



SDX 10

2015-05-19 11:30:54 UTC

Contents

SDX 10	6
SDX Administration.....	7
Introduction	8
Getting Started with the Management Service User Interface	9
Logging on to the Management Service User Interface	10
Provisioning Instances on an SDX Appliance	11
Single Sign-On to the Management Service and the NetScaler Instances	12
Managing the Home Page	13
Managing and Monitoring the NetScaler SDX Appliance.....	15
Modifying the Network Configuration of the SDX Appliance	16
Changing the Password of the Default User Account	17
Installing an SSL Certificate on the SDX Appliance.....	18
Viewing the SSL Certificate on the Management Service	19
Modifying the Time Zone on the Appliance	20
Modifying System Settings	21
Restarting the Appliance	22
Shutting Down the Appliance.....	23
Managing Licenses.....	24
Managing Interfaces.....	26
Display the Mapping of Virtual Interfaces on the VPX Instance to the Physical Interfaces on the NetScaler SDX Appliance	28
Assigning a MAC Address to an Interface	30
VLAN Filtering	33
Configuring Clock Synchronization	34
Viewing the Properties of the NetScaler SDX Appliance	37
Viewing Real-Time Appliance Throughput.....	40
Viewing Real-Time CPU and Memory Usage	41
Viewing CPU Usage for All Cores.....	42
SNMP	43

SNMP Trap Destinations	44
Downloading MIB Files	45
System Health Monitoring.....	46
Monitoring the Resources on the SDX Appliance	47
Monitoring the Storage Resources on the SDX Appliance	48
Monitoring the Hardware Sensors on the SDX Appliance	50
Monitoring the Interfaces on the SDX Appliance	52
Configuring the Management Service.....	53
Managing Client Sessions	54
Configuring User Accounts	55
Configuring Policies	57
Restarting the Management Service.....	58
Upgrading the Management Service	59
Uploading the Management Service Build and Documentation Files	60
Upgrading the Management Service to a Later Version.....	62
Upgrading the XenServer Software	63
Uploading the XenServer Build Files	64
Upgrading the Software.....	65
Uploading and Applying a XenServer Hotfix.....	66
Installing the XenServer Supplemental Pack	67
Backing Up and Restoring the Configuration Data of the SDX Appliance	69
Performing a Factory Reset.....	70
Removing Management Service Files.....	72
Generating a Tar Archive for Technical Support	73
Provisioning NetScaler Instances	74
Creating Admin Profiles	75
Uploading NetScaler .Xva Images	77
Adding a NetScaler Instance	79
Configuring and Managing NetScaler Instances	83
Creating a Mapped IP Address or a Subnet IP Address on a NetScaler Instance.....	84
Saving the Configuration	86
Installing SSL Certificates	87
Uploading the Certificate File to the SDX Appliance	88
Uploading SSL Key Files to the SDX Appliance.....	89
Installing an SSL Certificate on a NetScaler Instance	90
Updating an SSL Certificate on a NetScaler Instance	92
Polling for SSL Certificates on the NetScaler Instances	93

Upgrading a NetScaler Instance	94
Uploading NetScaler Resources	95
Upgrading NetScaler VPX Instances	97
Managing a NetScaler Instance	98
Allowing L2 Mode on a NetScaler Instance	99
Configuring VMACs on an Interface	101
Configuring LACP on a NetScaler VPX Instance	103
Removing NetScaler Instance Files	105
Applying the Administration Configuration.....	106
Change Management for NetScaler VPX Instances	107
Monitoring NetScaler Instances	109
Viewing the Properties of the NetScaler Instance	110
Viewing the Running and Saved Configuration of a NetScaler Instance	114
Pinging a NetScaler Instance	115
Tracing the Route of a NetScaler Instance	116
Rediscovering a NetScaler Instance	117
Using Logs to Monitor Operations and Events	118
Viewing Audit Logs	119
Viewing Task Logs	121
Viewing Events.....	123
Use Cases for NetScaler SDX Appliance	124
Consolidation When the Management Service and the NetScaler Instances are in the Same Network.....	125
Consolidation When the Management Service and the NetScaler Instances are in Different Networks.....	127
Consolidation Across Security Zones	129
Consolidation with Dedicated Interfaces for Each Instance.....	130
Consolidation With Sharing of a Physical Port by More Than One Instance	132
NITRO API	135
Obtaining the NITRO Package	136
How NITRO Works	137
Java SDK	138
System APIs	139
Configuration APIs	140
Exception Handling	144
.NET SDK.....	145
System APIs	146
Configuration APIs	147

Exception Handling	151
REST Web Services	152
System APIs	153
Configuration APIs	154
Exception Handling	159

SDX 10

The Citrix© NetScaler© SDX platform optimizes delivery of applications over the Internet and private networks, combining application-level security, optimization, and traffic management into a single, integrated appliance. You install a NetScaler SDX appliance in your server room and route all connections to your managed servers through it. The NetScaler features that you enable and the policies that you set are then applied to incoming and outgoing traffic.

What's New in SDX 10

NetScaler SDX release 10 adds wizards for adding and modifying NetScaler instances. It also adds support for:

- Layer 2 (L2) mode
- Virtual MAC (VMAC) addresses
- Backing up and restoring the configuration
- Performing a factory reset
- Upgrading the XenServer software
- Installing SSL certificates
- Assigning multiple CPU cores to an instance
- Generating a certificate signing request
- Monitoring CPU core usage on the appliance

For a summary of the updates, see the Citrix NetScaler 10 Release Notes.

Quick Links

- [Quick Start Guide for SDX 11500/13500/14500/16500/18500/20500](#)
- [Quick Start Guide for SDX 17500/19500/21500](#)
- [Quick Start Guide for SDX 17550/19550/20550/21550](#)

Introduction

The Citrix NetScaler SDX appliance is a multitenant platform on which you can provision and manage multiple virtual NetScaler machines (instances). The SDX appliance addresses cloud computing and multitenancy requirements by allowing a single administrator to configure and manage the appliance and delegate the administration of each hosted NetScaler instance to tenants. The SDX appliance enables the appliance administrator to provide each tenant the following benefits:

- One complete NetScaler instance. Each instance has the following privileges:
 - Dedicated CPU and memory resources
 - A separate space for NetScaler entities
 - The independence to run the NetScaler release and build of their choice
 - Lifecycle independence
- A completely isolated network. Traffic meant for a particular instance is sent only to that instance.

Note: Link aggregation control protocol (LACP) is not supported on the NetScaler instances provisioned on the NetScaler SDX appliance.

The Citrix NetScaler SDX appliance provides a Management Service that is pre-provisioned on the appliance. The Management Service provides a user interface (HTTP and HTTPS modes) and an API to configure, manage, and monitor the appliance, the Management Service, and the NetScaler instances. A Citrix self-signed certificate is prepackaged for HTTPS support. Citrix recommends that you use the HTTPS mode to access the Management Service user interface.

Introduction

The Citrix NetScaler SDX appliance is a multitenant platform on which you can provision and manage multiple virtual NetScaler machines (instances). The SDX appliance addresses cloud computing and multitenancy requirements by allowing a single administrator to configure and manage the appliance and delegate the administration of each hosted NetScaler instance to tenants. The SDX appliance enables the appliance administrator to provide each tenant the following benefits:

- One complete NetScaler instance. Each instance has the following privileges:
 - Dedicated CPU and memory resources
 - A separate space for NetScaler entities
 - The independence to run the NetScaler release and build of their choice
 - Lifecycle independence
- A completely isolated network. Traffic meant for a particular instance is sent only to that instance.

Note: Link aggregation control protocol (LACP) is not supported on the NetScaler instances provisioned on the NetScaler SDX appliance.

The Citrix NetScaler SDX appliance provides a Management Service that is pre-provisioned on the appliance. The Management Service provides a user interface (HTTP and HTTPS modes) and an API to configure, manage, and monitor the appliance, the Management Service, and the NetScaler instances. A Citrix self-signed certificate is prepackaged for HTTPS support. Citrix recommends that you use the HTTPS mode to access the Management Service user interface.

Getting Started with the Management Service User Interface

To begin configuring, managing, and monitoring the appliance, the Management Service, and the virtual instances, you need to connect to the Management Service user interface by using a browser, and then provision the virtual instances on the appliance.

Logging on to the Management Service User Interface

You can connect to the Management Service user interface by using one of the following supported browsers:

- Internet Explorer
- Google Chrome
- Apple Safari
- Mozilla Firefox

To log on to the Management Service user interface

1. In your Web browser address field, type one of the following:

`http://Management Service IP Address`

or

`https://Management Service IP Address`

2. On the Login page, in User Name and Password, type the user name and password of the Management Service. The default user name and password are nsroot and nsroot. However, Citrix recommends that you change the password after initial configuration. For information about changing the nsroot password, see [Changing the Password of the Default User Account](#).
3. Click Show Options, and then do the following:
 - a. In the Start in list, select the page that must be displayed immediately after you log on to the user interface. The available options are Home, Monitoring, Configuration, Documentation, and Downloads. For example, if you want the Management Service to display the Configuration page when you log on, select Configuration in the Start in list.
 - b. In Timeout, type the length of time (in minutes, hours, or days) after which you want the session to expire. The minimum timeout value is 15 minutes. The Start in and Timeout settings persist across sessions. Their default values are restored only after you clear the cache.
4. Click Login to log on to the Management Service user interface.

Provisioning Instances on an SDX Appliance

You can provision one or more NetScaler instances on the SDX appliance by using the Management Service. The number of instances that you can install depends on the license you have purchased. If the number of instances added is equal to the number specified in the license, the Management Service does not allow provisioning more instances.

For information about provisioning NetScaler instances, see [Provisioning NetScaler Instances](#).

Single Sign-On to the Management Service and the NetScaler Instances

Logging on to the Management Service gives you direct access to the NetScaler instances that are provisioned on the appliance, if the instances are running release 10 build 53 and later. If you log on to the Management Service by using your user credentials, you do not have to provide the user credentials again for logging on to an instance. By default, the **Timeout** value is set to 30 minutes and the configuration tab is opened in a new browser window.

To log on to a NetScaler instance from the Management Service

1. In the navigation pane, expand NetScaler, and then click Instances.
2. In the Instances pane, click the IP address of the NetScaler instance that you want to log on to. You are not prompted for your user credentials.

If you have added the NetScaler Instances gadget on the Home page, click the IP address of the NetScaler instance that you want to log on to from that gadget. You are not prompted for your user credentials.

Managing the Home Page

The Management Service Home page provides you with a high-level view of the performance of the SDX appliance and the instances provisioned on your appliance. SDX appliance and NetScaler instance information is displayed in gadgets that you can add and remove depending on your requirement.

The following gadgets are available on the Home page by default.

System Resources

Displays the total number of CPU cores, total number of SSL chips, number of free SSL chips, total memory, and free memory on the appliance.

System CPU | Memory Usage (%)

Displays the percentage of CPU and memory utilization of the appliance in graphical format.

System WAN/LAN Throughput (Mbps)

Displays the total throughput of the SDX appliance for incoming and outgoing traffic in a graph that is plotted in real time and updated at regular intervals.

NetScaler Instances

Displays the properties of the NetScaler instances. The properties displayed are Name, VM State, Instance State, IP Address, Rx (Mbps), Tx (Mbps), HTTP Req/s, and CPU Usage (%) and Memory Usage (%).

Note: On first log on, the Home page does not display any data related to the NetScaler instances because you have not provisioned any instances on your appliance.

Health Monitoring Events

Displays the last 25 events, with their severity, message, and the date and time that the event occurred.

You can do the following on the Home page:

View and hide NetScaler instance details

You can view and hide the details of a particular NetScaler instance by clicking the name of the instance in the Name column. You can also click Expand All to expand all the instance nodes and Collapse All to collapse all the instance nodes.

Add and remove gadgets

You can also add gadgets to view additional system information.

To add these gadgets, click the arrow (<<) button at the top right corner of the Home page, enter keywords in the search box, and then click Go. The allowed characters are:

a-z, A-Z, 0-9, ^, \$, *, and _. Click Go without typing any characters in the search box to display all the gadgets that are available. After the gadget is displayed, click Add to dashboard.

Currently, you can add the following gadgets to the Home page:

Hypervisor Details

The Hypervisor Details gadget displays details about XenServer uptime, edition, version, iSCSI Qualified Name (IQN), product code, serial number, build date, and build number.

Licenses

The Licenses gadget displays details about the SDX hardware platform, the maximum number of NetScaler instances supported on the platform, the maximum supported throughput in Mbps, and the available throughput in Mbps.

If you remove a gadget that is available on the Home page by default, you can add them back to the Home page by performing a search for the gadget, as described earlier.

Managing and Monitoring the NetScaler SDX Appliance

After your SDX appliance is up and running, you can perform various tasks to manage and monitor the appliance from the Management Service user interface.

Modifying the Network Configuration of the SDX Appliance

You can modify the network configuration details that you provided for the NetScaler SDX appliance during initial configuration.

To modify the network configuration of the SDX appliance

1. In the navigation pane, click System.
2. In the System pane, under Setup Appliance, click Network Configuration.
3. In the Modify Network Configuration dialog box, specify values for the following parameters:
 - Interface*—The interface through which clients connect to the Management Service. Possible values: 0/1, 0/2. Default: 0/1.
 - XenServer IP Address*—The IP address of the XenServer.
 - Management Service IP Address*—The IP address of the Management Service.
 - Netmask*—The netmask for the subnet in which the SDX appliance is located.
 - Gateway*—The default gateway for the network.
 - DNS Server—The IP address of the DNS server.

* A required parameter
4. Click OK.

Changing the Password of the Default User Account

The default user account provides complete access to all features of the Citrix NetScaler SDX appliance. Therefore, to preserve security, the nsroot account should be used only when necessary, and only individuals whose duties require full access should know the password for the nsroot account. Citrix recommends changing the nsroot password frequently. If you lose the password, you can reset the password to the default by reverting the appliance settings to factory defaults , and you can then change the password.

You can change the password of the default user account in the Users pane. In the Users pane, you can view the following details:

Name

Lists the user accounts configured on the SDX appliance.

Permission

Displays the permission level assigned to the user account.

To change the password of the default user account

1. On the Configuration tab, in the navigation pane, expand System, and then click Users.
2. In the Users pane, click the default user account, and then click Modify.
3. In the Modify System User dialog box, in Password and Confirm Password, enter the password of your choice.
4. Click OK.

Installing an SSL Certificate on the SDX Appliance

The NetScaler SDX appliance is shipped with a default SSL certificate. For security reasons, you may want to replace this certificate with your own SSL certificate. To do so, you must first upload your SSL certificate to the Management Service and then install the certificate. Installing an SSL certificate terminates all current client sessions with the Management Service, so you have to log back on to the Management Service for any additional configuration tasks.

To install an SSL certificate on the Management Service

1. In the navigation pane, click System.
2. In the System pane, click Install SSL Certificate.
3. In the Install SSL Certificate on the Management Service dialog box, set the following parameters:
 - Certificate File*—The file name of a valid certificate. The certificate file must be present on the SDX appliance.
 - Key File*—The file name of the private-key used to create the certificate. The key file must be present on the SDX appliance.
 - Password*—The pass-phrase that was used to encrypt the private-key. This option can be used to load encrypted private-keys. Max length: 32.

Note: Password protected private key is supported only for the PEM format.

* A required parameter
4. Click OK, and then click Close.

Viewing the SSL Certificate on the Management Service

The Management Service uses an SSL certificate for secure client connections. You can view the details of this certificate, such as validity status, issuer, subject, days to expire, valid from and to dates, version, and serial number.

To view the SSL certificate on the Management Service

1. In the navigation pane, click System.
2. In the System pane, click View SSL Certificate. The certificate details are displayed.

Modifying the Time Zone on the Appliance

You can modify the time zone of the Management Service and the Xen Server. The default time zone is UTC.

To modify the time zone on the appliance

1. On the Configuration tab, in the navigation pane, click System.
2. In the System pane, under System Settings, click Change Time Zone.
3. In the Modify Time Zone dialog box, select a time zone from the list, and then click OK.

Modifying System Settings

For security reasons, you can specify that the Management Service and a NetScaler VPX instance should communicate with each other only over a secure channel. You can also restrict access to the Management Service user interface. Clients can log on the Management Service user interface only by using https.

To modify system settings

1. On the Configuration tab, in the navigation pane, click System.
2. In the System pane, under System Settings, click Change System Settings.
3. In the Modify System Settings dialog box, select https from the list.
4. Optionally, to restrict secure-only access to the Management Service, select Secure Access only.
5. Click OK.

Restarting the Appliance

The Management Service provides an option to restart the SDX appliance. During the restart, the appliance shuts down all hosted NetScaler instances, and then restarts XenServer. When XenServer restarts, it starts all hosted NetScaler instances along with the Management Service.

To restart the appliance

1. On the Configuration tab, in the navigation pane, click System.
2. In the System pane, click Reboot Appliance.

Shutting Down the Appliance

You can shut down the NetScaler SDX appliance from the Management Service.

To shut down the appliance

1. On the Configuration tab, in the navigation pane, click System.
2. In the System pane, click Shutdown Appliance.

Managing Licenses

The SDX instance pack license determines the maximum number of NetScaler instances that can be hosted on the appliance, and is obtained as a license file. Installing the license involves uploading the license file from a client computer to the SDX appliance and then applying the license. You can upload a license file to the SDX appliance and apply the license in the License Files pane. You can also download a license file to a local computer as a backup.

In the License Files pane, you can view the following details:

Name

The name of the license file.

Last Modified

The date and time at which the license file was last modified.

Size

The size of the license file, in bytes.

Note: If you want to upgrade the platform license, remove the old license files from the Management Service and upload the new license files, and then click Apply Licenses. With this, you can ensure that you remove the license files that you no longer need.

To upload a license file to the SDX appliance

1. On the Configuration tab, in the navigation pane, expand System, and then click Licenses.
2. In the License Files pane, click Upload. The Upload button is unavailable when a license file is selected.
3. In the Upload License File dialog box, do the following:
 - a. Click Browse.
 - b. Navigate to the folder that contains the license file you want to upload, and then double-click the license file.
 - c. Click Upload.

To apply the licenses that have been uploaded to the SDX appliance

1. On the Configuration tab, in the navigation pane, expand System, and then click Licenses.
2. In the License Files pane, click Apply Licenses.
3. In the Confirm message box, click Yes.

To create a backup by downloading a license file

1. In the License Files pane, select the file you want to download, and then click Download.
2. In the File Download message box, click Save.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

Managing Interfaces

You can configure interface settings in the Interfaces pane. You can also reset interface parameters to their default values.

Note: Autonegotiation is not supported on an interface to which a direct attach cable (DAC) is connected.

In the Interfaces pane, you can view the following interface settings for each interface on the SDX appliance:

Interface

The interface ID.

State

State of the interface. UP indicates that the interface is receiving traffic normally, while DOWN indicates a network issue because of which the interface is unable to send or receive traffic.

To configure an interface

1. On the Configuration tab, in the navigation pane, expand System, and then click Interfaces.
2. In the Interfaces pane, click the interface that you want to configure, and then click Modify.
3. In the Modify Interface dialog box, under Link Speed and Flow Control, specify values for the following parameters:
 - Auto Negotiation*—Specifies whether auto-negotiation is enabled on the interface. Possible values: ON, OFF. Default: OFF.
 - Speed*—Specifies the Ethernet speed for the interface, in Mb/s. Possible values: 10, 100, 1000, and 10000.
 - Duplex*—Specifies the duplex setting for the interface. Possible values: Full, Half, NONE. Default: NONE.
 - Flow Control Auto Negotiation*—Specifies whether auto-negotiation is performed for flow control parameters.
 - Rx Flow Control*—Specifies whether or not Rx flow control is enabled.
 - Tx Flow Control*—Specifies whether or not Tx flow control is enabled.

* A required parameter
4. Click OK, and then click Close.

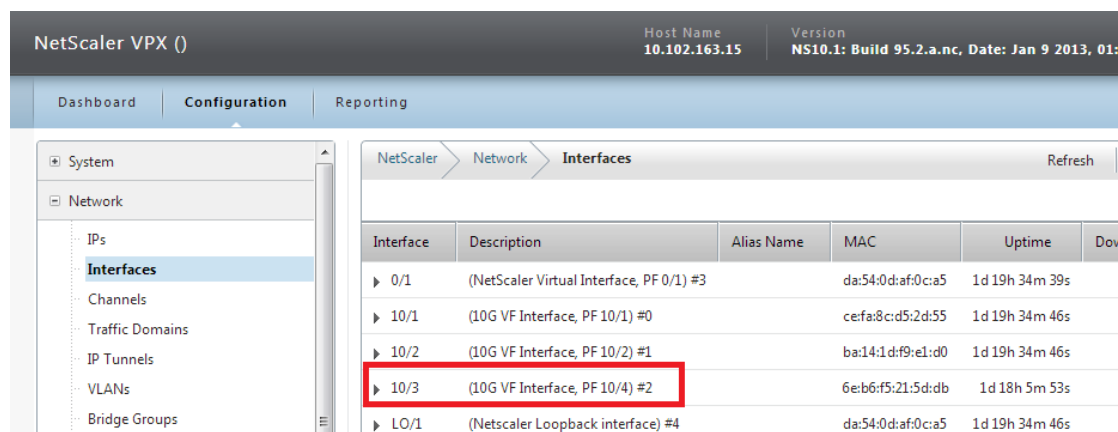
To reset the parameters of an interface to their default values

1. On the Configuration tab, in the navigation pane, expand System, and then click Interfaces.
2. In the Interfaces pane, click the interface that you want to reset, and then click Reset.

Display the Mapping of Virtual Interfaces on the VPX Instance to the Physical Interfaces on the NetScaler SDX Appliance

If you log on to the NetScaler virtual instance, the configuration utility and the command line interface display the mapping of the virtual interfaces on the instance to the physical interfaces on the appliance.

After logging on to the NetScaler VPX instance, in the configuration utility, navigate to **Network**, and then click **Interfaces**. The virtual interface number on the instance and the corresponding physical interface number on the appliance appear in the **Description** field, as shown in the following figure:



The screenshot shows the NetScaler configuration utility interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Reporting'. The left sidebar shows a tree view with 'System' expanded to 'Network', and 'Interfaces' selected. The main content area displays a table of interfaces. The table has columns for 'Interface', 'Description', 'Alias Name', 'MAC', 'Uptime', and 'Down'. The row for interface 10/3 is highlighted with a red box. The description for 10/3 is '(10G VF Interface, PF 10/4) #2', indicating its mapping to physical interface PF 10/4.

Interface	Description	Alias Name	MAC	Uptime	Down
0/1	(NetScaler Virtual Interface, PF 0/1) #3		da:54:0d:af:0c:a5	1d 19h 34m 39s	
10/1	(10G VF Interface, PF 10/1) #0		ce:fa:8c:d5:2d:55	1d 19h 34m 46s	
10/2	(10G VF Interface, PF 10/2) #1		ba:14:1d:f9:e1:d0	1d 19h 34m 46s	
10/3	(10G VF Interface, PF 10/4) #2		6e:b6:f5:21:5d:db	1d 18h 5m 53s	
LO/1	(NetScaler Loopback interface) #4		da:54:0d:af:0c:a5	1d 19h 34m 46s	

Figure 1. Mapping the Virtual Interfaces to the Physical Interfaces in the Configuration Utility

In the above example, the virtual interface 10/3, on the NetScaler VPX instance, is a 10G interface and is mapped to physical interface (PF) 10/4 on the NetScaler SDX appliance.

In the NetScaler command line interface, type the `show interface` command. For example:

```
> 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.
...
```

Display the Mapping of Virtual Interfaces on the VPX Instance to the Physical Interfaces on the NetScaler SDX Appliance

Assigning a MAC Address to an Interface

If, while you are provisioning a NetScaler instance on an SDX appliance, XenServer internally assigns a MAC address to a virtual interface associated with that instance, the same MAC address might be assigned to a virtual interface associated with another instance on the same appliance or on another appliance. To prevent assignment of duplicate MAC addresses, you can enforce unique MAC addresses.

There are two ways of assigning a MAC address to an interface:

1. Assign a base MAC address and a range to an interface: The Management Service assigns a unique MAC address by using the base address and range.
2. Assign a global base MAC address: A global base MAC address applies to all interfaces. The Management Service then generates the MAC addresses for all interfaces. If you set the global base MAC address, the range for a 1G interface is set to 8 and the range for a 10G interface is set to 64. See the following table for sample base MAC addresses if the global base MAC address is set to 00:00:00:00:00:00.

Table 1. Example of Base MAC Addresses Generated from a Global Base MAC Address

Physical Interface	Base MAC Address
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

The base MAC address for the management ports is for reference only. The Management Service generates MAC addresses, on the basis of the base MAC address, for 1/x and 10/x ports only.

Note: You cannot assign a base MAC address to a channel.

To set the base MAC address for an interface and generate a range of MAC addresses

1. On the Configuration tab, navigate to System > Interfaces and select the interface for which you want to set the MAC address.
2. In the Modify Interface dialog box, select Add MAC Address, and then set the following parameters:
 - Add MAC Address—Assign a base MAC address to the interface. If you do not select this option, XenServer assigns a MAC address to the virtual interface.
 - Base MAC Address—Enter the base MAC address. The Management Service uses this address to generate a MAC address for a virtual interface associated with an instance.
 - Range—Specify the MAC addresses allowed for the virtual interfaces that are assigned to this physical interface. These MAC addresses cannot be assigned to any other physical interface. For example, on a 1G interface, if the base MAC address is 00:00:00:00:00:00 and range is set to 8, a MAC address between 00:00:00:00:00:00 and 00:00:00:00:00:08 cannot be assigned to another physical interface. Maximum limit for a 1G interface is 8. Maximum limit for a 10G interface is 64.
3. To apply MAC addresses according to the base MAC address, click Apply MAC Address. All the virtual instances associated with this interface are restarted.
4. Click OK, and then click Close.

To set the global base MAC address and generate the base MAC address for all interfaces

1. On the Configuration tab, navigate to System > Interfaces, and then click Set Global Base MAC Address.
2. In the Generate MAC Address dialog box, in the Base MAC Address text box, type the base MAC address.
3. Click Apply MAC Address. All the virtual instances provisioned on the appliance are restarted.
4. Click Generate, and then click Close.

To assign a MAC address to an interface

1. In the **Provision NetScaler Wizard** or the **Modify NetScaler Wizard**, on the Network Settings page, in the **Select Mode** list, choose one of the following options:
 - **Default**—XenServer assigns a MAC address.
 - **Custom**—SDX Administrator assigns a MAC address. The SDX administrator can use this setting to override the generated MAC address.
 - **Generated**— Generate a MAC address by using the base MAC address set earlier.
2. If you select **Custom**, enter a MAC Address.
3. Follow the instructions in the wizard.
4. Click **Finish**, and then click **Close**.

VLAN Filtering

VLAN filtering provides segregation of data between NetScaler VPX instances that share a physical port. For example, if you have configured two NetScaler VPX instances on two different VLANs and you enable VLAN filtering, one instance cannot view the other instance's traffic. If VLAN filtering is disabled, all of the instances can see the tagged or untagged broadcast packets, but the packets are dropped at the software level. If VLAN filtering is enabled, each tagged broadcast packet reaches only the instance that belongs to the corresponding tagged VLAN. If none of the instances belong to the corresponding tagged VLAN, the packet is dropped at the hardware level (NIC).

If VLAN filtering is enabled on an interface, a limited number of tagged VLANs can be used on that interface (63 tagged VLANs on a 10G interface and 32 tagged VLANs on a 1G interface). A VPX instance receives only the packets that have the configured VLAN IDs. Restart the NetScaler VPX instances associated with an interface if you change the state of the VLAN filter from DISABLED to ENABLED on that interface.

VLAN filtering is enabled by default on the NetScaler SDX appliance. If you disable VLAN filtering on an interface, you can configure up to 4096 VLANs on that interface.

Note: VLAN filtering can be disabled only on a NetScaler SDX appliance running XenServer version 6.0.

To enable VLAN filtering on an interface

1. On the Configuration tab, in the navigation pane, expand System, and then click Interfaces.
2. In the Interfaces pane, click VLAN Filter.
3. In the Enable/Disable VLAN Filter dialog box, click Add to enable VLAN filtering on an interface.
4. Optionally, select Reboot associated Instances.
5. Click OK.

Configuring Clock Synchronization

You can configure your NetScaler SDX appliance to synchronize its local clock with a Network Time Protocol (NTP) server. As a result, the clock on the SDX appliance has the same date and time settings as the other servers on your network. The clock synchronization configuration does not change if the appliance is restarted, upgraded, or downgraded. However, the configuration does not get propagated to the secondary NetScaler instance in a high availability setup.

The clock is synchronized immediately if you add a new NTP server or change any of the authentication parameters. You can also explicitly enable and disable NTP synchronization.

Note: If you do not have a local NTP server, you can find a list of public, open access, NTP servers at the official NTP site, <http://www.ntp.org>. Before configuring your NetScaler to use a public NTP server, be sure to read the Rules of Engagement page (link included on all Public Time Servers pages).

To configure an NTP server

1. In the navigation pane, expand System, and then click NTP Servers.
2. In the details pane, do one of the following:
 - To add a new NTP server, click Add.
 - To modify settings for an existing NTP server, select the NTP server, and then click Open.
3. In the Create NTP Server or Configure NTP Server dialog box, set the following parameters:
 - **Server Name/IP Address***—The domain name of the NTP server or the IP address of the NTP server. The name or IP address cannot be changed for an existing NTP server.
 - **Minimum Poll Interval**— The minimum number of seconds after which the NTP server must poll the NTP messages, expressed as a power of 2. Minimum value: 4 ($2^4=16$ seconds). Maximum value: 6 ($2^6=64$ seconds). Default: 6 ($2^6=64$ seconds).
 - **Maximum Poll Interval**— The maximum number of seconds after which the NTP server must poll the NTP messages, expressed as a power of 2. Minimum value: 10 ($2^{10}=1024$ seconds). Maximum value: 17 ($2^{17}=36$ hours). Default : 10 ($2^{10}=1024$ seconds).
 - **Key Identifier**—The key to be used for the specified server. This key identifier should be added to the list of Trusted Key IDs in the Authentication Parameters. Minimum value: 1. Maximum value: 65534.

Note: Do not add if Autokey is selected.
 - **Autokey**—Use the Autokey protocol for the specified server.
 - **Preferred**—Synchronize with this server first. Applicable if more than one server is configured.

*A required parameter
4. Click Add, and then click Close.
5. In the details pane, verify that the settings displayed for the NTP server that you just created are correct.

To enable NTP synchronization

1. In the navigation pane, expand System, and then click NTP Servers.
2. In the details pane, click NTP Synchronization.
3. In the NTP Synchronization dialog box, select Enable NTP Sync.
4. Click OK, and then click Close.

To modify Authentication options

1. In the navigation pane, expand System, and then click NTP Servers.
2. In the details pane, click Authentication Parameters.
3. In the Modify Authentication Options dialog box, set the following parameters:
 - Authentication—Enable NTP authentication. Possible values: YES, NO. Default: YES.
 - Trusted Key IDs—The trusted key IDs. While adding an NTP server, you select a key identifier from this list. Minimum value: 1. Maximum value: 65534.
 - Revoke Interval—The interval between re-randomization of certain cryptographic values used by the Autokey scheme, as a power of 2, in seconds. Default value: 17 ($2^{17}=36$ hours).
 - Automax Interval—The interval between regeneration of the session key list used with the Autokey protocol, as a power of 2, in seconds. Default value: 12 ($2^{12}=1.1$ hours).
4. Click OK, and then click Close.

Viewing the Properties of the NetScaler SDX Appliance

You can view system properties such as the number of CPU cores and SSL chips, total available memory and free memory, and various product details on the Configuration tab.

To view the properties of the NetScaler SDX appliance, click the Configuration tab.

You can view the following information about system resources, Hypervisor, License, and System:

System Resources

Total CPU Cores

The number of CPU cores on the SDX appliance.

Total SSL Chips

The total number of SSL chips on the SDX appliance.

Free SSL chips

The total number of SSL chips that have not been assigned to a NetScaler instance.

Total Memory (GB)

Total appliance memory in gigabytes.

Free Memory (GB)

Free appliance memory in gigabytes.

Hypervisor Information

Uptime

Time since the appliance was last restarted, in number of days, hours, and minutes.

Edition

The edition of XenServer that is installed on the SDX appliance.

Version

The version of XenServer that is installed on the SDX appliance.

iSCSI IQN

The iSCSI Qualified Name.

Product Code

Product code of XenServer.

Serial Number

Serial number of XenServer.

Build Date

Build date of XenServer.

Build Number

Build number of XenServer.

Supplemental Pack

Version of the supplemental pack installed on the SDX appliance.

License Information

Platform

Model number of the hardware platform, based on the installed license.

Maximum NetScaler Instances

The maximum number of instances that you can set up on the SDX appliance, based on the installed license.

Available NetScaler Instances (Shared)

The number of instances that can be configured depending on the number of CPU cores that are still available.

Maximum Throughput (Mbps)

The maximum throughput that can be achieved on the appliance, based on the installed license.

Available Throughput (Mbps)

The available throughput based on the installed license.

System Information

Platform

Model number of the hardware platform.

Product

Type of NetScaler product.

Build

NetScaler release and build running on the SDX appliance.

IP Address

IP address of the Management Service.

Host ID

XenServer host ID.

System ID

XenServer system ID.

Serial Number

XenServer serial number.

System Time

System time displayed in Day Month Date Hours:Min:Sec Timezone Year format.

Uptime

Time since the Management Service was last restarted, in number of days, hours, and minutes.

BIOS version

BIOS version.

Viewing Real-Time Appliance Throughput

The total throughput of the SDX appliance for incoming and outgoing traffic is plotted in real time in a graph that is updated at regular intervals. By default, throughputs for both incoming and outgoing traffic are plotted together on the graph.

To view the throughput of the SDX appliance, on the Monitoring tab, in the navigation pane, expand Monitoring, and then click Throughput.

Viewing Real-Time CPU and Memory Usage

You can view a graph of CPU and memory usage of the appliance. The graph is plotted in real time and updated at regular intervals.

To view the CPU and memory usage of the SDX appliance, on the Monitoring tab, in the navigation pane, expand Monitoring, and then click CPU / Memory Usage.

Viewing CPU Usage for All Cores

You can view the usage of each CPU core on the NetScaler SDX appliance.

The CPU Core Usage pane displays the following details:

Core Number

The CPU core number on the appliance.

Physical CPU

The physical CPU number of that core.

Hyper Threads

The hyper threads associated with that CPU core.

Instances

The instances that are using that CPU core.

Average Core Usage

The average core usage, expressed as a percentage.

To view the CPU usage for all the cores on the SDX appliance, on the Monitoring tab, in the navigation pane, expand Monitoring, and then click CPU Core Usage.

SNMP

You can configure a Simple Network Management Protocol (SNMP) agent on the NetScaler SDX appliance to generate asynchronous events, which are called traps. The traps are generated whenever there are abnormal conditions on the NetScaler SDX appliance. The traps are then sent to a remote device called a *trap listener*, which signals the abnormal condition on the NetScaler SDX appliance.

The following figure illustrates a network with a NetScaler SDX appliance that has SNMP enabled and configured. In the figure, each SNMP network management application uses SNMP to communicate with the SNMP agent on the NetScaler SDX appliance.

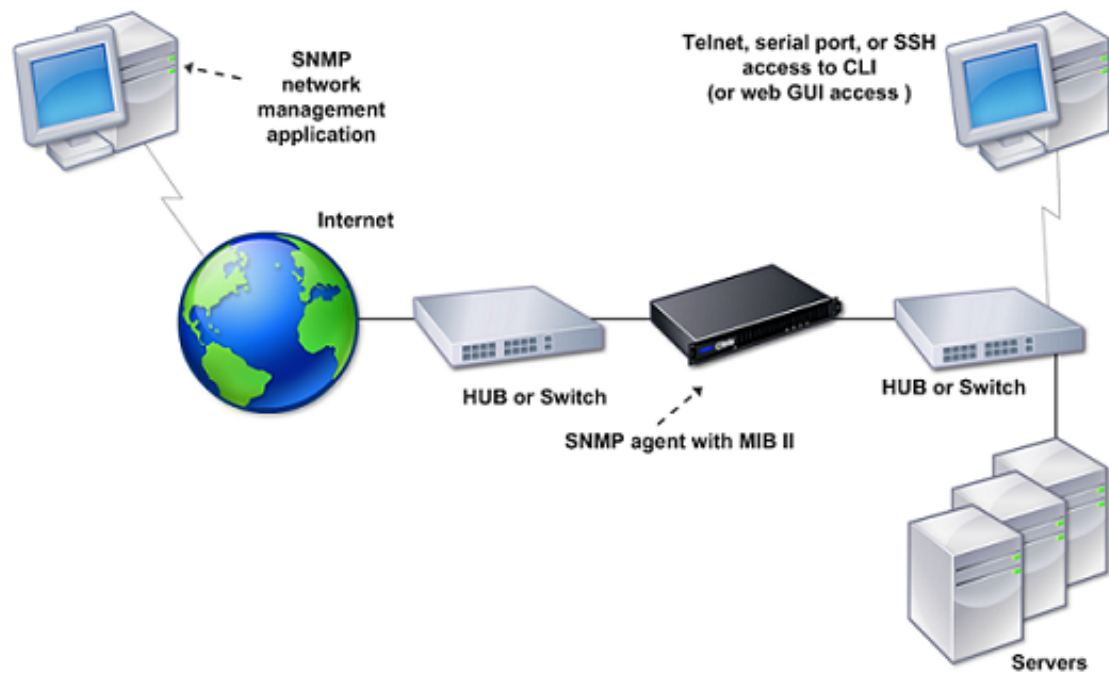


Figure 1. NetScaler SDX Appliance Supporting SNMP

SNMP Trap Destinations

The SNMP agent on the SDX appliance generates traps that are compliant with SNMPv2 only. The supported traps can be viewed in the SDX MIB file. You can download this file from the Downloads page in the SDX user interface.

To add an SNMP trap destination

1. On the configuration tab, in the navigation pane, expand System, and then click SNMP Trap Destinations.
2. In the SNMP Trap Destinations pane, click Add.
3. In the Add SNMP Trap Destinations dialog box, specify values for the following parameters:
 - Destination Server—IPv4 address of the trap listener to which to send the SNMP trap messages.
 - Port—UDP port at which the trap listener listens for trap messages. Must match the setting on the trap listener, or the listener drops the messages. Minimum value: 1. Default: 162.
 - Community—Password (string) sent with the trap messages, so that the trap listener can authenticate them. Can include letters, numbers, and hyphen (-), period (.) hash (#), space (), at (@), equals (=), colon (:), and underscore (_) characters.

Note: You must specify the same community string on the trap listener device, or the listener drops the messages. Default: public.
4. Click Add, and then click Close. The SNMP trap destination that you added appears in the SNMP Traps pane.

To modify the values of the parameters of an SNMP trap destination, in the SNMP Trap Destinations pane, select the trap destination that you want to modify, and then click Modify. In the Modify SNMP Trap Destination dialog box, modify the parameters.

To remove an SNMP trap, in the SNMP Trap Destinations pane, select the trap destination that you want to remove, and then click Delete. In the Confirm message box, click to remove the SNMP trap destination.

Downloading MIB Files

You must download the following file before you start monitoring a NetScaler SDX appliance.

SDX-MIB-smiv2.mib. This file is used by SNMPv2 managers and SNMPv2 trap listeners.

The file includes a NetScaler enterprise MIB that provides NetScaler SDX-specific events.

To download MIB files

1. Log on to the Downloads page of the NetScaler SDX appliance user interface.
2. Under SNMP Files, click SNMP v2 - MIB Object Definitions. You can open the file by using a MIB browser.

System Health Monitoring

System health monitoring detects errors in the monitored components, so that you can take corrective action to avoid a failure. The following components are monitored on a NetScaler SDX appliance:

- Hardware and software resources
- Physical and virtual disks
- Hardware sensors, such as fan, temperature, voltage, and power supply sensors
- Interfaces

In the Monitoring tab, click System Health. A summary of all the components is displayed. To view details of the monitored components, expand System Health, and then click the component that you want to monitor.

Monitoring the Resources on the SDX Appliance

You can monitor the hardware and software components on the NetScaler SDX appliance and take corrective action if required. To view the components monitored, in the Monitoring tab, expand System Health, and then click Resources. Details are displayed for hardware and software resources. For all hardware components, current and expected values are displayed. For software components, except the BMC firmware version, current and expected values are displayed as not applicable (NA).

Name

Name of the component, such as CPU, memory, or BMC firmware version.

Status

State (condition) of the component. For Hardware and for BMC Firmware Version, ERROR indicates a deviation from the expected value. For calls to XenServer, ERROR indicates that the Management Service is unable to communicate with XenServer by using an API, HTTP, PING, or SSH call. For Health Monitor Plugin, ERROR indicates that the plugin is not installed on XenServer.

Current Value

Current value of the component. In normal conditions, current value is the same as the expected value.

Expected Value

Expected value for the component. Does not apply to software calls to XenServer.

Monitoring the Storage Resources on the SDX Appliance

You can monitor the disks on the NetScaler SDX appliance and take corrective action if required. To view the components monitored, in the Monitoring tab, expand System Health, and then click Storage. Details are displayed for physical disks and for virtual disks or partitions created from physical disks.

For disks (Disk), the following details are displayed:

Name

Name of the physical disk.

Size

Size of the disk, in gigabytes (GB).

Utilized

Amount of data on the disk, in gigabytes (GB).

Transactions/s

Number of blocks being read or written per second. This number is read from the iostat output.

Blocks Read/s

Number of blocks being read per second. You can use this value to measure the rate of output from the disk.

Blocks Written/s

Number of blocks being written per second. You can use this value to measure the rate of input to the disk.

Total Blocks Read

Number of blocks read since the appliance was last started.

Total Blocks Written

Number of blocks written since the appliance was last started.

For virtual disks or partitions (Storage Repository), the following details are displayed:

Drive Bay

Number of the drive in the drive bay. You can sort the data on this parameter.

Status

State (condition) of the drive in the drive bay. Possible values:

- GOOD: The drive is in a good state and is ready for use.
- FAIL: The drive has failed and has to be replaced.
- MISSING: A drive is not detected in the drive bay.
- UNKNOWN: A new unformatted drive exists in the drive bay.

Name

System defined name of the storage depository.

Size

Size of the storage repository, in gigabytes (GB).

Utilized

Amount of data in the storage repository, in gigabytes (GB).

Monitoring the Hardware Sensors on the SDX Appliance

You can monitor the hardware components on the NetScaler SDX appliance and take corrective action if required. In the Monitoring tab, expand System Health, and then click Hardware Sensors. The monitoring function displays details about the speed of different fans, the temperature and voltage of different components, and the status of the power supply.

For fan speed, the following details are displayed:

Name

Name of the fan.

Status

State (condition) of the fan. ERROR indicates a deviation from the expected value. NA indicates that the fan is not present.

Current Value (RPM)

Current rotations per minute.

Temperature information includes the following details:

Name

Name of the component, such as CPU or memory module (for example, P1-DIMM1A.)

Status

State (condition) of the component. ERROR indicates that the current value is out of range.

Current Value (Degree C)

Current temperature, in degrees, of the component.

Voltage information includes the following details:

Name

Name of the component, such as CPU core.

Status

State (condition) of the component. ERROR indicates that the current value is out of range.

Current Value (Volts)

Current voltage present on the component.

Information about the power supply includes the following details:

Name

Name of the component.

Status

State (condition) of the component. Possible values:

- **Error:** Only one power supply is connected or working.
- **OK:** Both the power supplies are connected and working as expected.

Monitoring the Interfaces on the SDX Appliance

You can monitor the interfaces on the NetScaler SDX appliance and take corrective action if required. In the Monitoring tab, expand System Health, and then click Interfaces. The monitoring function details the following information about each interface:

Interface

Interface number on the SDX appliance.

Status

State of the interface. Possible values: UP, DOWN.

VFs Assigned/Total

Number of virtual functions assigned to the interface, and the number of virtual functions available on that interface. You can assign up to seven virtual functions on a 1G interface and up to 40 virtual functions on a 10G interface.

Tx Packets

Number of packets transmitted since the appliance was last started.

Rx Packets

Number of packets received since the appliance was last started.

Tx Bytes

Number of bytes transmitted since the appliance was last started.

Rx Bytes

Number of bytes received since the appliance was last started.

Tx Errors

Number of errors in transmitting data since the appliance was last started.

Rx Errors

Number of errors in receiving data since the appliance was last started.

Configuring the Management Service

The Management Service lets you manage client sessions and perform configuration tasks, such as creating and managing user accounts and tweaking backup and pruning policies according to your requirements. You can also restart the Management Service and upgrade the version of the Management Service. You can further create tar files of the Management Service and the XenServer and send it to technical support.

Managing Client Sessions

A client session is created when a user logs on to the Management Service. You can view all the client sessions on the appliance in the Sessions pane.

In the Sessions pane, you can view the following details:

User Name

The user account that is being used for the session.

IP Address

The IP address of the client from which the session has been created.

Port

The port being used for the session.

Login Time

The time at which the current session was created on the SDX appliance.

Last Activity Time

The time at which user activity was last detected in the session.

Session Expires In

Time left for session expiry.

To view client sessions, on the Configuration tab, in the navigation pane, expand System, and then click Sessions.

To end a client session, in the Sessions pane, click the session you want to remove, and then click End Session.

You cannot end a session from the client that has initiated that session.

Configuring User Accounts

A user logs on to the NetScaler SDX appliance to perform appliance management tasks. To allow a user to access the appliance, you must create a user account on the SDX appliance for that user. Users are authenticated locally, on the appliance.

Important: The password applies to the SDX appliance, Management Service, and XenServer. Do not change the password directly on the XenServer.

To configure a user account

1. In the navigation pane, expand System, and then click Users. The Users pane displays a list of existing user accounts, with their permissions.
2. In the Users pane, do one of the following:
 - To create a user account, click Add.
 - To modify a user account, select the user, and then click Modify.
3. In the Create System User or Modify System User dialog box, set the following parameters:
 - Name*—The user name of the account. The following characters are allowed in the name: letters a through z and A through Z, numbers 0 through 9, period (.), space, and underscore (_). Maximum length: 128. You cannot change the name.
 - Password*—The password for logging on to the appliance.
 - Confirm Password*—The password.
 - Permission*—The user's privileges on the appliance. Possible values:
 - Superuser—The user can perform all administration tasks related to the Management Service.
 - Readonly—The user can only monitor the system and change the password of the account.
Default: superuser.

*A required parameter
4. Click Create or OK, and then click Close. The user that you created is listed in the Users pane.

To remove a user account

1. On the Configuration tab, in the navigation pane, expand System, and then click Users.
2. In the Users pane, select the user account, and then click Delete.
3. In the Confirm message box, click OK.

Configuring Policies

To keep the size of logged data within manageable limits, the SDX appliance runs backup and data-pruning policies automatically at a specified time.

The prune policy runs at 00:00 A.M every day and specifies the number of days of data to retain on the appliance. By default, the appliance prunes data older than 3 days, but you can specify the number of days of data that you want to keep. Only event logs, audit logs, and task logs are pruned.

The backup policy runs at 00:30 A.M. every day and creates a backup of logs and configuration files. By default, the policy retains three backups, but you can specify the number of backups you want to keep.

To specify the number of days for which logged data is pruned

1. On the Configuration tab, in the navigation pane, click System.
2. In the System pane, under Policy Administration, click Prune Policy.
3. In the Modify Prune Policy dialog box, in Data to keep (days), specify the number of days of data that the appliance must retain at any given time.
4. Click OK.

To specify the number of backups that the appliance must retain

1. On the Configuration tab, in the navigation pane, click System.
2. In the System pane, under Policy Administration, click Backup Policy.
3. In the Modify Backup Policy dialog box, in #Previous Backups to retain, specify the number of backups that the appliance must retain at any given time.
4. Click OK.

Restarting the Management Service

You can restart the Management Service from the System pane. Restarting the Management Service does not affect the working of the NetScaler instances. The NetScaler instances continue to function during the Management Service restart process.

To restart the Management Service

1. On the Configuration tab, in the navigation pane, click System.
2. In the System pane, under System Administration, click Reboot Management Service.

Upgrading the Management Service

The process of upgrading the Management Service involves uploading the build file of the target build and the documentation file to the SDX appliance, and then upgrading the Management Service.

Uploading the Management Service Build and Documentation Files

You can upload the Management Service build and documentation files from a client computer to the SDX appliance. You can also download build and documentation files to a local computer as a backup.

To upload the Management Service build file

1. In the navigation pane, expand Management Service, and then click Software Images.
2. In the Software Images pane, click Upload.
3. In the Upload Management Service Software Image dialog box, click Browse, navigate to the folder that contains the build file, and then double-click the build file.
4. Click Upload.

To create a backup by downloading a Management Service build file

1. In the Software Images pane, select the file you want to download, and then click Download.
2. In the message box, from the Save list, select Save as.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

To upload the Management Service documentation file

1. In the navigation pane, expand Management Service, and then click Software Images.
2. In the Software Images pane, on the Documentation Files tab, click Upload.
3. In the Upload Management Service Documentation File dialog box, click Browse, navigate to the folder that contains the documentation file, and then double-click the file.
4. Click Upload.

To create a backup by downloading a Management Service documentation file

1. In the Software Images pane, select the file you want to download, and then click Download.
2. In the message box, from the Save list, select Save as.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

Upgrading the Management Service to a Later Version

After you have uploaded the Management Service image to the SDX appliance, use this image to upgrade the version of the Management Service. The Management Service will restart after the upgrade. Restarting the Management Service does not affect your NetScaler VPX instances and the appliance.

To upgrade the Management Service

1. In the navigation pane, click System.
2. In the System pane, under System Administration, click Upgrade Management Service.
3. In the Upgrade Management Service dialog box, in Software Image, select the software image file to which you want to upgrade the Management Service.
4. In Documentation File, select the documentation file you want to use during upgrade.
5. Click OK.

Upgrading the XenServer Software

You need to upgrade to a later version of the XenServer software to enable functionality of some features, such as VLAN filtering, L2 mode, and VMAC support. The process of upgrading the XenServer software involves uploading the build file of the target build to the Management Service, and then upgrading the XenServer software.

Uploading the XenServer Build Files

You can upload the XenServer build files from a client computer to the SDX appliance. You can also download the build files to a local computer as a backup.

To upload the XenServer build file

1. In the navigation pane, expand Management Service, and then click XenServer Files.
2. In the details pane, click the ISO Images tab, and then click Upload.
3. In the Upload XenServer ISO Image File dialog box, click Browse, navigate to the folder that contains the build file, and then double-click the build file.
4. Click Upload.

To create a backup by downloading a XenServer build file

1. In the details pane, click the ISO Images tab, select the file you want to download, and then click Download.
2. In the message box, from the Save list, select Save as.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

For information about uploading and applying a XenServer hotfix, see [Uploading and Applying a XenServer Hotfix](#).

Upgrading the Software

You can upgrade to the latest version of the XenServer software. The upgrade process may take up to 20 minutes. Before upgrading the software, upload the ISO image file to the appliance. The current version of the software is displayed in the Upgrade XenServer dialog box.

To upgrade the XenServer software

1. In the navigation pane, click System.
2. In the details pane, click Upgrade XenServer.
3. In the Upgrade XenServer dialog box, select the Image file from the list.
4. Click OK, and then click Close.

Uploading and Applying a XenServer Hotfix

You can upload the XenServer hotfix files from a client computer to the SDX appliance. You can also download the hotfix files to a local computer as a backup.

Important: Citrix recommends that you make a backup before applying a XenServer hotfix. Apply only the hotfix that is available in the NetScaler download page.

XenServer 6.0 should be installed on your SDX appliance. To upgrade to XenServer 6.0, see [Upgrading the XenServer Software to a Later Version](#).

To upload and apply a XenServer hotfix

1. In the navigation pane, expand Management Service, and then click XenServer Files.
2. In the Hotfixes pane, click Upload.
3. In the Upload XenServer Hotfix dialog box, click Browse, navigate to the folder that contains the build file, and then double-click the build file.
4. Click Upload. The hotfix appears in the details pane.
5. Click Apply. In the Confirm dialog box, click Yes.

Note: In the details pane, if the After Apply Guidance column contains "rearthost", then restart the appliance.

Important: If the appliance does not restart correctly, perform a factory reset, and then restore the configuration from the backup that was taken before applying the hotfix. For information about performing a factory reset, see [Performing a Factory Reset](#). For information about restoring the configuration, see [Backing Up and Restoring the Configuration Data of the SDX Appliance](#).

To create a backup by downloading a XenServer hotfix file

1. In the Hotfixes pane, select the file you want to download, and then click Download.
2. In the message box, from the Save list, select Save as.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

Installing the XenServer Supplemental Pack

The XenServer supplemental pack for NetScaler SDX contains updated igb-modules, ixgbe-modules, and iovirt plugins. It provides support for the following features:

- Layer 2 networking
- Virtual MAC
- System health monitoring support
- Creating a cluster of NetScaler instances
- MAC-address assignment by the system administrator
- Restricting a VLAN to a specific virtual interface
- Link aggregation control protocol (LACP)

The following table lists the supplemental pack version required for specific XenServer and Management Service versions.

Table 1. Supplemental Pack Version Supported on the NetScaler SDX Appliance

XenServer Version	Supplemental Pack Version	Management Service Version
XenServer 6.0	Build 100003	Release 10.0, Build 69.4 or later
XenServer 6.0	Build 100006	Release 10.1, Build 112.13 or later

The appliance and all the instances restart after you install the supplemental pack.

To upload the supplemental pack

1. In the navigation pane, expand Management Service, and then click XenServer Files.
2. In the Supplemental Packs pane, click Upload.
3. In the Upload XenServer Supplemental Pack dialog box, click Browse, navigate to the folder that contains the .iso file, and then double-click the file.
4. Click Upload. The supplemental pack appears in the details pane.

To install the supplemental pack

XenServer 6.0 should be installed on your SDX appliance. To upgrade to XenServer 6.0, see [Upgrading the XenServer Software to a Later Version](#).

1. In the Supplemental Packs pane, click Install.
2. In the Confirm dialog box, click Yes.

To create a backup by downloading the supplemental pack

1. In the Supplemental Packs pane, select the file you want to download, and then click Download.
2. In the message box, from the Save list, select Save as.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

Backing Up and Restoring the Configuration Data of the SDX Appliance

The backup policy runs at 00:30 A.M. every day. You do not have to wait until midnight for creating a backup file. You can create a backup file at any time if, for example, you want to immediately back up changes to the configuration.

You can use the backup file to restore the configuration data on the appliance. You can restore the configuration data of the XenServer, Management Service, and all the NetScaler instances, only the NetScaler instances, or selected NetScaler instances.

To perform an immediate backup

1. In the navigation pane, expand Management Service, and then click Backup Files.
2. In the Backup Files pane, click Back Up.
3. In the Confirm dialog box, click Yes. This process may take a few minutes, depending on the amount of data to be backed up.

To restore the configuration

1. In the navigation pane, expand Management Service, and then click Backup Files.
2. In the Backup Files pane, click Restore.
3. In the Restore Wizard, select one of the following:
 - Restore Appliance—Restores the XenServer, Management Service, and all the NetScaler instances.
Note: Perform a Factory Reset before selecting this option.
 - All instances—Restores all the NetScaler instances.
 - Specific instances—Restores only the selected NetScaler instances.
4. Click Next, and then click Finish. The progress status is displayed.
5. Click Close.

Performing a Factory Reset

Before performing a factory reset, back up all the data stored on the appliance, including the settings of all the NetScaler instances provisioned on the appliance. Citrix recommends that you store the files outside the appliance. Performing a factory reset terminates all current client sessions with the Management Service, so you have to log back on to the Management Service for any additional configuration tasks. When you are ready to restore the data, import the backup files by using the Management Service.

You also have the option to reset while retaining the current IP addresses of the Management Service and XenServer or to reset with the default IP addresses of the Management Service and XenServer. In either case, the software automatically performs the following actions:

- Deletes NetScaler VPX instances.
- Deletes SSL certificate and key files.
- Deletes license and technical archive files.
- Deletes the NTP configuration on the appliance.
- Restores the time zone to UTC.
- Restores prune and backup policies to their default settings.
- Deletes the Management Service image and documentation files.
- Deletes the NetScaler image and documentation files.
- Deletes all XVA images except the last image file that was accessed on the appliance.
- Restores default interface settings.
- Restores the default configuration of the appliance, including default profiles, users, and system settings.
- Restores default IP addresses for XenServer and the Management Service.
- Restores default passwords for XenServer and the Management Service.
- Restarts the Management Service.

To perform a factory reset

The factory reset process takes approximately one hour.

1. In the navigation pane, expand Management Service, and then click Backup Files.
2. In the Backup Files pane, click Factory Reset.

3. In the Factory Reset dialog box, select the type of reset from the following options:
 - Reset (Without Network Configuration)—Retain the IP addresses of the Management Service and XenServer.
 - Reset (With Network Configuration)—Management Service and XenServer restart with the default IP addresses.
 - Appliance Reset—The appliance settings are restored to the default factory settings, such as default IP addresses for Management Service and XenServer. No instances are installed, and only the default SSL certificate is available on the appliance.
4. Click OK, and then click Close.
5. When the reset is complete, log on with the default credentials and run the configuration wizard.

Removing Management Service Files

You can remove any unneeded Management Service build and documentation files from the SDX appliance.

To remove a Management Service file

1. On the Configuration tab, in the navigation pane, expand Management Service, and then click the file that you want to remove.
2. In the details pane, select the file name, and then click Delete.

Generating a Tar Archive for Technical Support

You can use the Technical Support option to generate a tar archive of data and statistics for submission to Citrix technical support. This tar can be generated for the Management Service or the XenServer, or for both at the same time. You can then download the file to your local system and send it to Citrix technical support.

In the Technical Support pane, you can view the following details.

Name

The name of the tar archive file. The file name indicates whether the tar is for the Management Service or the XenServer server.

Last Modified

The date when this file was last modified.

Size

The size of the tar file.

To generate the tar archive for technical support

1. On the Configuration tab, navigate to Diagnostics > Technical Support.
2. In the details pane, from the Action list, select Generate Technical Support File.
3. In the Generate Technical Support File dialog box, from the Mode list, select the appropriate option for whether you want to archive data of XenServer, Management Service, Appliance (including XenServer and Management Service), Instances, or Appliance (including instances).
4. Click OK.

To download the tar archive for technical support

1. In the Technical Support pane, select the technical support file that you want to download.
2. From the Action list, select Download. The file is saved to your local computer.

Provisioning NetScaler Instances

You can provision one or more NetScaler instances on the SDX appliance by using the Management Service. The number of instances that you can install depends on the license you have purchased. If the number of instances added is equal to the number specified in the license, the Management Service does not allow provisioning more NetScaler instances.

To provision NetScaler instances on the SDX appliance, first, you need to define an admin profile to attach to the NetScaler instance. This profile specifies the user credentials that are used by the Management Service to provision the NetScaler instance and later, to communicate with the instance to retrieve configuration data. You can also use the default admin profile. Next, you need to upload the .xva image file to the Management Service. After uploading the .xva file, you can begin adding NetScaler instances using the Management Service. The Management Service implicitly deploys the NetScaler instances on the SDX appliance and then downloads configuration details of the instances.

Note: By default, a .xva image file based on the NetScaler 9.3 release is available on the SDX appliance.

Creating Admin Profiles

Admin profiles specify the user credentials that are used by the Management Service when provisioning the NetScaler instances, and later when communicating with the instances to retrieve configuration data. The user credentials specified in an admin profile are also used by the client when logging on to the NetScaler instances through the CLI or the configuration utility.

The default admin profile for an instance specifies a user name of `nsroot`, and the password is also `nsroot`. This profile cannot be modified or deleted. However, you should override the default profile by creating a user-defined admin profile and attaching it to the instance when you provision the instance. The Management Service administrator can delete a user-defined admin profile if it is not attached to any NetScaler instance.

Important:

Do not change the password directly on the NetScaler VPX instance. If you do so, the instance becomes unreachable from the Management Service. To change a password, first create a new admin profile, and then modify the NetScaler instance, selecting this profile from the Admin Profile list.

To change the password of NetScaler instances in a high availability setup, first change the password on the instance designated as the secondary node, and then change the password on the instance designated as the primary node. Remember to change the passwords only by using the Management Service.

To create an admin profile

1. On the Configuration tab, in the navigation pane, expand NetScaler Configuration, and then click Admin Profiles.
2. In the Admin Profiles pane, click Add.
3. In the Create Admin Profile dialog box, set the following parameters:
 - Profile Name*—Name of the admin profile. The default profile name is nsroot. You can create user-defined profile names.
 - User Name—User name used to log on to the NetScaler instances. The user name of the default profile is nsroot and cannot be changed.
 - Password*—The password used to log on to the NetScaler instance. Maximum length: 31 characters.
 - Confirm Password*—The password used to log on to the NetScaler instance.

* A required parameter
4. Click Create, and then click Close. The admin profile you created appears in the Admin Profiles pane.

If the value in the Default column is `true` the default profile is the admin profile. If the value is `false`, a user-defined profile is the admin profile.

If you do not want to use a user-defined admin profile, you can remove it from the Management Service. To remove a user-defined admin profile, in the Admin Profiles pane, select the profile you want to remove, and then click Delete.

Uploading NetScaler .Xva Images

You have to upload the NetScaler .xva files to the SDX appliance before provisioning the NetScaler instances. You can also download an .xva image file to a local computer as a backup. The .xva image file format is: NSVPX-XEN-ReleaseNumber-BuildNumber_nc.xva

Note: By default, an .xva image file based on the NetScaler 9.3 release is available on the SDX appliance.

In the NetScaler XVA Files pane, you can view the following details.

Name

Name of the .xva image file. The file name contains the release and build number. For example, the file name NSVPX-XEN-9.3-25_nc.xva refers to release 9.3 build 25.

Last Modified

Date when the .xva image file was last modified.

Size

Size, in MB, of the .xva image file.

To upload a NetScaler .xva file

1. On the Configuration tab, in the navigation pane, expand NetScaler Configuration, and then click XVA Files.
2. In the NetScaler XVA Files pane, click Upload.
3. In the Upload NetScaler Instance XVA dialog box, click Browse and select the XVA image file that you want to upload.
4. Click Upload. The XVA image file appears in the NetScaler XVA Files pane after it is uploaded.

To create a backup by downloading a NetScaler .xva file

1. In the NetScaler Build Files pane, select the file that you want to download, and then click Download.
2. In the File Download message box, click Save.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

Adding a NetScaler Instance

When you add NetScaler instances from the Management Service, you need to provide values for some parameters, and the Management Service implicitly configures these settings on the NetScaler instances.

Typically, the Management Service and the management address (NSIP) of the NetScaler VPX instance are in the same subnetwork, and communication is over a management interface. However, if the Management Service and the instance are in different subnetworks, you have to specify a VLAN ID at the time of provisioning a NetScaler VPX instance, so that the instance can be reached over the network when it starts. If your deployment requires that the NSIP not be accessible through any interface other than the one selected at the time of provisioning the VPX instance, select the NSVLAN option.

Citrix recommends the default setting—NSVLAN not selected. You cannot change this setting after you have provisioned the NetScaler instance.

Note: For a high availability setup (active-active or active-standby), Citrix recommends that you configure the two NetScaler instances on different SDX appliances. Make sure that the instances in the setup have identical resources, such as CPU, memory, interfaces, packets per second (PPS), and throughput.

Name*

The host name assigned to the NetScaler instance.

IP Address*

The NetScaler IP (NSIP) address at which you access a NetScaler instance for management purposes. A NetScaler instance can have only one NSIP. You cannot remove an NSIP address.

Netmask*

The subnet mask associated with the NSIP address.

Gateway*

The default gateway that you must add on the NetScaler instance if you want access through SSH or the configuration utility from an administrative workstation or laptop that is on a different network.

XVA File*

The .xva image file that you need to provision. This file is required only when you add a NetScaler instance.

Feature License*

Specifies the license you have procured for the NetScaler. The license could be Standard, Enterprise, and Platinum.

Admin Profile*

The profile you want to attach to the NetScaler instance. This profile specifies the administrator (nsroot) user credentials that are used by the Management Service to provision the NetScaler instance and later, to communicate with the instance to retrieve configuration data. The user credentials used in this profile are also used while logging on to the NetScaler instance by using the GUI or the CLI. It is recommended that you change the default password of the admin profile. This is done by creating a new profile with a user-defined password. For more information, see [Configuring Admin Profiles](#).

Description

Add a description or comments related to the administrator profile.

Total Memory (MB)*

The total memory allocated to the NetScaler instance.

#SSL chips*

Number of SSL chips assigned to the NetScaler instance. SSL chips cannot be shared. The instance is restarted if you modify this value.

Throughput (Mbps)*

The total throughput allocated to the NetScaler instance. The total used throughput should be less than or equal to the maximum throughput allocated in the SDX license. If the administrator has already allocated full throughput to multiple instances, no further throughput can be assigned to any new instance.

Packets per second*

The maximum number of packets that the instance can receive per second.

CPU

Assign a dedicated core or cores to the instance, or the instance shares a core with other instance(s). If you select shared, then one core is assigned to the instance but the core might be shared with other instances if there is a shortage of resources.

Reboot affected Instances if CPU cores are reassigned

Restart the instances on which CPU cores are reassigned to avoid any performance degradation.

User Name*

The user name for the NetScaler instance administrator. This user has superuser access, but does not have access to networking commands to configure VLANs and interfaces.

Password*

The password for the instance administrator's user name.

Confirm Password*

The password for the instance administrator's user name.

Shell/Sftp/Scp Access*

The access allowed to the NetScaler instance administrator.

Allow L2 Mode

Allow L2 mode on the NetScaler instance. Select this option before you log on to the instance and enable L2 mode. For more information, see [Allowing L2 Mode on a NetScaler Instance](#).

Note: If you disable L2 mode for an instance from the Management Service, you must log on to the instance and disable L2 mode from that instance. Failure to do so might cause all the other NetScaler modes to be disabled after you restart the instance

Interface Settings

This specifies the network interfaces assigned to a NetScaler instance. You can selectively assign interfaces to an instance. For each interface, if you select Tagged, specify a VLAN ID.

Important: The interface IDs of interfaces that you add to an instance do not necessarily correspond to the physical interface numbering on the SDX appliance. For example, if the first interface that you associate with instance 1 is SDX interface 1/4, it appears as interface 1/1 when you log on to the instance and view the interface settings, because it is the first interface that you associated with instance 1.

- If a non-zero VLAN ID is specified for a NetScaler instance interface, all the packets transmitted from the NetScaler instance through that interface will be tagged with the specified VLAN ID. If you want incoming packets meant for the NetScaler instance that you are configuring to be forwarded to the instance through a particular interface, you must tag that interface with a VLAN ID and ensure that the incoming packets specify that VLAN ID.
- For an interface to receive packets with multiple VLAN tags, you must specify a VLAN ID of 0 for the interface, and you must specify the required VLAN IDs for the NetScaler instance interface.

VLAN ID

An integer that uniquely identifies the VLAN. Minimum value: 2. Maximum value: 4095.

Allowed VLANs

Specify a list of VLAN IDs that can be associated with a NetScaler instance.

VRID IPV4

The IPv4 VRID that identifies the VMAC. Possible values: 1 to 255. For more information, see [Configuring VMACs on an Interface](#).

VRID IPV6

The IPv6 VRID that identifies the VMAC. Possible values: 1 to 255. For more information, see [Configuring VMACs on an Interface](#).

NSVLAN

A VLAN to which the subnet of the NetScaler management IP (NSIP) address is bound. The NSIP subnet is available only on interfaces that are associated with the NSVLAN. Select this check box if your deployment requires that the NSIP not be accessible through any interface other than the one you select in the VLAN Settings dialog box. This setting cannot be changed after the NetScaler instance is provisioned.

Note:

- HA heartbeats will be sent only on the interfaces that are part of the NSVLAN.
- You can configure an NSVLAN only from VPX XVA build 9.3-53.4 and later.

Important: If NSVLAN is not selected, running the "clear config full" command on the VPX instance deletes the VLAN configuration.

Tagged

Designate all interfaces associated with the VLAN as 802.1q tagged interfaces.

Note: If you select tagged, make sure that management interfaces 0/1 and 0/2 are not added.

Interfaces

Bind the selected interfaces to the VLAN.

To provision a NetScaler instance

1. On the Configuration tab, in the navigation pane, expand NetScaler Configuration, and then click Instances.
2. In the NetScaler Instances pane, click Add.
3. In the Provision NetScaler Wizard follow the instructions on the screen.
4. Click Create, and then click Close. The provisioning progress and any failures, such as failure to assign a virtual function to the VPX instance, are displayed.

To modify the values of the parameters of a provisioned NetScaler instance, in the NetScaler Instances pane, select the instance that you want to modify, and then click Modify. In the Modify NetScaler Wizard, modify the parameters.

Note: If you modify the following parameters: number of SSL chips, interfaces, memory, and feature license, the NetScaler instance implicitly stops and restarts to bring these parameters into effect.

You cannot modify the Image and User Name parameters.

If you want to remove a NetScaler instance provisioned on the SDX appliance, in the NetScaler Instances pane, select the instance that you want to remove, and then click Delete. In the Confirm message box, click Yes to remove the NetScaler instance.

Configuring and Managing NetScaler Instances

After you have provisioned NetScaler instances on your appliance, you can perform the following tasks to configure and manage these instances.

- Save the Configuration
- Install SSL Certificates
- Upgrade a NetScaler Instance
- Manage a NetScaler Instance
- Apply the Administration Configuration

Creating a Mapped IP Address or a Subnet IP Address on a NetScaler Instance

You can assign mapped IP address (MIP) and subnet IP address (SNIP) to the NetScaler instances after they are provisioned on the SDX appliance.

A SNIP is used in connection management and server monitoring. It is not mandatory to specify a SNIP when you initially configure the NetScaler appliance. You can assign SNIP to the NetScaler instance from the Management Service.

A MIP is used for server-side connections. A MIP can be considered a default Subnet IP (SNIP) address, because MIPs are used when a SNIP is not available or use SNIP (USNIP) mode is disabled. You can create or delete a MIP during runtime without restarting the NetScaler instance.

To add a MIP or SNIP on a NetScaler instance

1. On the Configuration tab, in the navigation pane, click NetScaler.
2. In the details pane, under NetScaler Configuration, click Create IP.
3. In the Create NetScaler IP dialog box, specify values for the following parameters.

IP Address*

Specify the IP address assigned as the SNIP or the MIP address.

Netmask*

Specify the subnet mask associated with the SNIP or MIP address.

Type*

Specify the type of IP address. Possible values: SNIP, MIP. Default value: SNIP.

Save Configuration*

Specify whether the configuration should be saved on the NetScaler. Default value is false.

Instance IP Address*

Specify the IP address of the NetScaler instance.

4. Click Create, and then click Close.

Saving the Configuration

You can save the running configuration of a NetScaler instance from the Management Service.

To save the configuration on a NetScaler instance

1. On the Configuration tab, in the navigation pane, click NetScaler.
2. In the details pane, under NetScaler Configuration, click Save Configuration.
3. In the Save Configuration dialog box, in Instance IP Address, select the IP addresses of the NetScaler instances whose configuration you want to save.
4. Click OK, and then click Close.

Installing SSL Certificates

The process of installing SSL certificates involves uploading the certificate and key files to the SDX appliance, and then installing the SSL certificate on the NetScaler instances.

Uploading the Certificate File to the SDX Appliance

For any SSL transaction, the server needs a valid certificate and the corresponding private and public key pair. The certificate file must be present on the SDX appliance when you install the SSL certificate on the NetScaler instances. You can also download the SSL Certificate files to a local computer as a backup.

In the SSL Certificates pane, you can view the following details.

Name

The name of the certificate file.

Last Modified

The date when the certificate file was last modified.

Size

The size of the certificate file in bytes.

To upload SSL certificate files to the SDX appliance

1. In the navigation pane, expand Management Service, and then click SSL Certificate Files.
2. In the SSL Certificates pane, click Upload.
3. In the Upload SSL Certificate dialog box, click Browse and select the certificate file you want to upload.
4. Click Upload. The certificate file appears in the SSL Certificates pane.

To create a backup by downloading an SSL certificate file

1. In the SSL Certificates pane, select the file that you want to download, and then click Download.
2. In the message box, from the Save list, select Save as.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

Uploading SSL Key Files to the SDX Appliance

For any SSL transaction, the server needs a valid certificate and the corresponding private and public key pair. The key file must be present on the SDX appliance when you install the SSL certificate on the NetScaler instances. You can also download the SSL key files to a local computer as a backup.

In the SSL Keys pane, you can view the following details.

Name

The name of the key file.

Last Modified

The date when the key file was last modified.

Size

the size of the key file in bytes.

To upload SSL key files to the SDX appliance

1. In the navigation pane, expand Management Service, and then click SSL Certificate Files.
2. In the SSL Certificate pane, on the SSL Keys tab, click Upload.
3. In the Upload SSL Key File dialog box, click Browse and select the key file you want to upload.
4. Click Upload to upload the key file to the SDX appliance. The key file appears in the SSL Keys pane.

To create a backup by downloading an SSL key file

1. In the SSL Certificate pane, on the SSL Keys tab, select the file that you want to download, and then click Download.
2. In the message box, from the Save list, select Save as.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

Installing an SSL Certificate on a NetScaler Instance

The Management Service lets you install SSL certificates on one or more NetScaler instances. Before you begin installing the SSL certificate, make sure that you have uploaded the SSL certificate and key files to the SDX appliance.

To install SSL certificates on a NetScaler instance

1. In the navigation pane, click NetScaler.
2. In the details pane, under NetScaler Configuration, click Install SSL Certificates.
3. In the Install SSL Certificates dialog box, specify values for the following parameters.

Certificate File*

Specify the file name of the valid certificate. The certificate file must be present on the SDX appliance.

Key File*

Specify the file name of the private-key used to create the certificate. The key file must be present on the SDX appliance.

Certificate Name*

Specify the name of the certificate-key pair to be added to the NetScaler. Maximum length: 31

Certificate Format*

Specify the format of the SSL certificate supported on the NetScaler. A NetScaler appliance supports the PEM and DER formats for SSL certificates.

Password

Specify the pass-phrase that was used to encrypt the private-key. This option can be used to load encrypted private-keys. Max length: 32.

Note: Password protected private key is supported only for the PEM format.

Save Configuration*

Specify whether the configuration needs to be saved on the NetScaler. Default value is false.

Instance IP Address*

Specify the IP addresses of the NetScaler instances on which you want to install the SSL certificate.

4. Click OK, and then click Close.

Updating an SSL Certificate on a NetScaler Instance

You can update some parameters, such as the certificate file, key file, and certificate format of an SSL certificate that is installed on a NetScaler instance. You cannot modify the IP address and certificate name.

To update the SSL certificate on a NetScaler instance

1. In the navigation pane, expand NetScaler, and then click SSL Certificates.
2. In the SSL Certificates pane, click Update.
3. In the Modify SSL Certificate dialog box, set the following parameters:
 - **Certificate File***—The file name of the valid certificate. The certificate file must be present on the SDX appliance.
 - **Key File**—The file name of the private-key used to create the certificate. The key file must be present on the SDX appliance.
 - **Certificate Format***—The format of the SSL certificate supported on the NetScaler. A NetScaler appliance supports the PEM and DER formats for SSL certificates.
 - **Password**—The pass-phrase that was used to encrypt the private-key. This option can be used to load encrypted private-keys. Maximum length: 32 characters.
Note: Password protected private key is supported only for the PEM format.
 - **Save Configuration**—Specify whether the configuration needs to be saved on the NetScaler. Default value is false.
 - **No Domain Check**—Do not check the domain name while updating the certificate.

*A required parameter
4. Click OK, and then click Close.

Polling for SSL Certificates on the NetScaler Instances

If you add a new SSL certificate directly on a NetScaler instance after logging on to that instance, the Management Service is not aware of this new certificate. To avoid this, specify a polling interval after which the Management Service will poll all the NetScaler instances to check for new SSL certificates. You can also perform a poll at any time from the Management Service if, for example, you want to immediately get a list of all the SSL certificates from all the NetScaler instances.

To configure a polling interval

1. In the navigation pane, expand NetScaler, and then click SSL Certificates.
2. In the SSL Certificates pane, click Configure Polling Interval.
3. In the Configure Polling Interval dialog box, set the following parameters:
 - Polling Interval*—The time after which the Management Service polls the NetScaler instances.
 - Interval Unit*—The unit of time. Possible values: Hours, Minutes. Default: Hours.

*A required parameter
4. Click OK, and then click Close.

To perform an immediate poll

1. In the navigation pane, expand NetScaler, and then click SSL Certificates.
2. In the SSL Certificates pane, click Poll Now.
3. In the Confirm dialog box, click Yes. The SSL Certificates pane is refreshed and new certificates, if any, appear in the list.

Upgrading a NetScaler Instance

The process of upgrading the NetScaler instances involves uploading the build file and the documentation file of the target build to the SDX appliance, and then upgrading the NetScaler instance.

Uploading NetScaler Resources

You have to upload the NetScaler software images to the SDX appliance before upgrading the NetScaler instances. Citrix recommends that you upload the latest documentation file along with the image file. You can also download the image and documentation files to a local computer as a backup. For installing a new instance, you need the NetScaler XVA file.

In the NetScaler Software Images pane, you can view the following details.

Name

Name of the NetScaler instance software image file. The file name contains the release and build number. For example, the file name build-10-53.5_nc.tgz refers to release 10 build 53.5 .

Last Modified

Date when the file was last modified.

Size

Size, in MB, of the file.

To upload a NetScaler software image

1. In the navigation pane, expand NetScaler, and then click Software Images .
2. In the Software Images pane, click Upload.
3. In the Upload NetScaler Software Image dialog box, click Browse and select the NetScaler image file that you want to upload.
4. Click Upload. The image file appears in the NetScaler Software Images pane.

To create a backup by downloading a NetScaler build file

1. In the Software Images pane, select the file you want to download, and then click Download.
2. In the message box, from the Save list, select Save as.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

To upload a NetScaler documentation file

1. In the navigation pane, expand NetScaler, and then click Software Images.
2. In the Software Images pane, on the Documentation Files tab, click Upload.
3. In the Upload NetScaler Documentation File dialog box, click Browse and select the NetScaler documentation file you want to upload.
4. Click Upload. The documentation file appears in the Documentation Files pane.

To create a backup by downloading a NetScaler documentation file

1. In the Documentation Files pane, select the file you want to download, and then click Download.
2. In the message box, from the Save list, select Save as.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

To upload a NetScaler XVA file

1. In the navigation pane, expand NetScaler, and then click Software Images.
2. In the Software Images pane, on the XVA Files tab, click Upload.
3. In the Upload NetScaler XVA File dialog box, click Browse and select the NetScalerXVA file you want to upload.
4. Click Upload. The XVA file appears in the XVA Files pane.

To create a backup by downloading a NetScaler XVA file

1. In the XVA Files pane, select the file you want to download, and then click Download.
2. In the message box, from the Save list, select Save as.
3. In the Save As message box, browse to the location where you want to save the file, and then click Save.

Upgrading NetScaler VPX Instances

You can use the Management Service to upgrade one or more of the NetScaler VPX instances running on the appliance. Before upgrading an instance, make sure that you have uploaded the correct build and documentation files to the SDX appliance.

Important:

Make sure that you understand the licensing framework and types of licenses before you upgrade any instances. A software edition upgrade might require new licenses, such as upgrading from the standard edition to the enterprise edition, the standard edition to the platinum edition, or the enterprise edition to the platinum edition. Also note the following:

- To prevent any loss of configuration, save the configuration on each instance before you upgrade any instances.
- You can also upgrade an individual instance from the Instances node. To do so, select the instance from the Instances node and click Upgrade. To display the Upgrade button, click the right arrow at the bottom of the details pane.
- If you have configured a channel from the NetScaler instance and want to upgrade the instance from NetScaler release 10 to NetScaler release 10.1 or later, you must delete all the channels from the NetScaler instance, upgrade the instance, and then create LACP channels from the SVM. If you are downgrading the NetScaler instance from NetScaler release 10.1 to NetScaler release 10.0, you must delete all the LACP channels from the SVM, downgrade the instance, and then create the LACP channels from the NetScaler VPX.

To upgrade NetScaler VPX instances

1. On the Configuration tab, in the navigation pane, click NetScaler.
2. In the details pane, under NetScaler Configuration, click Upgrade.
3. In the Upgrade NetScaler dialog box, in Build File, select the NetScaler upgrade build file of the version to which you want to upgrade.
4. From the Documentation File drop-down list, select the documentation file to which you want to upgrade.
5. From the Instance IP Address drop-down list, select the IP addresses of the instances that you want to upgrade.
6. Click OK, and then click Close.

Managing a NetScaler Instance

The Management Service lets you perform the following operations on the NetScaler instances, both from the NetScaler Instances pane in the Configuration tab and in the NetScaler Instances gadget on the Home page.

Start a NetScaler Instance

Start any NetScaler instance from the Management Service user interface. When the Management Service UI forwards this request to the Management Service, it starts the NetScaler instance.

Shut down a NetScaler instance

Shut down any NetScaler instance from the Management Service user interface. When the Management Service UI forwards this request to the Management Service, it stops the NetScaler instance.

Reboot a NetScaler instance

Restart the NetScaler instance.

Delete a NetScaler instance

If you do not want to use a NetScaler instance, you can delete that instance by using the Management Service. Deleting an instance permanently removes the instance and its related details from the database of the SDX appliance.

To start, stop, delete, or restart a NetScaler instance

1. On the Configuration tab, in the navigation pane, click NetScaler Instances.
2. In the NetScaler Instances pane, select the NetScaler instance on which you want to perform the operation, and then click Start or Shut Down or Delete or Reboot.
3. In the Confirm message box, click Yes.

Allowing L2 Mode on a NetScaler Instance

In Layer 2 (L2) mode, a NetScaler instance acts as a learning bridge and forwards all packets for which it is not the destination. Some features, such as Cloud Bridge, require that L2 mode be enabled on the NetScaler instance. With L2 mode enabled, the instance can receive and forward packets for MAC addresses other than its own MAC address. However, if a user wants to enable L2 mode on a NetScaler instance running on an SDX appliance, the administrator must first allow L2 mode on that instance. If you allow L2 mode, you must take precautions to avoid bridging loops.

Precautions:

1. On a given 1/x interface, untagged packets must be allowed on only one instance. For all other instances enabled on the same interface, you must select Tagged.

Note:

Citrix recommends that you select Tagged for all interfaces assigned to instances in L2 mode. Note that if you select tagged, you cannot receive untagged packets on that interface.

If you have selected Tagged for an interface assigned to an instance, log on to that instance and configure a 802.1q VLAN to receive packets on that interface.

2. For 1/x and 10/x interfaces that are shared by NetScaler instances on which L2 mode is allowed, make sure that the following conditions are met:
 - VLAN filtering is enabled on all the interfaces.
 - Each interface is on a different 802.1q VLAN.
 - Only one instance can receive untagged packets on the interface. If that interface is assigned to other instances, you must select Tagged on that interface for those instances.
3. If you allow untagged packets for an instance on a 1/x interface, and L2 mode is allowed for that instance, no other instance (with L2 mode allowed or disallowed) can receive untagged packets on that interface.
4. If you allow untagged packets for an instance on a 1/x interface, and L2 mode is not allowed for that instance, no instance with L2 mode allowed can receive untagged packets on that interface.
5. If you have provisioned an instance (for example VPX1) in L2 mode on a 0/x interface, and the same interface is also assigned to another instance (for example VPX2), select Tagged for all other interfaces (1/x and 10/x) that are assigned to the second instance (VPX2).

Note: If L2 mode is enabled on a NetScaler instance, and both of the management interfaces (0/1 and 0/2) are associated with that instance, only one of the management

interfaces can be associated with another NetScaler instance on which L2 mode is enabled. You cannot associate both management interfaces with more than one NetScaler instance on which L2 mode is enabled.

To allow L2 mode on an instance

1. In the Provision NetScaler Wizard or the Modify NetScaler Wizard, on the Network Settings page, select Allow L2 Mode.

Note: You can activate the Allow L2 Mode setting on an instance when you provision the instance, or while the instance is running.

2. Follow the instructions in the wizard.
3. Click Finish, and then click Close.

Configuring VMACs on an Interface

A NetScaler instance uses Virtual MACs (VMACs) for high availability (active-active or active-standby) configurations. A Virtual MAC address (VMAC) is a floating entity shared by the primary and the secondary nodes in a high availability setup.

In a high availability setup, the primary node owns all of the floating IP addresses, such as the MIP, SNIP, and VIP addresses. The primary node responds to Address Resolution Protocol (ARP) requests for these IP addresses with its own MAC address. As a result, the ARP table of an external device (for example, an upstream router) is updated with the floating IP address and the primary node's MAC address.

When a failover occurs, the secondary node takes over as the new primary node. It then uses Gratuitous ARP (GARP) to advertise the floating IP addresses that it acquired from the primary. However, the MAC address that the new primary advertises is the MAC address of its own interface.

Some devices (notably a few routers) do not accept the GARP messages generated by the NetScaler appliance. Such devices retain the old IP to MAC mapping advertised by the old primary node, and a site can go down as a result.

You can overcome this problem by configuring a VMAC on both nodes of an HA pair. Both nodes then possess identical MAC addresses. Therefore, when failover occurs, the MAC address of the secondary node remains unchanged, and the ARP tables on the external devices do not need to be updated.

To configure a VMAC, you add a VRID for an interface. The Management Service internally generates a VMAC. You must specify the same VRID when you configure active-active mode on the NetScaler instance.

Important:

1. You must add a VRID from the Management Service. The same VRID must be specified in the NetScaler instance. If you add a VRID directly in the NetScaler instance, the instance cannot receive a packet that has a VMAC address as the destination MAC address.
2. You can use the same VRIDs in different instances on a 10G interface if VLAN filtering is enabled on the interface and the instances associated with that interface belong to different tagged 802.1q VLANs.
3. You cannot use the same VRIDs in different instances on a 1G interface.
4. You can add or delete the VRIDs for an interface assigned to an instance while the Instance is running.
5. In an active-active configuration, you can specify more than one VRID for an interface assigned to an instance.
6. A maximum of 86 VMACs are allowed on a 10G interface, and a maximum of 16 VMACs on a 1G interface. If no more VMAC filters are available, reduce the number of VRIDs on another instance.

You can add a VRID at the time of provisioning a NetScaler instance, or you can modify an existing NetScaler instance.

To add an IPv4 or IPv6 VRID to an interface

1. In the Provision NetScaler Wizard or the Modify NetScaler Wizard, on the Network Settings page, select an interface and set one or both of the following values:
 - VRID IPv4—The IPv4 VRID that identifies the VMAC. Possible values: 1 to 255.
 - VRID IPv6—The IPv6 VRID that identifies the VMAC. Possible values: 1 to 255.

Note: Use a comma to separate multiple VRIDs. For example, 12,24.
2. Follow the instructions in the wizard.
3. Click Finish, and then click Close.

Configuring LACP on a NetScaler VPX Instance

Link aggregation combines data coming from multiple ports into a single high-speed link. Configuring link aggregation increases the capacity and availability of the communication channel between the NetScaler virtual appliance and other connected devices. An aggregated link is also referred to as a "channel."

You can configure LACP from within a NetScaler VPX instance hosted on a NetScaler SDX appliance. However, the SDX administrator must take the following precautions:

- Interfaces must not be shared between instances. Even after an interface is part of a channel on one instance, it continues to appear in the interfaces list and another instance administrator might configure LACP on the same interface. An error message does not appear in this case.
- Configure a dedicated channel for an instance.

The following figure illustrates an LACP configuration on VPX instances hosted on a NetScaler SDX appliance. Interfaces 10/1 and 10/2 are dedicated to VPX instance 1 (VPX1) and interfaces 10/3 and 10/4 are dedicated to VPX instance 2 (VPX2). Channel 1 (LA/1) is dedicated to instance 1 and channel 2 (LA/2) is dedicated to instance 2.

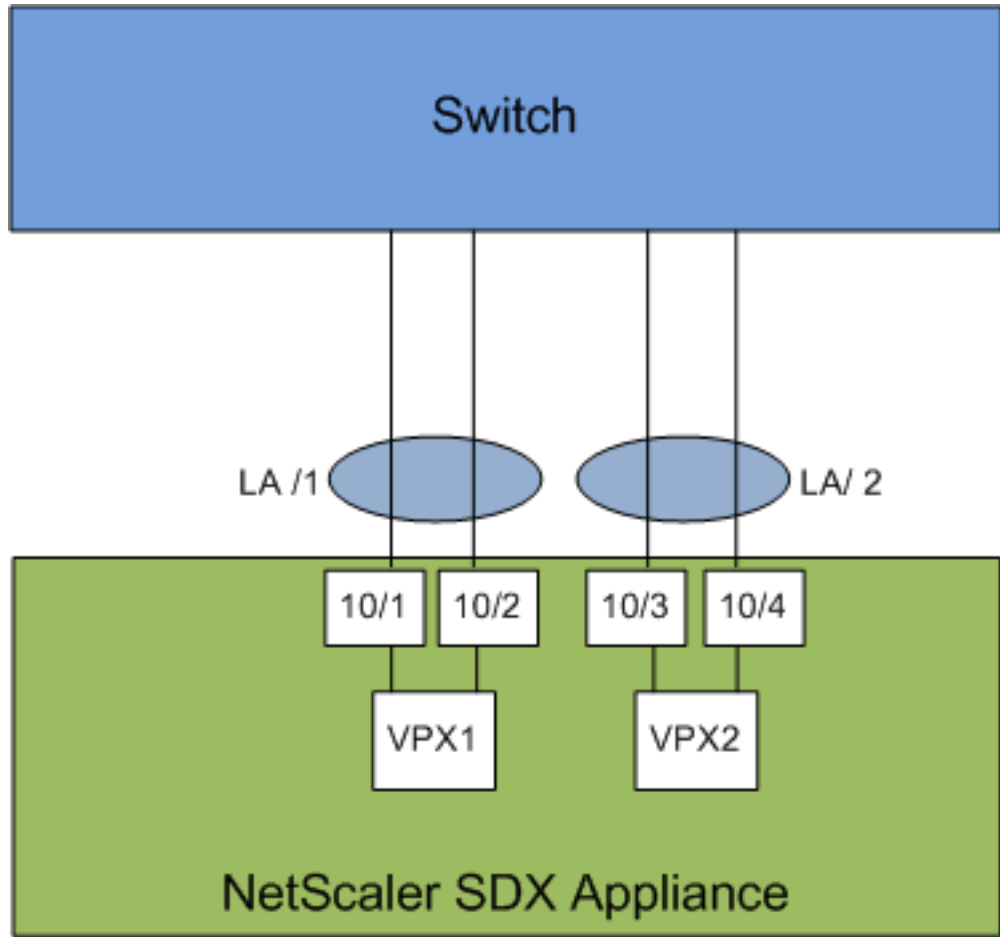


Figure 1. Network topology for LACP configuration: single channel with no shared interface

For more information about configuring LACP from within the VPX instance, see [Configuring Link Aggregation by Using the Link Aggregation Control Protocol](#).

For information about link aggregation on a NetScaler SDX appliance, see <http://support.citrix.com/article/CTX134962>.

For information about manual link aggregation, see [Configuring Link Aggregation Manually](#).

Removing NetScaler Instance Files

You can remove any NetScaler instance files, such as XVAs, builds, documentation, SSL keys or SSL certificates, from the appliance.

To remove NetScaler instance files

1. On the Configuration tab, in the navigation pane, expand NetScaler Configuration, and then click the file that you want to remove.
2. In the details pane, select the file name, and then click Delete.

Applying the Administration Configuration

At the time of provisioning a NetScaler VPX instance, the Management Service creates some policies, instance administration (admin) profile, and other configuration on the VPX instance. If the Management Service fails to apply the admin configuration at this time due to any reason (for example, the Management Service and the NetScaler VPX instance are on different subnetworks and the router is down or if the Management Service and NetScaler VPX instance are on the same subnet but traffic has to pass through an external switch and one of the required links is down), you can explicitly push the admin configuration from the Management Service to the NetScaler VPX instance at any time.

To apply the admin configuration on a NetScaler instance

1. On the Configuration tab, in the navigation pane, click NetScaler.
2. In the details pane, under NetScaler Configuration, click Apply Admin Configuration.
3. In the Apply Admin Configuration dialog box, in Instance IP Address, select the IP address of the NetScaler VPX instance on which you want to apply the admin configuration.
4. Click OK.

Change Management for NetScaler VPX Instances

You can track any changes to the configuration on a NetScaler VPX instance from the Management Service. The details pane lists the device name with IP address, date and time when it was last updated, and whether there is any difference between the saved configuration and the running configuration. Select a device to view its running configuration, saved configuration, history of configuration changes, and any difference between the configurations before and after an upgrade. You can download the configuration of a NetScaler VPX instance to your local computer. By default, the Management Service polls all the instances every 24 hours, but you can change this interval.

To view change management for NetScaler VPX instances

1. On the Configuration tab, navigate to NetScaler > Change Management.
2. In the Change Management pane, select a VPX instance, and then select one of the following:
 - Running Configuration—Displays the running configuration of the selected VPX instance in a new window.
 - Saved Configuration—Displays the saved configuration of the selected VPX instance in a new window.
 - Saved Vs. Running Diff—Displays the saved configuration, the running configuration, and the corrective command (the difference).
 - Revision History Diff—Displays the difference between the base configuration file and the second configuration file.
 - Pre vs. Post Upgrade Diff—Displays the difference in the configuration before and after an upgrade, and the corrective command (the difference).
 - Download—Downloads the configuration of the selected VPX instance and saves it on a local device.

To poll for updates to the configuration of any of the NetScaler instances

1. On the Configuration tab, navigate to NetScaler > Change Management.
2. In the Change Management pane, select one of the following:
 - Poll Now—Management Service performs an immediate poll for updates to the configuration (ns.conf) of any of the NetScaler VPX instances installed on the appliance.
 - Configure Polling Interval—Time after which the Management Service polls for updates to the configuration (ns.conf) of any of the NetScaler VPX instances installed on the appliance. The default polling interval is 24 hours.

Monitoring NetScaler Instances

A high-level view of the performance of the appliance and the NetScaler VPX instances provisioned on the appliance are displayed on the Monitoring page of the Management Service user interface. After provisioning and configuring the NetScaler instance, you can perform various tasks to monitor the NetScaler instance.

Viewing the Properties of the NetScaler Instance

The Management Service user interface displays the list and description of all the NetScaler VPX instances provisioned on the SDX appliance. Use the NetScaler Instances pane to view details, such as the instance name and IP address, CPU and memory utilization, number of packets received and transmitted on the instance, the throughput and total memory assigned to the instance.

Clicking the IP address of the NetScaler VPX instance opens the configuration utility (GUI) of that instance in a new tab or browser.

To view the properties of NetScaler VPX instances

1. On the Configuration tab, in the left pane, expand NetScaler Configuration, and then click Instances.

Note: You can also view the properties of a NetScaler VPX instance from the Home tab.

2. In the NetScaler Instance pane, you can view the following details for the NetScaler instance:

Name

The host name assigned to the NetScaler instance while provisioning.

VM State

The state of the virtual machine.

NetScaler State

The state of the NetScaler instance.

IP Address

The IP address of the NetScaler instance. Clicking the IP address opens the GUI of this instance in a new tab or browser.

Rx (Mbps)

The packets received on the NetScaler instance.

Tx (Mbps)

The packets transmitted by the NetScaler instance.

HTTP Req/s

The total number of HTTP requests received on the NetScaler instance every second.

CPU Usage (%)

The percentage of CPU utilization on the NetScaler.

Memory Usage (%)

The percentage of memory utilization on the NetScaler.

3. Click the arrow next to the name of a NetScaler instance to view the properties of that instance, or click Expand All to view the properties of all the NetScaler instances. You can view the following properties:

Netmask

The netmask IP address of the NetScaler instance.

Gateway

The IP address of the default gateway, the router that forwards traffic outside of the subnet in which the instance is installed.

Packets per second

The total number of packets passing every second.

NICs

The names of the network interface cards used by the NetScaler instance, along with the virtual function assigned to each interface.

Version

The build version, build date, and time of the NetScaler software currently running on the instance.

Host Name

The host name of the NetScaler instance.

Total Memory (GB)

The total memory being assigned to the NetScaler instance.

Throughput (Mbps)

The total throughput of the NetScaler instance.

Up Since

The date and time since when the instance has been continuously in the UP state.

#SSL Chips

The total number of SSL chips
assigned to the instance.

Peer IP address

The IP address of the peer of this NetScaler instance if it is in an HA setup.

Status

The status of the operations being performed on a NetScaler instance, such as status of whether inventory from the instance is completed or whether reboot is in progress.

HA Master State

The state of the device. The state indicates whether the instance is configured in a standalone or primary setup or is part of a high availability setup. In a high availability setup, the state also displays whether it is in primary or secondary mode.

HA Sync Status

The mode of the HA sync status, such as enabled or disabled.

Description

The description entered while provisioning the NetScaler instance.

Viewing the Running and Saved Configuration of a NetScaler Instance

By using the Management Service you can view the currently running configuration of a NetScaler instance. You can also view the saved configuration of a NetScaler instance and the time when the configuration was saved.

To view the running and saved configuration of a NetScaler instance

1. On the Configuration tab, in the left pane, expand NetScaler Configuration, and then click Instances.
2. In the NetScaler Instances pane, click the NetScaler instance for which you want to view the running or saved configuration.
3. To view the running configuration, click Running Configuration, and to view the saved configuration, click Saved Configuration.
4. In the NetScaler Running Config window or the NetScaler Saved Config window, you can view the running or saved configuration of the NetScaler instance.

Pinging a NetScaler Instance

You can ping a NetScaler instance from the Management Service to check whether the device is reachable.

To ping a NetScaler instance

1. On the Configuration tab, in the left pane, expand NetScaler Configuration, and then click Instances.
2. In the NetScaler Instances pane, click the NetScaler instance you want to ping, and then click Ping. In the Ping message box, you can view whether the ping is successful.

Tracing the Route of a NetScaler Instance

You can trace the route of a packet from the Management Service to a NetScaler instance by determining the number of hops used to reach the instance.

To trace the route of a NetScaler instance

1. On the Configuration tab, in the left pane, expand NetScaler Configuration, and then click Instances.
2. In the NetScaler Instances pane, click the NetScaler instance you want to trace, and then click TraceRoute. In the Traceroute message box, you can view the route to the NetScaler.

Rediscovering a NetScaler Instance

You can rediscover a NetScaler instance when you need to view the latest state and configuration of a NetScaler instance.

During rediscovery, the Management Service fetches the configuration. By default, the Management Service schedules devices for rediscovery once every 30 minutes.

To rediscover a NetScaler instance

1. On the Configuration tab, in the left pane, expand NetScaler Configuration, and then click Instances.
2. In the NetScaler Instances pane, click the NetScaler instance you want to rediscover, and then click Rediscover.
3. In the Confirm message box, click Yes.

Using Logs to Monitor Operations and Events

Use audit and task logs to monitor the operations performed on the Management Service and on the NetScaler instances . You can also use the events log to track all events for tasks performed on the Management Service and the XenServer.

Viewing Audit Logs

All operations performed by using the Management Service are logged in the appliance database. Use audit logs to view the operations that a Management Service user has performed, the date and time of each operation, and the success or failure status of the operation. You can also sort the details by user, operation, audit time, status, and so on by clicking the appropriate column heading.

Pagination is supported in the Audit Log pane. Select the number of records to display on a page. By default, 25 records are displayed on a page.

To view audit logs

1. In the navigation pane, expand System, and then click Audit.
2. In the Audit Log pane, you can view the following details.

User Name

The Management Service user who has performed the operation.

IP Address

The IP address of the system on which the operation was performed.

Port

The port at which the system was running when the operation was performed.

Resource Type

The type of resource used to perform the operation, such as xen_vpx_image and login.

Resource Name

The name of the resource used to perform the operation, such as vpx_image_name and the user name used to log in.

Audit Time

The time when the audit log was generated.

Operation

The task that was performed, such as add, delete, and log out.

Status

The status of the audit, such as Success or Failed.

Message

A message describing the cause of failure if the operation has failed and status of the task, such as Done, if the operation was successful.

3. To sort the logs by a particular field, click the heading of the column.

Viewing Task Logs

Use task logs to view and track tasks, such as upgrading instances and installing SSL certificates, that are executed by the Management Service on the NetScaler instances. The task log lets you view whether a task is in progress or has failed or has succeeded.

Pagination is supported in the Task Log pane. Select the number of records to display on a page. By default, 25 records are displayed on a page.

To view the task log

1. In the navigation pane, expand Diagnostics, and then click Task Log.
2. In the Task Log pane, you can view the following details.

ID

The auto-generated ID assigned to a task. For a task performed on multiple instances, such as installing SSL certificate or upgrading instances, a single unique ID is generated in the task log.

Name

The name of the task that is being executed or has already been executed.

Status

The status of the task, such as In progress, Completed, or Failed.

Executed By

The Management Service user who has performed the operation.

Start Time

The time at which the task started.

End Time

The time at which the task ended.

Viewing Task Device Logs

Use task device logs to view and track tasks being performed on each NetScaler instance. The task device log lets you view whether a task is in progress or has failed or has succeeded. It also displays the IP address of the instance on which the task is performed.

To view the task device log

1. In the navigation pane, expand Diagnostics, and then click Task Log.
2. In the Task Log pane, double-click the task to view the task device details.
3. In the Task Device Log pane, to sort the logs by a particular field, click the heading of the column.

Viewing Task Command Logs

Use task command logs to view the status of each command of a task executed on a NetScaler instance. The task command log lets you view whether a command has been successfully executed or has failed. It also displays the command that is executed and the reason why a command has failed.

To view the task command log

1. In the navigation pane, expand Diagnostics, and then click Task Log.
2. In the Task Log pane, double-click the task to view the task device details.
3. In the Task Device Log pane, double-click the task to view the task command details.
4. In the Task Command Log pane, to sort the logs by a particular field, click the heading of the column.

Viewing Events

Use the Events pane in the Management Service user interface to monitor the events generated by the Management Service for tasks performed on the Management Service.

To view the events

1. On the Monitoring tab, in the left pane, expand Monitoring, and then click Events.
2. In the Events pane, you can view the following details.

Severity

The severity of an event, which could be critical, major, minor, clear, and information.

Source

The IP address on which the event is generated.

Date

The date when the event is generated.

Category

The category of event, such as PolicyFailed and DeviceConfigChange.

Message

The message describing the event.

3. To sort the events by a particular field, click the heading of the column.

Use Cases for NetScaler SDX Appliance

For networking components (such as firewalls and Application Delivery Controllers), support for multi-tenancy has historically involved the ability to carve a single device into multiple logical partitions. This approach allows different sets of policies to be implemented for each tenant without the need for numerous, separate devices. Traditionally, however it is severely limited in terms of the degree of isolation that is achieved.

By design, the NetScaler SDX appliance is not subject to the same limitations. In the SDX architecture, each instance runs as a separate virtual machine (VM) with its own dedicated NetScaler kernel, CPU resources, memory resources, address space, and bandwidth allocation. Network I/O on the SDX appliance not only maintains aggregate system performance but also enables complete segregation of each tenant's data-plane and management-plane traffic. The management plane includes the 0/x interfaces. The data plane includes the 1/x and 10/x interfaces. A data plane can also be used as a management plane.

The primary use cases for an SDX appliance are related to consolidation, reducing the number of networks required while maintaining management isolation. Following are the basic consolidation scenarios:

- Consolidation when the Management Service and the NetScaler instances are in the same network
- Consolidation when the Management Service and the NetScaler instances are in different networks but all the instances are in the same network
- Consolidation across security zones
 - Consolidation with dedicated interfaces for each instance
 - Consolidation with sharing of a physical port by more than one instance

Consolidation When the Management Service and the NetScaler Instances are in the Same Network

A simple type of consolidation case on the SDX appliance is configuration of the Management Service and the NetScaler instances as part of the same network. This use case is applicable if the appliance administrator is also the instance administrator and your organization's compliance requirement does not specify that separate management networks are required for the Management Service and the NSIP addresses of the different instances. The instances can be provisioned in the same network (for management traffic), but the VIP addresses can be configured in different networks (for data traffic), and thus in different security zones.

In the following example, the Management Service and the NetScaler instances are part of the 10.1.1.x. network. Interfaces 0/1 and 0/2 are the management interfaces, 1/1 to 1/8 are 1G data interfaces, and 10/1 to 10/4 are 10G data interfaces. Each instance has its own dedicated physical interface. Therefore, the number of instances is limited to the number of physical interfaces available on the appliance. By default, VLAN filtering is enabled on each interface of the NetScaler SDX appliance, and that restricts the number of VLANs to 32 on a 1G interface and 63 on a 10G interface. VLAN filtering can be enabled and disabled for each interface. Disable VLAN filtering to configure up to 4096 VLANs per interface on each instance. In this example, VLAN filtering is not required because each instance has its own dedicated interface. For more information about VLAN filtering, see [VLAN Filtering](#).

The following figure illustrates the above use case.

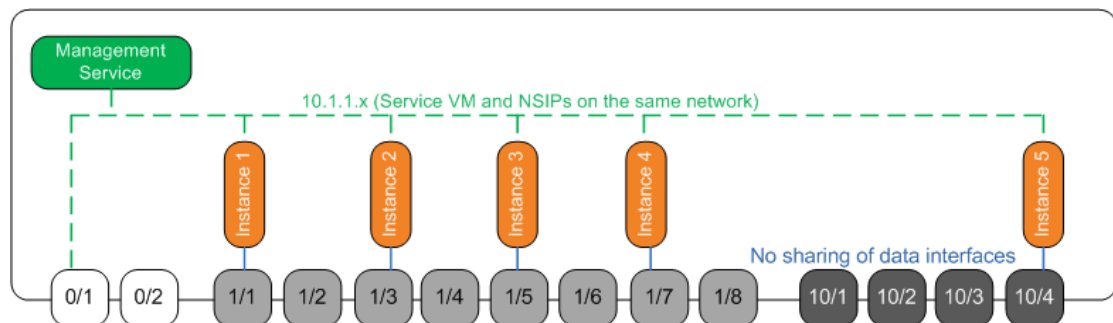


Figure 1. Network topology of an SDX appliance with Management Service and NetScaler NSIPs for instances in the same network

The following table lists the names and values of the parameters used for provisioning NetScaler Instance 1 in the above example.

Parameter Name	Values for Instance 1
Name	vpx8
IP Address	10.1.1.2
Netmask	255.255.255.0

Gateway	10.1.1.1
XVA File	NS-VPX-XEN-10.0-51.308.a_nc.xva
Feature License	Platinum
Admin Profile	ns_nsroot_profile
User Name	vpx8
Password	Sdx
Confirm Password	Sdx
Shell/Sftp/Scp Access	True
Total Memory (MB)	2048
#SSL Chips	1
Throughput (Mbps)	1000
Packets per second	1000000
CPU	Shared
Interface	0/1 and 1/1

To provision NetScaler Instance 1 as shown in this example

1. On the Configuration tab, in the navigation pane, expand NetScaler Configuration, and then click Instances.
2. In the NetScaler Instances pane, click Add.
3. In the Provision NetScaler Wizard follow the instructions in the wizard to specify the parameter values shown in the above table.
4. Click Create, and then click Close. The NetScaler instance you provisioned appears in the NetScaler Instances pane.

Consolidation When the Management Service and the NetScaler Instances are in Different Networks

In certain cases, the appliance administrator might allow other administrators to perform administration tasks on individual instances. This can be safely done by giving an individual instance administrator login rights to just that instance. But, for security reasons, the appliance administrator might not want to allow the instance to be on the same network as the Management Service. This is a very common scenario in service provider environments, and it is becoming increasingly common in enterprises as they adopt virtualization and cloud architectures.

In the following example, the Management Service is in the 10.1.1.x network and the NetScaler instances are in the 10.1.2.x network. Interfaces 0/1 and 0/2 are the management interfaces, 1/1 to 1/8 are 1G data interfaces, and 10/1 to 10/4 are 10G data interfaces. Each instance has its own dedicated administrator and its own dedicated physical interface. Therefore, the number of instances is limited to the number of physical interfaces available on the appliance. VLAN filtering is not required, because each instance has its own dedicated interface. Optionally, disable VLAN filtering to configure up to 4096 VLANs per instance per interface. In this example, you do not need to configure an NSVLAN, because instances are not sharing a physical interface and there are no tagged VLANs. For more information about NSVLANs, see [Adding a NetScaler Instance](#).

The following figure illustrates the above use case.

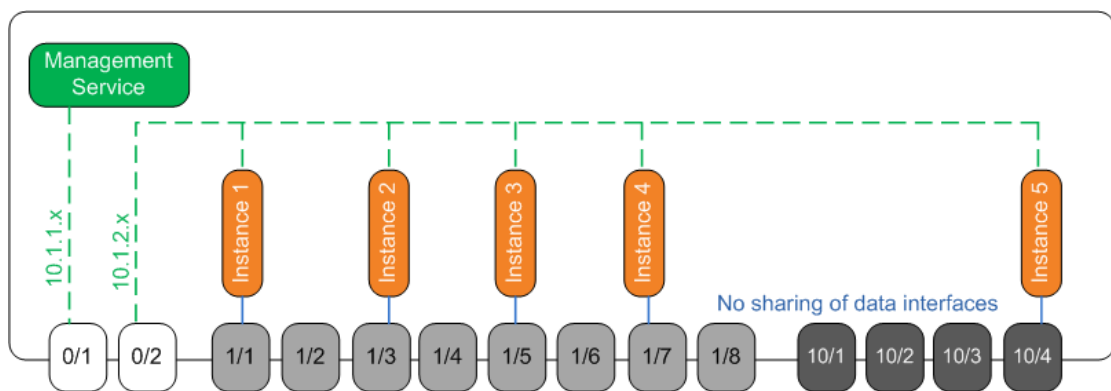


Figure 1. Network topology of an SDX appliance with Management Service and NetScaler NSIPs for Instances in different networks

As the appliance administrator, you have the option to keep the traffic between the Management Service and the NSIP addresses on the SDX appliance, or to force the traffic off the device if, for example, you want traffic to go through an external firewall or some other security intermediary and then return to the appliance.

The following table lists the names and values of the parameters used for provisioning NetScaler Instance 1 in this example.

Parameter Name	Values for Instance 1
Name	vpx1
IP Address	10.1.2.2
Netmask	255.255.255.0
Gateway	10.1.2.1
XVA File	NS-VPX-XEN-10.0-51.308.a_nc.xva
Feature License	Platinum
Admin Profile	ns_nsroot_profile
User Name	vpx1
Password	Sdx
Confirm Password	Sdx
Shell/Sftp/Scp Access	True
Total Memory (MB)	2048
#SSL Chips	1
Throughput (Mbps)	1000
Packets per second	1000000
CPU	Shared
Interface	0/2 and 1/1

To provision NetScaler Instance 1 as shown in this example

1. On the Configuration tab, in the navigation pane, expand NetScaler Configuration, and then click Instances.
2. In the NetScaler Instances pane, click Add.
3. In the Provision NetScaler Wizard follow the instructions in the wizard to set the parameters to the values shown in the above table.
4. Click Create, and then click Close. The NetScaler instance you provisioned appears in the NetScaler Instances pane.

Consolidation Across Security Zones

An SDX appliance is often used for consolidation across security zones. The DMZ adds an extra layer of security to an organization's internal network, because an attacker has access only to the DMZ, not to the internal network of the organization. In high-compliance environments, a single NetScaler instance with VIP addresses in both the DMZ and an internal network is generally not acceptable. With SDX, you can provision instances hosting VIP addresses in the DMZ, and other instances hosting VIP addresses in an internal network.

In some cases, you might need separate management networks for each security zone. In such cases, you have to put the NSIP addresses of the instances in the DMZ on one network, and put the NSIP addresses of the instances with VIPs in the internal network on a different management network. Also, in many cases, communication between the Management Service and the instances might need to be routed through an external device, such as a router. You can configure firewall policies to control the traffic that is sent to the firewall and to log the traffic.

The SDX appliance has two management interfaces (0/1 and 0/2) and, depending on the model, up to eight 1G data ports and eight 10G data ports. You can also use the data ports as management ports (for example, when you need to configure tagged VLANs, because tagging is not allowed on the management interfaces). If you do so, the traffic from the Management Service must leave the appliance and then return to the appliance. You can route this traffic or, optionally, specify an NSVLAN on an interface assigned to the instance. If the instances are configured on a management interface that is common with the Management Service, the traffic between the Management Service and NetScaler instances does not have to be routed, unless your setup explicitly requires it.

Note: Tagging is supported in XenServer version 6.0.

Consolidation with Dedicated Interfaces for Each Instance

In the following example, the instances are part of multiple networks. Interface 0/1 is assigned to the Management Service, which is part of the internal 10.1.1.x network. NetScaler instances 2 and 3 are part of the 10.1.200.x network (VLAN 100), and NetScaler instances 4 and 5 are part of the 10.1.3.x network (VLAN 200).

Optionally, you can configure an NSVLAN on all of the instances.

The following figure illustrates the above use case.

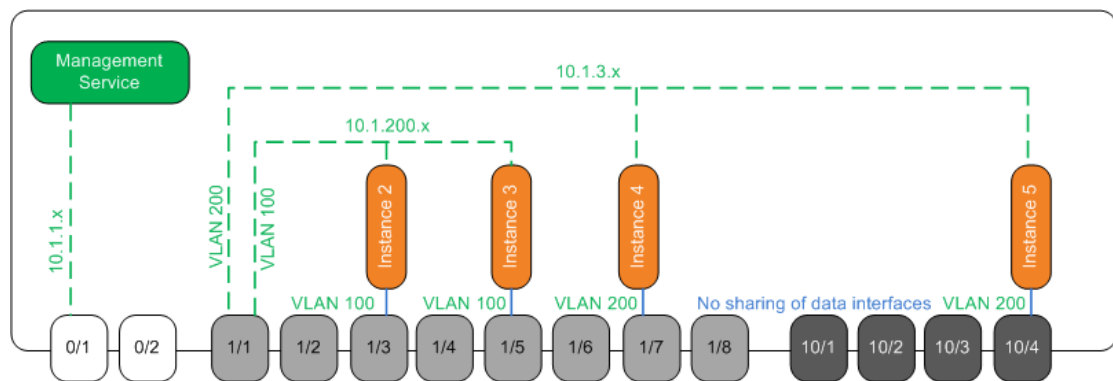


Figure 1. Network topology of an SDX appliance with NetScaler instances in multiple networks

The SDX appliance is connected to a switch. Make sure that VLAN IDs 100 and 200 are configured on the switch port to which port 1/1 on the appliance is connected.

The following table lists the names and values of the parameters used for provisioning NetScaler instances 5 and 3 in this example.

Parameter Name	Values for Instance 5	Values for Instance 3
Name	vpx5	vpx3
IP Address	10.1.3.2	10.1.200.2
Netmask	255.255.255.0	255.255.255.240
Gateway	10.1.3.1	10.1.200.1
XVA File	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
Feature License	Platinum	Platinum
Admin Profile	ns_nsroot_profile	ns_nsroot_profile
User Name	vpx5	vpx3
Password	Sdx	root

Confirm Password	Sdx	root
Shell/Sftp/Scp Access	True	True
Total Memory (MB)	2048	2048
#SSL Chips	1	1
Throughput (Mbps)	1000	1000
Packets per second	1000000	1000000
CPU	Shared	Shared
Interface	1/1 and 10/4	1/1 and 1/5
NSVLAN	200	100
Add (interface)	1/1	1/1
Tagged Interface	Select Tagged	Select Tagged

To provision NetScaler Instances 5 and 3 as shown in this example

1. On the Configuration tab, in the navigation pane, expand NetScaler Configuration, and then click Instances.
2. In the NetScaler Instances pane, click Add.
3. In the Provision NetScaler Wizard follow the instructions in the wizard to set the parameters to the values shown in the above table.
4. Click Create, and then click Close. The NetScaler instance you provisioned appears in the NetScaler Instances pane.

Consolidation With Sharing of a Physical Port by More Than One Instance

You can enable and disable VLAN filtering on an interface as required. For example, if you need to configure more than 100 VLANs on an instance, assign a dedicated physical interface to that instance and disable VLAN filtering on that interface. Enable VLAN filtering on instances that share a physical interface, so that traffic for one instance is not seen by the other instance.

Note: VLAN filtering is not a global setting on the appliance. You enable or disable VLAN filtering on an interface, and the setting applies to all instances associated with that interface. If VLAN filtering is disabled, you can configure up to 4096 VLANs. If VLAN filtering is enabled, you can configure up to 63 tagged VLANs on a 10G interface and up to 32 tagged VLANs on a 1G interface.

In the following example, the instances are part of multiple networks.

- Interface 1/1 is assigned as a management interface to all the instances. Interface 0/1 is assigned to the Management Service, which is part of the internal 10.1.1.x network.
- NetScaler instances 2 and 3 are in the 10.1.200.x network, and instances 4, 5, 6, and 7 are in the 10.1.3.x network. Instances 2 and 3 each have a dedicated physical interface. Instances 4 and 7 share physical interface 1/7, and instances 5 and 6 share physical interface 10/4.
- VLAN filtering is enabled on interface 1/7. Traffic for Instance 4 is tagged for VLAN 4, and traffic for Instance 7 is tagged for VLAN 7. As a result, traffic for Instance 4 is not visible to Instance 7, and vice versa. A maximum of 32 VLANs can be configured on interface 1/7.
- VLAN filtering is disabled on interface 10/4, so you can configure up to 4096 VLANs on that interface. Configure VLANs 500-599 on Instance 5 and VLANs 600-699 on Instance 6. Instance 5 can see the broadcast and multicast traffic from VLAN 600-699, but the packets are dropped at the software level. Similarly, Instance 6 can see the broadcast and multicast traffic from VLAN 500-599, but the packets are dropped at the software level.

The following figure illustrates the above use case.

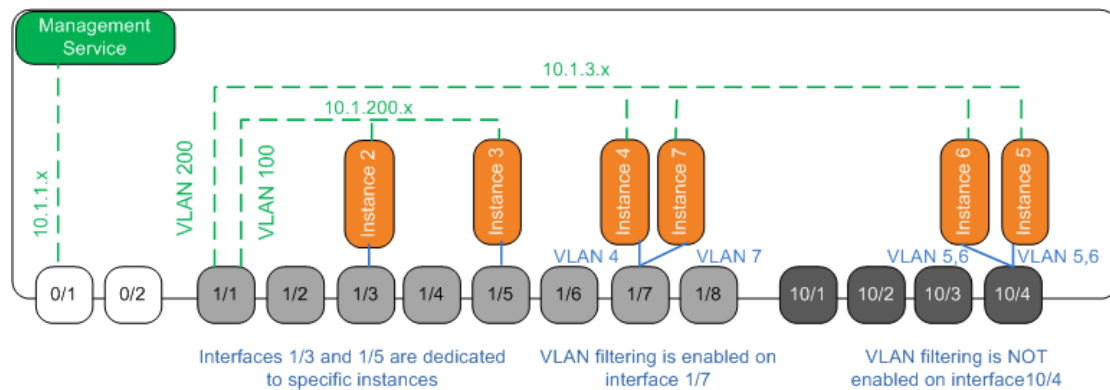


Figure 1. Network topology of an SDX appliance with Management Service and NetScaler instances distributed across networks

The following table lists the names and values of the parameters used for provisioning NetScaler instances 7 and 4 in this example.

Parameter Name	Values for Instance 7	Values for Instance 4
Name	vp7	vp4
IP Address	10.1.3.7	10.1.3.4
Netmask	255.255.255.0	255.255.255.240
Gateway	10.1.3.1	10.1.3.1
XVA File	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
Feature License	Platinum	Platinum
Admin Profile	ns_nsroot_profile	ns_nsroot_profile
User Name	vp4	vp4
Password	Sdx	Sdx
Confirm Password	Sdx	Sdx
Shell/Sftp/Scp Access	True	True
Total Memory (MB)	2048	2048
#SSL Chips	1	1
Throughput (Mbps)	1000	1000
Packets per second	1000000	1000000
CPU	Shared	Shared
Interface	1/1 and 1/7	1/1 and 1/7
NSVLAN	200	200

To provision NetScaler Instances 7 and 4 in this example

1. On the Configuration tab, in the navigation pane, expand NetScaler Configuration, and then click Instances.
2. In the NetScaler Instances pane, click Add.
3. In the Provision NetScaler Wizard follow the instructions in the wizard to set the parameters to the values shown in the above table.
4. Click Create, and then click Close. The NetScaler instance you provisioned appears in the NetScaler Instances pane.

NITRO API

The Citrix® NetScaler® SDX NITRO protocol allows you to configure and monitor the NetScaler SDX appliance programmatically.

NITRO exposes its functionality through Representational State Transfer (REST) interfaces. Therefore, NITRO applications can be developed in any programming language. Additionally, for applications that must be developed in Java or .NET, the NITRO protocol is exposed as Java and .NET libraries that are packaged as separate Software Development Kits (SDKs).

Note: You must have a basic understanding of the NetScaler SDX appliance before using the NITRO protocol.

To use the NITRO protocol, the client application needs the following:

- Access to a NetScaler SDX appliance, version 9.3 48.x or later.
- To use REST interfaces, you must have a system to generate HTTP or HTTPS requests (payload in JSON format) to the NetScaler SDX appliance. You can use any programming language or tool.
- For Java clients, you must have a system where Java Development Kit (JDK) 1.5 or later is available. The JDK can be downloaded from <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.
- For .NET clients, you must have a system with .NET framework 3.5 or later installed. The .NET framework can be downloaded from <http://www.microsoft.com/downloads/en/default.aspx>.

Obtaining the NITRO Package

The NITRO package is available as a tar file on the Downloads page of the NetScaler SDX appliance's configuration utility. You must download and un-tar the file to a folder on your local system. This folder is referred to as <NITRO_SDK_HOME> in this documentation.

The folder contains the NITRO libraries (JARs for Java and DLLs for .NET) in the lib subfolder. The libraries must be added to the client application classpath to access NITRO functionality. The <NITRO_SDK_HOME> folder also provides samples and documentation that can help you understand the NITRO SDK.

Note: The REST package contains only documentation for using the REST interfaces.

How NITRO Works

The NITRO infrastructure consists of a client application and the NITRO Web service running on a NetScaler appliance. The communication between the client application and the NITRO web service is based on REST architecture using HTTP or HTTPS.

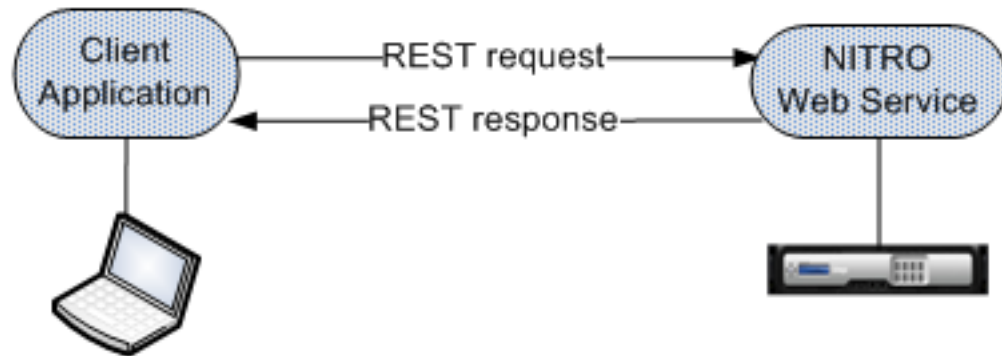


Figure 1. NITRO execution flow

As shown in the above figure, a NITRO request is executed as follows:

1. The client application sends REST request message to the NITRO web service. When using Java or .NET SDKs, an API call is translated into the appropriate REST request message.
2. The web service processes the REST request message.
3. The NITRO web service returns the corresponding REST response message to the client application. When using Java or .NET SDKs, the REST response message is translated into the appropriate response for the API call.

To minimize traffic on the network, you retrieve the whole state of a resource from the server, make modifications to the state of the resource locally, and then upload it back to the server in one network transaction.

Note: Local operations on a resource (changing its properties) do not affect its state on the server until the state of the object is explicitly uploaded.

NITRO APIs are synchronous in nature. This means that the client application waits for a response from the NITRO web service before executing another NITRO API.

Java SDK

NetScaler SDX NITRO APIs are categorized depending on the scope and purpose of the APIs into system APIs and configuration APIs. You can also troubleshoot NITRO operations.

System APIs

The first step towards using NITRO is to establish a session with the NetScaler SDX appliance and then authenticate the session by using the administrator's credentials.

You must create an object of the `nitro_service` class by specifying the IP address of the appliance and the protocol to connect to the appliance (HTTP or HTTPS). You then use this object and log on to the appliance by specifying the user name and the password of the administrator.

Note: You must have a user account on that appliance. The configuration operations that you can perform are limited by the administrative role assigned to your account.

The following sample code connects to a NetScaler SDX appliance with IP address 10.102.31.16 by using HTTPS protocol:

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

//Specify the login credentials
nitroservice.login("nsroot", "verysecret");
```

Note: You must use the `nitro_service` object in all further NITRO operations on the appliance.

To disconnect from the appliance, invoke the `logout()` method as follows:

```
nitroservice.logout();
```

Configuration APIs

The NITRO protocol can be used to configure resources of the NetScaler SDX appliance.

The APIs to configure a resource are grouped into packages or namespaces that have the format `com.citrix.sdx.nitro.resource.config.<resource_type>`. Each of these packages or namespaces contain a class named `<resource_type>` that provides the APIs to configure the resource.

For example, the NetScaler resource has the `com.citrix.sdx.nitro.resource.config.ns` package or namespace.

A resource class provides APIs to perform other operations such as creating a resource, retrieving resource details and statistics, updating a resource, deleting resources, and performing bulk operations on resources.

Creating a Resource

To create a new resource (for example, a NetScaler instance) on the NetScaler SDX appliance, do the following:

1. Set the value for the required properties of the resource by using the corresponding property name. The result is a resource object that contains the details required for the resource.

Note: These values are set locally on the client. The values are not reflected on the appliance till the object is uploaded.

2. Upload the resource object to the appliance, using the static `add()` method.

The following sample code creates a NetScaler instance named "ns_instance" on the NetScaler SDX appliance:

```
ns newns = new ns();

//Set the properties of the NetScaler locally
newns.set_name("ns_instance");
newns.set_ip_address("10.70.136.5");
newns.set_netmask("255.255.255.0");
newns.set_gateway("10.70.136.1");
newns.set_image_name("nsvpx-9.3.45_nc.xva");
newns.set_profile_name("ns_nsroot_profile");
newns.set_vm_memory_total(new Double(2048));
newns.set_throughput(new Double(1000));
newns.set_pps(new Double(1000000));
newns.set_license("Standard");
newns.set_username("admin");
newns.set_password("admin");

int number_of_interfaces = 2;
network_interface[] interface_array = new network_interface[number_of_interfaces]
```

```
//Adding 10/1
interface_array[0] = new network_interface();
interface_array[0].set_port_name("10/1");

//Adding 10/2
interface_array[1] = new network_interface();
interface_array[1].set_port_name("10/2");

newns.set_network_interfaces(interface_array);

//Upload the NetScaler instance
ns result = ns.add(nitroservice, newns);
```

Retrieving Resource Details

To retrieve the properties of a resource on the NetScaler SDX appliance, do the following:

1. Retrieve the configurations from the appliance by using the `get()` method. The result is a resource object.
2. Extract the required property from the object by using the corresponding property name.

The following sample code retrieves the details of all NetScaler resources:

```
//Retrieve the resource object from the NetScaler 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());
```

Retrieving Resource Statistics

A NetScaler SDX appliance collects statistics on the usage of its features. You can retrieve these statistics using NITRO.

The following sample code retrieves statistics of a NetScaler instance with ID 123456a:

```
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());
```

Updating a Resource

To update the properties of an existing resource on the appliance, do the following:

1. Set the `id` property to the ID of the resource to be updated.

2. Set the value for the required properties of the resource by using the corresponding property name. The result is a resource object.

Note: These values are set locally on the client. The values are not reflected on the appliance till the object is uploaded.

3. Upload the resource object to the appliance, using the update() method.

The following sample code updates the name of the NetScaler instance with ID 123456a to '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);
```

Deleting a Resource

To delete an existing resource, invoke the static method delete() on the resource class, by passing the ID of the resource to be removed, as an argument.

The following sample code deletes a NetScaler instance with ID 1:

```
ns obj = new ns();
obj.set_id("123456a");
ns.delete(nitroservice, obj);
```

Bulk Operations

You can query or change multiple resources simultaneously and thus minimize network traffic. For example, you can add multiple NetScaler appliances in the same operation.

Each resource class has methods that take an array of resources for adding, updating, and removing resources. To perform a bulk operation, specify the details of each operation locally and then send the details at one time to the server.

To account for the failure of some operations within the bulk operation, NITRO allows you to configure one of the following behaviors:

- **Exit.** When the first error is encountered, the execution stops. The commands that were executed before the error are committed.
- **Continue.** All the commands in the list are executed even if some commands fail.

Note: You must configure the required behavior while establishing a connection with the appliance, by setting the `onerror` param in the `nitro_service()` method.

The following sample code adds two NetScalers in one operation:

```
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);
```

Exception Handling

The `errorCode` field indicates the status of the operation.

- An `errorCode` of 0 indicates that the operation is successful.
- A non-zero `errorCode` indicates an error in processing the NITRO request.

The error message field provides a brief explanation and the nature of the failure.

All exceptions in the execution of NITRO APIs are caught by the `com.citrix.sdx.nitro.exception.nitro_exception` class. To get information about the exception, you can use the `getErrorCode()` method.

For a more detailed description of the error codes, see the API reference available in the `<NITRO_SDK_HOME>/doc` folder.

.NET SDK

NetScaler SDX NITRO APIs are categorized depending on the scope and purpose of the APIs into system APIs and configuration APIs. You can also troubleshoot NITRO operations.

System APIs

The first step towards using NITRO is to establish a session with the NetScaler SDX appliance and then authenticate the session by using the administrator's credentials.

You must create an object of the `nitro_service` class by specifying the IP address of the appliance and the protocol to connect to the appliance (HTTP or HTTPS). You then use this object and log on to the appliance by specifying the user name and the password of the administrator.

Note: You must have a user account on that appliance. The configuration operations that you can perform are limited by the administrative role assigned to your account.

The following sample code connects to a NetScaler SDX appliance with IP address 10.102.31.16 by using HTTPS protocol:

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

//Specify the login credentials
nitroservice.login("nsroot", "verysecret");
```

Note: You must use the `nitro_service` object in all further NITRO operations on the appliance.

To disconnect from the appliance, invoke the `logout()` method as follows:

```
nitroservice.logout();
```

Configuration APIs

The NITRO protocol can be used to configure resources of the NetScaler SDX appliance.

The APIs to configure a resource are grouped into packages or namespaces that have the format `com.citrix.sdx.nitro.resource.config.<resource_type>`. Each of these packages or namespaces contain a class named `<resource_type>` that provides the APIs to configure the resource.

For example, the NetScaler resource has the `com.citrix.sdx.nitro.resource.config.ns` package or namespace.

A resource class provides APIs to perform other operations such as creating a resource, retrieving resources and resource properties, updating a resource, deleting resources, and performing bulk operations on resources.

Creating a Resource

To create a new resource (for example, a NetScaler instance) on the NetScaler SDX appliance:

1. Set the value for the required properties of the resource by using the corresponding property name. The result is a resource object that contains the details required for the resource.

Note: These values are set locally on the client. The values are not reflected on the appliance till the object is uploaded.

2. Upload the resource object to the appliance, using the static `add()` method.

The following sample code creates a NetScaler instance named "ns_instance" on the NetScaler SDX appliance:

```
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);
```

Retrieve Resource Details

To retrieve the properties of a resource on the NetScaler SDX appliance, do the following:

1. Retrieve the configurations from the appliance by using the `get()` method. The result is a resource object.
2. Extract the required property from the object by using the corresponding property name.

The following sample code retrieves the details of all NetScaler resources:

```
//Retrieve the resource object from the NetScaler 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);
```

Retrieve Resource Statistics

A NetScaler SDX appliance collects statistics on the usage of its features. You can retrieve these statistics using NITRO.

The following sample code retrieves statistics of a NetScaler instance with ID 123456a:

```
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);
```

Updating a Resource

To update the properties of an existing resource on the appliance, do the following:

1. Set the `id` property to the ID of the resource to be updated.

2. Set the value for the required properties of the resource by using the corresponding property name. The result is a resource object.

Note: These values are set locally on the client. The values are not reflected on the appliance till the object is uploaded.

3. Upload the resource object to the appliance, using the update() method.

The following sample code updates the name of the NetScaler instance with ID 123456a to '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);
```

Deleting a Resource

To delete an existing resource, invoke the static method delete() on the resource class, by passing the ID of the resource to be removed, as an argument.

The following sample code deletes a NetScaler instance with ID 1:

```
ns obj = new ns();
obj.id = "123456a";
ns.delete(nitroservice, obj);
```

Bulk Operations

You can query or change multiple resources simultaneously and thus minimize network traffic. For example, you can add multiple NetScaler appliances in the same operation.

Each resource class has methods that take an array of resources for adding, updating, and removing resources. To perform a bulk operation, specify the details of each operation locally and then send the details at one time to the server.

To account for the failure of some operations within the bulk operation, NITRO allows you to configure one of the following behaviors:

- **Exit.** When the first error is encountered, the execution stops. The commands that were executed before the error are committed.
- **Continue.** All the commands in the list are executed even if some commands fail.

Note: You must configure the required behavior while establishing a connection with the appliance, by setting the `onerror` param in the `nitro_service()` method.

The following sample code adds two NetScalers in one operation:

```
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 NetScalers to the NITRO server
ns[] result = ns.add(nitroservice, newns);
```

Exception Handling

The `errorCode` field indicates the status of the operation.

- An `errorCode` of 0 indicates that the operation is successful.
- A non-zero `errorCode` indicates an error in processing the NITRO request.

The error message field provides a brief explanation and the nature of the failure.

All exceptions in the execution of NITRO APIs are caught by the `com.citrix.sdx.nitro.exception.nitro_exception` class. To get information about the exception, you can use the `getErrorCode()` method.

For a more detailed description of the error codes, see the API reference available in the `<NITRO_SDK_HOME>/doc` folder.

REST Web Services

REST (Representational State Transfer) is an architectural style based on simple HTTP requests and responses between the client and the server. REST is used to query or change the state of objects on the server side. In REST, the server side is modeled as a set of entities where each entity is identified by a unique URL.

Each resource also has a state on which the following operations can be performed:

- **Create.** Clients can create new server-side resources on a "container" resource. You can think of container resources as folders, and child resources as files or subfolders. The calling client provides the state for the resource to be created. The state can be specified in the request by using XML or JSON format. The client can also specify the unique URL that will identify the new object. Alternatively, the server can choose and return a unique URL identifying the created object. The HTTP method used for create requests is POST.
- **Read.** Clients can retrieve the state of a resource by specifying its URL with the HTTP GET method. The response message contains the resource state, expressed in JSON format.
- **Update.** You can update the state of an existing resource by specifying the URL that identifies that object and its new state in JSON or XML, using the PUT HTTP method.
- **Delete.** You can destroy a resource that exists on the server-side by using the DELETE HTTP method and the URL identifying the resource to be removed.

In addition to these four CRUD operations (Create, Read, Update, and Delete), resources can support other operations or actions. These operations use the HTTP POST method, with the request body in JSON specifying the operation to be performed and parameters for that operation.

NetScaler SDX NITRO APIs are categorized depending on the scope and purpose of the APIs into system APIs and configuration APIs.

System APIs

The first step towards using NITRO is to establish a session with the NetScaler SDX appliance and then authenticate the session by using the administrator's credentials.

You must specify the username and password in the login object. The session ID that is created must be specified in the request header of all further operations in the session.

Note: You must have a user account on that appliance. The configurations that you can perform are limited by the administrative role assigned to your account.

To connect to a NetScaler SDX appliance with IP address 10.102.31.16 by using the HTTPS protocol:

- **URL.** `https://10.102.31.16/nitro/v1/config/login`
- **HTTP Method.** POST
- **Request Payload.**

```
object=  
{  
  "login":  
  {  
    "username":"nsroot",  
    "password":"verysecret"  
  }  
}
```

- **Response Payload.**

```
{  
  "errorcode": 0,  
  "message":"Done",  
  "sessionid":"##78C060..."  
}
```

Note: By default, the connection to the appliance expires after 30 minutes of inactivity. You can modify the timeout period by specifying a new timeout period (in seconds) in the login object.

To disconnect from the appliance, use the DELETE method:

- **URL.** `https://10.102.31.16/nitro/v1/config/login`
- **HTTP Method.** DELETE
- **Cookie.** `SESSID=##78C060...`

Configuration APIs

The NITRO protocol can be used to configure resources of the NetScaler SDX appliance.

Each NetScaler SDX resource has a unique URL associated with it, depending on the type of operation to be performed. URLs for configuration operations have the format `http://<IP>/nitro/v1/config/<resource_type>`.

For example, to configure a NetScaler resource, the URL is `http://10.102.31.16/nitro/v1/config/ns`.

Creating a Resource

To create a new resource (for example, a NetScaler instance) on the NetScaler SDX appliance, specify the resource name and other related arguments in the specific resource object. For example, to create a NetScaler instance named `vp1`:

- **URL.** `https://10.102.31.16/nitro/v1/config/ns`
- **HTTP Method.** POST
- **Cookie.** `SESSID=##78C060...`
- **Request Payload.**

```
object=
{
  "ns":
  {
    "name":"vp1",
    "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"
      }
    ]
  }
}
```

```
    }
  }
```

Retrieving Resource Details and Statistics

NetScaler SDX resource details can be retrieved as follows:

- To retrieve details of a specific resource on the NetScaler SDX appliance, specify the id of the resource in the URL.
- To retrieve the properties of resources on the basis of some filter, specify the filter conditions in the URL.

The URL has the form:

```
http://<IP>/nitro/v1/config/<resource_type>?filter=<property1>:<value>,<property2>:<value>
```

- If your request is likely to result in a large number of resources returned from the appliance, you can retrieve these results in chunks by dividing them into "pages" and retrieving them page by page.

For example, assume that you want to retrieve all NetScaler instances on a NetScaler SDX that has 53 of them. Instead of retrieving all 53 in one big response, you can configure the results to be divided into pages of 10 NetScaler instances each (6 pages total), and retrieve them from the server page by page.

You specify the page count with the `pagesize` query string parameter and use the `pageno` query string parameter to specify the page number that you want to retrieve.

The URL has the form:

```
http://<IP>/nitro/v1/config/<resource_type>?pageno=<value>&pagesize=<value>
```

You do not have to retrieve all the pages, or retrieve the pages in order. Each request is independent, and you can even change the `pagesize` setting between requests.

Note: If you want to have an idea of the number of resources that are likely to be returned by a request, you can use the `count` query string parameter to ask for a count of the resources to be returned, rather than the resources themselves. To get the number of NetScaler instances available, the URL would be

```
http://<IP>/nitro/v1/config/<resource_type>?count=yes
```

To retrieve the configuration information for the NetScaler instance with ID 123456a:

- **URL.** `http://10.102.31.16/nitro/v1/config/ns/123456a`
- **HTTP Method.** GET
- **Cookie.** `SESSID=##78C060...`
- **Response Payload.**

```
{
  "errorcode":0,
  "message":"Done",
  "ns":
  [
    {
```

```

        "name": "vpx1",
        "id": "123456a",
        "ip_address": "192.168.100.2",
        "gateway": "192.168.100.1",
        "netmask": "255.255.255.255",
        "vm_state": "DOWN",
        "vm_memory_total": 2048,
        ...
    }
]
}

```

Updating a Resource

To update an existing NetScaler SDX resource, use the PUT HTTP method. In the HTTP request payload, specify the name and the other arguments that have to be changed. For example, to change the name of NetScaler instance with ID 123456a to vpx2:

- **URL.** `https://10.102.31.16/nitro/v1/config/ns`
- **HTTP Method.** PUT
- **Cookie.** `SESSID=##78C060...`
- **Request Payload.**

```

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

```

Deleting a Resource

To delete an existing resource, specify the name of the resource to be deleted in the URL. For example, to delete a NetScaler instance with ID 123456a:

- **URL.** `http://10.102.31.16/nitro/v1/config/ns/123456a`
- **HTTP Method.** DELETE
- **Cookie.** `SESSID=##78C060...`

Bulk Operations

You can query or change multiple resources simultaneously and thus minimize network traffic. For example, you can add multiple NetScaler appliances in the same operation. You can also add resources of different types in one request.

To account for the failure of some operations within the bulk operation, NITRO allows you to configure one of the following behaviors:

- **Exit.** When the first error is encountered, the execution stops. The commands that were executed before the error are committed.

- **Continue.** All the commands in the list are executed even if some commands fail.

Note: You must configure the required behavior in the request header using the X-NITRO-ONERROR parameter.

To add 2 NetScaler resources in one operation:

- **URL.** <http://10.102.29.60/nitro/v1/config/ns>
- **HTTP Method.** POST
- **Cookie.** SESSID=##78C060...
- **Request Payload.**

```
object=
{
  "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"
    }
  ]
}
```

To add multiple resources (two NetScalers and two MPS users) in one operation:

- **URL.** <https://10.102.29.60/nitro/v1/config/>
- **HTTP Method.** POST
- **Cookie.** SESSID=##78C060...
- **Request Payload.**

```
object=
{
  "ns":
  [
    {
      "name":"ns_instance1",
      "ip_address":"10.70.136.5",
      "netmask":"255.255.255.0",
      "gateway":"10.70.136.1"
    },
    {
      "name":"ns_instance2",
      "ip_address":"10.70.136.8",
```

```
        "netmask":"255.255.255.0",
        "gateway":"10.70.136.1"
    },
    "mpuser":
    [
        {
            "name":"admin",
            "password":"admin",
            "permission":"superuser"
        },
        {
            "name":"admin",
            "password":"admin",
            "permission":"superuser"
        }
    ]
}
```

Exception Handling

The `errorcode` field indicates the status of the operation.

- An errorcode of 0 indicates that the operation is successful.
- A non-zero errorcode indicates an error in processing the NITRO request.

The error message field provides a brief explanation and the nature of the failure.

The response payload of all operations, specifies the error code and error message. For example, to get the status of a operation:

- **URL.** `http://10.102.31.16/nitro/v1/config/ping`
- **HTTP Method.** GET
- **Cookie.** `SESSID=##78C060...`
- **Response Payload.**

```
{
  "errorcode":-1,
  "message":"IP address is missing"
}
```