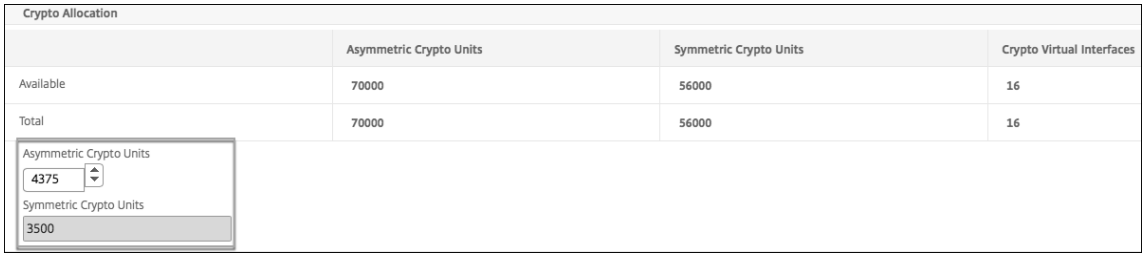
在 SDX 设备上配置 VPX 实例时，您可以在 加密分配下为 VPX 实例分配 ACU 和 SCU 的数量。有关预配 VPX 实例的说明，请参阅预配 NetScaler 实例。

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。分配 ACU 和 SCU 的方式因 SDX 设备而异：

   a. 对于不同 SDX 设备可用的 ACU 计数器的最小值中列出的装置，您可以按指定数量的倍数分配 ACU。SCU 会自动分配，SCU 分配字段不可编辑。您可以使用该型号可用的最小 ACU 的倍数来增加 ACU 分配。例如，如果最小 ACU 为 4375，则 ACU 增量为 8750、13125，依此类推。

   示例。加密分配，其中自动分配 SCU，ACU 以指定数量的倍数分配。

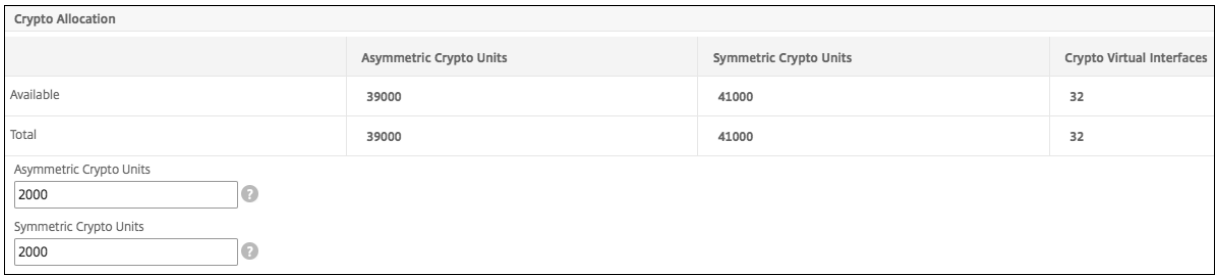


适用于不同 **SDX** 设备的 **ACU** 计数器的最小值

SDX 平台	ACU 计数器最小值
22040、22060、22080、22100、22120、24100、24150（36 个端口）	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 40S	4375
14xxx 40G	4375
14xxx FIPS	4375
25xxx	4375
25xxx A	4575

b. 对于上表中未列出的其余 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。

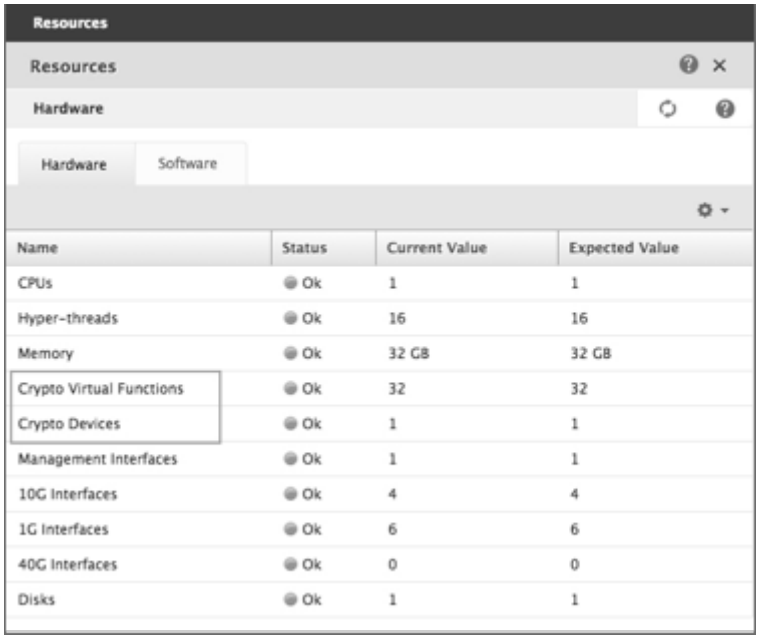
示例。ACU 和 SCU 均可自由分配的加密货币分配



4./ 完成配置 VPX 实例的所有步骤，然后单击 完成。有关更多信息，请参阅预配 NetScaler 实例。

查看加密硬件运行状况

在管理服务中，您可以查看随 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 控制板 **>** 资源。



注意事项

将 SDX 设备升级到最新版本时，请记住以下几点。

- 只有 SDX 用户界面得到升级，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 上的表示会发生变化。
- 加密接口向后兼容，不会影响使用 NITRO 接口管理 SDX 设备的任何现有自动化机制。
- SDX 设备升级后，分配给现有 VPX 实例的加密不会更改；只会更改其在管理服务中的表示形式。

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、24150（36 个端口）	2187	12497	2187	312	256	190

SDX 平台	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
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、22080,22100、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, 14000-40G, 25000, 25000A	4375	25000	4375	625	512	381
14000 FIPS	4375	25000	4375	625	512	381
14000-40S	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

SDX 平台	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
*26000-100G (26100、26160、26200 和 26250)	1000	4615	1000	136	397	494
*15000	1000	4615	1000	136	397	494
*15000-50G	1000	4615	1000	136	397	494
*16000	1000	4615	1000	136	397	494
*26000-50S	1000	4615	1000	136	397	494

* 在这些平台上，PKE 数字是最低保证值。

如何读取 **ACU** 到 **PKE** 的资源转换表

ACU 到 PKE 的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单独的 VPX。管理服务不能分配或承诺绩效。
- 实际性能因数据包大小、使用的 cipher/Keyex/HMAC（或其变体）等而异

以下示例可帮助您了解如何读取 ACU 并将其应用于 PKE 资源转换表。

示例。SDX 22040 平台的 ACU 到 PKE 资源转换

在 SDX 22040 平台上向 VPX 实例分配 2187 个 ACU 会分配相当于 256 个 ECDHE-RSA 操作或 2187 个 RSA-2K 操作等同的加密资源。

传统 **SSL** 芯片到 **ACU** 和 **SCU** 的转换表

有关如何将旧版 SSL 芯片转换为 ACU 和 SCU 的更多信息，请参阅下表。

ACU 和 SCU 转换表

置备第三方虚拟机

November 23, 2023

> 警告：
>
> 从版本 13.1 Build 37.x 起，NetScaler SDX GUI 中已不再支持 第三方实例。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 设备支持置备以下第三方虚拟机（实例）：

- SECUREMATRIX GSB
- InterScan Web Security
- 网信保护器
- BlueCat DNS/DHCP 服务器
- CA Access Gateway
- Palo Alto VM 系列

SECUREMATRIX GSB 提供了一个高度安全的密码系统，无需携带任何令牌设备。Websense Protector 提供监视和阻止功能，防止数据丢失和敏感信息泄露。BlueCat DNS/DHCP 服务器为您的网络提供 DNS 和 DHCP。NetScaler SDX 上的 Palo Alto VM 系列支持在单个平台上整合高级安全和 ADC 功能，使企业和服务提供商客户能够安全、可靠地访问应用程序。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 ADC 解决方案。

您可以通过管理服务预置、监视、管理和排除实例故障。上述所有第三方实例都使用 `SDXTools` 守护程序与管理服务进行通信。守护程序已预先安装在预配置的实例上。当有新版本可用时，您可以升级守护进程。

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，因为第三方虚拟机不支持通道。

> 注意：
>
> 您可以在 SDX 设备上置备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，必须将 Citrix Hypervisor 版本升级到版本 6.1.0。

SECUREMATRIX GSB

November 23, 2023

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，易于使用且具有成本效益。它使用列表表中的位置、序列和图像模式的组合来生成一次性密码。带有 SECUREMATRIX 身份验证服务器的 SECUREMATRIX

GSB 服务器大大增强了 VPN/SSL-VPN 端点、基于云的应用程序和资源、桌面/虚拟桌面登录和 Web 应用程序（带有 OTP 的反向代理）的安全性。它提供了与 PC，虚拟桌面，平板电脑和智能手机兼容的解决方案。

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其他租户或通过 NetScaler 提供的云服务集成，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。

有关更多信息，请参阅 SECUREMATRIX。

预置 **SECUREMATRIX GSB** 实例

SECUREMATRIX GSB 需要一个必须在 SDX 设备外部配置的 SECUREMATRIX 身份验证服务器。只选择一个接口，然后仅为该接口指定网络设置。

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。SECUREMATRIX GSB 实例不支持通道。

在开始配置实例之前，请从 SECUREMATRIX 网站下载 XVA 映像并将其上载到 SDX 设备。有关下载 XVA 映像的更多信息，请参阅 SECUREMATRIX 网站。确保在 SDX 设备上使用管理服务版本 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，请执行以下操作：

1. 在详细信息窗格的 **XVA** 文件 **>** 操作下，单击 上载。
2. 在出现的对话框中，单击“浏览”，然后选择要上载的 XVA 文件。
3. 单击上载。XVA 文件出现在 XVA 文件窗格中。

预置 **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 预配 **SECUREMATRX GSB** 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”。

预配置实例后，登录实例并执行详细配置。有关更多信息，请参阅 SECUREMATRIX 网站。

要修改已置备的 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的名称，则实例会停止并重新启动以使更改生效。

生成 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 为技术支持生成 Tar 存档。

备份 SECUREMATRIX GSB 实例的配置，然后使用备份数据在 SDX 设备上还原实例的配置。有关备份和还原实例的信息，请参阅 备份和还原 SDX 设备的配置数据。

监视 **SECUREMATRIX GSB** 实例

SDX 设备收集统计信息，例如 SDXTools 的版本、SSH 和 CRON 守护程序的状态以及 SECUREMATRIX GSB 实例的 Web 服务器状态。

要查看与 SECUREMATRIX GSB 实例相关的统计信息，请执行以下操作：

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、重启、强制停止或强制重启 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，请执行以下操作：

1. 单击“实例”。
2. 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，用于管理服务和实例之间的通信。

升级 SDXTools 包括将文件上载到 SDX 设备，然后 SDXTools 在选择实例后进行升级。您可以将 SDXTools 文件从客户端计算机上载到 SDX 设备。

要上传 **SDXTools** 文件，请执行以下操作：

1. 在导航窗格中，展开“管理服务”，然后单击“**SDxTools** 文件”。
2. 在详细信息窗格的 操作 列表中，选择 上载。
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. 单击上载。

要升级 **SDxTools**，请：

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 **SDxT**ools”。
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载到 SDX 设备，然后升级实例。降级会加载较早版本的实例。

在“配置”选项卡上，展开 **SECUREMATRIX GSB**。

要上载软件映像，请执行以下操作：

1. 单击“软件映像”。
2. 在详细信息窗格的 操作 列表中，选择 上载。
3. 在对话框中，单击“浏览”，导航到包含构建文件的文件夹，然后双击构建文件。
4. 单击上载。

要升级实例，请执行以下操作：

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，请执行以下操作：

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”。

对 **SECUREMATRIX GSB** 实例进行故障排除

从管理服务 ping 一个 SECUREMATRIX GSB 实例以检查设备是否可访问。您可以跟踪数据包从管理服务到实例的路由，以确定到达实例所涉及的跳数。

重新发现实例以查看实例的最新状态和配置。在重新发现过程中，管理服务会获取 SDX 设备上运行的 SECUREMATRIX GSB 的配置和版本。默认情况下，管理服务会每隔 30 分钟安排一次实例进行重新发现。

在“配置”选项卡上，展开 **SECUREMATRIX GSB**。

要 **ping** 实例，请执行以下操作：

1. 单击“实例”。
2. 在详细信息窗格中，选择要执行 ping 操作的实例，然后从 操作 列表中单击 **Ping**。Pingmessage 框显示 ping 是否成功。

要跟踪实例的路由，请执行以下操作：

1. 单击“实例”。
2. 在详细信息窗格中，选择要跟踪其路由的实例，然后从 操作 列表中单击 **TraceRoute**。Traceroute 消息框显示通往实例的路由。

要重新发现实例，请执行以下操作：

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”。

TrendMicro InterScan Web Security

November 23, 2023

TrendMicro InterScan Web Security 是一款软件虚拟设备，可在互联网网关上动态防御传统和新兴的 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，对于网络上越来越多地使用基于云的应用程序，它可以提供卓越的保护、更好的可视性和控制力。实时报告和集中管理为您的管理员提供了一个主动的决策工具，实现了现场风险管理。

InterScan Web Security：

- 允许更深入地了解最终用户的互联网活动
- 集中管理以实现最大程度的控制
- 监视 Web 使用情况
- 实现现场补救
- 减少设备蔓延和能源成本
- 提供可选的数据丢失保护和沙盒执行分析

必须先从 TrendMicro Web 站点下载 XVA 映像，然后才能置备 InterScan Web Security 实例。下载 XVA 映像后，将其上载到 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 Security 防护实例不支持通道。

要将 **XVA** 映像上传到 **SDX** 设备，请执行以下操作：

1. 从“配置”选项卡中，导航到 **TrendMicro IWSVA >** 软件映像。

2. 在详细信息窗格的“**XVA** 文件”选项卡下，单击“上载”。
3. 在出现的对话框中，单击“浏览”，然后选择要上载的 XVA 文件。
4. 单击上载。XVA 文件出现在 XVA 文件窗格中。

要预配 **TrendMicro IWSVA** 实例，请执行以下操作：

1. 在 配置 选项卡上，导航到 **TrendMicro IWSA >** 实例。
2. 在详细信息窗格中，单击“添加”。
3. 在 Provis **ion TrendMicro IWSA** 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”。

预配置实例后，登录该实例并执行详细配置。

要修改预置实例的参数值，请在详细信息窗格中选择要修改的实例，然后单击“编辑”。在修改 **TrendMicro IWSVA** 向导中，将参数设置为适合您环境的值。

网信保护器

November 23, 2023

Websense（现在称为 Forcepoint）数据安全保护器是一种拦截出站 HTTP 流量（帖子）的虚拟机。然后，它会分析流量，以防止数据丢失和敏感数据在网络上泄漏。保护程序与专用 Windows 服务器通信以获取 DLP 策略信息，并且可以在检测到匹配项时监视或阻止发布数据。内容分析是在包装盒上执行的，因此在此过程中不会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。

有关更多信息，请参阅 Websense Protector 网站。

预配一个 **Websense** 保护器实例

Websense© Protector 需要一个必须在 SDX 设备外部配置的数据安全管理服务器。只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器。对于名称服务器，键入提供此保护程序的域名服务器 (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 保护器实例不支持频道。

在开始配置实例之前，请从 Websense 网站下载保护器映像并将其上载到 SDX 设备。有关下载保护者图片的更多信息，请参阅 [Websense 网站。确保在 SDX 设备上使用管理服务版本 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** 映像上载到 **SDX** 设备

1. 在详细信息窗格的 **XVA** 文件 **>** 操作下，单击 上载。
2. 在出现的对话框中，单击“浏览”，然后选择要上载的 XVA 文件。
3. 单击上载。XVA 文件出现在 XVA 文件窗格中。

预配 **Websense** 保护器实例

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“配置 **Websense** 保护器”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”。

预配置实例后，登录实例并执行详细配置。

若要修改已置备的 Websense 保护器实例的设置，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 保护器”向导中，设置参数。请勿修改在预配 Websense 实例时选择的接口。只有在删除实例并配置新实例后，才能更改 XVA 文件。

您可以生成 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 为技术支持生成 Tar 存档。

监控 **Websense** 保护器实例

SDX 设备收集统计信息，例如 `SDXTools` 的版本、Websense© 数据安全策略引擎的状态以及数据安全代理状态。

要查看与 Websense 保护器实例相关的统计信息，请执行以下操作：

1. 导航到 **Websense** 保护器 **>** 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** 保护器实例

您可以从管理服务启动、停止、重启、强制停止或强制重启 Websense© 保护器实例。

在“配置”选项卡上，展开 **Websense** 保护器。

启动、停止、重启、强制停止或强制重启 **Websense** 保护器实例

1. 单击“实例”。
2. 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
- 强制重启

3. 在“确认”消息框中，单击“是”。

升级 **Websense Protector** 实例的 **SDX** 工具文件

SDXTools（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 包括将文件上载到 SDX 设备，然后 SDXTools 在选择实例后进行升级。您可以将 SDXTools 文件从客户端计算机上载到 SDX 设备。

上载 **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. 在详细信息窗格的 操作 列表中，选择 上载。
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. 单击上载。

升级 **SDX** 工具

在“配置”选项卡上，展开
Websense 保护器。

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 **SDxT**ools”。
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”。

将 **Websense Protector** 实例升级到更高版本

升级 Websense© protector 实例的过程包括将目标版本的软件映像上载到 SDX 设备，然后升级实例。

在“配置”选项卡上，展开 **Websense** 保护器。

上载软件映像

1. 单击“软件映像”。
2. 在详细信息窗格的 操作 列表中，选择 上载。
3. 在对话框中，单击“浏览”，导航到包含构建文件的文件夹，然后双击构建文件。
4. 单击上载。

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”。

排除 **Websense** 保护器实例故障

从管理服务 ping 一个 Websense 保护器实例，以检查设备是否可访问。您可以跟踪数据包从管理服务到实例的路由，以确定到达实例所涉及的跳数。

重新发现实例以查看实例的最新状态和配置。在重新发现过程中，管理服务会获取 SDX 设备上运行的 Websense 保护器的配置和版本。默认情况下，管理服务会每隔 30 分钟安排一次实例进行重新发现。

在“配置”选项卡上，展开 **Websense** 保护器。

ping 实例

1. 单击“实例”。
2. 在详细信息窗格中，选择要执行 ping 操作的实例，然后从 操作 列表中单击 **Ping**。Pingmessage 框显示 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，选择要跟踪其路由的实例，然后从 操作 列表中单击 **TraceRoute**。Traceroute 消息框显示通往实例的路由。

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/DH

November 23, 2023

BlueCat DNS/DHCP Server™ 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、可扩展和安全的 DNS 和 DHCP 核心网络服务，而不会产生额外的管理成本或数据中心空间。关键的 DNS 服务可以在单个系统中的多个 DNS 节点之间或多个 SDX 设备之间进行负载平衡，而无需更多硬件。

BlueCat DNS/DHCP Server™ 的虚拟实例可以托管在 SDX 上，以提供更智能的方式来连接移动设备、应用程序、虚拟环境和云。

要了解有关 BlueCat 和 Citrix 的更多信息，请访问 BlueCat 网站，网址为 https://citrixready.citrix.com/bluecat-networks.html。

如果您是 BlueCat 的现有客户，则可以通过 BlueCat 支持门户网站下载软件和文档，网址为 https://care.bluecatnetworks.com/。

预配 **BlueCat DNS/DHCP** 实例

从 BlueCat 客户关怀中心下载 XVA 映像，网址为 https://care.bluecatnetworks.com。下载 XVA 映像后，请先将其上载到 SDX 设备，然后再开始置备实例。确保在 SDX 设备上使用管理服务版本 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** 映像上载到 **SDX** 设备，请执行以下操作：

1. 在详细信息窗格的 **XVA** 文件 **>** 操作下，单击 上载。
2. 在出现的对话框中，单击“浏览”，然后选择要上载的 XVA 文件。
3. 单击上载。XVA 文件出现在 XVA 文件窗格中。

要预配 **BlueCat DNS/DHCP** 实例，请执行以下操作：

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 Add（添加）。此时将打开“设置 BlueCat DNS/DHCP 服务器”页面。
3. 在配置 BlueCat DNS/DHCP 向导中，按照屏幕上的说明进行操作。

    - 在实例创建下的名称字段中，输入实例的名称，然后从 XVA 文件下拉菜单中选择上载的映像，然后单击下一步。或者，在域名字段中，输入实例的域名。

      注意：名称不得包含空格。
    - 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，为该接口设置 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：

您可以为所有三个接口选择相同的接口。
您可以为所有三个接口选择不同的接口。

您可以为管理和服务选择相同的接口，但选择不同的接口以实现高可用性。
单击“完成”，然后单击“关闭”。实例创建、启动并使用选定的 IP 地址进行配置。

配置实例后，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 地址管理器控制下的详细信息，请参阅 BlueCat 文档，网址为 https://care.bluecatnetworks.com。

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，则实例会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，例如在实例上 SDXTools 运行的版本。

要查看与 **BlueCat DNS/DHCP** 实例相关的统计信息，请执行以下操作：

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、重启、强制停止或强制重启 BlueCat DNS/DHCP 实例。

在“配置”选项卡上，展开 **BlueCat DNS/DHCP**。

要启动、停止、重启、强制停止或强制重启 **BlueCat DNS/DHCP** 实例，请执行以下操作：

1. 单击“实例”。
2. 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
   - 强制重启
3. 在“确认”消息框中，单击“是”。

升级 **BlueCat DNS/DHCP** 实例的 **SDXTools** 文件

SDXTools（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 包括将文件上载到 SDX 设备，然后 SDXTools 在选择实例后进行升级。您可以将 SDXTools 文件从客户端计算机上载到 SDX 设备。

要上载 **SDXTools** 文件，请执行以下操作：

1. 在导航窗格中，展开“管理服务”，然后单击“**SDxTools** 文件”。
2. 在详细信息窗格的 操作 列表中，选择 上载。
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. 单击上载。

要升级 **SDXTools**，请执行以下操作：

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。在重新发现过程中，管理服务会获取配置。默认情况下，管理服务计划每 30 分钟对所有实例进行一次重新发现的实例。

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 Access Gateway

November 23, 2023

CA Access Gateway 是一款可扩展、可管理且可扩展的独立服务器，为访问控制提供基于代理的解决方案。CA Access Gateway 采用代理引擎，该引擎为企业提供网络网关，并支持不依赖传统基于 cookie 的技术的多个会话方案。

嵌入式 Web 代理可在整个企业中启用单点登录 (SSO)。CA Access Gateway 为 HTTP 和 HTTPS 请求以及无 cookie 的 SSO 提供访问控制。此外，该产品还会将会话信息存储在内存中的会话存储中。代理规则定义了 CA Access Gateway 如何将请求转发或重定向到位于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 将企业网络分开并集中访问控制。

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 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

您必须先下载 XVA 映像，然后才能预置 CA Access Gateway 实例。下载 XVA 映像后，将其上载到 SDX 设备。确保在 SDX 设备上使用管理服务版本 10.5 build 52.3.e 或更高版本。要配置 CA Access Gateway，首先需要将 XVA 映像上载到 SDX 设备，然后配置实例。

要将 **XVA** 映像上传到 **SDX** 设备，请执行以下操作：

1. 在 配置 选项卡上，导航到 **CA Access Gateway** > 软件映像。
2. 在详细信息窗格的“**XVA** 文件”下的“操作”下拉列表中，单击“上载”。
3. 在出现的对话框中，单击“浏览”，然后选择要上载的 XVA 文件。
4. 单击上载。XVA 文件出现在 **XVA** 文件窗格中。

要配置 **CA Access Gateway** 实例，请：

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. 在预配 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”。

配置实例后，登录实例并执行详细配置。

要修改已置备实例的参数值，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 CA Access Gateway 向导中，将参数设置为适合您环境的值。

注意：

如果您修改了任何接口参数或实例的名称，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，例如在实例上运行的 `SDXTools` 版本。

要查看与 **CA Access Gateway** 实例相关的统计信息，请执行以下操作：

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

您可以从管理服务启动、停止、重启、强制停止或强制重启 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
    - 强制重启
4. 在“确认”消息框中，单击“是”。

Palo Alto 网络 VM 系列

November 23, 2023

Palo Alto Networks 虚拟机系列虚拟防火墙使用与公司物理安全设备中相同的泛操作系统功能集，提供所有关键的网络安全功能。NetScaler SDX 上的 VM 系列支持在单个平台上整合高级安全和 ADC 功能，使企业、业务部门和服务提供商客户能够安全、可靠地访问应用程序。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。

您可以通过管理服务预置、监视、管理和排除实例故障。

注意事项：

- 您可以在 SDX 设备上预配置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 网络文档。

预置 Palo Alto 虚拟机系列实例

您必须先从 Palo Alto 网络网站下载 XVA 映像，然后才能置备 Palo Alto VM 系列实例。下载 XVA 映像后，将其上载到 SDX 设备。

要将 **XVA** 映像上传到 **SDX** 设备，请执行以下操作：

1. 在 配置 选项卡上，导航到 **Palo Alto VM** 系列 **>** 软件映像。
2. 在详细信息窗格的“**XVA** 文件”下的“操作”下拉列表中，单击“上载”。
3. 在出现的对话框中，单击“浏览”，然后选择要上载的 XVA 文件。
4. 单击上载。XVA 文件出现在 **XVA** 文件窗格中。

要预置 **Palo Alto VM** 系列实例，请执行以下操作：

1. 在 配置 选项卡上，导航到 **Palo Alto** 虚拟机系列 **>** 实例。

2. 在详细信息窗格中，单击“添加”。
3. 在预配 Palo Alto VM 系列向导中，按照屏幕上的说明进行操作。
4. 单击“完成”，然后单击“关闭”。

预配置实例后，登录实例并执行详细配置。

要修改已置备实例的参数值，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 系列向导中，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** 虚拟机系列实例

SDX 设备会收集 Palo Alto 虚拟机系列实例的统计信息，例如在实例上运行的 SDXTools 版本。

要查看与 **Palo Alto** 虚拟机系列实例相关的统计信息，请执行以下操作：

1. 导航到 **Palo Alto VM** 系列 **>** 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** 虚拟机系列实例

您可以从管理服务启动、停止、重启、强制停止或强制重启 Palo Alto 虚拟机系列实例。

在配置选项卡上，展开 **Palo Alto VM** 系列。

1. 导航到 **Palo Alto VM** 系列 **>** 实例。
2. 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
   - 强制重启
3. 在“确认”消息框中，单击“是”。

对 **Palo Alto** 虚拟机系列实例进行故障排除

通过管理服务 ping 一个 Palo Alto 虚拟机系列实例以检查设备是否可访问。您可以跟踪数据包从管理服务到实例的路由，以确定到达实例所涉及的跳数。

重新发现实例以查看实例的最新状态和配置。在重新发现过程中，管理服务会获取 SDX 设备上运行的 Palo Alto VM 系列的配置和版本。默认情况下，管理服务会每隔 30 分钟安排一次实例进行重新发现。

在配置选项卡上，展开 **Palo Alto VM** 系列。

要 **ping** 实例，请执行以下操作：

1. 单击“实例”。
2. 在详细信息窗格中，选择要执行 ping 操作的实例，然后从 操作 列表中单击 **Ping**。P **ingmes** sage 框显示 ping 是否成功。

要跟踪实例的路由，请执行以下操作：

1. 单击“实例”。
2. 在详细信息窗格中，选择您想要 ping 的实例，然后从 操作 列表中单击 **TraceRoute**。**Traceroute** 消息框显示通往实例的路由。

要重新发现实例，请执行以下操作：

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

November 23, 2023

Citrix SD-WAN 技术将软件定义网络 (SDN) 概念应用于广域网连接。该技术将流量管理和监视从网络硬件中抽象出来，并将其应用于各个应用程序。其结果是提高了性能，在地理位置分散的位置提供高质量的用户体验，并简化了广域网和云接入网络的部署。有关详细信息，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：确保正确安装了 SDX 硬件。有关详细信息，请参阅 安装硬件。
- 设置和配置 SDX 管理服务。有关详细信息，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 上配置 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 和客户端站点之间的虚拟路径服务。

必备条件

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 既可以充当站点，也可以充当 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 的双向吞吐量
- MCN 支持 64 个站点

支持的吞吐量的硬件要求　站点

- 4 个 CPU 到 16 个 CPU
- 4 GB 到 16 GB 内存
- 60 GB 到 250 GB 的磁盘存储空间
- 最少 4 个 NIC：一个用于管理，其余最少 3 个用于数据路径

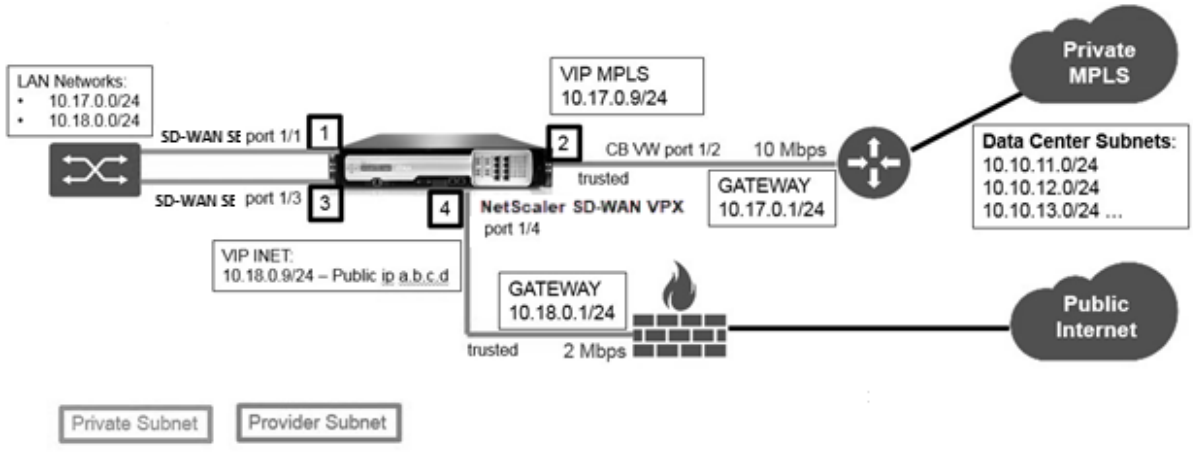
主控节点 (MCN)

- 4、8 和 16 个 CPU
- 16 GB 内存
- 250 GB 的磁盘存储空间
- 最少 4 个 NIC：一个用于管理，其余 3 个用于数据路径，以及用于数据路径的专用 NIC

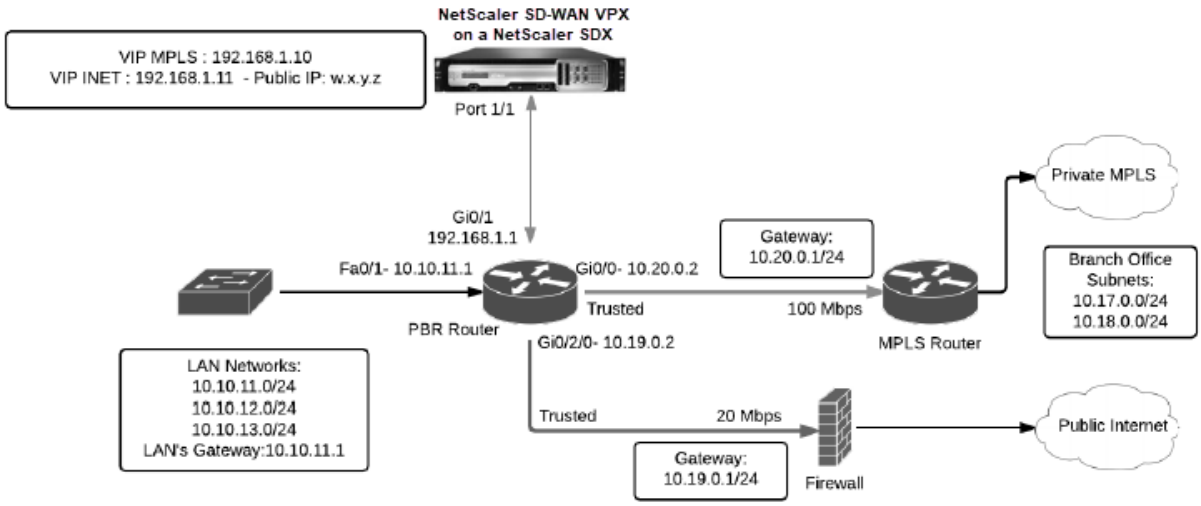
数据中心拓扑

您可以以基于策略的路由 (PBR) 模式或内联模式在 NetScaler SDX 上部署 Citrix SD-WAN VPX 设备。有关这两种支持的模式，请参阅数据中心拓扑的场景 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

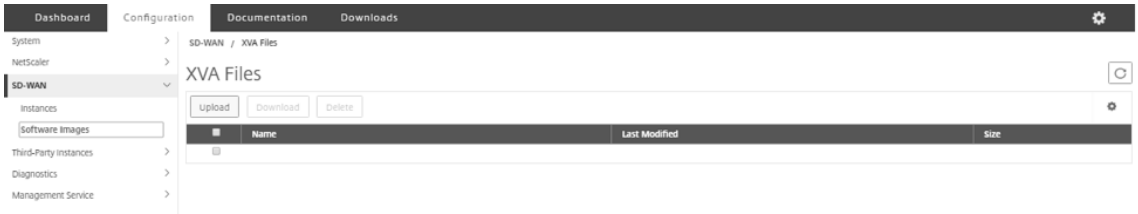


在 **NetScaler SDX** 上配置 **Citrix SD-WAN VPX** 实例

在配置 Citrix SD-WAN VPX 设备之前，请从 NetScaler 产品下载网站下载 SD-WAN VPX 映像：https://www.citrix.com/downloads/netscaler-sd-wan/。

请按照以下步骤配置 Citrix SD-WAN VPX 设备。

1. 登录 NetScaler SDX 设备。
2. 导航到 配置 **> SD-WAN >** 实例。
3. 选择 软件映像 **>** 上载 并上载 SD-WAN XVA 文件。



4. 选择 实例 **>** 添加。此时将显示 预置 **SD-WAN** 实例 页面。
5. 在“配置 **SD-WAN** 实例”页面中，输入以下内容：

   a. 名称

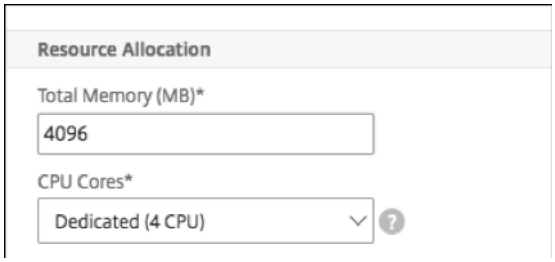
   b. IP 地址

   c. 网络掩码

   d. 网关地址

   e. 上载 XVA 文件

f. 在 资源分配下，分配资源。



g. 在 网络设置下，置备管理接口，然后选择 确定 创建以在 SDX 设备上置备 SD-WAN VPX 实例。

> 注意： SDX 管理服务按接口名称的升序将接口绑定到 VPX 实例。例如，如果添加 1/4 和 1/1，管理服务将它们排列为 1/1、1/4。
> 添加新接口时，将保留现有序列并创建新序列。例如，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 实例将显示在“实例”页面下方。下面是一个例子。

```
1 ![Image](/en-us/sdx/media/sd-wan-vpx-example.png)
```

要编辑实例，请导航到 配置 **> SD-WAN >** 实例。选择并单击实例。完成编辑后，单击“确定”保存更改。

配置 **Citrix SD-WAN VPX** 实例

在 SDX 设备上创建 SD-WAN 实例后，请通过完成以下两个任务来配置 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 与客户端站点之间的虚拟路径服务

相关信息

有关开始使用 Citrix SD-WAN 设备的更多信息，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

February 16, 2024

NetScaler SDX 带宽计量为您提供准确、可靠且易于使用的计量方案，使您可以高效地分配处理容量并从带宽使用中获利。为了在各种资源之间以最佳方式分配带宽，需要使用计量方案，同时牢记所有用户在任何时候都能获得分配的带宽。

带宽分配可以通过以下两种模式完成：

- 具有固定吞吐速率的专用带宽
- 具有最低保证吞吐量和带宽突增能力的专用带宽

具有固定吞吐速率的专用带宽

在带宽分配方法中，会为每个 VPX 实例分配一个专用带宽。允许实例使用不超过设定的限制的带宽。在专用模式下，分配的最小和最大带宽相同。如果在一段时间内，VPX 实例需要的带宽超过分配的带宽，则在专用模式下，该实例将无法增加其吞吐量。如果 VPX 实例为关键请求提供服务，则此问题可能会带来不利影响。

此外，如果 SDX 设备有少数 VPX 实例，而其中一些实例没有使用分配的带宽，则无法在专用模式下共享其未使用的带宽。为了克服所有这些挑战，具有最低保证速率且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增能力的专用带宽

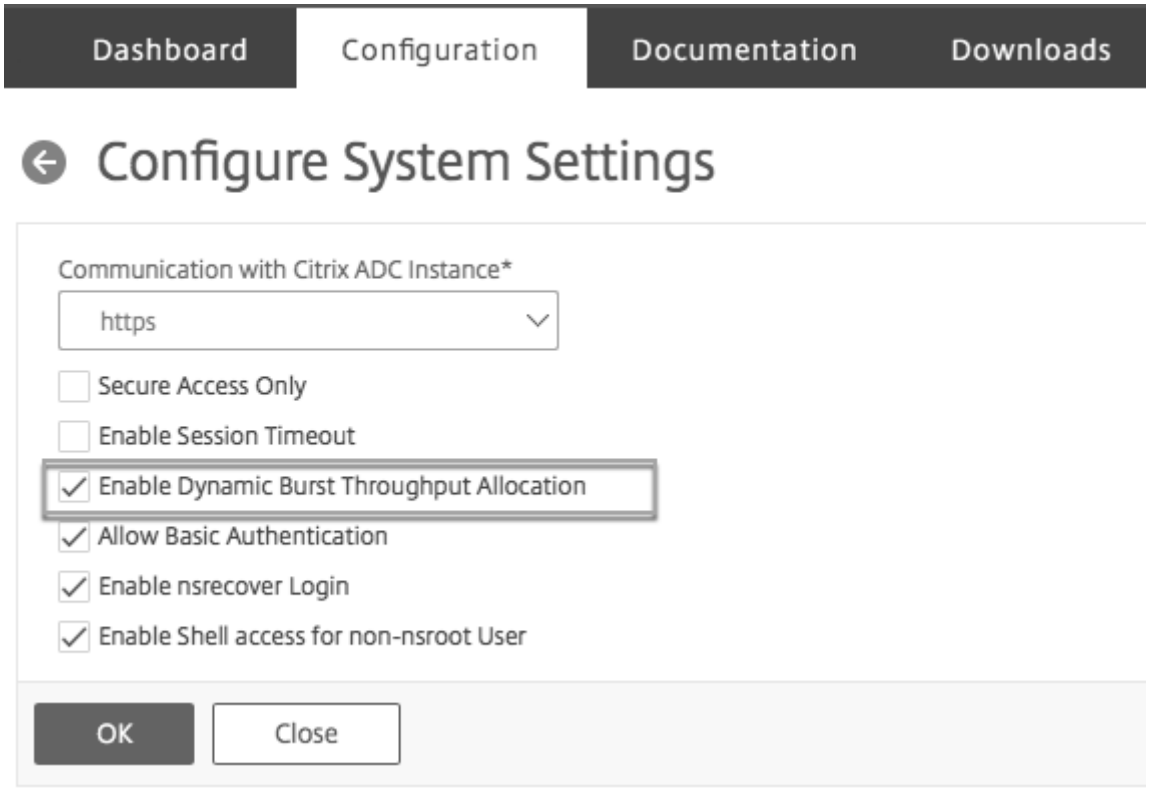
在这种带宽分配方法中，VPX 被分配了保证的最小带宽，并且可以灵活地将其带宽增加到预设的限制。VPX 可以使用的额外带宽称为突增容量。

当您有一些实例具有额外的容量而有些 VPX 具有未使用的容量时，就可以看到突增容量的好处。这些 VPX 实例的额外容量可以分配给已充分利用分配带宽且在一段时间内需要更多带宽的其他 VPX 实例。各种服务提供商也有兴趣为需要专用容量的客户提供各种附加服务。同时，他们不想过度配置带宽。在这种情况下，突发带宽会有所帮助，在这种情况下，客户可以放心使用特定的带宽，并可以选择在高需求时期增加带宽。

选择带宽分配模式

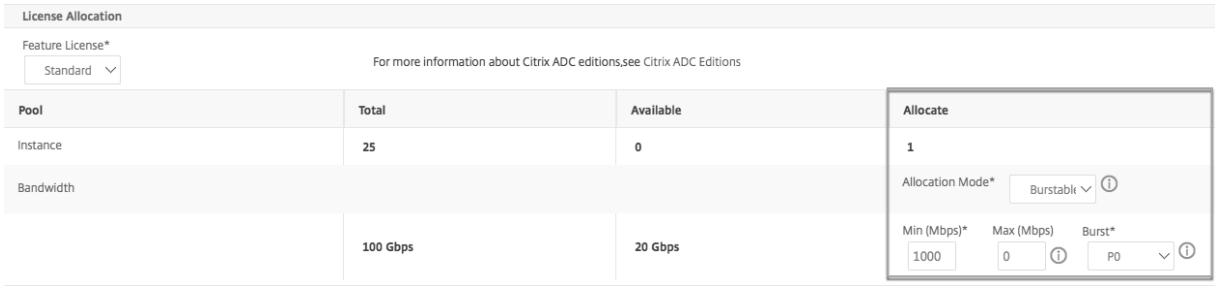
在选择突增吞吐量之前，您需要启用动态突增吞吐量分配。要启用此选项，请按照下列步骤操作。

1. 在 SDX 管理控制台中，导航到 配置 **>** 系统。
2. 从“系统设置”组中，选择“更改系统设置”。
3. 单击 启用动态突增吞吐量分配 复选框以启用动态吞吐量。



配置 VPX 时，可以选择带宽突增或动态吞吐量。

1. 在 **SDX** 管理服务中，单击“配置”**>**“**NetScaler**”**>**“实例”**>**“添加”。
2. 配置 **NetScaler** 页面将打开。在“许可证分配”下，从“分配模式”中选择“突发性”。



有关如何预配 NetScaler 实例的更多信息，请参阅预配 NetScaler 实例。

如果要使用固定吞吐率，请选择 固定。默认情况下，固定模式设置为带宽分配。不必所有 VPX 实例都在同一模式下工作。每个 VPX 实例都可以在不同的模式下进行配置。

注意：如果要从 10.5.e 及更早版本迁移 SDX，默认情况下，所有 VPX 实例都处于固定分配模式。

确定 **VPX** 实例的最大突增带宽

允许每个 VPX 突发的程度是通过算法计算的。当您配置具有突发带宽的 VPX 时，必须为每个这样的 VPX 指定优先级。突发带宽的分配取决于此突发优先级。优先级从 P0 到 P4 不等，其中 P0 为最高优先级，P4 为最低优先级。

让我们举一个有 2 个 VPX 的案例，即 VPX1 和 VPX2。分配给 VPX1 和 VPX2 的最小带宽分别为 4 Gbps 和 2 Gbps，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	保证的最小带宽	4Gbps
-	-	Maximum Burstable bandwidth	2Gbps
-	-	Priority	P0
VPX2	Minimum assured bandwidth	2Gbps
-	-	Maximum Burstable bandwidth	1Gbps
-	-	Priority	P1

在这种情况下，假设总许可带宽为 8 Gbps。如果两个 VPX 实例都突增至其最大突发限制，那就是：

1. VPX1 正在使用其最大突发带宽，即 2 Gbps，然后总共使用 4 + 2 = 6 Gbps
2. VPX2 正在使用其最大突发带宽，即 1 Gbps，然后总共使用 2 + 1 = 3 Gbps

在这种情况下，使用的最大带宽超过了许可的 8 Gbps 容量。因此，要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 1 Gbps 的突发带宽。VPX1 将继续突增，因为它的优先级高于 VPX2。在所有这些情况下，都要确保始终遵守最低保证带宽。

检查吞吐量和数据消耗统计信息

对于每个 VPX，您可以在图表中查看吞吐量和数据消耗统计信息。要访问图表，请执行以下步骤：

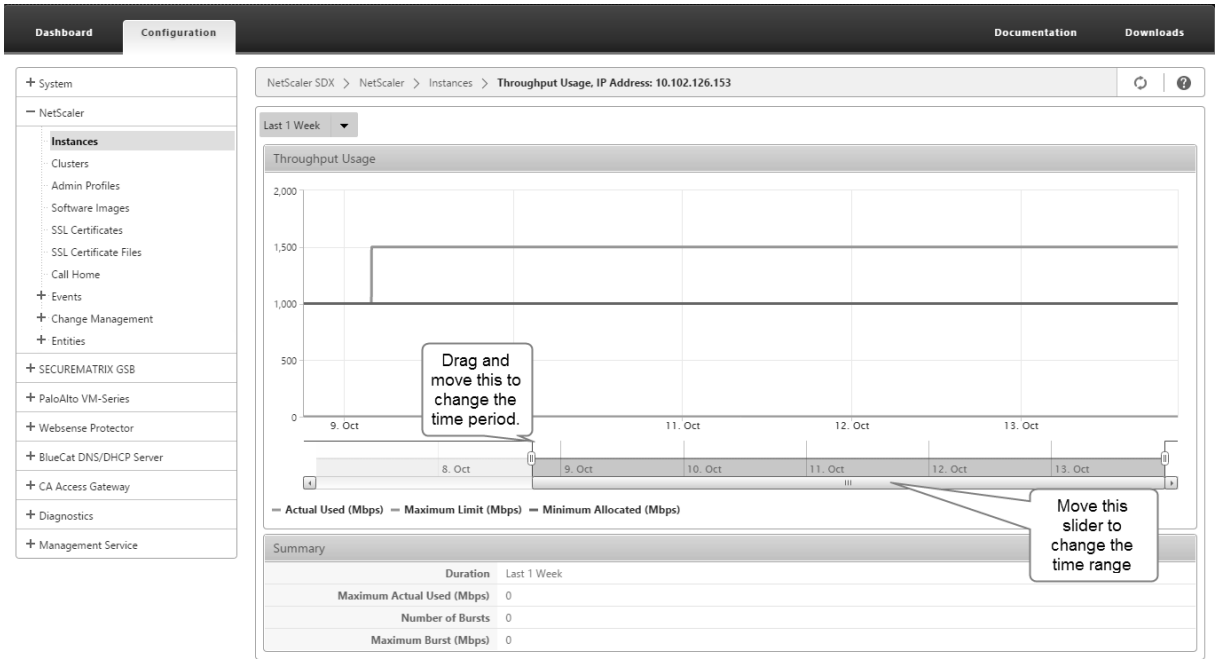
1. 从 SDX 管理服务转到配置 **> NetScaler >** 实例页面。
2. 选择一个 VPX 实例，然后单击 操作下拉 列表。
3. 从列表中选择 吞吐量统计信息 或 数据使用情况统计信息。

通过这些图表，您可以检查不同时间段的数据消耗和吞吐量统计信息，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。将鼠标移到图表中的线条上可查看特定时间的数据消耗量或吞吐量数据。

下图显示了 1 周吞吐量数据的示例图形：



配置和管理 **NetScaler** 实例

November 23, 2023

在设备上配置 NetScaler 实例后，就可以配置和管理实例了。首先创建子网 IP (SNIP) 地址，然后保存配置。然后，您可以对实例执行基本管理任务。检查是否必须应用管理配置。

警告：请确保使用管理服务修改实例的预配置网络接口或 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 设备上配置 SNIP 地址后，您可以为 NetScaler 实例分配 SNIP 地址。

SNIP 用于连接管理和服务器监视。在最初配置 NetScaler SDX 设备时，不一定要指定 SNIP。您可以通过管理服务将 SNIP 分配给 NetScaler 实例。

在 **NetScaler** 实例上添加 **SNIP** 地址

1. 在 配置 选项卡的导航窗格中，单击 **NetScaler**。
2. 在详细信息窗格的 **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：指定指定作为 SNIP 地址的 IP 地址。

- 网络掩码：指定与 SNIP 地址关联的子网掩码。
- 类型：默认情况下，该值为 SNIP。
- 保存配置：选择将配置保存在 NetScaler 上。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

您可以从管理服务中保存
NetScaler 实例的运行配置。

在 **NetScaler** 实例上保存配置

1. 在 配置 选项卡的导航窗格中，单击 **NetScaler**。
2. 在详细信息窗格的 **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. 单击“确定”，然后单击“关闭”。

管理 **NetScaler** 实例

管理服务允许您在 NetScaler 实例上执行以下操作。您可以从“配置”选项卡的“**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：从管理服务用户界面启动任何 NetScaler 实例。当管理服务 UI 将此请求转发给管理服务时，它会启动 NetScaler 实例。

关闭 **NetScaler** 实例：从管理服务用户界面关闭任何 NetScaler 实例。当管理服务 UI 将此请求转发给管理服务时，它会停止 NetScaler 实例。

重启 **NetScaler** 实例：重启 NetScaler 实例。

删除 **NetScaler** 实例：如果您不想使用 NetScaler 实例，则可以使用管理服务删除该实例。删除实例会从
SDX 设备的数据库中永久删除该实例及其相关详细信息。

启动、停止、删除或重启 **NetScaler** 实例

1. 在 配置 选项卡的导航窗格中，单击 **NetScaler** 实例。
2. 选择要在其上执行操作的 NetScaler 实例，然后单击“启动”或“关闭”或“删除”或“重启”。
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 选项卡的导航窗格中，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

在配置 VPX 实例时，管理服务会在 VPX 实例上创建一些策略、实例管理 (admin) 配置文件和其他配置。如果管理服务无法应用管理员配置，则可以将配置从管理服务显式推送到 VPX 实例。失败的原因之一可能是管理服务和 VPX 实例位于不同的子网上，而路由器已关闭。另一个原因可能是两者都在同一个子网上，但流量必须通过外部交换机，并且其中一条链路已关闭。

在 **NetScaler** 实例上应用管理员配置

1. 在 配置 选项卡的导航窗格中，单击 **NetScaler**。
2. 在详细信息窗格的 **NetScaler** 配置下，单击“应用管理员配置”。
3. 在 应用管理员配置 对话框的 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

November 23, 2023

安装 SSL 证书的过程包括首先将证书和密钥文件上载到 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。

将证书文件上载到 **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

上次修改证书文件的日期。

- 大小

证书文件的大小（以字节为单位）。

将 **SSL** 证书文件上载到 **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“上载”。
3. 在“上载 SSL 证书”对话框中，单击“浏览”，然后选择要上载的证书文件。
4. 单击上载。证书文件将显示在“SSL 证书”窗格中。

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. 在消息框的“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** 密钥文件上载到 **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

上次修改密钥文件的日期。

- 大小

密钥文件的大小（以字节为单位）。

将 **SSL** 密钥文件上载到 **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”窗格的“SSL 密钥”选项卡上，单击“上载”。
3. 在“上载 SSL 密钥文件”对话框中，单击“浏览”，然后选择要上载的密钥文件。
4. 单击上载将密钥文件上载到 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”窗格的“SSL 密钥”选项卡上，选择要下载的文件，然后单击“下载”。
2. 在消息框的“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，请确保已将 SSL 证书和密钥文件上载到 SDX 设备。

在 **NetScaler** 实例上安装 **SSL** 证书

1. 在导航窗格中，单击 NetScaler。
2. 在详细信息窗格中的 NetScaler 配置下，单击安装 SSL 证书。
3. 在“安装 SSL 证书”对话框中，指定以下参数的值。(*) 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 支持的 SSL 证书的格式。NetScaler SDX 设备支持 SSL 证书的 PEM 和 DER 格式。
    - 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：只有 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在 NetScaler 上。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 OK（确定），然后单击 Close（关闭）。

在 **NetScaler** 实例上更新 **SSL** 证书

您可以更新某些参数，例如证书文件、密钥文件和安装在 NetScaler 实例上的 SSL 证书的证书格式。您无法修改 IP 地址和证书名称。

更新 **NetScaler** 实例上的 **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 设备支持的 SSL 证书格式。设备支持 SSL 证书的 PEM 和 DER 格式。
   - 密码：用于加密私钥的密码。此选项可用于加载加密的私钥。最大长度：32 个字符。

     注意：只有 PEM 格式支持受密码保护的私钥。
   - 保存配置：指定是否必须在 SDX 设备上保存配置。默认值为 false。
   - 无域名检查：更新证书时不要检查域名。
4. 单击 OK（确定），然后单击 Close（关闭）。

在 **NetScaler** 实例上轮询 **SSL** 证书

如果您在登录 NetScaler 实例后直接在 NetScaler 实例上添加 SSL 证书，则管理服务不知道这个新证书。为避免这种情况，请指定轮询间隔，在此间隔之后，管理服务将轮询所有 NetScaler 实例以检查是否有新的 SSL 证书。您也可以随时通过管理服务执行轮询。例如，如果您想立即从所有 NetScaler 实例获取 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 OK（确定），然后单击 Close（关闭）。

执行即时投票

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，新证书（如果有）将显示在列表中。

允许在 **NetScaler** 实例上使用 **L2** 模式

November 23, 2023

在第 2 层 (L2) 模式下，NetScaler 实例充当学习桥并转发它不是目的地的所有数据包。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，实例可以接收和转发其自己的 MAC 地址以外的 MAC 地址的数据包。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，只能在一个实例上允许未标记的数据包。对于在同一接口上启用的所有其他实例，必须选择 Tagged。

   注意：

   Citrix 建议您为在 L2 模式下分配给实例的所有接口选择 Tagged。如果选择 tagged，则无法在该接口上接收未标记的数据包。

   如果您为分配给实例的接口选择了 Tagged，请登录该实例并配置 802.1q VLAN 以在该接口上接收数据包。

2. 对于允许使用 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：

   - 所有接口上都启用了 VLAN 过滤。
   - 每个接口位于不同的 802.1q VLAN 上。
   - 只有一个实例可以在接口上接收未标记的数据包。如果该接口已分配给其他实例，则必须在该接口上为这些实例选择“已标记”。

3. 如果允许使用 L2 模式的实例在 1/x 接口上允许未标记的数据包，则其他实例无法在该接口上接收未标记的数据包。无论在其他实例上是否允许 L2 模式，此条件都适用。

4. 如果您允许禁用 L2 模式的实例在 1/x 接口上使用未标记的数据包，则允许使用 L2 模式的实例将无法在该接口上接收未标记的数据包。

5. 如果将 0/x 接口分配给在 L2 模式下置备的实例 1，并且该接口也分配给 instance2，请为分配给 instance2 的所有其他接口选择 Tagged。

注意：如果两个管理接口都分配给具有 L2 模式的实例，则只能将其中一个接口分配给另一个启用了 L2 模式的 ADC 实例。也就是说，您不能将两个管理接口与启用了 L2 模式的多个 NetScaler 实例相关联。

在实例上允许 **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：您可以在置备实例时或在实例运行时激活该实例上的允许 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**

November 23, 2023

NetScaler 实例使用虚拟 MAC (VMAC) 进行高可用性（活动-活动或活动-备用）配置。虚拟 MAC 地址 (VMAC) 是在高可用性设置中由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 表将使用浮动 IP 地址和主节点的 MAC 地址进行更新。

发生故障转移时，辅助节点将接管作为新的主节点。然后，它使用免费 ARP (GARP) 来通告从主服务器获取的浮动 IP 地址。但是，新的主节点通告的 MAC 地址是其自身接口的 MAC 地址。

某些设备（尤其是一些路由器）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，因此站点可能会关闭。

您可以通过在 HA 对的两个节点上配置 VMAC 来解决此问题。然后，两个节点都拥有相同的 MAC 地址。因此，发生故障切换时，辅助节点的 MAC 地址保持不变，并且不需要更新外部设备上的 ARP 表。

配置 VMAC 的过程分为两步：

1. 在 SDX 管理服务上配置 VMAC。您可以为接口或局域网通道添加 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 通道组上配置 VMAC 支持一文。

在 **SDX** 管理服务上配置 **VMAC**

要配置 VMAC，请通过管理服务将 IPv4 或 IPv6 VRID 添加到接口或 LA 通道。管理服务在内部生成一个 VMAC。在 NetScaler 实例上配置主动模式时，请指定相同的 VRID。Mellanox 接口不支持这种主动-主动配置。

请记住以下几点：

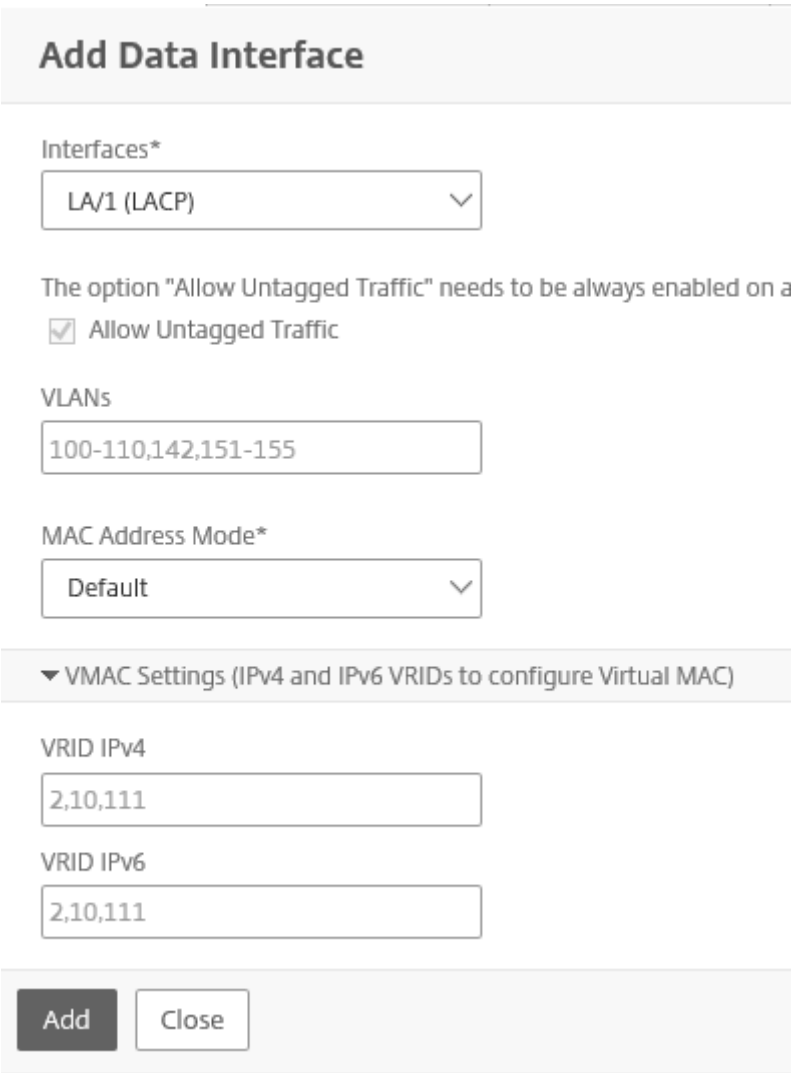
1. 从管理服务添加一个 VRID，然后在 NetScaler 实例中指定相同的 VRID。如果您直接在 NetScaler 实例中添加 VRID，则该实例无法接收以 VMAC 地址作为目标 MAC 地址的数据包。
2. 不能在同一 SDX 设备中运行的不同实例上使用同一 VRID。
3. 您可以在实例运行时为分配给实例的接口添加或删除 VRID。
4. 在主动-主动配置中，您可以为分配给实例的接口指定多个 VRID。Mellanox 接口不支持主动部署。
5. 10G 接口上最多允许 86 个 VMAC，在 1G 接口上最多允许 16 个 VMAC。如果不再有 VMAC 筛选器可用，请减少另一个实例上的 VRID 数量。

您可以在添加 NetScaler VPX 实例时添加 VRID，也可以修改现有的 NetScaler 实例来添加 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** 设置添加到接口中。
5. 单击“完成”，然后单击“关闭”。



如果实例已预置，要添加 IPv4 或 IPv6 VRID，请按照以下步骤操作。

1. 从 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** 设备的 **NetScaler** 实例上配置管理分区

November 23, 2023

NetScaler SDX 设备上的 NetScaler 实例可以分区为称为管理员分区的逻辑实体。每个分区都可以配置并用作单独的 NetScaler 实例。有关管理分区的更多信息，请参阅 管理员分区。

要使用具有共享 VLAN 配置的管理分区，每个分区都需要一个虚拟 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，使用管理服务用户界面生成和配置 PMAC 地址。管理服务使您能够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“使用基地址”。
6. 在 基本 **MAC** 地址 字段中，输入基本 MAC 地址。
7. 在“增量依 据”字段中，输入每个后续的 MAC 地址的基本 MAC 地址必须递增的值。
   例如，如果您将基本 MAC 地址指定为 00:A1:C9:11:C8:11 并将增量值指定为 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 地址的数量。
9. 单击 **Generate**（生成）。

要通过指定自定义 **MAC** 地址来生成分区 **MAC** 地址，请执行以下操作：

1. 在 配置 选项卡的左侧窗格中，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。重复以指定更多自定义 MAC 地址。
8. 单击 **Generate**（生成）。

要随机生成分区 **MAC** 地址，请执行以下操作：

1. 在 配置 选项卡的左侧窗格中，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“随机”。
6. 在“计数”字段中，输入要生成的分区 MAC 地址的数量。
7. 单击 **Generate**（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。

VPX 实例的变更管理

November 23, 2023

您可以从管理服务跟踪对 NetScaler VPX 实例上的配置所做的任何更改。详细信息窗格列出了设备名称以及上次更新的 IP 地址、日期和时间。它还会列出保存的配置和正在运行的配置之间是否存在任何差异。选择设备以查看其运行配置、保存的配置、配置更改的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 小时轮询一次所有实例，但您可以更改此时间间隔。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 **VPX** 实例的更改管理

1. 在 配置 选项卡上，导航到 **NetScaler >** 变更管理。
2. 在 更改管理 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：

    - 运行配置 - 在新窗口中显示选定 VPX 实例的运行配置。
    - 保存的配置-在新窗口中显示选定 VPX 实例的已保存配置。
    - 已保存 Vs. 运行差异-显示保存的配置、正在运行的配置和更正命令（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。
    - 预置与升级后差异-显示升级前后配置的差异，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。您可以将此差异另存为批处理文件。要将模板中的配置应用到实例，请将此批处理文件应用于实例。
- 下载-下载选定 VPX 实例的配置并将其保存在本地设备上。

轮询任何 **NetScaler** 实例的配置更新

1. 在 配置 选项卡上，导航到 **NetScaler >** 变更管理。
2. 在“更改管理”窗格的“操作”列表中，选择以下选项之一：
   - 立即轮询-管理服务会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。

为 **NetScaler** 实例配置审计模板

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 >** 变更管理 **>** 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，粘贴从配置文件复制的命令列表。
6. 单击“创建”，然后单击“关闭”。

监视 **NetScaler** 实例

November 23, 2023

管理服务用户界面的“监视”页面上将显示设备和设备上置备的 VPX 实例的性能的高级视图。预置和配置 NetScaler 实例后，您可以执行各种任务来监视 NetScaler 实例。

查看 **VPX** 实例的属性

管理服务用户界面显示在 SDX 设备上置备的所有 VPX 实例的列表和说明。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、吞吐量和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. 在配置选项卡的左侧窗格中，展开 NetScaler 配置，然后单击实例。
   注意：您还可以从“
   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：配置时分配给 NetScaler 实例的主机名。
   - 虚拟机状态：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。单击该 IP 地址将在新选项卡或浏览器中打开此实例的 GUI。
   - **Rx (Mbps)**：在 NetScaler 实例上收到的数据包。
   - **Tx (Mbps)**：由 NetScaler 实例传输的数据包。
   - **HTTP Req/s**：每秒在 NetScaler 实例上收到的 HTTP 请求总数。
   - **CPU** 使用率 **(%)**： NetScaler 上的 CPU 利用率百分比。
   - 内存使用率 **(%)**： NetScaler 上内存利用率的百分比。
3. 单击 NetScaler 实例名称旁边的箭头以查看该实例的属性。您也可以单击“全部展开”以查看所有 NetScaler 实例的属性。您可以查看以下属性：
   - 网络掩码： NetScaler 实例的网络掩码 IP 地址。
   - **Gateway**：默认网关的 IP 地址，即将流量转发到安装实例的子网之外的路由器。
   - 每秒数据包数：每秒传递的数据包总数。
   - **NIC**： NetScaler 实例使用的网卡的名称，以及分配给每个接口的虚拟函数。
   - 版本：当前在实例上运行的 NetScaler 软件的构建版本、构建日期和时间。
   - 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：自 实例持续处于 UP 状态以来的日期和时间。
   - **SSL** 芯片：分配给实例的 SSL 芯片总数。
   - 对等 **IP** 地址：此 NetScaler 实例的对等体的 IP 地址（如果在 HA 设置中）。
   - 状态：在 NetScaler 实例上执行的操作的状态，例如该实例的清单是否已完成的状态。
   - **HA** 主设备状态：设备的状态。状态表示实例是在独立设置还是主设置中配置，还是属于高可用性设置的一部分。在高可用性设置中，状态还会显示其处于主模式还是辅助模式。
   - 高可用性同步状态：高可用性同步状态的模式，例如启用或禁用。
   - 描述：在配置 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：
>
> - ADC 实例密码可直接使用实例 CLI 进行更改。

> - 密码与存储在管理服务中的实例管理员配置文件密码不匹配。
> - 首次重启实例后，上一个会话将丢失。
>
> 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：
>
> - 在实例 CLI 中，修改实例的密码，使其与实例的管理员配置文件中的密码匹配。然后从管理服务重新发现实例。
> - 使用与 ADC 实例的当前密码相同的密码创建管理员配置文件。然后，使用新的管理员配置文件更新 ADC 实例。

查看 **NetScaler** 实例的运行和保存的配置

通过使用管理服务，您可以查看 NetScaler 实例当前正在运行
的配置。您还可以查看 NetScaler 实例的保存配置以及保存配置的时间。

查看 **NetScaler** 实例的运行和保存配置

1. 在配置选项卡的左侧窗格中，展开 NetScaler 配置，然后单击实例。
2. 在 NetScaler 实例窗格中，单击要查看正在运行或保存的配置的 NetScaler 实例。
3. 要查看运行配置，请单击“运行配置”；要查看保存的配置，请单击“保存的配置”。
4. 在 NetScaler 运行配置窗口或 NetScaler 保存的配置窗口中，您可以查看 NetScaler 实例的正在运行或保存的配置。

Ping 一个 **NetScaler** 实例

您可以从管理服务 ping NetScaler 实例，以检查该设备是否可以访问。

ping NetScaler 实例

1. 在配置选项卡的左侧窗格中，展开 NetScaler 配置，然后单击实例。
2. 在 NetScaler 实例窗格中，单击要执行 ping 操作的 NetScaler 实例，然后单击 Ping。在 Ping 消息框中，您可以查看 ping 是否成功。

追踪 **NetScaler** 实例的路线

通过确定到达该实例所用的跳数，您可以跟踪数据包从管理服务到 NetScaler 实例的路由。

追踪 **NetScaler** 实例的路线

1. 在配置选项卡的左侧窗格中，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，您可以查看通往 NetScaler 的路线。

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，您可以重新发现 NetScaler 实例。

在重新发现过程中，管理服务会获取配置。默认情况下，管理服务会每隔 30 分钟安排一次设备进行重新发现。

重新发现 **NetScaler** 实例

1. 在配置选项卡的左侧窗格中，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”。

使用日志监视操作和事件

November 23, 2023

使用审计和任务日志监视在管理服务和 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 上执行的任务的所有事件。

查看审核日志

使用管理服务执行的所有操作都记录在设备数据库中。使用审核日志可以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、审核时间、状态等对详细信息进行排序。

审核日志窗格支持分页。选择要在页面上显示的记录数。默认情况下，一个页面上显示 25 条记录。

要查看审核日志，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“审核日志”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：执行操作时系统正在运行的端口。
- 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。
- 审核时间：生成审核日志的时间。
- 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：描述操作失败时失败原因的消息；如果操作成功，则说明任务的状态，如完成。

3. 要按特定字段对日志进行排序，请单击该列的标题。

查看任务日志

使用任务日志查看和跟踪管理服务在 NetScaler 实例上运行的任务，例如升级实例和安装 SSL 证书。通过任务日志，您可以查看任务是否正在进行中、是否已失败或已成功。

任务日志 窗格支持分页。选择要在页面上显示的记录数。默认情况下，一个页面上显示 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：正在运行或已经运行的任务的名称。
   - 状态：任务的状态，例如“进行中”、“已完成”或“失败”。
   - 执行者：执行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。通过任务设备日志，您可以查看任务是否正在进行中、是否已失败或已成功。它还会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的详细信息。
3. 在 任务设备日志 窗格中，要按特定字段对日志进行排序，请单击该列的标题。

查看任务命令日志

使用任务命令日志查看在 NetScaler 实例上运行的任务的每条命令的状态。通过任务命令日志，您可以查看命令是否已成功运行或已失败。它还会显示正在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的详细信息。
3. 在“任务设备日志”窗格中，双击任务以查看任务命令的详细信息。
4. 在“任务命令日志”窗格中，要按特定字段对日志进行排序，请单击该列的标题。

查看事件

使用管理服务用户界面中的“事件”窗格监视管理服务为在管理服务上执行的任务生成的事件。

要查看事件，请按照下列步骤操作：

1. 导航到 **System**（系统）**> Events**（事件）。
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，可能是严重、重大、次要、明确和信息。
    - 来源：生成事件的 IP 地址。
    - 日期：事件生成的日期。
    - 类别：事件类别，例如策略失败和设备配置更改。
    - 消息：描述事件的消息。
3. 要按特定字段对事件进行排序，请单击该列的标题。

NetScaler SDX 设备的用例

November 23, 2023

对于网络组件（例如防火墙和应用程序交付控制器），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能力。这种方法允许为每个租户实施不同的策略集，而无需使用大量单独的设备。但是，传统上，就实现的孤立程度而言，它受到严重限制。

根据设计，SDX 设备不受同样的限制。在 SDX 架构中，每个实例都作为独立的虚拟机 (VM) 运行，具有自己的专用 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 不仅可以保持聚合系统性能，还可以完全隔离每个租户的数据平面和管理平面流量。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有关，在保持管理隔离的同时减少所需的网络数量。以下是基本的整合方案：

- 当管理服务和 NetScaler 实例位于同一个网络中时进行整合。
- 当管理服务和 NetScaler 实例位于不同的网络中但所有实例都在同一个网络中时进行整合。
- 跨安全整合。

- 使用每个实例的专用接口进行整合。
- 通过多个实例共享一个物理端口进行整合。

管理服务和 **NetScaler** 实例位于同一个网络中时的整合

November 23, 2023

SDX 设备上一种简单的整合案例是将管理服务和 NetScaler 实例配置为同一个网络的一部分。在以下情况下，此用例适用：

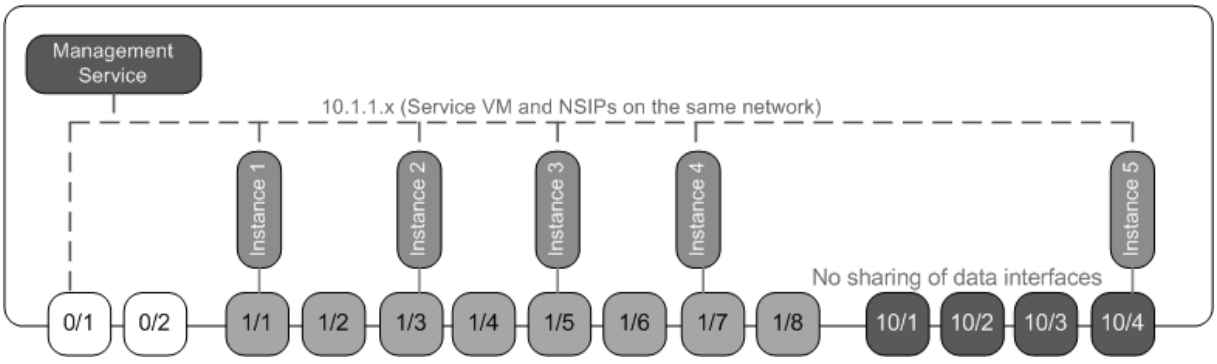
- 设备管理员也是实例管理员。
- 贵组织的合规性要求并未指定管理服务和不同实例的 NSIP 地址需要单独的管理网络。

可以在同一网络中预配置实例（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），因此可以在不同的安全区域中配置。

在以下示例中，管理服务和 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。每个实例都有自己的专用物理接口。因此，实例数量限制为设备上可用的物理接口数量。默认情况下，在 SDX 设备的每个接口上启用 VLAN 过滤。在 1G 接口上，VLAN 的数量限制为 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，以便在每个实例上为每个接口配置多达 4096 个 VLAN。在此示例中，VLAN 过滤不是必需的，因为每个实例都有自己的专用接口。有关 VLAN 筛选的更多信息，请参阅 管理和监视 SDX 设备 中的 **VLAN** 筛选部分。

下图说明了前面的用例。

图 1. 具有管理服务和 NSIP 的 SDX 设备的网络拓扑（适用于同一网络中的实例）



下表列出了在前面的示例中用于配置 NetScaler 实例 1 的参数的名称和值。

参数名称	实例 1 的值
名称	vpx8
IP 地址	10.1.1.2

参数名称	实例 1 的值
网络掩码	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	Platinum
管理员配置文件	ns_nsroot_profile
用户名	vpx8
密码	Sdx1
确认密码	Sdx1
Shell/sftp/Scp 访问	True
总内存 (MB)	2048
#SSL Chips	1
吞吐量 (Mbps)	1000
每秒数据包数	1000000
CPU	共享虚拟机
接口	0/1 和 1/1

配置 **NetScaler** 实例 **1**，如本示例所示

1. 在配置选项卡的导航窗格中，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 Provisioning Citrix 向导中，按照向导中的说明指定上表中显示的参数值。
4. 单击 Create（创建），然后单击 Close（关闭）。您配置的 NetScaler 实例显示在 NetScaler 实例窗格中。

当管理服务和 **NetScaler** 实例位于不同的网络中时进行整合

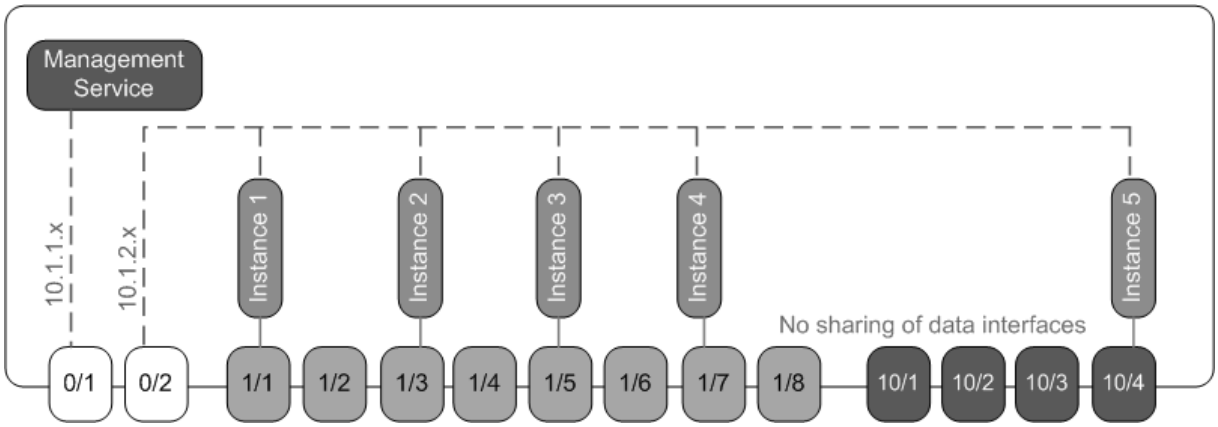
November 23, 2023

在某些情况下，设备管理员可能会允许其他管理员对单个实例执行管理任务。通过仅授予单个实例管理员对该实例的登录权限，可以安全地完成此操作。但是，出于安全考虑，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。这是服务提供商环境中的常见情况，随着企业采用虚拟化和云架构，这种情况在企业中变得越来越普遍。

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。每个实例都有自己的专用管理员和专用的物理接口。因此，实例数量限制为设备上可用的物理接口数量。VLAN 过滤不是必需的，因为每个实例都有自己的专用接口。或者，禁用 VLAN 过滤，以便为每个接口的每个实例配置最多 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，也没有标记的 VLAN。有关 NSVLAN 的更多信息，请参阅 添加 NetScaler 实例

下图说明了前面的用例。

图 1. 具有管理服务和 NSIP 的 SDX 设备的网络拓扑结构（适用于不同网络中的实例）



作为设备管理员，您可以在 SDX 设备上保持管理服务与 NSIP 地址之间的流量。或者，如果您希望流量通过外部防火墙或其他安全中介，然后返回设备，则可以强制将流量从设备中移出。

下表列出了本示例中用于配置 NetScaler 实例 1 的参数的名称和值。

参数名称	实例 1 的值
名称	vpx1
IP 地址	10.1.2.2
网络掩码	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	Platinum
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	True
总内存 (MB)	2048

参数名称	实例 1 的值
#SSL Chips	1
吞吐量 (Mbps)	1000
每秒数据包数	1000000
CPU	共享虚拟机
接口	0/2 和 1/1

如本示例所示，配置 **NetScaler** 实例 **1**

1. 在配置选项卡的导航窗格中，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 **Provision 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 实例显示在 NetScaler 实例窗格中。

跨安全区域整合

November 23, 2023

SDX 设备通常用于跨安全区域的整合。DMZ 为组织的内部网络增加了一层额外的安全保护，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，在 DMZ 和内部网络中均具有 VIP 地址的单个 NetScaler 实例是不可接受的。借助 SDX，您可以预置在 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单独的管理网络。DMZ 中实例的 NSIP 地址可以位于同一个网络中。内部网络中具有 VIP 的实例的 NSIP 地址可以位于不同的管理网络中。此外，管理服务与实例之间的通信通常需要通过外部设备（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 设备有两个管理接口（0/1 和 0/2），以及多达八个 1G 数据端口和八个 10G 数据端口（视型号而定）。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进行标记）。如果这样做，来自管理服务的流量必须离开设备，然后返回到设备。您可以路由此流量，也可以选择在分配给实例的接口上指定 NSVLAN。如果实例和管理服务之间的管理接口是通用的，则不必路由两者之间的流量。但是，如果您的设置明确需要它，则可以路由流量。

注意 Citrix Hypervisor 6.0 版支持标记。

使用每个实例的专用接口进行整合

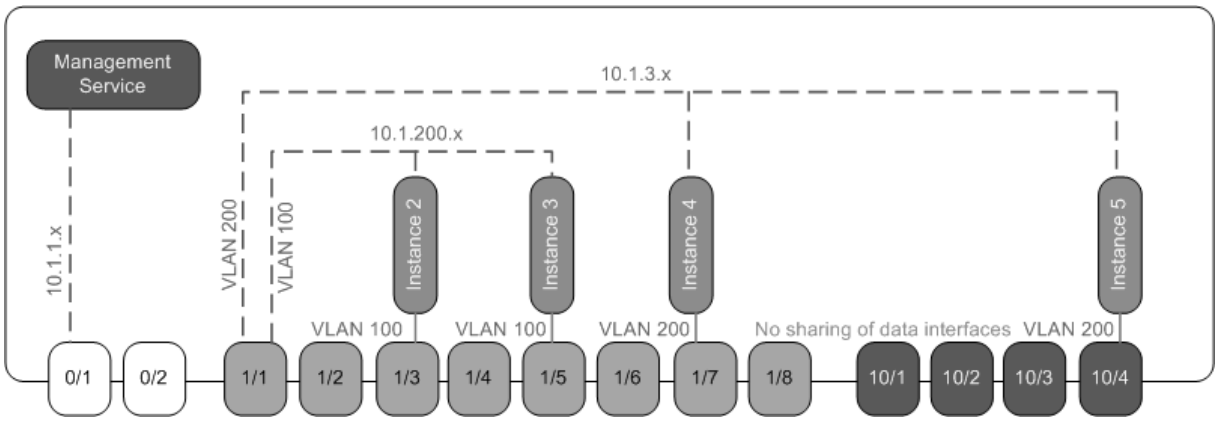
November 23, 2023

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，管理服务是内部 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。

或者，您可以在所有实例上配置 NSVLAN。

下图说明了前面的用例。

图 1. 在多个网络中使用 NetScaler 实例的 SDX 设备的网络拓扑



SDX 设备已连接到交换机。确保在设备端口 1/1 所连接的交换机端口上配置了 VLAN ID 100 和 200。

下表列出了本示例中用于配置 NetScaler 实例 5 和 3 的参数的名称和值。

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
网络掩码	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	Platinum	Platinum
管理员配置文件	ns_nsroot_profile	ns_nsroot_profile
用户名	vpx5	vpx3
密码	Sdx1	根

参数名称	实例 5 的值	实例 3 的值
确认密码	Sdx1	根
Shell/sftp/Scp 访问	True	True
总内存 (MB)	2048	2048
#SSL Chips	1	1
吞吐量 (Mbps)	1000	1000
每秒数据包数	1000000	1000000
CPU	共享虚拟机	共享虚拟机
接口	1/1 和 10/4	1/1 和 1/5
NSVLAN	200	100
添加（接口）	1/1	1/1
标记的接口	选择“已标记”	选择“已标记”

如本示例所示，配置 **NetScaler** 实例 **5** 和 **3**

1. 在配置选项卡的导航窗格中，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 **Provision 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 实例显示在 NetScaler 实例窗格中。

通过多个实例共享一个物理端口进行整合

November 23, 2023

您可以根据需要在接口上启用和禁用 VLAN 过滤。例如，要在一个实例上配置 100 个以上的 VLAN，请为该实例分配一个专用的物理接口，然后在该接口上禁用 VLAN 过滤。在共享物理接口的实例上启用 VLAN 过滤，这样一个实例就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，该设置将应用于与该接口关联的所有实例。如果禁用了 VLAN 过滤，则最多可以配置 4096 个 VLAN。如果启用了 VLAN 过滤，则可以在 10G 接口上配置最多 63 个带标记的 VLAN，在 1G 接口上最多可以配置 32 个带标记的 VLAN。

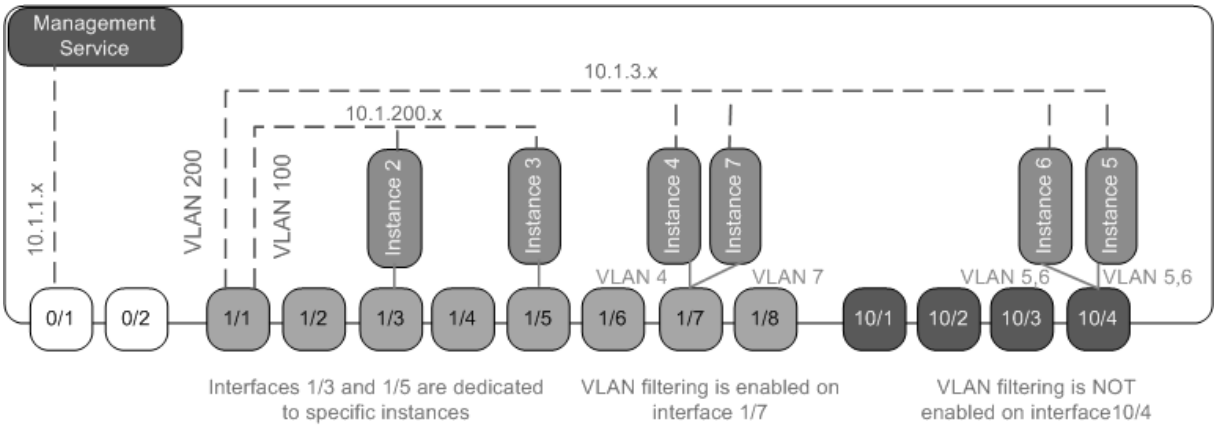
在以下示例中，实例是多个网络的一部分。

- 接口 1/1 作为管理接口分配给所有实例。接口 0/1 分配给管理服务，管理服务是内部 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 和实例 3 各有一个专用的物理接口。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 上已启用 VLAN 过滤。实例 4 的流量被标记为 VLAN 4，实例 7 的流量被标记为 VLAN 7。因此，实例 4 的流量对实例 7 不可见。相反，实例 7 的流量对实例 4 不可见。在接口 1/7 上最多可以配置 32 个 VLAN。
- 在接口 10/4 上禁用了 VLAN 过滤，因此您最多可以在该接口上配置 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。

下图说明了前面的用例。

图 1. SDX 设备的网络拓扑，其管理服务和 NetScaler 实例分布在网络上



下表列出了本示例中用于配置 NetScaler 实例 7 和 4 的参数的名称和值。

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
网络掩码	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
功能许可	Platinum	Platinum
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	True	True

参数名称	实例 7 的值	实例 4 的值
总内存 (MB)	2048	2048
#SSL Chips	1	1
吞吐量 (Mbps)	1000	1000
每秒数据包数	1000000	1000000
CPU	共享虚拟机	共享虚拟机
接口	1/1 和 1/7	1/1 和 1/7
NSVLAN	200	200

在本示例中配置 **NetScaler** 实例 **7** 和 **4**

1. 在配置选项卡的导航窗格中，展开“NetScaler 配置”，然后单击实例。
2. 在 **NetScaler** 实例窗格中，单击“添加”。
3. 在配置 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 实例显示在 NetScaler 实例窗格中。

NITRO API

November 23, 2023

NetScaler SDX NITRO 协议允许您以编程方式配置和监视 SDX 设备。

NITRO 通过表述性状态转移 (REST) 接口提供功能。因此，可以用任何编程语言来开发 NITRO 应用程序。此外，对于必须使用 Java、.NET 或 Python 开发的应用程序，NITRO 协议作为打包为单独的软件开发工具包的相关库公开。

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以下内容：

- 访问 SDX 设备。
- 要使用 REST 接口，您必须拥有一个能够向 SDX 设备生成 HTTP 或 HTTPS 请求（JSON 格式的有效负载）的系统。可以使用任何编程语言或工具。
- 对于 Java 客户端，必须有一个提供 Java 开发工具包 (JDK) 1.5 或更高版本的系统。可以从 http://www.oracle.com/technetwork/java/javase/downloads/index.html 下载 JDK。
- 对于.NET 客户端，您必须拥有可用.NET framework 3.5 或更高版本的系统。可以从 http://www.microsoft.com/downloa 载.NET 框架。

- 对于 Python 客户端，您必须有一个 <NITRO_SDK_HOME> 安装了 Python 2.7 或更高版本的系统以及请求库（在 /lib 中可用）。

获取 **NITRO** 软件包

November 23, 2023

NITRO 软件包以 tar 文件的形式在 SDX 设备的配置实用程序的“下载”页面上提供。您必须将文件下载并取消 tar 到本地系统上的某个文件夹中。此文件夹 <NITRO_SDK_HOME> 在本文档中被称为。

该文件夹包含
lib 子文件夹中的 NITRO 库。必须将这些库添加到客户端应用程序类路径中才能访问 NITRO 功能。该 <NITRO_SDK_HOME> 文件夹还提供示例和文档，可帮助您了解 NITRO SDK。

注意：

- REST 软件包仅包含如何使用 REST 接口的文档。
- 对于 Python SDK，库必须安装在客户端路径上。有关安装说明，请阅读 \/README.txt 文件。

.NET SDK

November 23, 2023

SDX NITRO API 根据 API 的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。

系统接口

使用 NITRO 的第一步是与 SDX 设备建立会话，然后使用管理员的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）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用户帐户。您可以执行的配置操作受分配给您的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：

```
1 //Specify the IP address of the appliance and service type
2 nitro_service nitroservice = new nitro_service ("10.102.31.16", "https"
      );
3
```



```
//Specify the login credentials
nitroservice.login("nsroot", "verysecret");
<!--NeedCopy-->
```

注意：在设备上的所有
后续的 NITRO 操作中使用 nitro_service 对象。

要断开与设备的连接，请按如下所示调用 logout () 方法：

```
nitroservice.logout();
<!--NeedCopy-->
```

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 分组为格式为 com.citrix.sdx.nitro.resource.config 的包或命名空间。. 这些包或命名空间中的每一个都包含一个名为 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），请执行以下操作：

1. 使用相应的属性名称设置资源所需属性的值。结果是一个包含资源所需详细信息的资源对象。
   注意：这些值是在客户端上本地设置的。在上载对象之前，这些值不会反映在设备上。
2. 使用静态 add () 方法将资源对象上载到设备。

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);
<!--NeedCopy-->
```

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);
<!--NeedCopy-->
```

检索资源统计信息

SDX 设备收集有关其功能使用情况的统计信息。您可以使用 NITRO 检索这些统计数据。

以下示例代码检索 ID 为 123456a 的 NetScaler 实例的统计数据：

```
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);
```



```
<!--NeedCopy-->
```

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所需属性的值。结果是一个资源对象。

   注意：这些值是在客户端上本地设置的。在上载对象之前，这些值不会反映在设备上。
3. 使用 update () 方法将资源对象上载到设备。

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);
<!--NeedCopy-->
```

删除资源

要删除现有资源，请在资源类上调用静态方法 delete ()，方法是将要删除的资源的 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.id = "123456a";
ns.delete(nitroservice, obj);
<!--NeedCopy-->
```

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，您可以在同一个操作中添加多个 NetScaler SDX 设备。

每个资源类都有一些方法，这些方法使用一组资源来添加、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。

为了解决批量操作中某些操作失败的原因，NITRO 允许您配置以下行为之一：

- 退出。遇到第一个错误时，执行将停止。在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，也会运行列表中的所有命令。

注意：通过在
nitro_service() 方法中设置
onerror 参数，在与设备建立连接时配置所需的行为。

以下示例代码在一次操作中添加了两个 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);
<!--NeedCopy-->
```

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故障的简要说明和故障性质。

com.citrix.sdx.nitro.exception.nitro_exception 类会捕获执行 NITRO API 时的所有异常。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

November 23, 2023

REST（代表性状态传输）是一种基于客户端和服务器之间简单 HTTP 请求和响应的架构样式。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。

每个资源还有一个状态，可以在该状态下执行以下操作：

- 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。调用客户端为要创建的资源提供状态。可以在请求中使用 XML 或 JSON 格式指定状态。客户端还可以指定用于标识新对象的唯一 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。客户端可以通过使用 HTTP GET 方法指定资源的 URL 来检索资源的状态。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 方法在 JSON 或 XML 中指定标识该对象及其新状态的 URL，从而更新现有资源的状态。
- 删除。您可以使用 DELETE HTTP 方法和标识要删除的资源的 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操作。这些操作使用 HTTP POST 方法，JSON 格式的请求正文指定要执行的操作以及该操作的参数。

SDX NITRO API 根据 API 的范围和用途分为系统 API 和配置 API。

系统接口

使用 NITRO 的第一步是与 SDX 设备建立会话，然后使用管理员的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标头中指定。

注意：您必须在该设备上拥有用户帐户。您可以执行的配置受分配给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，请执行以下操作：

- 网址 `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
<!--NeedCopy-->
```

注意：也可以使用早期版本的 NITRO 中支持的内容类型，例如“application/x-www-form-urlencoded”。确保负载与早期版本中使用的负载相同。本文档中提供的有效负载仅在内容类型为“application/vnd.com.citrix.sdx.login+json”的形式时才适用。

- 有效负载

```
{

    "login":
    {

        "username":"nsroot",
        "password":"verysecret"
     }

 }

<!--NeedCopy-->
```

- 响应有效负载
  - 标头

```
HTTP/1.0 201 Created
Set-Cookie:
NITRO_AUTH_TOKEN=##87305E9C51B06C848F0942; path=/nitro/v2
<!--NeedCopy-->
```

注意：在对设备进行的所有其他 NITRO 操作中使用会话 ID。

注意：默认情况下，与设备的连接将在处于非活动状态 30 分钟后过期。您可以通过在
登录对象中指定新的超时周期（以秒为单位）来修改超时期限。例如，要将超时期限修改为 60 分钟，请求负载为：

```
{

    "login":
    {

        "username":"nsroot",
        "password":"verysecret",
        "timeout":3600
     }

 }

<!--NeedCopy-->
```

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，要在创建 NetScaler 实例时连接到设备，请执行以下操作：

- **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
<!--NeedCopy-->
```

- 有效负载

```
{

    "ns":
    {

        ...
     }

 }

<!--NeedCopy-->
```

- 响应。
  - 标头

```
HTTP/1.0 201 Created
<!--NeedCopy-->
```

要断开与设备的连接，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
<!--NeedCopy-->
```

配置 **API**

NITRO 协议可用于配置 SDX 设备的资源。

每个 SDX 资源都有一个与之关联的唯一 URL，具体取决于要执行的操作类型。用于配置操作的 URL 的格式如下：
`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，请执行以下操作：

- **URL**
- **HTTP** 方法
- 请求
  - 标头

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
<!--NeedCopy-->
```

  - 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"
             }

        ]
     }

 }

<!--NeedCopy-->
```


检索资源详细信息和统计信息

可以按如下方式检索 SDX 资源详细信息：

- 要检索 SDX 设备上特定资源的详细信息，请在 URL 中指定资源的 ID。
- 要根据某个过滤器检索资源的属性，请在 URL 中指定过滤条件。

  该 URL 的格式为：`http://<IP>/nitro/v2/config/<resource_type>?filter=<property1>:<value>,<property2>:<value>`
- 如果您的请求可能导致从设备返回许多资源，则可以通过将这些结果划分为“页面”并逐页检索它们来以区块形式检索这些结果。

  例如，假设您要在包含 53 个 NetScaler 实例的 SDX 上检索所有 NetScaler 实例。与其在一个大型响应中检索全部 53 个，不如将结果配置为分成每页 10 个 NetScaler 实例（共 6 页）。然后，逐页从服务器中检索它们。

  您可以使用页码查询字符串参数指定页数，然后使用页码查询字符串参数指定要检索的页码。
  该 URL 的格式为：`http://<IP>/nitro/v2/config/<resource_type>?pageno=<value>&pagesize=<value>`

  您不必按顺序检索所有页面或检索页面。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：要了解请求可能返回的资源数量，您可以使用 count query string 参数来请求要返回的资源的计数，而不是资源本身。要获取可用的 NetScaler 实例的数量，URL 应为
  `http://<IP>/nitro/v2/config/<resource_type>?count=yes`

要检索 ID 为 123456a 的 NetScaler 实例的配置信息，请执行以下操作：

- **URL**
- **HTTP** 方法 GET

更新资源

要更新现有的 SDX 资源，请使用 PUT HTTP 方法。在 HTTP 请求负载中，指定名称和其他必须更改的参数。例如，要将 ID 为 123456a 的 NetScaler 实例的名称更改为 vpx2：

- **URL**
- **HTTP** 方法
- 请求有效负载
  - 标头

    ```
    1 Cookie:NITRO_AUTH_TOKEN=tokenvalue
    2 Content-Type:application/vnd.com.citrix.sdx.ns+json
    3 <!--NeedCopy-->
    ```

  - 有效负载


```
{

    "ns":
    {

        "name":"vpx2",
        "id":"123456a"
     }

 }

<!--NeedCopy-->
```

删除资源

要删除现有资源，请在 URL 中指定要删除的资源的名称。例如，要删除 ID 为 123456a 的 NetScaler 实例，请执行以下操作：

- **URL**
- **HTTP** 方法
- 请求
  - 标头

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
<!--NeedCopy-->
```

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，您可以在同一个操作中添加多个 NetScaler SDX 设备。您还可以在一个请求中添加不同类型的资源。

为了解决批量操作中某些操作失败的原因，NITRO 允许您配置以下行为之一：

- 退出。遇到第一个错误时，执行将停止。在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，也会运行列表中的所有命令。

注意：使用 `X-NITRO-ONERROR` 参数在请求标头中配置所需的行为。

要在一个操作中添加 2 个 NetScaler 资源并在一个命令失败时继续，请执行以下操作：

- **URL**。
- **HTTP** 方法。
- 请求有效负载。

- 标头

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
X-NITRO-ONERROR:continue
<!--NeedCopy-->
```

- 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"
         }

    ]
 }

<!--NeedCopy-->
```

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：

- **URL**。
- **HTTP** 方法。POST
- 请求有效负载。

- 标头

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
X-NITRO-ONERROR:continue
<!--NeedCopy-->
```

- 有效负载

```
{

    "ns":
    [
```



```
5           {
6
7               "name":"ns_instance1",
8               "ip_address":"10.70.136.5",
9               "netmask":"255.255.255.0",
10              "gateway":"10.70.136.1"
11           }
12  ,
13          {
14
15              "name":"ns_instance2",
16              "ip_address":"10.70.136.8",
17              "netmask":"255.255.255.0",
18              "gateway":"10.70.136.1"
19           }
20
21      ],
22       "mpsuser":
23      [
24          {
25
26              "name":"admin",
27              "password":"admin",
28              "permission":"superuser"
29           }
30  ,
31          {
32
33              "name":"admin",
34              "password":"admin",
35              "permission":"superuser"
36           }
37
38      ]
39   }
40
41  <!--NeedCopy-->
```

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。

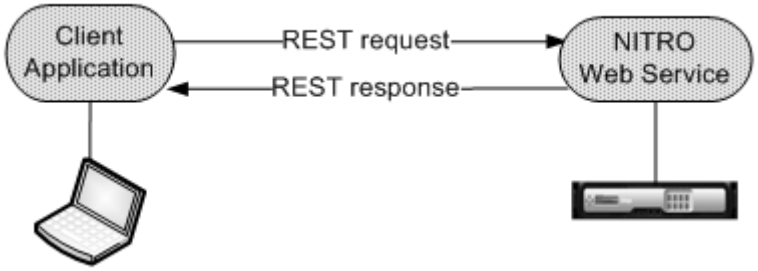
错误消息字段提供了故障的简要说明和故障性质。

NITRO 的工作原理

November 23, 2023

NITRO 基础架构由客户端应用程序和在 NetScaler SDX 设备上运行的 NITRO Web 服务组成。客户端应用程序与 NITRO Web 服务之间的通信基于使用 HTTP 或 HTTPS 的 REST 体系结构。

图 1. NITRO 工作流程



详细说明工作流程的步骤：

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 响应消息返回到客户端应用程序。使用 SDK 时，REST 响应消息将转换为 API 调用的相应响应。

要最大限度地减少网络上的流量，请从服务器检索资源的整个状态。在本地修改资源的状态。然后通过一次网络事务将其上载回服务器。

注意：在显式上载对象的状态之前，对资源的本地操作（更改其属性）不会影响其在服务器上的状态。

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 之前等待来自 NITRO Web 服务的响应。

Java SDK

November 23, 2023

SDX NITRO API 根据 API 的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。

系统接口

使用 NITRO 的第一步是与 SDX 设备建立会话，然后使用管理员的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）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用户帐户。您可以执行的配置操作受分配给您的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：

```
1 //Specify the IP address of the appliance and service type
2 nitro_service nitroservice = new nitro_service ("10.102.31.16", "https"
      );
3
4 //Specify the login credentials
5 nitroservice.login("nsroot", "verysecret");
6 <!--NeedCopy-->
```

注意：在设备上的所有
后续的 NITRO 操作中使用 nitro_service 对象。

要断开与设备的连接，请按如下方式调用 `logout()` 方法：

```
1 nitroservice.logout();
2 <!--NeedCopy-->
```

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 分组为格式为 com.citrix.sdx.nitro.resource.config 的包或命名空间。. 这些包或命名空间中的每一个都包含一个名为 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所需属性的值。结果是一个包含资源所需详细信息的资源对象。
   注意：这些值是在客户端上本地设置的。在上载对象之前，这些值不会反映在设备上。
2. 使用静态 add () 方法将资源对象上载到设备。

以下示例代码在 SDX 设备上创建了一个名为“ns_instance”的 NetScaler 实例：

```
1 ns newns = new ns();
2
3 //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);
<!--NeedCopy-->
```

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
System.out.println(returned_ns[i].get_ip_address());
System.out.println(returned_ns[i].get_netmask());
<!--NeedCopy-->
```


检索资源统计信息

SDX 设备收集有关其功能使用情况的统计信息。您可以使用 NITRO 检索这些统计数据。

以下示例代码检索 ID 为 123456a 的 NetScaler 实例的统计数据：

```
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());
<!--NeedCopy-->
```

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所需属性的值。结果是一个资源对象。

   注意：这些值是在客户端上本地设置的。在上载对象之前，这些值不会反映在设备上。
3. 使用 update () 方法将资源对象上载到设备。

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);
<!--NeedCopy-->
```

删除资源

要删除现有资源，请在资源类上调用静态方法 delete ()，方法是将要删除的资源的 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);
<!--NeedCopy-->
```

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，您可以在同一个操作中添加多个 NetScaler SDX 设备。

每个资源类都有一些方法，这些方法使用一组资源来添加、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。

为了解决批量操作中某些操作失败的原因，NITRO 允许您配置以下行为之一：

- 退出。遇到第一个错误时，执行将停止。在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，也会运行列表中的所有命令。

注意：通过在
nitro_service() 方法中设置
`onerror` 参数，在与设备建立连接时配置所需的行为。

以下示例代码在一次操作中添加了两个 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);
<!--NeedCopy-->
```


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故障的简要说明和故障性质。

com.citrix.sdx.nitro.exception.nitro_exception 类捕获执行 NITRO API 时的所有异常。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。